UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

FACULTAD DE INGENIERÍA CIENCIAS INFORMATICAS.

PROYECTO DE INVESTIGACIÓN

TEMA:

"IMPLANTACIÓN DE AUDITORÍAS INTERNAS PARA LA PRESERVACIÓN, CORRECCIÓN Y MANTENIMIENTO DEL SGSI DE LA FACCI"

DIRECTOR DE PROYECTO:

A. S. OSCAR GONZÁLEZ LÓPEZ

AUTORA:

DELGADO LUCAS KIMBERLY NAYESKA

MANTA – MANABÍ – ECUADOR

2018 - 2019

TRABAJO DE TITULACIÓN MODALIDAD PROYECTO DE INVESTIGACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERA EN SISTEMAS

"IMPLANTACIÓN DE AUDITORÍAS INTERNAS PARA LA PRESERVACIÓN, CORRECCIÓN Y MANTENIMIENTO DEL SGSI DE LA FACCI"

Tribunal examinador que declara APROBADO el Grado de INGENIERA EN SISTEMAS a la señorita: DELGADO LUCAS KIMBERLY NAYESKA

Mg. Juan Carlos Sendón Varela(presidente Tribunal) _____

Mg. Winther Molina Loor (Miembro del tribunal) _____

Mg. Robert Moreira Centeno (Miembro del Tribunal) _____

Manta, 25 de febrero de 2019

ACEPTACIÓN DEL DIRECTOR

En calidad de tutor del trabajo de la Facultad de Ciencias Informáticas de la Universidad Laica Eloy Alfaro de Manabí, certifico:

Que hemos dirigido y revisado el trabajo de titulación modalidad proyecto de investigación sobre el tema "IMPLANTANCIÓN DE AUDITORIAS INTERNAS PARA LA PRESERVACIÓN, CORRECIÓN Y MANTENIMIENTO DEL SGSI DE LA FACCI", proyecto que cumple con los requisitos que exige la guía Metodológica de titulación y el instructivo de normativa para trabajos de titulación de la carrera Ingeniería en Sistemas de la Facultad de Ciencias Informáticas y, reúne los méritos suficientes para ser sometido a la evaluación del jurado examinador que designen las autoridades.

La autoría del tema desarrollado corresponde a la Señorita DELGADO LUCAS KIMBERLY NAYESKA, estudiante con estudios concluidos de la Carrera de Ingeniería en Sistemas, periodo académico 2018-2019 (2), quien se encuentra aptos para la defensa.

Particular que confirmamos para los fines, salvo a disposición de Ley en contrario.

Atentamente:

Ing. Oscar González López Mg.

Universidad Laica Eloy Alfaro de Manabí

Manta, 30 de enero del 2019

DEDICATORIA

Lleno de regocijo, de amor y esperanza, dedico este proyecto, a cada uno de mis seres queridos, quienes han sido mis pilares para seguir adelante.

Familia, amigos, maestros y personas especiales en mi vida, no son nada más y nada menos que un solo conjunto: seres queridos que suponen benefactores de importancia inimaginable en mis circunstancias de humano. No podría sentirme más ameno con la confianza puesta sobre mi persona, especialmente cuando he contado con su mejor apoyo desde que siquiera tengo memoria.

Para el desarrollo de mi tesis tuve que lidiar con toda clase de obstáculo, y muchos de ellos los supere gracias a sus enseñanzas.

Kimberly Delgado Lucas.

AGRADECIMIENTO

El amor recibido, la dedicación y la paciencia con la que cada día se preocupaban mis padres por mi avance y desarrollo de esta tesis, es simplemente único y se refleja en la vida de un hijo.

Gracias a mis padres por ser los principales promotores de mis sueños, gracias a ellos por cada día confiar y creer en mí y en mis expectativas, gracias a mi madre por estar dispuesta a acompañarme cada larga y agotadora noche de estudio, agotadoras noches en la que su compañía y la llegada de sus cafés era para mí como agua en el desierto; gracias a mi padre por siempre desear y anhelar siempre lo mejor para mi vida, gracias por cada consejo y por cada una de sus palabras que me guiaron durante mi vida.

Gracias a ellos porque a pesar de lo ocurrido en nuestra familia por el 16A, fueron el motor y pilar fundamental para poder salir adelante tras lo ocurrido, seguir teniendo su apoyo incondicional me llena de optimismo y no me alcanzara la vida para agradecerles tanto.

Gracias a Dios por la vida de mis padres, también porque cada día bendice mi vida con la hermosa oportunidad de estar y disfrutar al lado de las personas que sé que más me aman, y a las que yo sé que más amo en mi vida, gracias a Dios por permitirme amar a mis padres, gracias a mis padres por permitirme conocer a Dios y de su infinito amor.

Gracias a la vida por este nuevo triunfo, gracias a todas las personas que me apoyaron y creyeron en la realización de esta tesis.

Kimberly Delgado Lucas.

Tabla de Contenido

GLOSARIO

Amenaza: Según (ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según (ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Datos: Termino general para la información procesada por un ordenador.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Dominio: Agrupación de objetivos de control en etapas lógicas en el ciclo de vida inversión en TI.

Evaluación de riesgos: Según (ISO/IEC Guía 73:2002): proceso de comparar el riesgo estimado contra de riesgo dado con el objetivo de determinar la importancia del riesgo.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de

riesgo y el tratamiento de riesgos. Según (ISO/IEC Guía 73:2002): actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: El coste para la empresa de un incidente de la escala que sea, que puede o no ser medio en términos estrictamente financieros ej., perdida de reputación, implicaciones legales, etc.

Información: En sentido general, es todo lo que reduce la incertidumbre y sirve para realizar acciones y tomar decisiones.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según (ISO/IEC 13335-1:2004): propiedad / característica de salvaguardar la exactitud y completitud de los activos.

Infraestructura: La tecnología, los recursos y las instalaciones que permiten el procesamiento de las aplicaciones.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: (International Organization For Standardization) Organización Internacional para la Normalización. Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

Mantenimiento Correctivo: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad, con el fin de prevenir su repetición.

Mantenimiento Preventivo: Medida de tipo pro-activo orientada a prevenir potenciales no-conformidades.

Objetivo: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimiento de control en una actividad de TI determinada.

Organización: Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones. Una organización puede ser pública o privada.

Políticas de seguridad: Según (ISO/IEC 27001:2005): intención y dirección general expresa formalmente por la Dirección.

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso.

Proceso: Por lo general, un conjunto de procedimiento influenciados por las políticas y estándares de la organización, que toman las entradas provenientes de un numero de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables, rol claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir desempeño.

R: según la norma (ISO/IEC 27001:2005): requerimientos de los objetivos y controles a utilizar.

Riesgo: Según (ISO Guía 73:2002): combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: Según (ISO Guía 73:2002): El riesgo que permanece tras el tratamiento de riesgos.

Seguridad de la Información: Según (ISO/IEC 27001:2005): Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Servidor: Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo denominación inglesa ´server.´.

TI: Tecnologías de Información.

Tratamiento de riesgos: Según (ISO Guía 73:2002): Proceso de selección e implementación de medidas pata modificar el riesgo.

Usuario: Una persona o una entidad externa o interna que recibe los servicios empresariales de TI.

Valoración de riesgos: Según (ISO Guía 73:2002): Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidades: Según (ISO/IEC 13335-1:2004): debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

RESUMEN

La decisión de una institución de dar el adecuado tratamiento a los riesgos asociados a la seguridad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), sustentada en el análisis de la naturaleza de la institución, el ámbito donde se desarrolla y produce, las necesidades de la facultad, área administrativa, sus docentes y estudiantes. El trabajo debe ser arduo en la implantación del SGSI y más aún en la puesta en marcha y mantención. El presente trabajo de investigación apoyará a la Facultad de Ciencias Informáticas (FACCI) en la parte de verificación, con lo cual valorará el estado situacional de su SGSI, elaborando un plan de trabajo de la auditoria interna al sistema de seguridad de la información para el proceso estratégicamente escogido, verificando la implementación y operación de los controles de acuerdo al Anexo A de la norma ISO/IEC 27001:2005, documentando hallazgos, diferenciando no conformidades mayores, menores y oportunidades de mejora, además emitiendo un informe de hallazgos para presentarlo a la alta dirección, apoyando así a la elaboración del plan de acción a ejecutarse para el cierre de observaciones. También apoyará en la transición de concientizar a toda la FACCI para que acepte este nuevo reto y se comprometa enteramente en el rol que le toca asumir.

ABSTRACT

The decision of an institution to give adequate treatment to the risks associated with the security of its information through the implementation of an Information Security Management System (ISMS), based on the analysis of the nature of the institution, the scope where the needs of the faculty, its teachers and students are developed and produced. The work must be arduous in the implementation of the ISMS and even more in the start-up and maintenance. This research work will support the Faculty of Computer Science (FACCI) in the verification part, which will assess the situational status of your ISMS, developing a work plan of the internal audit to the information security system for the strategically chosen process, verifying the implementation and operation of the controls according to Annex A of ISO / IEC 27001: 2005, documenting findings, differentiating major, minor and major improvement nonconformities, also issuing a report of findings to present it to senior management, thus supporting the development of the action plan to be executed for the closure of observations. It will also support the transition to raise awareness throughout the FACCI so that it accepts this new challenge and is fully committed to the role it has to assume.

CAPITULO I

1.1 INTRODUCCIÓN

Las auditorías internas también llamadas auditorías de primera parte, actualmente tienen gran relevancia en las organizaciones que cuentan con Sistemas de Gestión, debido a que una adecuada gestión de los procesos son un pilar para lograr los objetivos estratégicos y obtener cumplimiento de los aspectos legales y contractuales, además de un posicionamiento en el mercado. La implementación de un Sistema De Gestión De Seguridad De La Información (SGSI) basados en la adopción de las mejores prácticas o en una o más metodologías o marcos tales como: ISO/IEC 27001:2005, ITIL, COBIT, es un mecanismo para apoyar tales objetivos.

En el presente trabajo de grado, se plantea la estrategia que permitirá la gestión de la auditoria interna del SGSI de la FACCI, bajo la Norma ISO/IEC 27001:2005. Inicialmente se propone realizar la planeación de la Auditoria Interna y posteriormente definir el plan de acción de las no conformidades encontradas.

Para la elaboración del siguiente trabajo de titulación se tuvo que realizar actividades de investigación, obteniendo resultados y datos los cuales han sido tabulados y verificados con las ayudas de instrumentos técnicos.

1.1.1 Tema 1: **"SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS"** Con aporte de (Acosta Mera, febrero 2017). Este trabajo propuso un aplicativo para gestionar la información y su seguridad, para que la FACCI pueda salvaguardar casa uno de sus activos.

1.1.2 Tema 2 "**ANALISIS DE RIESGOS INFORMÁTICOS DE LA FACULTAD DE CIENCIAS INFORMÁTICAS."**

Con aporte (Guerrero Bravo y Mera Quintero, septiembre 2018), Este trabajo propuso conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en custodia en la Facultad de Ciencias Informáticas de la Universidad Laica "Eloy Alfaro" de Manabí, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. Basado en una metodología MAGERIT de estudio de caso, este estudio permitió recoger información detallada usando una variedad de sistemas de recolección de datos, como entrevistas semiestructuradas, estructuradas y en profundidad, revisión bibliográfica y arqueo de fuentes. Igualmente, se realizaron visitas a las instalaciones de la dirección evaluada y se revisaron aspectos de seguridad física previstos en las Normas ISO-27001:2005. Se concluye que cada uno de los elementos en custodia de la FACCI es de suma importancia, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO, para cada uno de dichos activos.

1.1.3 Tema 3

"INSTAURACIÓN DE UN PLAN DE CONTINGENCIA Y CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS QUE BRINDA LA FACCI."

Con aporte de (Domínguez Alvia, septiembre 2018) Hoy en día la FACCI busca fortalecer sus estructuras con el fin de conseguir una faculta más consistente, frente a amenazas externas que pueden afectar a la misma. Por esta razón los planes de contingencia y los planes de continuidad, con el fin de que un desastre inesperado nos afecte en el menor grado posible. De este miedo por perder todo lo conseguido, nacieron los planes de contingencia y los planes de continuidad. Implantar un plan que consiga que sus bienes no caigan ante cualquier falla inesperada en el camino, antes que no invertir dinero y ver como el establecimiento cae por el precipicio sin que puedan poner remedio a su caída.

En referencia a este trabajo y en base a investigaciones similares indican:

1.1.4 Tema 4

"AUDITORÍA INFORMÁTICA Y SU INCIDENCIA EN LA FUNCIONALIDAD DEL SISTEMA DE INFORMACIÓN FINANCIERA DE LA COOPERATIVA DE AHORRO Y CRÉDITO UNIVERSITARIA LIMITADA (COPEU)."

Con aporte (Castro Núñez, Ecuador 2012) Las tendencias en la utilización de herramientas tecnológicas para el mejor desenvolvimiento laboral han generado gran interés en la sociedad. El hombre ha hecho del uso de la tecnología parte de su diario vivir.

Debido a que en la Cooperativa de Ahorro y Crédito Universitaria Limitada (COPEU) de Ambato no se ha efectuado ninguna auditoría informática, se considera de gran importancia que se ejecute una auditoría en la Cooperativa y permita tomar medidas correctivas, asegurando la funcionalidad y productividad del Sistema de Información Financiera encaminando a guiar al buen desarrollo y correcto funcionamiento del mismo, para de esta manera, en posteriores auditorías, se enfoque la auditoría a áreas específicas o áreas críticas existentes.

1.1.5 Tema 5

"AUDITORIA INTERNA AL SGSI DE LA CNT E.P, PARA EL PROCESO DE VENTA E INSTALACIONES DE PRODUCTOS Y SERVICIOS DE DATOS E INTERNET PARA CLIENTES COORPORATIVOS EN EL D.M.Q."

Con aporte (Ing. Pabón Molineros, diciembre 2013), La Corporación de Telecomunicaciones CNT EP., decidió dar el adecuado tratamiento a los riesgos asociados a la seguridad de su información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para obtener la certificación internacional ISO/IEC 27001:2005.

1.1.6 Tema 6

"AUDITORIA INFORMATICA EN EL AREA DE SISTEMAS E INDICADORES DE FUNCIOMAMIENTO DEL HARDWARE EN LA EMPRESA SOLIDARIA DE SALUD EMSSANAR E.S.S. DEL DEPARTAMENTO DE NARIÑO"

Con aporte (Noguera Quenguan – Sánchez Perenguez, San Juan de Pasto 2012), Una empresa debe estar en continua evaluación para mirar sus falencias y tomar acciones que mejoran la eficiencia y eficacia en sus procesos y así ubicarse dentro de un medio competitivo.

1.1.7 Tema 7

"PROTOTIPO PARA LA AUDITORIA SISTEMA DE GESTION SEGURIDAD DE LA INFORMACION (SGSI)."

Con aporte (Momphotes Parra, Pereira 2014). La auditoría, nace antes de la teneduría de libros a finales del siglo XV, para verificar las actividades de los administradores y evitar fraudes en las empresas. En un principio se consideró como una rama de la contaduría pública que solo se dedicaba a examinar registros, pero posteriormente se extendió a otras áreas como la administración, ingeniería, medicina, sistemas, etc. Así es como la Auditoría Informática se encarga de verificar que los sistemas y procesos informáticos funcionen adecuadamente para las funciones que han sido programados y sus activos digitales se encuentren debidamente protegidos.

1.1.8 Tema 8

"ELABORACIÓN DEL PLAN DE IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2005 EN UNA EMPRESA DEL SECTOR RETAIL"

Con aporte (Jácome Lobo, Colombia 2015). Una vez se ha establecido el contexto general de la empresa, en este trabajo se surten todas las etapas necesarias para establecer un sistema de seguridad de la información (SGSI) basado en la norma ISO 27001:2005, abordando inicialmente

la definición del alcance y los objetivos trazados para el plan director de seguridad de la información en la empresa, continuando con la presentación de los resultados de un estudio de análisis diferencial en relación a los principales requerimientos, objetivos de control y controles establecidos en dicha norma, con el cual, se podrá conocer el estado inicial de la seguridad de la información en la empresa.

1.1.9 Tema 9

"AUDITORÍA INTERNA ISO 27001: SELECCIÓN DEL AUDITOR."

Con aporte (por Ingertec | Sep. 30, 2016). La Norma ISO 27001 requiere la realización de una auditoria Interna como herramienta de evaluación de la fase de implementación y para proporcionar de forma periódica información del desempeño del sistema de Gestión de Seguridad de la Información en un esquema de mejora continua. La tarea de auditoria interna ISO 27001 será liderada por un Auditor que evaluará la documentación de evaluación del riesgo para determinar el grado de cumplimiento con los requisitos de la norma.

1.1.10 Tema 10

"PROCEDIMIENTO PARA LA AUDITORIA INTERNA A LOS SISTEMAS DE GESTION DE LA CALIDAD Y DE SEGURIDAD DE LA INFORMACION DE PROMPERU"

Con aporte (Gerardo Compo blanco, noviembre 2017). El presente procedimiento es administrado por la Unidad de Racionalización de la OPP y es fuente de consulta y aplicación para las áreas comprendidas en el alcance del SGC y del SGSI de PROMPERÚ. El procedimiento se inicia con la definición, por parte del RED/OSI, de si la auditoría interna al SGC/SGSI será realizada por personal de PROMPERÚ o por un proveedor externo, y culmina cuando el RED/OSI

dispone el tratamiento de los hallazgos de la auditoría del SGC/SGSI señalados en el Informe de Auditoría respectivo.

1.1.11 Tema 11

"AUDITORÍA INTERNA ISO: UNA GUÍA EN UN LENGUAJE SENCILLO"

Con aporte (Dejan Kosutic, 2017). Este libro cubre el proceso de auditoría interna para todos los sistemas de gestión ISO – ISO 9001, ISO 14001, ISO 27001, ISO 20000, e ISO 13485, pero también OHSAS 18001 e IATF 16949 (former ISO/TS 16949) – por tanto, cuando me refiera a "estándar ISO", o simplemente "estándar", realmente me refiero a todos estos estándares. Por otra parte, cuando mencione "sistema de gestión", me refiero al sistema que es conforme a estos estándares – por ejemplo, Sistema de Gestión de Calidad, de acuerdo con la ISO 9001, Sistema de Gestión de Seguridad de la Información, de acuerdo a la ISO 27001, etc.

El punto importante es que con las auditorías internas debería descubrir problemas que de lo contrario podrían quedar ocultos, y que por lo tanto podrían dañar el negocio. Vamos a ser realistas - es humano cometer errores, por lo que es imposible tener un sistema sin errores; sin embargo, es posible tener un sistema que se mejora a sí mismo, y que aprende de sus errores. Las auditorías internas son una parte crucial de ese sistema.

Conclusión de temas relacionados

En conclusión, en base a las investigaciones realizadas en los siguientes temas relacionados tenemos que la norma ISO 27001 es la principal de la serie. En ella se define el concepto de Sistema de Gestión de la Seguridad de la Información, se establece el marco de referencia y se desarrolla la propia norma que, como ya se ha indicado, es certificable. La norma es aplicable a todo tipo de organizaciones o de partes de ellas e incluye la estructura organizativa, las políticas, las actividades

de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

A continuación, se relacionan los diferentes tipos o categorías de activos de información identificables en las actividades propias del día a día:

- Información o datos que la materializan
- Servicio que presta un sistema de información o servicios auxiliares necesarios por el sistema
- Aplicaciones informáticas que permiten manejar datos
- Equipos informáticos que permiten almacenar datos o información, o que permiten prestar el servicio o soportar la aplicación.
- Dispositivos de almacenamiento de datos o información
- Equipamiento y suministros necesarios para garantizar el funcionamiento de los dispositivos y equipos informáticos. Ej.: Suministro eléctrico, climático
- Las redes y equipos de telecomunicaciones que permiten transmitir información o datos
- Instalaciones donde se encuentran los equipos informáticos o de telecomunicaciones
- Personas involucradas con los elementos anteriormente mencionados

CAPITULO II: PLANTEAMIENTO DE LA INVESTIGACIÓN.

2.1 JUSTIFICACIÓN

El presente trabajo de titulación se enfoca en la propuesta y planeación de la auditoría interna del SGSI de la Facultad de Ciencias Informáticas, para el cumplimiento del programa anual de auditorías. Dado que, para la facultad, es de vital importancia no solo validar el cumplimiento de las políticas y controles, así como también los requerimientos legales y la vigencia de las certificaciones.

Sin embargo, existe falta de personal con las competencias como auditores internos y líderes en ISO 27001, en la FACCI para la ejecución de la auditoría interna, finalmente se requiere una auditoría imparcial para la ejecución de la auditoría interna de dicha facultad. Por lo anterior la facultad decide realizar esta auditoría interna con personal capacitado con el fin de obtener un resultado más objetivo y económico.

Para la FACCI esta auditoria permite conocer el estado real de su SGSI, que a su vez permite tomar medidas correctivas que lleven al cumplimiento y calidad de los sistemas existentes, adicionalmente se pretende que la auditoría contemple la totalidad de los requisitos y controles de la norma y retroalimente al personal auditado enfatizando en el ciclo de mejora continua de los procesos.

2.2 PLANTEAMIENTO DE PROBLEMA

A nivel mundial la auditoría informática se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas del negocio.

La Auditoría Informática permite la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo, su utilización, eficiencia y seguridad de la organización que está inmersa en el procesamiento de la información con el fin de lograr una utilización más eficiente y segura de la misma que servirá para una adecuada toma de decisiones.

El propósito de un sistema de gestión de la seguridad de la información es 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, la ausencia del mismo presentan riesgos rutinarios con la información que allí se maneja.

Las Auditorías Informáticas deben hacerse de forma periódica de tal forma que detecten las fallas o falencias y ayuden a corregirlas. Además, hay que citar que el avance de la tecnología crece a pasos agigantados, creándose e inventándose día a día mejores y más sofisticados equipos que permiten optimizar la función de los Sistemas Informáticos Financieros.

La Facultad de Ciencias Informáticas, es una Institución que cada día sigue creciendo poco a poco y es consciente que los equipos e información que se maneja debe estar bien protegida y manejada, por esta razón tiene la necesidad de realizar una auditoria interna en el SGSI, que nos va a permitir tomar las medidas necesarias para salvaguardar el activo más importante que es la información y establecer los controles necesarios para tal fin.

2.2.1 ÁRBOL DEL PROBLEMA

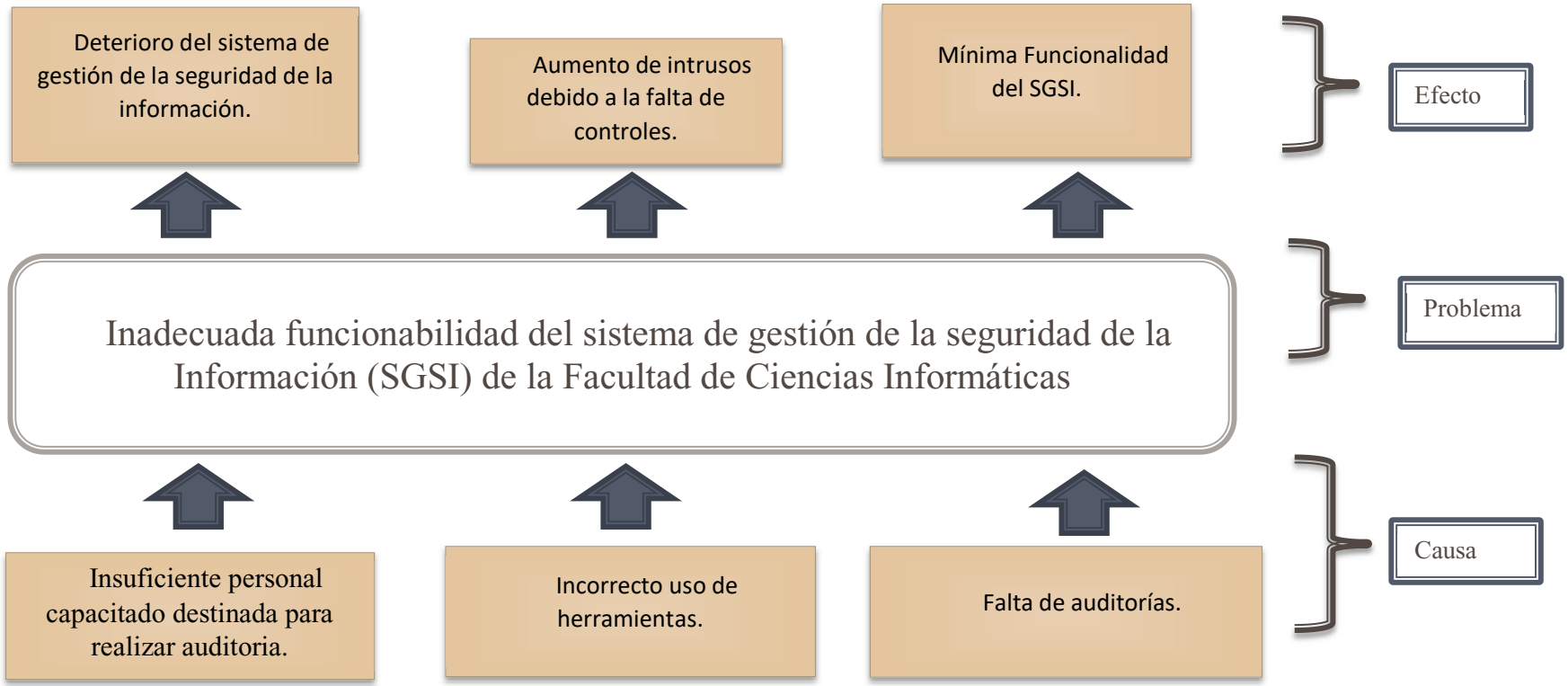


Ilustración 1. *Árbol del Problema*

2.3 OBJETIVO GENERAL.

Desarrollar una propuesta de auditoria interna del SGSI bajo la Norma NTC-ISO/IEC 27001:2015 para la preservación, corrección y mantenimiento de la FACCI.

2.3.1 Objetivos Específicos.

- Identificar, valorar y definir los criterios de la auditoria del SGSI.
- Elaborar, el plan de trabajo de la auditoria interna al SGSI de la FACCI, una vez realizada la revisión documental del SGSI en cada una de las áreas involucradas.
- Realizar simulacro de auditoria interna con los formularios propuestos.
- Informar los hallazgos encontrados en el simulacro a las autoridades de la FACCI.

CAPITULO III: REVISIÓN DE LITERATURA

3.1 MARCO TEÓRICO

3.1.1 Seguridad de la Información

La seguridad de la Información consiste en proteger uno de los activos más importantes de una institución, la información. Sim embargo debemos recalcar la distinción con lo que significa "Seguridad Informática".

Seguridad Informática es la protección de las infraestructuras tecnológicas, aplicaciones, sistemas operativos y base de datos sobre las que funciona una institución. Seguridad de la información tiene como objetivo la protección de los activos de información como: documentos físicos, hardware, software y personas entre otros.

Basada en que la información es clave importante para una organización para la operación y el cumplimiento de sus objetivos No es fácil controlar las vulnerabilidades asociadas a los activos de información, convirtiéndose en una tarea ardua de realizar pero que cuya respuesta se centra en un sistema de gestión de seguridad de la información.

Un Sistema de Gestión aplicado a la seguridad de la Información (SGSI), tiene como objetivo mantener siempre el riesgo por debajo de umbrales asumidos por la organización. Para esto es necesario implementar controles que mitiguen riesgos asociados a la integridad, disponibilidad y confidencialidad asociados a los activos de información, sin olvidar que la eficacia de estos controles depende de una revisión periódica, incorporando mejoras constantemente y siempre bajo las directrices de una política de seguridad definida por la institución.

Los costes derivados de la perdida de la información no son solo económicos directos, sino que también afectan a la imagen de la institución, por lo que, cada vez más, la seguridad de la información forma parte de los objetivos de las organizaciones, sin embargo, a pesar de esa

concienciación generalizada, aun muchas instituciones no enfrentan este aspecto con la globalidad con la que debe tratarse.

Existe otro factor que afecta a la estrategia de seguridad de una organización, las inversiones realizadas en materia de seguridad de la información a menudo no se ejecutan en base a una planificación de tratamiento de riesgos, lo cual permite generar trazabilidad entre el control implementado y el activo de información a proteger.

El punto fundamental de partida con garantía de éxito para el establecimiento y mantenimiento de la seguridad de la información es definir claramente objetivos a partir de los cuales debe desarrollar políticas que definan el marco para implementar medidas se seguridad, teniendo en cuenta aspectos como las leyes y regulaciones que rigen a la organización.

3.1.2. Seguridad de la Información VS. Seguridad informática.

A primera vista "Seguridad Informática" y "Seguridad de la Información" pueden parecer exactamente lo mismo, sobre todo si se tiene en cuenta que el desarrollo y la evolución de la tecnología tienden hacia el modelo de "digitalizar" y "manejar" cualquier tipo de información mediante un sistema informático. No obstante, aunque están destinados a vivir en armonía y trabajar conjuntamente, cada uno de las áreas de seguridad tiene objetivos y actividades diferentes.

Como conclusión la Seguridad de la Información es la disciplina que se encarga de tratar riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos de información. Mientras que la seguridad informática se encarga de tratar riesgos sobre activos tecnológicos; por consiguiente, la seguridad de la información a la seguridad informática.

3.1.3. Norma ISO/IEC 27001:2005 Tecnología de la Información- Técnicas de seguridad- Sistemas de gestión de Requerimientos.

ISO/27001 proporciona los requerimientos para el sistema de gestión de la seguridad de la información que permita a la organización establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI documentado dentro del contexto del conjunto de los riesgos de la actividad de una organización.

ISO/IEC 27001:2005 se diseña para "asegurar un adecuado y proporcionado control de la seguridad que proteja adecuadamente los activos de información y dar confianza a los clientes y otras partes interesadas." (27001:2005,2005). Es aplicable a cualquier organización independiente de su tipo, tamaño y la naturaleza de su actividad.

La norma ISO/IEC 27001:2005 define como organizar la seguridad de la información en cualquier tipo de organización: con o sin fines de lucro, privados o públicos, pequeños o grandes. Siendo hoy en día la norma que constituye la base para la gestión de la seguridad de la información.

La ISO/IEC 27001:2005 es para la seguridad de la información lo mismo que la ISO 9001es para la calidad: es una norma redactada por especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización se certifique, lo cual significa que una entidad de certificación independiente comprueba que la empresa ha definido e implementado el SGSI de acuerdo con la norma ISO/IEC 27001:2005.

La norma ISO/IEC 27001:2005 es un estándar internacional preparado por el Comité Técnico Conjunto ISO/IEC JTC, Tecnología de la Información, Subcomité SC 27, Técnicas de seguridad TI.

Este estándar proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejora un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción del SGSI debe ser una decisión estratégica de la organización cuyo diseño e implementación es influenciado por las necesidades y objetivos del negocio, requisitos de seguridad.

La norma específica el enfoque por procesos para la gestión de la seguridad de la información, enfatiza la importancia de entender los requisitos de seguridad de la información de la organización y la necesidad de establecer una política y objetivos para seguridad de la información, implementar controles para manejar los riesgos de seguridad, el monitoreo y revisión de desempeño del SGSI y el mejoramiento continuo en base a la medición del objetivo.

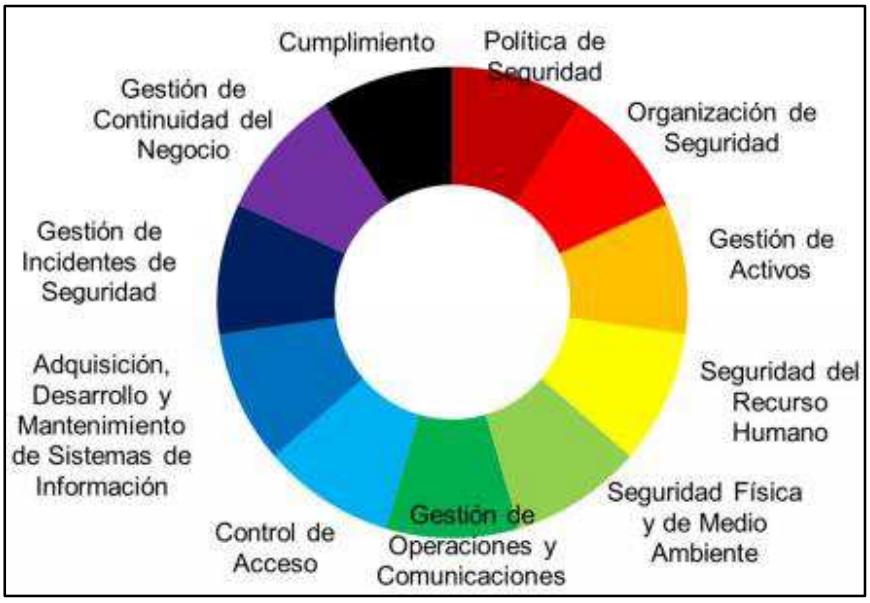


Ilustración 2. Áreas que abarcan la seguridad de la información (Deloitte, 2015)

ISO/IEC 27001:2005 adopta el modelo del proceso PDCA (Plan-Do-Check-Act) Planear, hacer, Chequear, Actuar, el cual se aplica en todos los procesos SGSI (27001:2005)

La imagen a continuación muestra el modelo PDCA además de los vínculos en los procesos presentados en la clausulas 4, 5, 6,7 y 8 de la Norma ISO/IEC 27001:2005.

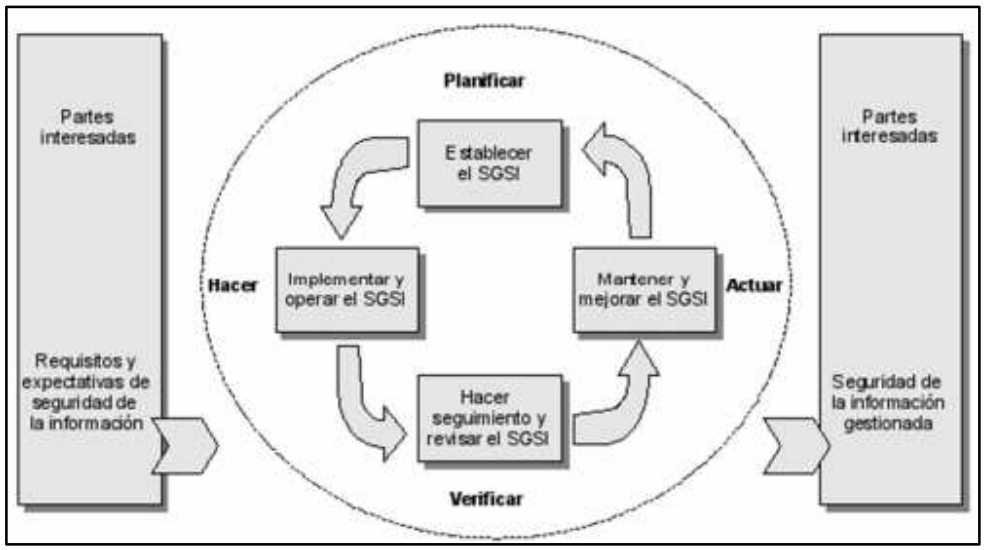


Ilustración 3. *Modelo PDCA para SGSI*

3.1.3.1 Componentes.

Requisitos: Los requisitos indicados en este estándar son genéricos y aplicables para cualquier organización para lo cual no es aceptable la exclusión de ningún requisito especificado en la norma.

Contiene las cláusulas descritas a continuación.

3.1.3.2 Cláusula 4: Sistemas de gestión de seguridad de la información.

"La organización debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades comerciales generales de la organización y los riesgos que enfrentan."

3.1.3.3 Cláusula 5: Responsabilidad del departamento de TI.

Compromiso del departamento de TI.

El departamento debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, revisión, mantenimiento y mejoramiento del SGSI al:

a. Establecer una política SGSI.

b. Asegurar que se establezcan objetivos y planes SGSI.

c. Establecer roles y responsabilidades para la seguridad de la información.
d. Comunicar a la organización la importancia de lograr los objetivos de seguridad de la información y cumplir la política de seguridad de la información, sus responsabilidades bajo la ley y la necesidad de su mejoramiento continuo;
e. Proporcionar los recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener, revisar, mantener y mejorar el SGSI;
f. Decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables
g. Asegurar que se realicen las auditorías internas SGSI; Y
h. Realizar revisiones gerenciales del SGSI" (27001:2005)

3.1.3.4 Cláusula 6: Auditorías Internas SGSI.

"La organización deben realizar auditorías internas SGSI a intervalos planeados para determinar si los Objetivos de control, controles, procesos y procedimiento del SGSI:

- Cumplen con los requisitos de este Estándar Internacional y la legislación y regulaciones relevantes.
- Cumplen con los requisitos de seguridad de la información identificados;
- Se implementan y mantiene de manera efectiva; y
- Se realizan conforme lo esperado.
- Se debe planear un programa de auditoria tomando en consideración el estatus e importancia de los procesos y áreas a ser auditados, así como los resultados de auditorías previas. Se debe definir el criterio, alcance, frecuencia y métodos de auditoria. La selección de los auditores y la realización de las auditorias deben asegurar la objetividad e imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo

- Las responsabilidades y requisitos para la planeación y realización de las auditorías, y para el reporte de resultados y mantenimiento de registros de deben definir en un procedimiento documentado.
- La gerencia responsable para el área siendo auditada debe asegurar que se den sin demoras las acciones para eliminar las no-conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y el reporte de los resultados de verificación".

3.1.3.5 Cláusula 7: Revisión Gerencial del SGSI

"La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos una vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad. Esta revisión debe incluir oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el SGSI, incluyendo la política de seguridad y los objetivos de seguridad de la información. Los resultados de las revisiones deben documentarse claramente y se deben mantener registros".

3.1.3.6 Cláusula 8: Mejoramiento del SGSI.

"8.1 Mejoramiento continuo.

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de la política de seguridad de la información, objetivos de seguridad de la información, resultados de auditoria, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión general.

8.2 Acción correctiva

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requisitos del SGSI para poder evitar la recurrencia. El procedimiento documentado para la acción correctiva debe definir los requisitos para:

a. Identificar las no-conformidades;
b. Determinar las causas de las no-conformidades;
c. Evaluar la necesidad de acciones para asegurar que las no-conformidades no vuelvan a ocurrir;
d. Determinar e implementar la acción correctiva necesaria;
e. Registrar los resultados de la acción tomada; y
f. Revisar la acción correctiva tomada.

8.3 Acción preventiva

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requisitos SGSI para evitar su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requisitos para;

a. Identificar las no-conformidades potenciales y sus causas;
b. Evaluar la necesidad para la acción para evitar la ocurrencia de no-conformidades;
c. Determinar e implementar la acción preventiva necesaria;
d. Registrar los resultados de la acción tomada; y
e. Revisar la acción preventiva tomada".

Cualquier exclusión de los requisitos para satisfacer el criterio de aceptación del riesgo tiene que ser justificada y debe ser debidamente evidenciada que los riesgos asociados han sido por los responsables.

Controles: Control es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.

El estándar ISO/IEC 27001:2005 especifica en su "Anexo A" un listado completo de objetivos de control y los controles de cada uno de ellos, los mismos que se alinean con ISO/IEC 27002:2005 Cláusulas del 5 al 15. Las listas en la tabla A.1 no son muy grandes por lo que la organización puede considerar o no todos los controles o adicionar algunos si los quiere.

Los Objetivos de control y los controles de estas tablas deben seleccionarse como parte del proceso SGSI especificado en el requisito 4 (Sistema de gestión de seguridad de la información) en el punto 4.2.1 (Establecer y manejar el SGSI) de la norma.

Cabe mencionar que el anexo A proporciona una base de referencia de 133 controles que son los mínimos que se deberán aplicar, o justificar su no aplicación, pero cabe especificar que si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramente el ciclo no estará cerrado y presentara huecos claramente identificables.

3.1.3.7 Los Controles del Anexo "A" están agrupados en los siguientes dominios:

- A.5 Política de seguridad.
- A.6 Organización de la información de seguridad.
- A.7 Administración de recursos.
- A.8 Seguridad de los recursos humanos.
- A.9 Seguridad física y del control.
- A.10 Administración de las comunicaciones y operaciones.
- A.11 Control de acceso.
- A.12 Adquisición se sistemas de información, desarrollo y mantenimiento.

- A.13 Administración de los incidentes de seguridad.
- A.14 Administración de la continuidad de negocio.
- A.15 Cumplimiento (Legales, de estándares, técnicas y auditorias).

3.1.4 Auditoria al SGSI

En la tradicional auditoria de sistemas, el auditor aplica directamente las herramientas de auditoria o sus mejores prácticas para comprobar la solidez del sistema. Incide de forma clara para determinar incumplimientos, en las auditorias de seguridad se explora para determinar agujeros de seguridad y amenazas. Se utilizan técnicas de hacking ético, aplicaciones específicas u otras de ingeniería social y muchas herramientas más.

En la Auditoria Interna del SGSI existen varias diferencias con las anteriores, está orientada hacia la mejora continua del SGSI, se basa en actividades que aporten hallazgos para la gestión de la seguridad. Requiere personal cualificado como auditor de la norma ISO/IEC 27001:2005, en auditoria de sistemas de gestión, en los procesos del negocio a ser auditados.

Resumiendo, la Auditoria de Sistemas Informáticos tiene una vertiente más técnica y se centra en la verificación de controles en el procesamiento de la información en sistemas informáticos, incidiendo sobre los mismos para poder evaluar su eficacia y poder presentar el correspondiente informe a la alta dirección, la Auditoria Interna del SGSI se enfoca a la mejora continua del Sistema de Gestión de Seguridad de la Información.

3.2. MARCO CONCEPTUAL

3.2.1 Sistema de Gestión de Seguridad de la Información (SGSI).

Los sistemas de gestión de la seguridad de la información (SGSI) proveen a las organizaciones los elementos para gestionar de manera efectiva la seguridad de la información.

El SGSI debe ayudar al mantenimiento y la mejora de las oportunidades competitivas, los movimientos monetarios, la rentabilidad, el cumplimiento legal y la imagen corporativa.

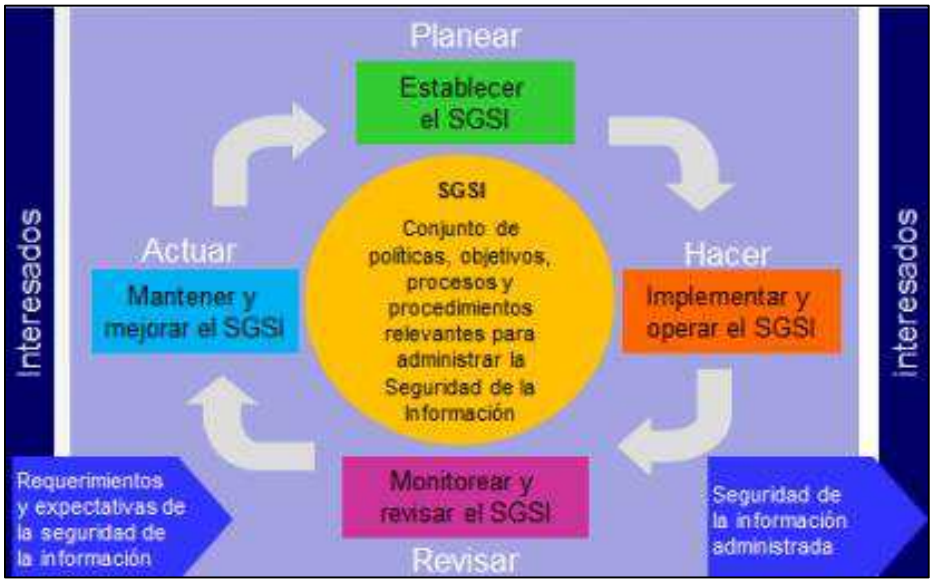


Ilustración 4. *Conceptos tomados de la noma BS ISO/IEC 27001; 2005*

El desarrollo de un SGSI representa un acercamiento "proactivo", sistemático y lógico para dirigir los problemas de la seguridad de la información, en sustitución de un lento acercamiento "reactivo" a las brechas de seguridad.

Las organizaciones están sometidas a amenazas internas y externas y existe el riego de que se materialicen.

- La organización puede responder mediante:
- Políticas y visiones corporativas;
- Cultura y valores corporativos;

- Marketing y comunicación;
- SGSI.

El SGSI se entiende como un entorno de trabajo para la organización que necesita de un seguimiento continuo y de revisión periódica para proveerlo de una dirección efectiva para las actividades de la organización en materia de seguridad de la información y como repuesta a los cambios internos y a los factores externos. Cada individuo en cada organización debe aceptar las responsabilidades en las mejoras de la seguridad de la información.

3.2.2. Beneficios del SGSI

El establecimiento y funcionamiento de un SGSI por sí mismo no necesariamente obtiene como resultado una inmediata reducción de los riesgos adversos de la seguridad de la información. En esencia, un SGSI es una herramienta que otorga a la organización de la capacidad de lograr controlar sistemáticamente un nivel de seguridad implantado.

Ilustración 5. *Beneficios*

El sistema debe proporcionar beneficios económicos tales como:

- Incrementa el conocimiento en seguridad de la información.

- Minimizar los riesgos en materia de confidencialidad, integridad y disponibilidad de la información.
- Reduce el tiempo de investigación de las brechas de seguridad.
- Mejora continua de la seguridad de la información mediante la supervisión, revisión, y eficacia de los procesos implantados.
- Aporta un valor añadido y/o diferencial a la organización.
- Reduce el adiestramiento del personal nuevo.
- Reduce litigios.
- Exterioriza una clara vocación del cumplimiento de leyes y regulaciones.
- Certifica una especial solvencia técnica en materia de seguridad de la información.
- Incrementa la confianza de los clientes y las partes interesadas.

Una vez que se obtiene la certificación del SGSI según la norma ISO/IEC 27001:2005 a través de un organismo independiente, la organización obtiene unos beneficios tales como:

- Incremento de la imagen corporativa.
- Perfil mejorado y credibilidad.
- Ventaja competitiva en el posicionamiento de mercado.

3.2.2 1 Alcance

Según el requisito cuatro de la ISO/IEC 27001:2005 el SGSI requiere definir un alcance tanto a nivel de procesos a nivel geográfico. La organización que seleccionar el proceso prioritario a controlar los riesgos de negocio y la ubicación geográfica.

3.2.2.2 Aplicación

Los requerimientos son genéricos y aplicables a todas las organizaciones, sea cual sea su tipología, tamaño y producto o servicio ofrecido, Cuando alguno de los requerimientos no pueda ser aplicado "debido a la naturaleza y su actividad" estos deben ser considerados por exclusión y detallados en el documento "declaración de aplicabilidad" de la organización.

3.2.2.3 Implementación

Para la implementación de un SGSI, se debe considerar los siguientes puntos esenciales:

- Definir al alcance del SGSI.
- Establecer el compromiso y la completa aplicación de la alta dirección en el proyecto desde el inicio hasta el fin.
- Establecer el nivel de seguridad deseado, tamaño y complejidad de la organización.

Como se había mencionado anteriormente, el estándar internacional adopta el modelo PDCA el mismo que menciona que no es suficiente con el diseño e implementación del SGSI, sino que es necesario garantizar la revisión periódica y realiza una continua actualización y mejora de este, permitiendo a cada organización utilizar los instrumentos que consideren oportunos para medir y controlar la mejora el sistema.

Un SGSI debe identificar fundamentalmente, los objetivos y alcance del sistema, los procesos de negocio críticos para la organización.

3.2.2.4 Certificación

La certificación del SGSI favorece a fomentar las actividades y procesos de protección de la información dentro de las organizaciones, mejorando su imagen y generando confianza ante terceros.

Cuando ha finalizado el proceso de implantación del SGSI y si la organización lo decide, tiene la opción de certificar su SGSI conforme a normativas internacionales ISO/IEC 27001:2005.

El SGSI según la norma ISO/IEC 27001:2005 se lo puede integrar a los sistemas de gestión de la calidad ISO 9001 y gestión medio ambiental ISO 14001.

El proceso de certificación lo realiza una tercera entidad acreditada, la misma que evaluara el SGSI de la organización y expedirá un certificado que demuestre que la organización satisface los requisitos de la norma ISO/IEC 27001:2005. El certificado se mantendrá siempre y cuando la organización continúe cumpliendo los requisitos de la norma.

La certificación demuestra a clientes, competidores, proveedores, personal e inversiones, que una organización emplea buenas prácticas revisadas y aprobadas a nivel internacional. Un certificado de seguridad de tercera parte ayuda a que una organización demuestre que gestiona eficientemente la seguridad de sus negocios, provee la implicación, participación y motivación del personal en mantener la política de seguridad de la organización, establece procedimiento que mejoran continuamente su actividad y evidencia un enfoque innovador con visión al futuro.

3.3.3 Auditoria de sistemas de gestión

3.3.3.1 Normas

En noviembre, fue publicada la norma 27007:2011 Tecnología de la información ISO/IEC – Técnicas de Seguridad – Directrices para la seguridad de la información de gestión de los sistemas de auditoria.

Esta norma proporciona orientación para auditores internos, auditores externos, organismos de certificación y otros, permite realizar la auditoria del sistema de gestión para el cumplimiento de la norma ISO/IEC 27001.

ISO/IEC 27007 se refiere en gran parte a la norma ISO 19011, el cual es el estándar ISO de auditoria para sistemas de gestión ambiental y de calidad, el cual proporcionar orientación adicional y específica para el SGSI.

La estructura de la norma abarca los aspectos específicos de auditorías de cumplimiento del SGSI.

- La gestión del programa de auditoria SGSI (Determinación de lo que se debe auditar, cuando y como; asignación de auditores apropiados, la gestión de auditoria, el mantenimiento de los riegos de auditoria, mejora continua de procesos);
- Realización de un SGSI auditoria (proceso de auditoria – la planificación, la realización, las actividades clave de la auditoria, incluyendo trabajo de campo, análisis, presentación de informes y seguimiento);
- Gestión de los auditores SGSI (competencias, habilidades, atributos, evaluación) ISO/IEC 19011.

Según la ISO/IEC 19011 a una auditoria se define como:

"Proceso sistemático, independiente y documentado para obtener evidencias de la auditoria y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios acordados", (SGS, 2012).

La ISO 19011 también contiene las siguientes directrices:

- Los principios de la auditoria.
- Gestión de los programas de auditoria.
- Actividades de la auditoria.
- La competencia de los auditores.

3.3.3.2 Principios de Auditoria

La auditoría se basa en un número de principios fundamentales que aseguran que la auditoria es una herramienta eficiente y segura. La comprensión y seguimiento de estos principios aseguran que las conclusiones de la auditoria sean relevantes y suficientes, y que auditores que están trabajando por separado alcancen conclusiones parecidas en circunstancias similares.

Tres de los principios de auditoria se relacionan con las características personales de los auditores:

Conducta Ética: La función del auditor engloba confianza, integridad, confidencialidad y discreción. Los auditores se rigen bajo estrictos códigos de conducta.

Objetividad: Los hallazgos de la auditoria, las conclusiones de la auditoria, las conclusiones de la auditoria y los informes de la auditoria reflejan la veracidad y precisión de las actividades de la auditoria. Cualquier opinión no resuelta o divergente entre el equipo auditor y el auditado y cualquier obstáculo encontrado debe ser informada.

- Ser profesional: Los auditores deben practicar y conocer la importancia de la tarea y de lo confidencial de sus actuaciones.
- Independencia: Los auditores son objetivos e independientes. Los miembros del equipo auditor deben estar libres de conflictos de intereses.
- Evidencias: La evidencia de la auditoria es verificable. Se basa en muestras de la información disponible, puesto que la auditoria se realiza en un periodo finito de tiempo y con recursos limitados. Sin embargo, las muestras deben ser apropiadas para confiar en las conclusiones de la auditoria. (SGS, 2012).

3.3.3.3 Tipos de Auditoria

Existen tres tipos de auditorías:

- **Auditoria de primera parte (Auditoría interna):** Es la auditoría realizada por la organización a sus propios sistemas y procedimientos. Su objetivo es asegurar el mantenimiento, desarrollo y mejora del sistema de calidad. En ISO/IEC 27001:2005 como requisito en la cláusula 6.
- **Auditoria de segunda parte (Auditoría externa):** Es la auditoría realizada por la organización a sus proveedores y subcontratistas. El objetivo es determinar la adecuación de los proveedores, determinar la capacidad de los proveedores para suministrar recursos de acuerdo con la seguridad de la información.
- **Auditoria de tercera parte (Auditoría externa):** Es una evaluación realizada por un organismo que es comercial y contractualmente independiente de la organización, sus proveedores y sus clientes. Generalmente, una evaluación realizada por un organismo de certificación de acuerdo con ISO/IEC 27001:2005. Su objetivo es determinar que el Sistema de Seguridad de la Información de una organización ha sido documentado e implementado de acuerdo con una norma determinada. (SGS, 2012)

3.3.3.4 Proceso de Auditoría

La realización de las tareas de cualquier auditoria en forma sistemática y organizada requiere del cumplimiento de tres etapas básicas que son:

- Planificación
- Ejecución
- Conclusiones

Cada una de esas etapas constituyen otros procesos: (SGS, 2012).

Planificación

La etapa de planificación es la determinación precisa de los objetivos y subobjetivos de la auditoria, genera el programa de trabajo que es el detalle de los procedimientos o técnicas seleccionados para reunir evidencia valida y suficiente, respecto de cada uno de los objetivos y subobjetivos determinados.

Ejecución

La etapa de ejecución es aquella donde llevamos a cabo los procedimientos definidos en la planificación y que se reflejan en los programas de trabajo.

De la aplicación de cada procedimiento obtenemos conclusiones respecto del objetivo vinculado al mismo, en muchos casos resulta necesaria la aplicación de más de un procedimiento por cada objetivo, para poder reunir evidencia suficiente que permita la obtención de conclusiones sobre el mismo. Esta última etapa del proceso de auditoria se caracteriza fundamentalmente, por la síntesis de las conclusiones particulares de cada procedimiento aplicado, para llegar a una o varias conclusiones generales sobre la tarea realizada. Esta etapa termina con la emisión del correspondiente informe de auditoría.

3.4. CONCLUSIONES RELACIONADAS AL MARCO TEÓRICO EN REFERENCIA AL TEMA PLANTEADO

3.4.1. Auditoria. La palabra auditoria viene del latín auditóriums y de esta proviene "auditor", el que tiene la virtud de oír; el diccionario lo define como "revisor de cuentas colegiado".

El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico, que es el de evaluar la eficiencia y eficacia con la se opera un sistema, con el objetivo de identificar oportunidades de mejora, tomar decisiones y corregir errores en los procesos y procedimientos.

Actualmente las normas y procedimientos para la gestión de auditorías en Sistemas de Gestión de Seguridad de la Información hacen parte de una profesión. Estas pueden estar basadas en las experiencias de otras profesiones, con algunas características propias y siempre guiándose por el concepto de que la auditoria y además de permitir mejorar lo existente, corregir errores y proponer alternativas de solución.

3.4.2 Construcción de una auditoria interna eficaz. El objetivo del departamento de auditoría interna debe ser promover los controles internos y ayudar a la Facultad a desarrollar soluciones efectivas teniendo en cuenta el costo/beneficio para brindar solución a los problemas evidenciados. Este departamento agrega valor a la empresa, a través de su experiencia y conocimiento de los controles internos y su forma de evaluarlos. De esto se pude concluir que la misión consta de dos puntos:

3.4.2.1 Garantizar independencia de la auditoría, debido a que conocen los controles internos de la empresa y pueden hacer que funcionen eficazmente.

3.4.2.2 Mejorar continuamente los controles internos de la Facultad, se deben identificar las debilidades del control y desarrollar soluciones costo/efectividad para abordar esas diferencias.

3.4.3 La independencia. El gran mito, según Webster´s College Dictionary universal, a independencia es "La calidad del estado de ser independiente" – "No influenciados o controlados por otros". Pero esto no es cierto, debido a que se deben reportar informes al presidente de la organización y al CEO (Chief Executive Officer), ya que el CEO es quien controla el presupuesto para el departamento de auditoría. Las personas que realizan la auditoria deben realizar su trabajo objetivamente y no subjetivamente.

3.4.4 Equipo auditor. La importancia del grupo de auditoría y su departamento, se debe a que se pueden identificar correcciones a los problemas a tiempo, beneficiando en costo (disminuyendo costos) y a su vez se podrán agregar controles después de identificar los casos. El departamento de auditoría también puede proporcionar una evaluación de los controles propuestos y aplicados.

3.4.5 Métodos de consultoría y participación temprana. Estos métodos se proponen para promover los controles internos en la organización, fuera de las auditorias formales y son los siguientes:

3.4.5.1 Participación temprana: El cambio cuesta más que la primera implementación.

3.4.5.2 Auditoria informal: No documentar.

3.4.5.3 Compartir conocimientos: A través de sitio web e email.

3.4.5.4 Directriz de control: El control no debe ser una política, pero si debe estar direccionado a cumplir con las políticas de la organización.

3.4.6 Problemas comunes, mejores prácticas y soluciones innovadoras. Muy pocas veces se comparan las auditorías realizadas entre organizaciones del mismo sector y se ignora la gran utilidad que pueden llegar a traer para las organizaciones la revisión de esas auditorías, cuando se realiza una auditoria y se encuentran hallazgos comunes es importante publicarlos en el sitio web

del departamento del auditoria y enviar e-mail a todo el personal pertinente informando el hallazgo y los controles a aplicar.

3.4.7 Herramientas. Se pueden compartir las herramientas con otros grupos para permitir autoevaluación de los controles. Sin embargo, es importante establecer políticas, permisos, horas y zonas de aplicación de estas herramientas, pero no se recomienda compartir herramientas que comprometan información sensible, personal o que viole la integridad.

3.4.8 El papel del equipo de auditoria. Existen auditores dedicados a: (aplicaciones, extracción y análisis de datos y auditoria de TI). Para ser auditor de cada uno de estos campos no es necesario ser especialista, pero si certificado en (CISA-CISSP) y tener experiencia en la realización de controles generales.

3.4.9 Mantenimiento de la experiencia. Invertir en renovar la capacitación y el conjunto de habilidades, esta renovación constante se debe realizar periódicamente debido a que la tecnología varía constantemente. Con todo este proceso lo que se busca es que el aporte que brinde el departamento de TI no solo sea de mantenimiento de software como la gran parte de personas de la organización lo piensa, el grupo de auditoría de TI, debe aliarse al grupo de auditoría externa y brindar juntos un valor agregado a la organización donde se permita contar con los controles pertinentes para para cada proceso de la organización.

3.4.10 Proceso de auditoría. Controles internos: El concepto de control interno es clave en la auditoría. Los controles internos, son mecanismos que garantizan el correcto funcionamiento de los procesos dentro de la Facultad.

3.4.11 Los controles Internos. Se pueden clasificar en preventivo, detectivo y reactivo, pueden tener implementaciones administrativas, técnicas o físicas. Las implementaciones administrativas incluyen elementos tales como políticas y procesos.

3.4.11.1 Controles preventivos. Los controles preventivos están diseñados para evitar que un evento negativo suceda. Desde el punto de vista teórico estos son los controles que deben privilegiarse.

3.4.11.2 Controles detectivos. Están diseñados para grabar los eventos negativos que hayan ocurrido.

3.4.11.3 Controles de reactivos (correctivos). Estos controles se ubican entre los controles preventivos y los detectivos y se destacan por detectar de manera sistemática cuando los malos sucesos han ocurrido y corregir la situación.

3.4.12 Determinar qué auditar. El plan de auditoría debe focalizarse en las áreas con mayor riesgo y en donde se pueda agregar mayor valor. Debe ser eficiente y eficaz el uso de los recursos limitados por el gasto. La auditoría del SGSI debe ser un proceso metódico y lógico que garantice transparencia y calidad.9 Es importante estudiar y validar los criterios de auditoria, para esto se requiere solicitar información del SGSI de la empresa como: política, alcance, objetivos, manuales y procedimientos del SGSI. Se debe tener en cuenta los requerimientos de la Norma NTC-ISO-IEC 27001:2005.

3.4.13 Metodología de la auditoria. A continuación, se describen los pasos de la metodología para el desarrollo de auditoria.

3.4.13.1 Planificación. Antes de empezar cualquier trabajo de auditoría, se debe organizar un plan de auditoria. Si el proceso de planificación es ejecutado eficazmente, llevara al equipo de auditoría al éxito.

3.4.13.2 El trabajo de campo y documentación. Este paso es el grueso de la auditoría, permite al equipo auditor evidenciar la gestión del SGSI, a través de entrevistas, revisiones y

validación de datos. Para posteriormente, analizados y obtener posibles riesgos, No conformidades, observaciones y oportunidades de mejora.

3.4.13.3 Descubrimiento de Problemas y validación. Mientras se ejecuta el trabajo de campo, los auditores elaborarán una lista de problemas potenciales y generarán la validación de los mismos en el campo.

3.4.13.4 Desarrollo de soluciones. Después de haber identificado los problemas potenciales en las áreas auditadas y una vez validado los hechos y riesgos se puede trabajar en desarrollar el plan de acción o cierre de no conformidades.

3.4.13.5 Emisión de informe. Posteriormente se debe redactar el Informe de auditoría. El informe de auditoría es el medio por el cual se documentan los resultados de la auditoría. Este informe permite llevar un registro de la auditoría, resultados y planes de acción.

3.4.13.6 Seguimiento del problema. Es común para los auditores sentir que la auditoría está "Terminada" una vez que el informe de auditoría se ha expedido. Sin embargo, la emisión de un informe de auditoría no añade valor a la empresa, a menos que se vean los resultados de las medidas adoptadas.

CAPITULO IV: METODOLOGÍA

4.1. TIPO (S) DE INVESTIGACIÓN

El tipo de investigación es aplicada correlacional, debido a que permite medir y establecer el grado de relación de la variable (SGSI).

4.2.1. Variables

En la tabla 1. Variables, se detalla las variables escogidas y su descripción.

Tabla 1. *Variables*

Variable	Abreviación	Descripción	Tipo
Independiente	SGSI	Auditoria del SGSI	Cualitativa
Independiente	Activos	Equipos Informáticos	

Fuente: FACCI

4.3. SITUACIÓN ACTUAL DE LA FACCI CON RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

4.3.1 Descripción De La Empresa

La Facultad de ciencias informáticas FACCI, Unidad educativa de nivel superior orienta sus procesos académicos hacia una formación de calidad y excelencia, en observancia a la normativa, a los derechos del buen vivir, y a los nuevos retos que la Academia ha delineado como prioritarios; a fin de potenciar las capacidades y habilidades de las personas, en la búsqueda permanente del conocimiento como un bien público.

Ilustración 6. *FACCI*

4.3.2.1 Misión

Proporcionar formación científica, técnica y cultural a los futuros profesionales en las ciencias informáticas, enmarcadas en la ética y la moral; con el fin de garantizar la eficiencia en la prestación de sus servicios y la producción de bienes a la sociedad.

4.3.2.2 Visión

Unidad académica de la educación superior líder en el ámbito informático, con criterio creativo e invocador. Reconocimiento local y nacional, en la formación integral de profesionales generadores de bienes y servicios.

4.3.2.3 Localización

La Facultad está ubicada en la Ciudadela Universitaria. Universidad Laica Eloy Alfaro de Manabí al lado del Vicerrectorado Administrativo.

Ilustración 7. *Punto de localización*

4.3.2.4 Estructura Organizacional

- **Decano:** Lic. Dolores Muñoz Verduga. PHD.
- **Coordinador de Carrera:** Ing. Winter Molina Loor. Mg
- **Coordinador de Académico:** Ing. Fabricio Rivadeneira Zambrano. Mg
- **Jefe Departamento Técnico:** Ing. Gilbert Loor

4.3.2.5 Organigrama organizacional

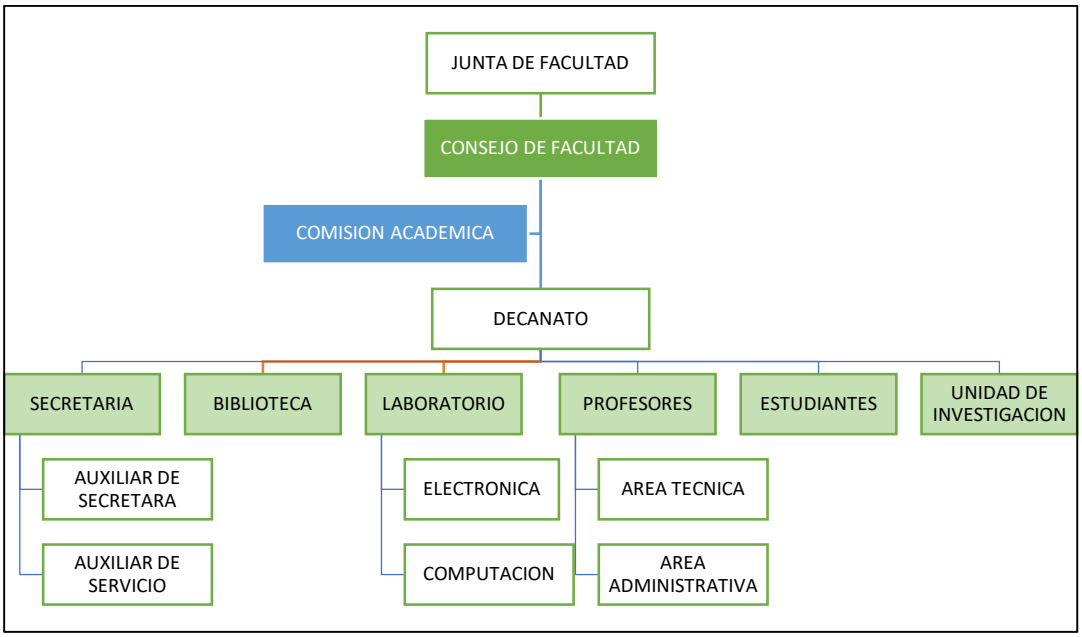


Ilustración 8. *Estructura Organizacional (FACCI)*

4.3.2 Área de seguridad de la información

De acuerdo con la estructura organizacional de la FACCI, el área de seguridad de la información se encuentra ubicada en el área técnica.

El nivel estratégico de la seguridad de la información esta materializado en el comité de Riesgos, que a su vez cumple como comité de Seguridad de la Información, este se encuentra conformado por el jefe del área y todos los que trabajan en la misma.

El enfoque del área de seguridad de la información en la FACCI está basado en temas proactivos como reactivos. La proactividad realiza un adecuado análisis de riesgos, identifica vulnerabilidades y amenazas para implementar oportunamente los distintos controles.

El enfoque reactivo se orienta a la gestión de requerimientos e incidentes de seguridad de la información.

El SGSI de la FACCI nació como un proyecto estratégico para cubrir la necesidad del área de administración debido al incremento de licitaciones que demandan poseer la certificación ISO/IEC 27001:2005, la iniciativa y dirección del proyecto fue encabezada por el grupo de seguridad de la información, a tal punto que una vez que le sistema ha sido implementado, la gestión, monitoreo y mejora depende del grupo de seguridad de la información.

El grupo que conforma el área de seguridad de la información está compuesto por un equipo de profesionales, tienen distintas ramas de especialización lo que permite administrar adecuadamente la seguridad de la información en base a una metodología de valoración de riesgos y con enfoque de mejora continua.

4.3.3 Sistema de Gestión de Seguridad de la Información (SGSI) de la FACCI.

Dentro de los riesgos a los que se expone la FACCI, existe el riesgo de seguridad de la información; por tal razón, la alta dirección tomo la decisión de desarrollar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI), alineado a la norma ISO/IEC 27001:2005.

En base al documento de Evaluación y Tratamiento del Riesgos Informático de la Facultad de Ciencias Informáticas, se ha realizado la evaluación de riesgos de seguridad de los activos de información para tomar medidas necesarias y mantener los riesgos en niveles aceptables, esta clasificación de activos determino el nivel de impacto cualitativo que tendría para la FACCI la perdida de cualquier de los atributos de la información: Integridad, disponibilidad y confidencialidad.

La selección de activos críticos fue determinada en base a un nivel de impacto y vulnerabilidad los cuales requerían la implementación de controles para aumentar la mitigación de los riesgos que tengan asociados.

En la identificación del universo de vulnerabilidades, se elaboró un documento con las posibles amenazas y vulnerabilidades a la seguridad de la información por tipo de activo de información que es afectado junto con los controles de la norma ISO27001. De la misma forma la identificación del universo de amenazas incluye una lista de referencia de aquellas que tienen una probabilidad de ocurrencia alta en el entorno de la organización.

Sobre el enfoque de riesgos: la facultad utilizo una metodología de valoración de riesgos que permitió determinar:

- Identificar los activos de información dentro del alcance del SGSI.
- Clasificar los activos críticos según su impacto.
- Identificar Amenazas y vulnerabilidades.
- Analizar y evaluar riesgos.
- Determinar la aceptación del riesgo.
- Identificar y evaluar opciones de tratamiento de riesgos.
- Identificar posibles controles a implementar.

Sobre todos los resultados obtenidos, la FACCI tiene registrado los documentos que hacen referencia a esta información:

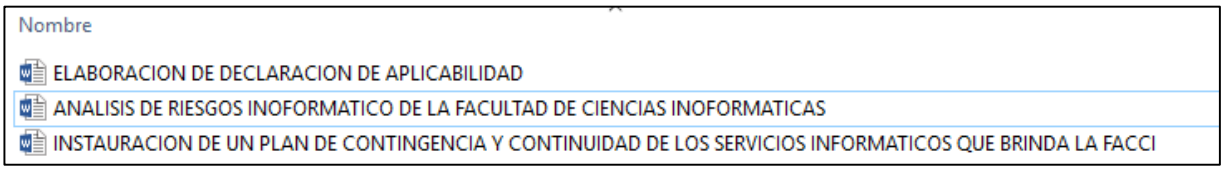


Ilustración 9. *Informes - FACCI*

Los controles aplicables fueron evaluados de acuerdo con la documentación entregada por la FACCI y su aplicabilidad con el Anexo A de la norma.

Sobre el establecimiento y gestión del SGSI de la FACCI, la facultad brinda sus servicios a estudiantes, docentes, personal administrativo, manteniendo un alto nivel de protección de la información que maneja a través de su SGSI, garantizando el cumplimiento, mantenimiento y mejora continua de dicho sistema concediendo los medios y recursos necesarios para cumplir con los objetivos establecidos. La pirámide documental del SGSI de la FACCI incluye los siguientes elementos:

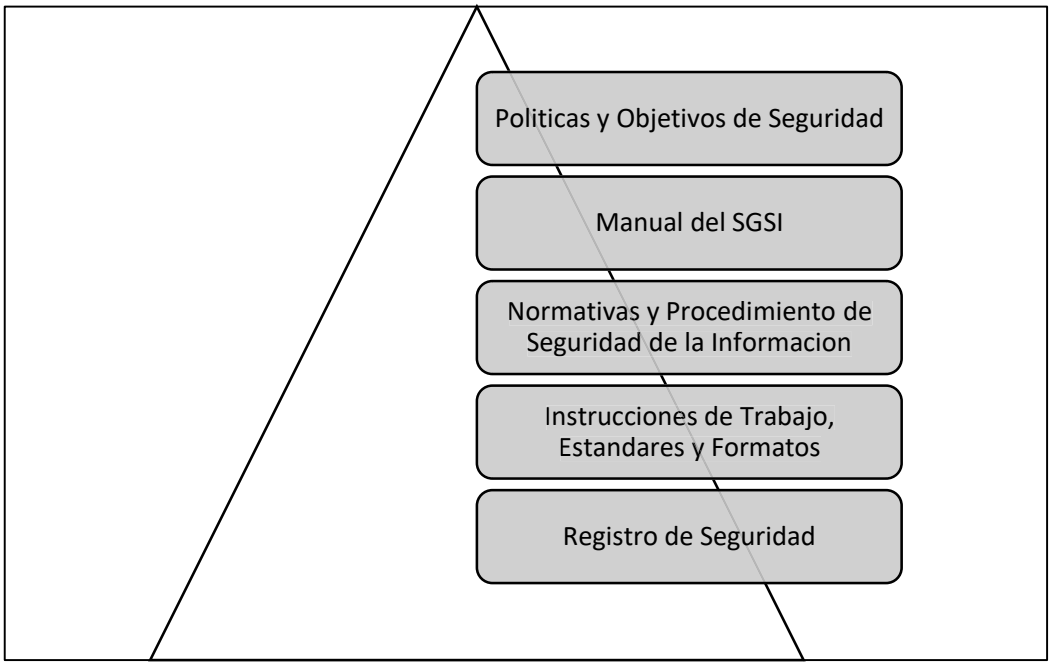


Ilustración 10. *Requisitos de Documentación - FACCI*

Sobre la responsabilidad de la dirección: Demuestra su compromiso comunicado la importancia ha de cumplir con los requisitos impuestos dentro de los distintos controles que forman parte del SGSI, realizando las revisiones de la dirección y asegurando la disponibilidad de los recursos necesarios para continuar operando y mejorando el SGSI.

La FACCI con el objetivo de cumplir con la formación, toma de conciencia y competencia, realiza charlas semestrales y actualizadas para la concientización y capacitación a sus colaboradores.

Para cumplir con dicha planificación, se hace uso de cualquier medio tecnológico, físico o publicitario que permita llegar a toda la FACCI, considerando evaluaciones al personal que ha sido capacitado para medir su nivel de asimilación del conocimiento y para determinar el grado de compromiso que tiene con la seguridad de información de la FACCI.

Sobre auditorías internas: en la FACCI se ha elaborado un plan de auditoria del SGSI concebido para realizarse anualmente con una periodicidad semestral.

Las auditorías internas buscan determinar si el sistema de gestión de la seguridad de la información se mantiene conforme con los requisitos de la Norma ISO27001:2005 y que ha sido implementado, mantenido y operado por el área técnica de la FACCI.

Sobre la mejora del SGSI: a través del modelo PDCA, la FACCI ha establecido su SGSI como un modelo que le permita mejorar continuamente incluyendo una política de SGSI, amparada por la Política de Seguridad de la Información y demás controles tanto técnicos como no técnicos asi como los resultados de las auditorias y demás revisiones que continuamente arrojan no conformidades u oportunidades de mejora, las mismas que se ven traducidos en acciones preventivas y correctivas.

Por acciones correctivas, la FACCI ha definido un proceso para la realización de acciones correctivas que busca eliminar las causas de las no conformidades para prevenir la recurrencia.

Con respecto a las acciones preventivas, la FACCI se preocupa por identificar no conformidades potenciales y sus causas por medio de revisiones periódicas realizadas por parte del equipo de Seguridad de la Información, las revisiones se ejecutan según lo indicado en cada procedimiento que forma parte del SGSI. Con lo anteriormente mencionado el SGSI de la FACCI, ha sido definido, desarrollado, implementado y monitoreado continuamente conforme los requisitos de la Norma ISO/IEC 27001:2005.

CAPÍTULO V: RESULTADOS

5. MARCO PROPOSITIVO

La auditoría interna consiste en verificar de manera objetiva si los controles del SGSI en la Facultad se encuentran operando correctamente y apalancando a la seguridad de la información de la FACCI, de manera objetiva.

Para cumplir con las auditorías internas, según lo estipulado en la Normativa para auditorías internas se debe realizar lo siguiente:

- Planificar la auditoria interna al SGSI según establecido en la Norma para Auditorias del SGSI.
- Elaborar el plan de auditoria.
- Realizar la auditoria interna.
- Elaborar el informe de auditoría interna y desarrollar el plan de acción preliminar.
- Presentar y entregar el informe final de la auditoria.

5.1. Planificar la auditoria interna al SGSI según lo establecido en la normativa para Auditorías Internas del SGSI.

Para la planificación de la auditoria, se hará referencia al documento "Normativa para Auditorías Internas al SGSI", el mismo que tiene como objetivo normalizar los distintos requisitos y controles que deben revisarse en cada auditoria interna realizada al SGSI de la FACCI, considerando que todo el SGSI es evaluado en el año.

Con esta aclaración, es responsabilidad del jefe del área técnica y de los delegados asegurar la ejecución de dos auditorías internas anuales.

Como consideración de debe tener presente que las auditorías internas son un requisito del capítulo seis de la Norma ISO/IEC 27001:2005 cuyo incumplimiento afectaría de manera significativa al SGSI; además, de ser uno de los pilares de la mejora continua.

Como referencias para la elaboración de la "Normativa para Auditorías Internas al SGSI" se toma:

- ISO/IEC 27001:2005.
- Procedimiento de Auditorías Internas de la FACCI.
- Normativa para Auditores del SGSI de la FACCI.

Con respecto a las auditorías internas del SGSI de la FACCI se debe:

- Realizar anualmente con una periodicidad semestral.
- Los registros que deben generarse por cada auditoria interna son:
  - Plan de trabajo de la auditoria interna.
  - Informe de auditoría interna (Resumen ejecutivo e informe detallado de hallazgo).
  - Listado de asistencia con firmas de los asistentes a la presentación de hallazgos.
  - Plan de acción para cerrar las no conformidades halladas.
- Los formatos de elaboración del registro de auditorías deberán ser tomados de los que se generaron en la última auditoria interna realizada.
- Todos los controles y requisitos de la norma ISO/IEC 27001:2005 deben ser probados en su totalidad en el periodo de un año; de tal modo que, la distribución de dichos controles y requisitos para las revisiones en las auditorías internas están detalladas en el documento de controles de la FACCI.
- El jefe del área técnica debe nombrar un delegado quien se encargue de:
  - Convocar y presentar los resultados de la auditoria.
  - Asegurar que se cumpla con el plan de acción.

- Proporcionar al encargado del SGSI todos los registros formalizados y en formato PDF para que queden en el departamento.

- Unas de las actividades de toda auditoria interna es validar el plan de acción generado "INSTAURACION DE UN PLAN DE CONTINGENCIA Y CONTINUIDAD DE LOS SERVICIOS INFORMATICOS QUE BRINDA LA FACCI" (Domínguez Alvia, septiembre, 2018).

Para este apartado es importante mencionar que los recursos asignados en la participación de la auditoria interna deben cumplir con la normativa establecida, el no cumplimiento de la misma acarreara sanciones de acuerdo en los procedimientos internos de la facultad que conforman parte del SGSI.

De acuerdo con el periodo planificado por parte de la normativa se realizará en la siguiente fecha:

Auditoria I (AI 1): Septiembre – octubre 2018.

Cabe indicar que de acuerdo con la normativa para auditorías internas del SGSI, y el objetivo de realizar la revisión de los requisitos y controles en el lapso de un año. Los requisitos para tomar en cuenta en la auditoria de finales de septiembre 2018 son:

Tabla 2.

Requisitos de ISO/IEC 27001:2005-R4

Requisitos
4. Sistemas de gestión de seguridad de la Información.

4.1 Requisitos generales.
4.2. Establecer y manejar el SGSI.
4.2.1 Establecer el SGSI.
4.2.2. Implementar y operar el SGSI.
4.2.3. Monitorear y revisar el SGSI.
4.2.4. Mantener y mejorar el SGSI
4.3. Requisitos de documentación.
4.3.1. General.
4.3.2. Control de documentos.
4.3.3 Control de riesgos.

Fuente: Requisitos tabla 4 de la ISO 27001:2005

Tabla 3.

Requisitos ISO/IEC 27001:2005 R4-R6-R7-R8

Requisitos
5.1 Compromiso de la gerencia.
5.2.1. Provisión de recursos.
5.2.2. Capacitación, conocimiento y capacidad.
7.1 General.
7.2 Insumo de la revisión.
7.3 Resultado de la revisión.
8.1 Mejoramiento continuo.
8.2 Acción correctiva.
8.3 Acción preventiva.

Fuente: Requisitos tomados de la tabla 4,6 7,8 de la ISO 27001:2005

Los controles para tomar en cuenta son:

Tabla 4.

Controles para validar en las Auditorias planificadas Anexo A5

Objetivos De Control Y Controles
A.5.1 Política de seguridad de Información.
A.5.1.1. Documento de la política de seguridad de la información.
A.5.1.2 Revisión Política de seguridad de la información.

Fuente: Controles del Anexo 5 de la ISO 27001:2005

Objetivos De Control Y Controles
A.6.1 Organización Interna.
A.6.1.1. Compromiso de la dirección en la seguridad de la información.
A.6.1.2 Coordinación de la seguridad de la información.
A.6.1.3 Asignación de responsabilidades de la seguridad de la información.
A.6.1.4 Proceso de autorización para medios de procesamiento de la información.
A.6.1.5. Acuerdo de Confidencialidad.
A.6.1.6 Contacto con las Autoridades.
A.6.1.7.Contacto con grupos interesados especialistas.
A.6.1.8Revision Independiente de seguridad de la información.
A.6.2 Partes externas.
A.6.2.1. Identificación de riesgos relacionados con partes externas.
A.6.2.2. Tratamiento de la seguridad cuando negociamos con clientes.
A.6.2.3. Requisitos de seguridad de acuerdos con terceras partes.

Fuente: Controles del Anexo 6 de la ISO 27001:2005

Tabla 5.

Controles para validar en las Auditorias planificadas ANEXO A6-A7.

Gestión De Activos
A.7.1. Responsabilidad.
A.7.1.1. Inventario de activos.
A.7.1.2. Propiedad de los activos.
A.7.1.3 Uso aceptable de los activos.
A.7.2. Clasificación de la información.
A.7.2.1. Guías de clasificación.
A.7.2.2. Etiquetado y gestión de información.

Fuente: Controles del Anexo 7 de la ISO 27001:2005

Tabla 6.

Controles para validar en las Auditorias Planificadas Anexo A8-A9

Objetivos De Control Y Controles
A.8.1 Antes del trabajo.
A.8.1.1 Funciones y Responsabilidades.
A.8.1.2 Selección.
A.8.1.3 Términos y condiciones de la relación laboral.
A.8.2 Durante del trabajo.
A.8.2.1 Gestión de las responsabilidades.
A.8.2.2. Educación y formación en seguridad de la información.
A.8.2.3 Proceso disciplinario.
A.8.3 Terminación o cambio de trabajo.

A.8.3.1 Terminación de responsabilidades.
A.8.3.2. Devolución de activos.
A.8.3.3 Eliminación de derecho de acceso.
A.9.1 Áreas seguras.
A.9.1.1. Perímetro de seguridad física.
A.9.1.2. Control de acceso físico.
A.9.1.3. Seguridad de oficinas, recintos e instalaciones.
A.9.1.4. Protección contra amenazas externas o medioambientales.
A.9.1.5. Trabajo en áreas seguras.
A.9.1.6. Acceso público, despacho y áreas de carga.
A.9.2. Seguridad de los equipos.
A.9.2.1. Ubicación y protección de los equipos.
A.9.2.2. Suministro de energía.
A.9.2.3. Seguridad del cableado.
A.9.2.4. Mantenimiento de los equipos.
A.9.2.5. Seguridad de los equipos fuera de las instalaciones
A.9.2.6. Disposición segura o reutilización de equipos.
A.9.2.7. Retiro de bienes.

Fuente: Controles del Anexo 8,9 de la ISO 27001:2005

Tabla 7.

Controles para validar en las Auditorias planificadas Anexo A 10-15

Objetivos De Control Y Controles
A.10.1 Procedimiento Operacionales y Responsabilidades.

A.10.1.1 Procedimiento de operación documentados.
A.10.1.2. Gestión de cambios.
A.10.1.3. Separación de funciones.
A.10.1.4. Separación de las instalaciones, desarrollo y producción.
A.10.2 Gestión de Servicios entregados por terceras partes.
A.10.2.1 Entrega de servicios.
A.10.2.2. Monitoreo y revisión de servicios suministrados por terceras partes.
A.10.2.3. Gestión de cambios en servicios hechos por terceras partes.
A.10.3. Planeación y Aceptación del Sistema.
A.10.3.1. Planeación de la capacidad.
A.10.3.2. Aceptación del sistema.
A.10.4 Protección contra software malicioso y código móvil.
A.10.4.1. Controles contra software malicioso.
A.10.4.2 Controles contra software Móvil.
A.10.5 Backup-up.
A.10.5.1. Back-up de la información.
A.10.6. Gestión de la seguridad de la red.
A.10.6.1. Controles de red.
A.10.6.2 Seguridad de los servicios de red.
A.10.7 Gestión de los medios.
A.10.7.1. Gestión de los medios removibles.
A.10.7.2. Eliminación de medios.

A.10.7.3. Procedimientos para el manejo de la información.
A.10.7.4. Seguridad de la documentación del sistema.
A.10.8. Intercambio de información.
A.10.8.1. Procedimientos y políticas para el intercambio de información.
A.10.8.2 Acuerdos de Intercambio.
A.10.8.3. Medios físicos en tránsito.
A.10.8.4. Correo Electrónico.
A.10.8.5. Sistemas de información de negocios.
A.11.1 Requisitos del negocio para el control de acceso.
A.11.1.1. Políticas para el control de acceso.
A.11.2 Administración de Acceso de Usuarios.
A.11.2.1. Registro de usuarios.
A.11.2.2. Administración de privilegios.
A.11.2.3. Administración de Contraseñas para usuarios.
A.11.2.4. Revisión de los derechos de acceso de los usuarios.
A.11.3 Responsabilidades de los Usuarios.
A.11.3.1. Uso de contraseña.
A.11.3.2. Equipo de cómputo de usuario desatendido.
A.11.3.3. Política de puesto de trabajo despejado y bloqueo de pantalla.
A.11.4 Control de acceso a redes.
A.11.4.1 Política de uso de los servicios en red.
A.11.4.2. Autenticación de usuarios para conexiones externas.

A.11.4.3. Identificación de equipos de red.
A.11.4.4. Protección de puertos de diagnóstico y configuración remota.
A.11.4.5. Segmentación de redes.
A.11.4.6. Control de conexión a las redes.
A.11.4.7. Control de enrutamiento en la red.
A.11.5. Control de acceso al sistema operativo.
A.11.5.1. Procedimiento de identificación de usuarios segura.
A.11.5.2. Identificación y Autenticación de usuarios.
A.11.5.3. Sistema de administración de contraseña.
A.11.5.4. Uso de utilidades del sistema.
A.11.5.5. Time-out de sesión.
A.11.5.6 Limitación del tiempo de conexión.
A.11.6 Control de Acceso en la información y a las aplicaciones.
A.11.6.1. Restricción de sistemas relevantes.
A.11.6.2. Aislamiento de sistemas relevantes.
A.11.7 Computación móvil y trabajo remoto.
A.11.7.1. Computación y comunicaciones móviles.
A.11.7.2. Trabajo remoto.
A.12.1. Requisitos de Seguridad de los Sistemas.
A.12.1.1. Análisis y especificación de los requisitos de seguridad.
A.12.2. Procesamiento correcto de aplicaciones.
A.12.2.1. Validación de los datos de entrada.

A.12.2.2. Control al procesamiento interno.
A.12.2.3. Autenticación de mensajes.
A.12.2.4. Validación de los datos de salida.
A.12.3. Controles Criptógrafos.
A.12.3.1. Política en el uso de controles Criptográficos.
A.12.3.2. Administración de llaves.
A.12.4. Seguridad de los archivos del sistema.
A.12.4.1. Control operativo del software.
A.12.4.2. Protección de los datos de prueba del sistema.
A.12.4.3. Control de acceso a código de programa fuente.
A.12.5. Seguridad en los procesos de Desarrollo y Soporte.
A.12.5.1 Procedimiento de control de los cambios.
A.12.5.2. Revisión técnica de aplicaciones después de cambios en sistema.
A.12.5.3. Restricciones en los cambios a los paquetes de software.
A.12.5.4. Fuga de información.
A.12.5.5. Desarrollo externo de software.
A.12.6. Gestión de vulnerabilidad Técnica.
A.12.6.1. Control de vulnerabilidades técnicas.
A.13.1. Reporte de incidentes y anomalías de Seguridad de información.
A.13.1.1. Reporte de los incidentes en seguridad de información.
A.13.1.2. Reporte de las debilidades en la seguridad.
A.13.2. Gestión de los incidentes e imprevistos en la seguridad de la información.

A.13.2.1 Responsabilidades y procedimientos.
A.13.2.2. Aprendizaje desde los incidentes en la seguridad de la información.
A.13.2.3. Recolección de evidencias.
A.14.1. Aspectos de seguridad e información en gestión de continuidad del negocio.
A.14.1.1. Incluyendo información de seguridad en el proceso de gestión de continuidad del negocio.
A.14.1.2. Continuidad del negocio y avaluó de riesgo.
A.14.1.3. Desarrollo e implementación del plan de continuidad incluyendo seguridad de la información.
A.14.1.4. Planeación de la estructura de la continuidad del negocio.
A.14.1.5. Prueba, mantenimiento y reevaluación del plan de continuidad del negocio.
A.15.1 Conformidad con los Requisitos legales.
A.15.1.1. Identificación de la legislación aplicable.
A.15.1.2. Derechos de propiedad intelectual.
A.15.1.3. Protección del registro de la organización.
A.15.1.4 Protección de los datos y privacidad de la información personal.
A.15.1.5. Protección del uso inadecuado de los recursos de procesamiento de la información.
A.15.1.6. Reglamentación de los controles criptográficos.
A.15.2. Conformidad de Política de seguridad, norma y el cumplimiento técnico.
A.15.2.1. Conformidad de la política de seguridad y normas.
A.15.2.2. Verificación de conformidad técnico.
A.15.3. Consideraciones de Auditoria de Sistemas de Información.

A.15.3.1. Controles de auditoria de sistemas de información.
A.15.3.2. Protección de las herramientas de auditoria de sistemas de información.

Fuente: Controles del Anexo 10 - 15 de la Iso 27001:2005

Las áreas por intervenir:

Tabla 8.

Áreas por intervenir - FACCI

Áreas
Admin 205
Sala De Servidores 205
Auditorio
Salón Académico
Decanato
Sala De Profesores
Secretaria
Sala De Sesiones
Coordinación Académica
Coordinación De Carrera
Vinculación Con La Colectividad
Comisión De Evaluación Interna
Archivo
Zona Estudiantil
Aso Estudiantil
Lab-201
Lab-202
Lab-203
Lab-206
Lab-Redes
Lab-Emsamblaje
Lab-Electronica
Comunidad Microsoft
Aulas Bloque A
Aulas Bloque B

Fuente: Áreas FACCI

5.2 Elaborar el Plan de Auditoria

Como parte de las actividades para la elaboración del plan de auditoria y en base a la Normativa para auditorías internas se han determinado cuatro aspectos con los cuales se procederá con la creación de dicho documento: identificación, agenda, logística y autoridad.

A continuación, se detalla en la tabla 9, los ítems por cada uno de estos aspectos y su resultado.

Elaboración de plan de auditoria:

Tabla 9

Plan de Auditoria

ITEM	DETALLE
Fecha de elaboración de Plan de Auditoria	La fecha de elaboración del plan se registra en: septiembre 2018. Como insumo para este documento se requirió: o Un Cronograma tentativo de la auditoria. o Controles por revisar. o Activos de Información. o Nombre de un delegado tentativo por cada área auditada. o Integrantes del equipo auditor.
Clase de auditoria	Auditoria Interna (Primera parte).
Proceso	Planeación de auditoria
Auditor Líder	Kimberly Delgado – Investigación
Objetivos de la auditoria	Realizar una auditoría interna de la implantación de la norma ISO/IEC 27001:2005, mediante la definición y aplicación de un plan de trabajo de auditoria.

	Detectar las no conformidades mayores, no conformidades menores y oportunidades de mejora asociadas al SGSI de la FACCI, con respecto a la Norma ISO 27001:2005. Realizar un informe de hallazgo de la Auditoria Interna ISO/IEC 27001:2005 del Sistema de Gestión de Seguridad de la Información de la FACCI. Proporcionar seguimiento al cierre de no conformidades.
Alcance de la auditoria	El alcance de la auditoria es el mismo del Sistema de Gestión de la Seguridad de la Información de la FACCI.
Criterios de la auditoria	Para determinar la valoración se realiza en base a hallazgo vs requisitos y controles de la Norma ISO/IEC 27001:2005, donde No conformidades mayores (en adelante NC+): Incumplimiento de requisitos del 2 al 4 de la Norma. Ej. Se considera una no conformidad mayor el no poseer un requisito el cual es obligatorio. No conformidades menores (en adelante NC-): Implantación de controles del A5 al A15 de la Norma. Ej.: Si existe el control, pero no está operando eficazmente se considera una no conformidad menor. Oportunidades de mejora (en adelante OP): Recomendaciones para mejorar el proceso.
AGENDA:	
Actividades de la auditoria	En este aspecto se realiza cada una de las actividades que se ejecutaran en la auditoria, con fechas, horarios (hora de inicio, hora final) las áreas a ser

	auditadas junto con los auditores que realizan dicha actividad y el lugar donde se realizara. Determinando: Actividades por realizarse para la auditoria interna de la norma ISO/IEC 27001:2005. Definición de Áreas involucradas para la realización de Auditoria Interna. Establecimiento de un programa General de auditoria por áreas involucradas. Definición de equipos de trabajo. Definición de personal a ser evaluado y establecimiento de cronograma de reuniones. Selección de activos de información a ser evaluados aplicando los controles de la norma ISO/IEC 27001:2005. Selección de procedimiento, estándares, normativas y documentos a ser evaluados aplicando los controles de la norma ISO/IEC 27001. Definición de un programa detallado de auditoria por áreas involucradas. **Reunión de apertura de la auditoria** Fecha: Hora de inicio: 9H00 Hora Fin: 11H00 **Áreas a ser auditadas** Considerando el procedimiento interno que brinda la facultad de Ciencias Informáticas a los docentes y estudiantes agregando los anexos A5 al A15 de la norma ISO/IEC 27001:2005; se han definido las siguientes áreas involucradas:

Definición de equipos de trabajo

Para la definición de equipos de trabajo como parte de la realización de tesis previo a la obtención del título del Ingeniera en sistemas, el grupo investigador formo parte del equipo para poder realizar las debidas actividades y esta se definirá por medio de un comité designado por el Honorable Consejo de Facultad o el Decanato de la FACCI,

Las áreas a ser auditadas son:

Tabla 10. Plan de auditoria - Áreas a ser Auditadas

Áreas
Admin 205
Sala De Servidores 205
Auditorio
Salón Académico
Decanato
Sala De Profesores
Secretaria
Sala De Sesiones
Coordinación Académica
Coordinación De Carrera
Vinculación Con La Colectividad
Comisión De Evaluación Interna
Archivo
Zona Estudiantil
Aso Estudiantil
Lab-201
Lab-202
Lab-203
Lab-206
Lab-Redes
Lab- Ensamblaje
Lab- Electrónica
Comunidad Microsoft
Aulas Bloque A
Aulas Bloque B

Fuente:FACCI

Una vez definidas las áreas involucradas, los equipos de trabajo y considerando: el tiempo, los requisitos y los controles a ser auditados; se establece en términos de tiempo la realización de las auditorias tomando en cuenta que en una sola visita se debe completar tanto las entrevistas como la auditoria de controles.

Tabla 11. *Cronograma de auditorías por Áreas 1*

Áreas	Lunes 1	Martes 2	Miércoles 3	Jueves 4	Viernes 5
Admin 205	X				
Sala De Servidores 205	X				
Auditorio	X				
Salón Académico		X			
Decanato		X			
Sala De Profesores		X			
Secretaria		X			
Sala De Sesiones			X		
Coordinación Académica			X		
Coordinación De Carrera			X		
Vinculación Con La Colectividad				X	
Comisión De Evaluación Interna				X	
Archivo				X	
Zona Estudiantil					X

Fuente: Áreas FACCI

Tabla 12. *Cronograma de auditorías por Áreas 2.*

Áreas	Lunes 8	Martes 9	Miércoles 10	Jueves 11	Viernes 12
Aso Estudiantil	X				
Lab-201	X				
Lab-202	X				
Lab-203	X				
Lab-206	X				

	Lab-Redes		X			
	Lab-Emsamblaje		X			
	Lab-Electronica		X			
	Comunidad Microsoft		X			
	Aulas Bloque A			X		
	Aulas Bloque B			X		

Fuente: Áreas FACCI

Activos Seleccionados

Por temas de confidencialidad la facultad no autoriza la divulgación de esta información.

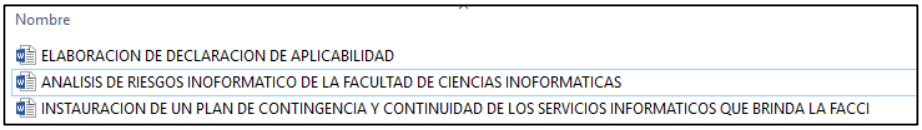


Ilustración 11. *Documentos - FACCI*

Procedimientos seleccionados:

Los procedimientos para revisar fueron seleccionados considerando aquellos que se alineen con los activos de información determinados y que cubran más áreas dentro de la facultad.

LOGÍSTICA	
Logística	En este aspecto se fijan elementos como, cronograma de trabajo, delegados por área a ser auditada. Cronograma de reuniones. Considerando los equipos de trabajo para las entrevistas donde se evaluaran tanto requisitos como controles de la norma ISO/IEC 27001:2005, se detallara el siguiente cronograma.

Tabla 13.

Delegado por cada área a ser auditada

ÁREA	CONTACTO	EDIFICIO
Admin 205	Ing. Gilberth Loor	Facci
Sala De Servidores 205		Facci
Auditorio		Facci
Salón Académico		Facci
Decanato		Facci
Sala De Profesores		Facci
Secretaria		Facci
Sala De Sesiones		Facci
Coordinación Académica		Facci
Coordinación De Carrera		Facci
Vinculación Con La Colectividad		Facci
Comisión De Evaluación Interna		Facci
Archivo		Facci
Zona Estudiantil		Facci
Aso Estudiantil		Facci
Lab-201		Facci
Lab-202		Facci
Lab-203		Facci
Lab-206		Facci
Lab-Redes		Facci
Lab-Emsamblaje		Facci
Lab-Electronica		Facci
Comunidad Microsoft		Facci
Aulas Bloque A		Facci
Aulas Bloque B		Facci

Fuente: Áreas Facci

Recursos

Para la realización de la auditoria, el equipo de trabajo coordino en algunos casos la movilización a las diferentes áreas.

Materiales

	Los documentos se elaboraron dentro de las instalaciones de la FACCI. **Idioma** Los delegados para entrevistar requieren de un traductor al hablar el idioma castellano y ser ciudadanos ecuatorianos. **Levantamiento de información** Para levantar la información que permita determinar si los hallazgos son no conformidades mayores, se realizó verificaciones, entrevistas revisiones vs preguntas y respuesta de los entrevistados, constatación de controles administrativos los cuales se tomara como evidencia para el informe preliminar.

Fuente: Autora del proyecto

5.3 Realizar la auditoria interna

La auditoría interna inicia con la reunión de apertura, en la que se presenta a los participantes los lineamientos para proseguir con la auditoria in situ a realizarse, además de definir fechas de revisiones, reunión de cierre y presentación de resultados.

5.3.1 Reunión de Aperturas y actividades

Fecha: jueves, 27 de septiembre de 2018 y Viernes 27 de Septiembre de 2018

En base al plan d auditoria elaborado y de acuerdo con los aspectos descritos en el punto 3.2, se ejecutó la auditoria interna iniciando con la reunión de apertura registrada con fecha jueves 27 de septiembre del 2018 desde las 9H00 a.m., hasta las 11H00a.m, presentándose el plan de auditoria acordado que el mismo sería ejecutado en el trascurso de las siguiente dos semanas laborales, fue revisado por el equipo, realizándose ajustes de acuerdo con la fase de planificación.

Se efectuaron ejercicios sobre cómo realizar las entrevistas, algunas pautas para mostrar confianza a los auditados, del cómo va a ser la comunicación con los delegados de cada área a ser auditada, como actuar si existen controversia entre auditor y auditado la misma que deberá quedar resuelta en el transcurso de la auditoria, como realizar las observaciones, revisiones de documentos donde deben mantener la confidencialidad de toda la información revisada y metodología para realizar la auditoria, siendo esta última propia de la FACCI.

Se definió el tiempo de duración para cada entrevista en la cual se tomó en cuenta la movilización y la auditoria misma, el mismo otorgado fue de dos horas; en este periodo se incluye el tiempo de espera para el inicio de cada entrevista de auditoria cuyo umbral fue de diez minutos, al igual que la fecha de la reunión de cierre.

Tabla 14.

Cronograma de trabajo acordado para la realización

	Lunes 1	Martes 2	Miércoles 3	Jueves 4	Viernes 5
S1	Auditoria				
S2	Inf. Preliminar Equipo Auditor	Inf. Preliminar Equipo Auditor	Inf. Preliminar /Reunión Cierre	Elaboración Inf. Auditoria/Plan Acción Preliminar	Presentación

Fuente: Autora del proyecto

Consecutivamente se realizó la actividad de acordar entrevistas con los delegados de cada área auditada, tomando la premisa que de acuerdo a la disposición del área TI es de carácter obligatorio colaborar con la auditoria a realizarse y participar activamente el día que haya sido designado para la entrevista, en casos de fuerza mayor el delegado debió asignar para la entrevista, en casos de fuerza mayor el delegado debió designar a personal de apoyo para que participe en la auditoria, esta actividad tomo un tiempo de dos días a partir de la reunión de apertura (27-09-2018) hasta el siguiente día (28-09-2018) en coordinar agendas y material de apoyo.

Para el contacto con el personal a ser auditado se determinó que al menos con cuarenta y ocho horas (48h) de anticipación se confirmara el lugar y fecha de la auditoria conforme al plan enviado por los medios de comunicación masiva interna de la FACCI. En caso de que se requiera una reprogramación de lo realizara dentro de los días de la auditoria ya establecidos.

5.3.2 Realización de Auditoria

Tabla 15.

Cronograma Semana 1 Auditoria I1

	Lunes 1 de Octubre	Martes 2 de Octubre	Miércoles 3 de Octubre	Jueves 4 de Octubre	Viernes 5 de Octubre
S1	Auditorias				

Fuente: Autora del proyecto

En la semana del 1 al 5 se realizó la auditoria propiamente dicha, los respectivos grupos de trabajo se trasladaron a las diferentes áreas a ser auditado de acuerdo al cronograma siguiente:

Áreas	Lunes 1	Martes 2	Miércoles 3	Jueves 4	Viernes 5
Admin 205	X				
Sala De Servidores 205	X				
Auditorio	X				
Salón Académico		X			
Decanato		X			
Sala De Profesores		X			
Secretaria		X			
Sala De Sesiones			X		
Coordinación Académica			X		
Coordinación De Carrera			X		
Vinculación Con La Colectividad				X	
Comisión De Evaluación Interna				X	
Archivo				X	
Zona Estudiantil					X

Fuente: Fuente: Autora del proyecto

Se ejecutaron las respectivas entrevistas y recopilaron la evidencia de cumplimiento con los cuales posteriormente se elaboraron los informes preliminares.

En esta misma semana se envió la convocatoria vía oficio a las áreas involucradas a la presentación oficial del informe de auditoría y la convocatoria a la reunión de cierre a los miembros para evitar contratiempo de última hora. Recopilación de datos (08-09-2018/ 12-09-2018) AI1.

La segunda semana, el día lunes 08 al viernes 12 de octubre de 2018, correspondió a seguir con la auditoria propiamente dicha y a su vez la recopilación de los informes preliminares de cada equipo, la elaboración del informe preliminar con la valoración de hallazgo vs controles de la norma y presentación.

Tabla 16.

Cronograma semana 2 Auditoria I1

	Lunes 08 de octubre	Martes 09 de octubre	Miércoles 10 de octubre	Jueves 11 de octubre	Viernes 12 de octubre
S2	Inf. Preliminar Equipo Auditor	Inf. Preliminar Equipo Auditor	Inf Preliminar/Reunión cierre	Elaboración Inf Auditoria/ Plan Acción Preliminar	Presentación

Fuente: Fuente: Autora del proyecto

Áreas	Lunes 8	Martes 9	Miércoles 10	Jueves 11	Viernes 12
Aso Estudiantil	X				
Lab-201	X				
Lab-202	X				
Lab-203	X				
Lab-206	X				
Lab-Redes		X			
Lab- Ensamblaje		X			
Lab- Electrónica		X			
Comunidad Microsoft		X			

Aulas Bloque A			X		
Aulas Bloque B			X		

Fuente: Fuente: Autora del proyecto

Para cumplir con esta acción se elaboró un formato preliminar de la designación descrita en el punto 3.3.2 para la previa revisión y aprobación.

Verificación de controles: Una vez que se ha completado la auditoria, se realizó una revisión privada de hallazgos, cuyo resultado fue puesto en consideración en la reunión de cierre

La revisión realizada incluyo:

- Revisión de las listas de verificación
- Un estudio de las notas y/u observaciones tomadas en las entrevistas
- Lista de hallazgos
- Enumeración de las no conformidades
- Redacción y clasificación de las acciones correctivas (Plan de Acción)

Los hallazgos de auditoria fueron clasificados de acuerdo con lo indicado en el plan de auditoria descrito en el punto 3.2, donde:

- Una NC+ se levanta cuando el proceso o procedimiento que está siendo auditado no opera o funciona como debería: en ISO/IEC 27001:2005, una NC+ es un incumplimiento de un requisito especifico.

Estas NC fueron registradas de acuerdo con la evaluación realizada con el apoyo de la respectiva evidencia de auditoria, la misma que fue revisada con el delegado con el área auditada obteniendo el reconocimiento de la evidencia, indicando que esta es precisa y que la NC es entendida

La declaración de los hallazgos se realizó incluyendo:

- Una visión global del hallazgo

- Una descripción de la no conformidad
- Si aplica un muestreo de evidencias
- Un resumen del requisito

En los hallazgos encontrados también se encontraron Oportunidades de Mejora, las mismas que en gran parte son un valor añadido a la auditoria y que posiblemente no requieran de una acción correctiva pero que si desean ser comentadas por la auditoria.

Estas observaciones incluyeron:

Puntos que preocupan, pero aún no lo suficiente como para ser considerados una NC y que necesiten encontrarse en el plan de acción.

Situaciones que si no se identifican, en lo posterior podrían incurrir en NC.

Con estas aclaraciones, a continuación, mostramos la matriz de hallazgos encontrados en la auditoria interna realizada en el mes de Octubre del 2018 con el desarrollo de los conceptos descritos en base a los anexos de la norma y los controles aplicables de la corporación, esto se podrá verificar en la sección anexos.

Elaboración el informe de auditoría interna y desarrollar un plan de acción preliminar.

El contenido de este informe fue puesto en consideración en la reunión de cierre que tuvo como fecha de registro miércoles 17 de octubre del 2018 desde las 14H30 hasta las 16H30, donde se expuso las novedades encontradas en la auditoria, auto evaluando la identificación o levantamiento de hallazgos y analizando cada uno de los hallazgos encontrados para clasificarlos como:

No Conformidades (NC+/-): las cuales serán tratadas con: Acciones correctivas o acción preventivas de acuerdo al procedimiento Acciones correctivas y Acciones Preventivas

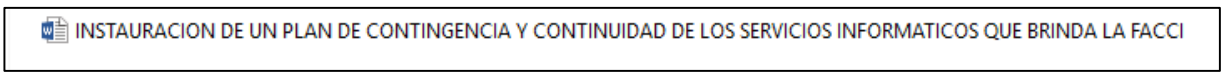


Ilustración 12. *Plan de Contingencia y Continuidad - FACCI*

Oportunidades de mejora: a las cuales se les dará tratamiento inmediato quedando solventadas en el lugar que se haya efectuado la auditoria interna.

Una vez con el informe preliminar se conversó con cada entrevistado para obtener su opinión y aprobación sobre el hallazgo encontrado: esto, con la finalidad de generar el respectivo plan de acción.

Una vez concluido el informe preliminar y formalizado el plan de acción, se elaboró el resumen y el informe detallado de la auditoria interna para posteriormente presentarlos a la parte técnica de la FACCI, estas presentaciones se realizaron los viernes 14 de septiembre del 2018 y el miércoles 19 de septiembre del 2018.

Presentación de hallazgos

El informe de auditoría es un medio formal para comunicar los objetivos, el alcance, las observaciones, hallazgos, conclusiones y recomendaciones. Este informe representa el momento adecuado para separar lo significativo de lo no significativo, debidamente evaluados por su importancia y vinculación con el factor riesgo, reflejados en una presentación lógica y organizada, el cual debe poseer la suficiente información para que sea comprendido por los destinatarios esperados y facilitar las acciones correctivas.

El resumen se realizó de acuerdo con las especificaciones incluidas en el plan de auditoria descrito en el punto 3.2.

Se detallaron los hallazgos en la auditoria registrando lo más significativo y los cuales fueron objeto de recomendaciones para ejecutar planes de acción inmediata.

Tabla 17

Fechas en la que se realizaron los hallazgos

Áreas	Lunes 1	Martes 2	Miércoles 3	Jueves 4	Viernes 5
Admin 205	X				
Sala De Servidores 205	X				

Auditorio	X				
Salón Académico		X			
Decanato		X			
Sala De Profesores		X			
Secretaria		X			
Sala De Sesiones			X		
Coordinación Académica			X		
Coordinación De Carrera			X		
Vinculación Con La Colectividad				X	
Comisión De Evaluación Interna				X	
Archivo				X	
Zona Estudiantil					X
Áreas	Lunes 8	Martes 9	Miércoles 10	Jueves 11	Viernes 12
Aso Estudiantil	X				
Lab-201	X				
Lab-202	X				
Lab-203	X				
Lab-206	X				
Lab-Redes		X			
Lab-Emsamblaje		X			
Lab-Electronica		X			
Comunidad Microsoft		X			
Aulas Bloque A			X		
Aulas Bloque B			X		

Fuente: Fuente: Autora del proyecto

5.4 RESUMEN DE HALLAZGOS IDENTIFICADOS EN LA AUDITORIA INTERNA

Producto de la auditoria interna realizada en fechas de septiembre se obtuvieron los resultados mostrados en el gráfico. En la auditoria de identificaron "No Conformidades mayores" que no permitirán al SGSI de la FACCI, ser recomendado para certificarse bajo la norma ISO/IEC 27001:2005:2005.

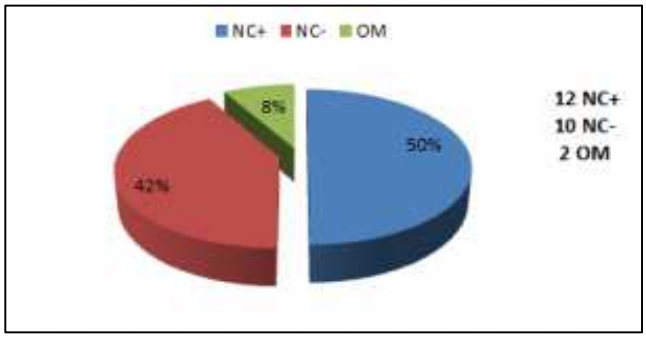


Ilustración 13. *Hallazgos de auditoria interna*

(NC+= No conformidades mayores; NC-= No conformidades menores; OM= Oportunidades de Mejora).

5.4.1. Hallazgos

A continuación, se muestran los hallazgos de la auditoria interna de septiembre:

Tabla 18

Hallazgos de auditoria

Nº	Aspectos	Ares/Activo	NC+	NC-/OM	N#
1	Aunque el manual del SGSI y los documentos anexos se encuentran en el departamento técnico, se identificó que no existe un adecuado conocimiento de las definiciones del SGSI, Manual	Áreas involucradas en el alcance del SGSI	X		5.2.2. Capacitación, sensibilización y competencia.

	del SGSI y Política de Seguridad de la información y su ubicación. En las entrevistas realizadas al personal responsable de las áreas involucradas en el proceso sobre el cual se está implantando el Sistema de Gestión de Seguridad de la Información en la FACCI, se verifico que con excepción del jefe del área técnica, el resto de los involucrados los representantes de las áreas en especial los laboratorios no manejan adecuadamente las definiciones del SGSI, Manual del SGSI, Política de Seguridad de la Información, registro de seguridad y su ubicación.				
2	Aunque existe un documento que establece el plan de tratamiento para los riesgos identificados en los activos de información, se evidencio que existe confusión y en otros casos desconocimiento de las acciones ejecutadas por cada área para el cumplimiento de dichos planes de tratamiento asociadas a los activos de información y la documentación soporte generada de tal actividad.	Áreas involucradas en el alcance del SGSI	X		4.2.3. Monitorear y revisar el SGSI
3	Aunque se ha definido una "Normativa de Administración de incidentes de Seguridad de la Información" u "Procedimiento de gestión de incidentes de seguridad de la información", se evidencio que no todo el personal entrevistado tiene claramente	Áreas involucradas en el alcance del SGSI	X		4.2.3. Monitorear y revisar el SGSI. A13.1.1. Reporte de eventos en la seguridad de la información. A13.1.2 Reporte de las debilidades en la seguridad

	definido a quien y como reportar un incidente de seguridad de la Información. Asi mismo, algunos de ellos confunden el concepto de incidente de seguridad de la información. En las entrevistas realizadas al personal responsable de las áreas involucradas en el SGSI, se verifico que los responsables de las áreas, no tienen claro a quién y cómo reportar un incidente de seguridad de la información.				A13.2.2. Aprender de los incidentes de la seguridad
4	Aunque se ha definido un programa de capacitación del SGSI para el personal de la FACCI, en las entrevistas realizadas al personal delegado de las áreas involucradas en el alcance SGSI, se identificó que el 30% de las personas entrevistadas no respondieron claramente si han tenido una capacitación formal de aspectos de seguridad de la información.	Áreas involucradas en el alcance del SGSI	X		5.2.2. Capacitación sensibilización y competencia
5	Aunque se ha definido un programa de capacitación del SGSI para el personal de la FACCI, en las entrevistas realizadas al personal delegado de las áreas involucradas en el alcance SGSI, se identificó que el 30% de las personas entrevistadas no respondieron claramente si han tenido una capacitación formal de aspecto de seguridad de la información	Áreas involucradas en el alcance del SGSI	X		5.2.2. Capacitación sensibilización y competencia

6	De las 20 reuniones programadas, 15 fueron cumplidas con normalidad de acuerdo a lo planificado, 2 fueron cambiadas en día y hora, 2 se iniciaron con retraso y una no fue dada.	Áreas involucradas en el alcance del SGSI	X		5.1d 5.1e Compromiso de la facultad
7	La declaración de aplicabilidad del SGSI, establece la existencia de la "Normativa De La Seguridad De La Información Para La Administración", sin embargo, no se encuentra difundida.	Áreas involucradas en el alcance del SGSI	X		5.1d Compromiso de la gerencia A8.1.2. Investigación de antecedentes A8.2.1. Responsabilidades de la gerencia A8.2.3 Proceso disciplinario
8	Existe una iniciativa por parte del grupo de seguridad de la información para el último viernes de cada mes dar charlas de sensibilización tanto a nuevos empleados de la FACCI como a proveedores, sin embargo, esta actividad no se cumple adecuadamente ni se encuentra documentada, formalizada ni difundida.	Seguridad de la información		X	5.2.2 Capacitación, sensibilización y competencia
9	En la declaración de aplicabilidad del SGSI, se establece que términos y definiciones se encuentran plasmados en el documento de la Normativa de seguridad, sin embargo, se evidencio que en la práctica esto ha sido plasmado en el contrato de trabajo de los servidores firman al ingresar a la FACCI.	Seguridad de la Información		X	A8.1.3 Términos y condiciones
10	En las revisiones efectuadas se evidencio que la facultad cuenta con el plan de	Seguridad de la Información		X	4.2 Establecimiento y manejo del SGSI

	continuidad ejecutando al momento de la auditoria interna, la cual permitirá seguir operando en una de una contingencia.				A.14 Gestión de la continuidad del negocio
11	Aunque se ha establecido una normativa de cumplimiento legal, este documento no se encuentra bajo el conocimiento de algunos miembros del departamento técnico a pesar de que participaron en la revisión de este.			X	4.2 b2 Establecer el SGSI A15.1 Cumplimiento de los requisitos legales A15.1.4 Protección y privacidad de gastos
12	Si bien se ha definido un área específica para la ubicación de equipos de comunicación de la red IP-MPLS, en la visita efectuada a este sitio se verifico que la puerta permanece sin seguro.	IP Equipos de comunicación de red de prestación de servicios de datos e internet			A9.1.2. Controles de ingreso físico
13	Aunque se han definido e implementado políticas y estándares de acceso y Autenticación de usuarios en los recursos de información, se verifico que no son revisados regularmente con el objetivo de verificar cumplimiento.	Seguridad de la Información		X	A15.2.2 Revisión del cumplimiento técnico
14	Si bien cada área del alcance del SGSI ingresa solicitudes de cambios y/o modificaciones en sistemas, aplicaciones y servicios especiales (Sistemas operativos), y estas pueden ser ubicadas en el sistema, se identificó que no mantiene un registro de todos los cambios y/o modificaciones realizadas. Además, se identificó que no se cuentan con procesos formales para soluciones de TI.	Áreas involucradas en el alcance del SGSI		X	A10.1.2 Gestión del cambio A12.5.1 Procedimiento de control de cambio

15	Si bien en los recursos de programación se ha configurado el cambio de clave en el primer inicio de sesión se evidencio que no existía un proceso formal para la entrega y recepción de claves asignadas a los usuarios con acceso a dichos recursos.			X	A11.2.3. Gestión de claves secretas de los usuarios
16	Aunque se aprobó el documento que establece una revisión semestral de los usuarios con acceso a documentos a la fecha de la auditoria dicha revisión no se ha realizado.	Áreas involucradas en el alcance del SGSI		X	A11.1.1 Política de control de acceso A11.2.4 Revisión de los derechos de acceso del usuario
17	Aunque la Facultad ha establecido personal autorizado para el acceso al Data Center, se identificó que no se realizan revisiones periódicas de tal acceso.	Tecnologías de la Información		X	A9.1.2 Controles de ingreso físico
18	Aunque existen controles físicos para el acceso a los diferentes departamentos de la Facultad, se identificó que estos no siguen un mismo lineamiento y estándar de control de acceso Se evidencio en las distintas visitas realizadas a los departamentos de la FACCI, que para el acceso a los conserjes mantienen diversos controles de revisión y bitácoras de registro no estandarizadas.	Seguridad de la Información		X	A9.1.2 Controles de ingreso físico
19	Se identificó que el archivo de propuesta no ha sido identificado y etiquetado como público o privado o confidencial según corresponda	Administración		X	A7.2 Clasificación de la información

20	En soluciones, se validó que no existe la difusión del nuevo formato de factibilidades técnicas, según se establece en el procedimiento.	Soluciones		X	A10.1.2 Gestión de Cambios
21	En el área de "Servidores" se evidencio que no cuenta con una normativa enfocada al borrado de datos en equipos que son reciclados.			X	A9.2.6 Seguridad de la eliminación o re-uso del equipo

Fuente: Autora del proyecto

5.4.2 Conclusiones De Auditoria Interna

Como conclusiones para esta auditoría, en la presentación del informe se indicó:

- El sistema de Gestión de Seguridad de la Información (SGSI) de la FACCI cumple parcialmente los requisitos que demanda la Norma Internacional ISO/IEC 27001:2005 ya que no hubo acercamiento suficiente a los objetivos de seguridad de la información establecidos en la política del SGSI, así mismo, que los controles implementados no se encuentran operando eficientemente.
- La documentación es adecuada ya que se encuentran orientada a cumplir con los parámetros definidos por la FACCI de acuerdo a su Sistema de Gestión de Seguridad de la Información ISO/IEC 27001:2005; sin embargo, es necesario que la facultad realice un esfuerzo adicional para garantizar que los directivos y sus colaboradores conozcan, comprendan y cumplan con los documentos regulatorios que fueron entregados al área de TI, así como para que se logre un cambio de cultura organización que permita madurar adecuadamente al SGSI.

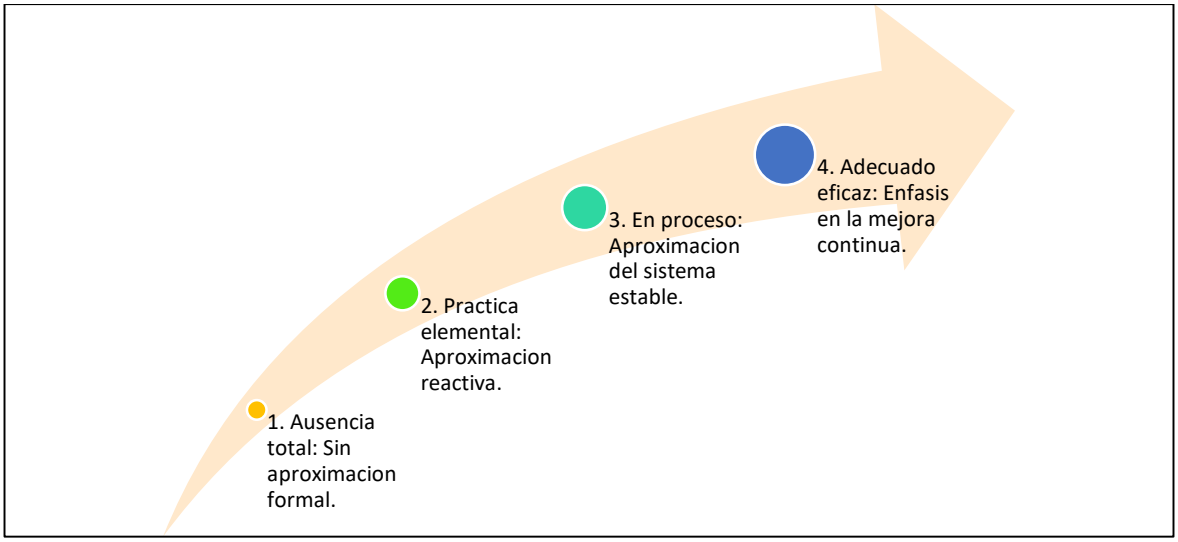
5.4.3 Tratamiento de hallazgo de Auditoria Interna

- Continuar con los planes de sensibilización a todos los colaboradores de todos los niveles de la FACCI involucrados en el SGSI, enfocándose más en aquellos que no han tenido un nivel adecuado de participación, compromiso y conocimiento.
- Fortalecer con apoyo de los jefes de cada área involucrados la difusión y aplicación de los controles administrativos del SGSI, mismos que fueron entregados al departamento de TI.
- Incentivar el compromiso y cambio de cultura organización en la FACCI para que la gestión del SGSI sea asumida por todos sus involucrados por convicción más que por obligación.
- La seguridad de la información y equipos hacen parte de la facultad por lo que se recomienda reubicar el nivel jerárquico del área técnica dentro de la FACCI.
- Realizar una actualización completa de todo el Sistema de Gestión de Seguridad de la Información de la FACCI, para poder evidenciar el cumplimiento del ciclo de vida (PDCA) y se actualice al menos anualmente el SGSI o cuando exista un cambio grande en la organización.

CAPÍTULO VI

6.1 CONCLUSIONES

La Facultad logró obtener un informe final de auditoria interna objetiva que permitió conocer el nivel madurez actual de su SGSI, así como las opciones de mejoras necesarias lograr el cumplimento del estándar acorde con la Norma NTC-ISO/IEC 27001:2005 y las obligaciones reglamentarias y contractuales.



Fuente: Autora del proyecto (Grado de madurez)

A partir de los resultados se definió el plan de cierre de las No conformidades encontradas muy alineadas a la misión de la FACCI. Adicionalmente, se plantearon las recomendaciones para el cierre de las observaciones encontradas.

Basado en el resultado de la auditoría, FACCI, debe enfocar sus esfuerzos en el cierre de las No conformidades, observaciones y en establecer la práctica de la mejora continua en cada uno de los requisitos exigidos.

Para la mejora continua de los procesos es necesario que la auditoria interna se realice semestral para así salvaguardar los activos.

6.2 RECOMENDACIONES

Fortalecer el ciclo de mejora continua de los requisitos del SGSI. Enfocándose en los dominios débiles identificados en la auditoria, al igual que las competencias técnicas, estratégicas y funcionales, así como la cultura organizacional de los funcionarios de la FACCI. A través de la mejora y actualización del plan de capacitación actual de la compañía definiendo más temas de Seguridad de la Información.

Ampliar el alcance actual del SGSI de tal manera que se cubra no solamente la FACCI, si no a su vez al campo académico de la Universidad Laica Eloy Alfaro de Manabí.

Realizar seguimiento al plan de cierre de las No conformidades y observaciones del informe de la auditoría interna. Revisar, actualizar y hacer seguimiento y definir nuevos indicadores que permitan una medición eficaz del estado del SGSI.

Se sugiere que se realice una auditoría de seguimiento que permita validar el cierre de las No conformidades y observaciones, previo a la programación de la auditoría externa para recertificación del SGSI.

Por otro lado cabe recalcar que para la mejora continua de los procesos de mejora es necesario avanzar, y para ello se debe de contar con la ISO 27001:2013, versión actualizada para salvaguardar los activos más importante de la FACCI.

6.3 BIBLIOGRAFIA

- 27001:2005, E. I. (15 de 10 de 2005). Tecnología de la Información – Tecnología de seguridad- Sistemas de Gestión de Seguridad de la Información – Requerimientos. España.
- Corletti. (s.f). www.revista-ays.com/Normas/.Obtenido de www.revista-ays.com: http://www-ays.com/DocsNum22/Corletti.pdf
- Deloitte. (2012). Informe TMT Predicciones 2012 de Deloitte. Quito, Pichincha, Ecuador.
- EY. (s.f.). www.ey.com/Seguridad_de_la:información_en_un_mundo_sin_fronteras. Obtenido de www.ey.com
- http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_inofrmacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_Informacion_en_un_mundo_sin_fronteras.pdf
- ISO, C. (2012). www.iso27001certificates.com. Obtenido de www.iso27001certificates.com/: http://www.iso27001certificates.com/
- ECHENIQUE GARCIA, José Antonio. Auditoria Informática. 2 ed. México, México.: McGraw-Hill, 2001, 300 p. ISBN0-07-015352-3 DAVIS, Chris y Schiller, Mike y Wheeler Kevin. IT Auditing: Using Controls to Protect Information Assets. 2 ed. Estados Unidos.: McGraw-Hill, 2011, 513 p. ISBN 978-0- 07-174239-9
- INSTITUTO ECUATORIANO DE NORMAS TÉCNICAS. Directrices para la auditoria de sistemas de gestión. NTC-ISO/IEC 19011. D.C.: ICONTEC, 2011. 59 p.
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y Vocabulario. NTC-ISO/IEC 27000. D.C.: ICONTEC, 2016. 38 p.

- INSTITUTO ECUATORINO DE NORMAS TÉCNICAS. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. NTC-ISO/IEC 27001. D.C.: ICONTEC, 2013. 25 p.
- [AnISO05]ANÁLISIS DE ISO-27001:2005, Alejandro Corletti Estrada abril de 2006. Disponible en: http://www.mastermagazine.info/informes/9544.php
- [SiGeISO06] Sistema de Gestión de Seguridad de la Información según ISO 27001:2005. 22 de junio de 2006. José Manuel Fernández Domínguez Disponible en:
- http://www.nexusasesores.com/docs/ISO27001-norma-e-implantacion-SGSI.pdf
- [ISO2700106] ISO27001. Portal de ISO 27001 en español. Disponible en: http://www.iso27000.es/iso27000.html
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2006 NIST SP 800 - 100 Manual de Seguridad de Información: Guía para gestores. Gaithersburg, 2006.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2011 NIST SP 800 - 39 Gestionar Riesgos de Seguridad de Información. Gaithersburg, 2011.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2013 NIST SP 800 – 53 Controles de Seguridad y Privacidad para Sistemas de Información Federales y Organizaciones – Revisión 4. Gaithersburg, 2013.
- MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS 2012 MAGERIT - versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información. Madrid, 2015.
- Organización Internacional para la Estandarización (ISO). http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm
- Norma ISO27001. http://www.iso27000.es/iso27000.html

- Alberto G. Alexander. Diseño de un Sistema de Gestión de Seguridad de Información-Óptica ISO 27001:2005. Alfaomega, 2007
- Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.

ANEXOS

ANEXO A

ISO-27001:2005

Evolución del estándar

1995 BS 7799-1:1995 (Norma británica)

1999 BS 7799-2:1999 (Norma británica)

1999 revisión BS 7799-1:1999

2000 ISO/IEC 17799:2000 (Norma internacional código de prácticas)

2002 revisión BS 7799-2:2002

2004 UNE 71502 (Norma española) UNE ISO 27001:

2005 revisión ISO/IEC 17799:2005

2005 revisión BS 7799-2:2005

2005 ISO/IEC 27001:2005 (Norma internacional certificable)

Actualmente el ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. Se debe dejar claro que este es la versión actual del ISO-17799:2002.

La ISO 27001 le permite:

1. Diseñar una herramienta para la implementación del sistema de gestión de seguridad de la información teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos.

2. A la dirección gestionar las políticas y los objetivos de seguridad en términos de integridad, confidencialidad y disponibilidad.

3. Determinar y analizar los riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial.

4. Prevenir o reducir eficazmente el nivel de riesgo mediante la implantación de los controles adecuados, preparando la organización ante posibles emergencias, garantizando la continuidad del negocio [ICONTEC06].

Familia 2700x

El conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta son:

ISO 27000 (2007) Vocabulario y Definiciones

ISO 27001 (2005) Estándar Certificable ya en Vigor (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005

ISO 27002 (2007) Código de Buenas Prácticas relevo de ISO 17799 Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005

ISO 27003 (2008) Guía para la Implantación (bajo desarrollo)

ISO 27004 (2008) Métricas e Indicadores (bajo desarrollo)

ISO 27005 (2008) Gestión de Riesgos (BS 7799-3:2006)

ISO 27006 (2007) Continuidad de Negocio / Recuperación Desastres (BC/DR)

En que consiste

La propuesta de esta norma no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la seguridad de la información", por ello propone toda una secuencia de acciones tendientes al "establecimiento, implementación, operación, monitorización, revisión,

mantenimiento y mejora del **ISMS** (Information Security Management System)". El ISMS, es el punto fuerte de este estándar.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en **tres grandes líneas**:

- **ISMS.**

- **Valoración de riegos (Risk Assesment)**

- **Controles**

El desarrollo de estos puntos y la documentación que generan será tratado continuación. Se tendrá en cuanta la misma enumeración y los puntos que se desarrollan en la norma

Introducción:

General:

Este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS, la adopción del ISMS debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa, la dinámica que implica su aplicación, ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones.

0.2. Aproximación (o aprovechamiento) del modelo:

Este estándar internacional adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el ISMS en una organización. Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

Este estándar internacional adopta también el modelo “Plan-Do-Check-Act” (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS, y significa lo siguiente:

- **Plan** (Establecer el ISMS): Implica, establecer a política ISMS, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

- **Do** (Implementar y operar el ISMS): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

- **Check** (Monitorizar y revisar el ISMS): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- **Act** (Mantener y mejorar el ISMS): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la continua mejora del ISMS.

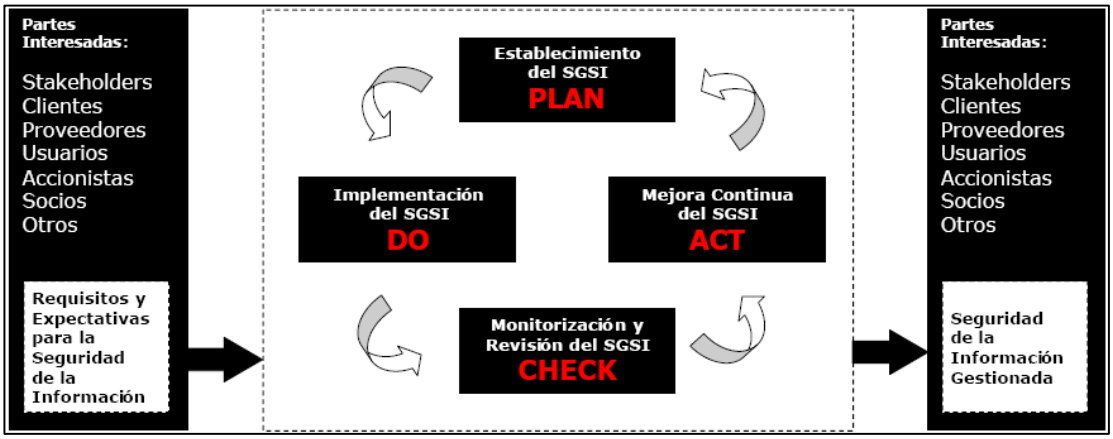


Ilustración 14 Anexo 1.1 Representación del modelo "Plan-Do-Check-Act"

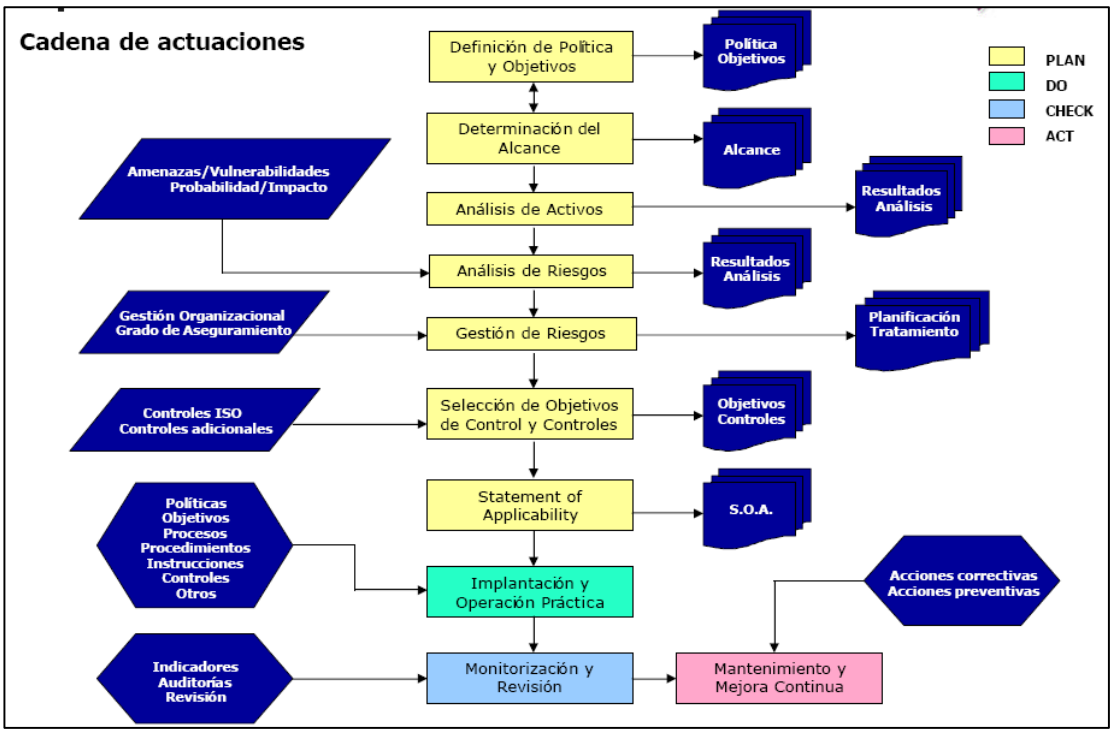


Ilustración 15 Anexo 1.2: Metodología de un SGI según ISO 27001

1.2. Aplicación:

Los requerimientos de este estándar internacional son genéricos y aplicables a la totalidad de las organizaciones. La exclusión de los requerimientos especificados en las cláusulas 4, 5, 6, 7 y 8, no son aceptables cuando una organización solicite su conformidad con esta norma.

Estas cláusulas son:

4. ISMS.

5. Responsabilidades de la Administración

6. Auditoría Interna del ISMS

7. Administración de las revisiones del ISMS

8. Mejoras del ISMS.

(Estas cláusulas realmente conforman el cuerpo principal de esta norma)

Cualquier exclusión a los controles detallados por la norma y denominados como "necesarios" para satisfacer los criterios de aceptación de riegos, debe ser justificada y se debe poner de manifiesto, o evidenciar claramente los criterios por los cuales este riesgo es asumido y aceptado.

2. Normativas de referencia:

Para la aplicación de este documento, es indispensable tener en cuenta la última versión de:

"ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management"*

3. Términos y definiciones:

La siguiente terminología aplica a esta norma:

3.1. Recurso (Asset): Cualquier cosa que tenga valor para la organización.

3.2. Disponibilidad (availability): Propiedad de ser accesible y usable bajo demanda por una entidad autorizada.

3.3. Confidencialidad (confidentiality): Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.

3.4. Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.

3.5. Eventos de seguridad de la información: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

3.6. Incidente de seguridad: uno o varios eventos de seguridad de la información, no deseada o inesperada que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.

3.7. Sistema de administración de la seguridad de la información (ISMS: Information Security Management System): Parte de los sistemas de la empresa, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

NOTA: el ISMS incluye las políticas, planes, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

3.8. Integridad: Propiedad de salvaguardar la precisión y completitud de los recursos.

3.9. Riesgo residual: El riesgo remanente luego de una amenaza a la seguridad.

3.10. Aceptación de riesgo: Decisión de aceptar un riesgo.

3.11. Análisis de riego: Uso sistemático de la información para identificar fuentes y estimar riesgos.

3.12. Valoración de riesgo: Totalidad de los procesos de análisis y evaluación de riesgo.

3.13. Evaluación de riesgo: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.

3.14. Administración del riesgo: Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.

3.15. Tratamiento del riesgo: Proceso de selección e implementación de mediciones para modificar el riesgo.

3.16. Declaración de aplicabilidad: Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del ISMS.

4. ISMS (Information Security Managemet System).

4.1. Requerimientos generales:

La organización, establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documentado ISMS en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos. Para este propósito esta norma el proceso está basado en el modelo PDCA comentado en el punto 0.2.

4.3.2. Control de documentos:

Todos los documentos requeridos por el ISMS serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

Aprobar documentos y prioridades o clasificación de empleo.

Revisiones, actualizaciones y reaprobaciones de documentos.

Asegurar que los cambios y las revisiones de documentos sean identificados.

Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.

Asegurar que los documentos permanezcan legibles y fácilmente identificables.

Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.

Asegurar que los documentos de origen externo sean identificados.

Asegurar el control de la distribución de documentos.

Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito

5. Responsabilidades de administración:

5.1. La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de:

- Establecimiento de la política del ISMS

- Asegurar el establecimiento de los objetivos y planes del ISMS.

- Establecer roles y responsabilidades para la seguridad de la información.

- Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.

- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el ISMS (5.2.1).

- Decidir los criterios de aceptación de riesgos y los niveles de este.

- Asegurar que las auditorías internas del ISMS, sean conducidas y a su vez conduzcan a la administración para la revisión del ISMS (ver 7.)

5.2.2. Formación, preparación y competencia:

La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el ISMS sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria (Documento: Planificación, guías y programas de formación y preparación).

6. Auditoría interna del ISMS:

La organización realizará auditorías internas al ISMS a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros serán definidos en un procedimiento

7. Administración de las revisiones del ISMS:

Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el ISMS incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, como se mencionó en el punto anterior serán claramente documentados y los mismos darán origen a esta actividad.

Esta actividad está constituida por la revisión de entradas (7.2.) y la de salidas (7.3.) y dará como resultado el documento correspondiente.

8. Mejoras al ISMS

La organización deberá mejorar continuamente la eficiencia del ISMS a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración.

8.2. Acciones correctivas:

La organización llevará a cabo acciones para eliminar las causas que no estén en conformidad con los requerimientos del ISMS con el objetivo de evitar la recurrencia de los mismos. Cada una de estas acciones correctivas deberá ser documentada

El anexo A de esta norma propone una detallada tabla de los controles, los cuales quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad

A.6 Organización de la información de seguridad

A.7 Administración de recursos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

A.10 Administración de las comunicaciones y operaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad de negocio

A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

El anexo B, que es informativo, a su vez proporciona una breve guía de los principios de OECD (guía de administración de riesgos de sistemas de información y redes - París, Julio del 2002, "www.oecd.org") y su correspondencia con el modelo PDCA.

Por último, el **Anexo C**, también informativo, resume la correspondencia entre esta norma y los estándares ISO 9001:2000 y el ISO 14001:2004

PLANTILLA DE AUDITORIA

Auditoria Informática

Auditoria No:		
Institución:	Facultad de Ciencias Informáticas	**Fecha:**
Departamento:		
Grupo auditor:		

Fuente: Autora del proyecto

Fuente: Autora del proyecto

Objetivo:
Correcta planeación del Área de Sistemas, el control de la función informática, el análisis de la eficiencia de los Sistemas Informáticos que comporta, la verificación del cumplimiento de la Normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos
Alcance:

Personal a cargo	
NOMBRE	**CARGO**

Fuente: Autora del proyecto

ACTIVIDADES PRINCIPALES:

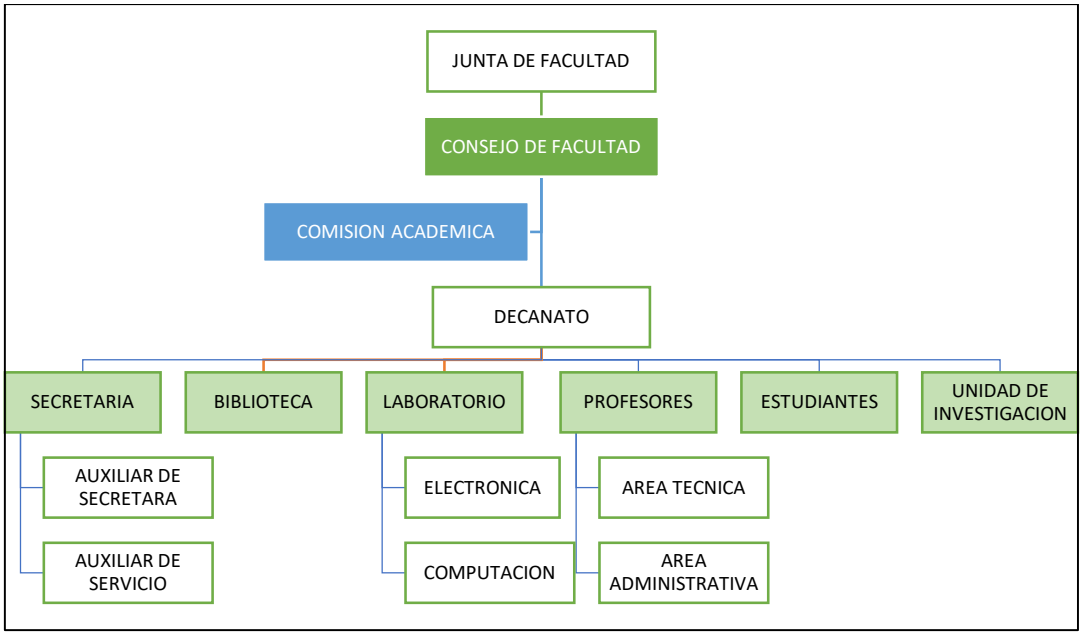
1. _____

2. _____

3. _____

4. _____

ORGANIGRAMA DE LA INSTIRUCION Y/ DEPARTAMENTO



Fuente: FACCI

ANÁLISIS FODA

_____

_____

_____

_____

METODOLOGÍA

(METODOLOGÍA CON LA QUE VAS A REALIZAR LA AUDITORÍA, CON SUS RESPECTIVAS ACTIVIDADES)

PREGUNTAS	SI	NO	NOTA
A.5 Políticas de Seguridad			
Se conocen y han sido comunicadas las políticas de seguridad, tanto al personal administrativo como a docentes y estudiantes.			
A.5.1 Política de seguridad de Información			
A.5.1.1. Documento de la política de seguridad de la información			
A.5.1.2 Revisión Política de seguridad de la información			
A.6 Organización de la seguridad de la Información			
Se tiene el alcance documentado y existe evidencia que se han identificado todas las interfaces			
A.6.1 Organización Interna			

A.6.1.1. Compromiso de la dirección en la seguridad de la información			
A.6.1.2 Coordinación de la seguridad de la información			
A.6.1.3 Asignación de responsabilidades de la seguridad de la información			
A.6.1.4 Proceso de autorización para medios de procesamiento de la información			
A.6.1.5. Acuerdo de Confidencialidad			
A.6.1.6 Contacto con las Autoridades			
A.6.1.7. Contacto con grupos interesados especialistas			
A.6.1.8Revision Independiente de seguridad de la información			
A.6.2 Partes externas			
A.6.2.1. Identificación de riesgos relacionados con partes externas			
A.6.2.2. Tratamiento de la seguridad cuando negociamos con clientes			
A.6.2.3. Requisitos de seguridad de acuerdos con terceras partes			
A.7 Gestión de Activos			
La facultad cuenta con el inventario de los activos, clasificada por áreas			
Todos los sistemas informáticos cuentan con procedimiento de aceptación de los sistemas antes de su funcionamiento			
A.7.1. Responsabilidad			
A.7.1.1. Inventario de activos			

A.7.1.2. Propiedad de los activos			
A.7.1.3 Uso aceptable de los activos			
A.7.2. Clasificación de la información			
A.7.2.1. Guías de clasificación			
A.7.2.2. Etiquetado y gestión de información			
A.8 Seguridad de los Recursos Humanos			
Existen responsables asociados a las áreas frente al SGSI			
A.8.1 Antes del trabajo			
A.8.1.1 Funciones y Responsabilidades			
A.8.1.2 Selección			
A.8.1.3 Términos y condiciones de la relación laboral			
A.8.2 Durante del trabajo			
A.8.2.1 Gestión de las responsabilidades			
A.8.2.2. Educación y formación en seguridad de la información			
A.8.2.3 Proceso disciplinario			
A.8.3 Terminación o cambio de trabajo			
A.8.3.1 Terminación de responsabilidades			

A.8.3.2. Devolución de activos			
A.8.3.3 Eliminación de derecho de acceso			
A.9.1 Áreas seguras			
A.9.1.1. Perímetro de seguridad física			
A.9.1.2. Control de acceso físico			
A.9.1.3. Seguridad de oficinas, recintos e instalaciones			
A.9.1.4. Protección contra amenazas externas o medioambientales			
A.9.1.5. Trabajo en áreas seguras			
A.9.1.6. Acceso público, despacho y áreas de carga			
A.9.2. Seguridad de los equipos			
A.9.2.1. Ubicación y protección de los equipos			
A.9.2.2. Suministro de energía			
A.9.2.3. Seguridad del cableado			
A.9.2.4. Mantenimiento de los equipos			
A.9.2.5. Seguridad de los equipos fuera de las instalaciones			
A.9.2.6. Disposición segura o reutilización de equipos			
A.9.2.7. Retiro de bienes			

A.9 Seguridad física y ambiental			
Los sistemas de cómputo estan adecuadamente protegidas contra amenazas físicas y ambientales			
Existe una persona responsable de la seguridad			
Existe personal de vigilancia en la facultad			
Son controladas las visitas y demostraciones en el centro de computo			
Se registra el acceso al departamento de computo de personas ajenas a la dirección informática			
Se ha adiestrado el personal en el manejo de los extintores			
Los interruptores de energía estan debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos			
Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego			
El personal ajeno a operación sabe qué hacer en el caso de una emergencia(incendio)			
Existe salida de emergencia			
Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia			
Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo			
A.9.1.6. Acceso público, despacho y áreas de carga			
A.9.2. Seguridad de los equipos			
A.9.2.1. Ubicación y protección de los equipos			

A.9.2.2. Suministro de energía			
A.9.2.3. Seguridad del cableado			
A.9.2.4. Mantenimiento de los equipos			
A.9.2.5. Seguridad de los equipos fuera de las instalaciones			
A.9.2.6. Disposición segura o reutilización de equipos			
A.9.2.7. Retiro de bienes			
A.10 Gestión de las comunicaciones y operaciones			
Se encuentran documentados todos los procesos operativos			
Se controlan de manera adecuada los cambios en plataforma y sistema de información para la reducción de riesgos			
Se tiene el control de acceso a las redes para reducir los riegos			
Se tiene el control y planes de sensibilización de los medios removibles			
Se tiene los planes de sensibilización que fortalecen la reducción de riesgos sobre el inadecuado manejo de la información			
Son protegidas las áreas que hacen uso de mensajería y aplicaciones de transacciones (online) que hacen uso de trabajo			
Los sistemas son monitoreados de manera permanente			
A.10.1 Procedimiento Operacionales y Responsabilidades			
A.10.1.1 Procedimiento de operación documentados			
A.10.1.2. Gestión de cambios			

A.10.1.3. Separación de funciones			
A.10.1.4. Separación de las instalaciones, desarrollo y producción			
A.10.2 Gestión de Servicios entregados por terceras partes			
A.10.2.1 Entrega de servicios			
A.10.2.2. . Monitoreo y revisión de servicios suministrados por terceras partes			
A.10.2.3. Gestión de cambios en servicios hechos por terceras partes			
A.10.3. Planeación y Aceptación del Sistema			
A.10.3.1. Planeación de la capacidad			
A.10.3.2. Aceptación del sistema			
A.10.4 Protección contra software malicioso y código móvil			
A.10.4.1. Controles contra software malicioso			
A.10.4.2 Controles contra software Móvil			
A.10.5 Backup-up			
A.10.5.1. Back-up de la información			
A.10.6. Gestión de la seguridad de la red			
A.10.6.1. Controles de red			
A.10.6.2 Seguridad de los servicios de red			

A.10.7 Gestión de los medios			
A.10.7.1. Gestión de los medios removibles			
A.10.7.2. Eliminación de medios			
A.10.7.3. Procedimientos para el manejo de la información			
A.10.7.4. Seguridad de la documentación del sistema			
A.10.8. Intercambio de información			
A.10.8.1. Procedimientos y políticas para el intercambio de información			
A.10.8.2 Acuerdos de Intercambio			
A.11 Control de acceso			
Tiene una aplicabilidad en todo el SGSI			
Los usuarios son identificados, autenticados y autorizado de acuerdo a los accesos permitidos			
Se controla el acceso a las redes para reducir riesgos			
Los sistemas sensibles tienen un nivel de seguridad alto			
A.11.1 Requisitos del negocio para el control de acceso			
A.11.1.1. Políticas para el control de acceso			
A.11.2 Administración de Acceso de Usuarios			
A.11.2.1. Registro de usuarios			

A.11.2.2. Administración de privilegios			
A.11.2.3. Administración de Contraseñas para usuarios			
A.11.2.4. Revisión de los derechos de acceso de los usuarios			
A.11.3 Responsabilidades de los Usuarios			
A.11.3.1. Uso de contraseña			
A.11.3.2. Equipo de cómputo de usuario desatendido			
A.11.3.3. Política de puesto de trabajo despejado y bloqueo de pantalla			
A.11.4 Control de acceso a redes			
A.11.4.1 Política de uso de los servicios en red			
A.11.4.2. Autenticación de usuarios para conexiones externas			
A.11.4.3. Identificación de equipos de red			
A.11.4.4. Protección de puertos de diagnóstico y configuración remota			
A.11.4.5. Segmentación de redes			
A.11.4.6. Control de conexión a las redes			
A.11.4.7. Control de enrutamiento en la red			
A.11.5. Control de acceso al sistema operativo			
A.11.5.1. Procedimiento de identificación de usuarios segura			

A.11.5.2. Identificación y Autenticación de usuarios			
A.11.5.3. Sistema de administración de contraseña			
A.11.5.4. Uso de utilidades del sistema			
A.11.5.5. Time-out de sesión			
A.11.5.6 Limitación del tiempo de conexión			
A.11.6 Control de Acceso en la información y a las aplicaciones			
A.11.6.1. Restricción de sistemas relevantes			
A.11.6.2. Aislamiento de sistemas relevantes			
A.11.7 Computación móvil y trabajo remoto			
A.11.7.1. Computación y comunicaciones móviles			
A.11.7.2. Trabajo remoto			
A.12 Adquisición desarrollo y mantenimiento de los sistemas de información			
Existe un plan de mantenimiento preventivo para cada dispositivo del sistema de computo			
Se ha implementado el plan de mantenimiento			
Se notifican las fallas de equipos			
Se les da seguimiento (plan de mantenimiento)			
A.12.1. Requisitos de Seguridad de los Sistemas			

A.12.1.1. Análisis y especificación de los requisitos de seguridad			
A.12.2. Procesamiento correcto de aplicaciones			
A.12.2.1. Validación de los datos de entrada			
A.12.2.2. Control al procesamiento interno			
A.12.2.3. Autenticación de mensajes			
A.12.2.4. Validación de los datos de salida			
A.12.3. Controles Criptógrafos			
A.12.3.1. Política en el uso de controles Criptográficos			
A.12.3.2. Administración de llaves			
A.12.4. Seguridad de los archivos del sistema			
A.12.4.1. Control operativo del software			
A.12.4.2. Protección de los datos de prueba del sistema			
A.12.4.3. Control de acceso a código de programa fuente			
A.12.5. Seguridad en los procesos de Desarrollo y Soporte			
A.12.5.1 Procedimiento de control de los cambios			
A.12.5.2. Revisión técnica de aplicaciones después de cambios en sistema			
A.12.5.3. Restricciones en los cambios a los paquetes de software			

A.12.5.4. Fuga de información			
A.12.5.5. Desarrollo externo de software			
A.12.6. Gestión de vulnerabilidad Técnica			
A.12.6.1. Control de vulnerabilidades técnicas			
A.13 Gestión de incidentes de seguridad de la información			
Herramienta para la documentación de incidentes de seguridad			
Documentación con las responsabilidades de las áreas frente a los incidentes de seguridad			
A.13.1. Reporte de incidentes y anomalías de Seguridad de información			
A.13.1.1. Reporte de los incidentes en seguridad de información			
A.13.1.2. Reporte de las debilidades en la seguridad			
A.13.2. Gestión de los incidentes e imprevistos en la seguridad de la información			
A.13.2.1 Responsabilidades y procedimientos			
A.13.2.2. Aprendizaje desde los incidentes en la seguridad de la información			
A.13.2.3. Recolección de evidencias			
A.14 Gestión de la continuidad del negocio			
Documentación de los procesos para la continuidad de negocio			
A.14.1. Aspectos de seguridad e información en gestión de continuidad del negocio			

A.14.1.1. Incluyendo información de seguridad en el proceso de gestión de continuidad del negocio			
A.14.1.2. Continuidad del negocio y avaluó de riesgo			
A.14.1.3. Desarrollo e implementación del plan de continuidad incluyendo seguridad de la información			
A.14.1.4. Planeación de la estructura de la continuidad del negocio			
A.14.1.5. Prueba, mantenimiento y reevaluación del plan de continuidad del negocio			
A.15 Cumplimiento			
Plan de mantenimientos preventivos y correctivos de los SGSI			
Documentación con las normas y leyes que se aplican al SGSI			
Controles persuasivos y disuasivos en los sistemas y plataforma			
A.15.1 Conformidad con los Requisitos legales			
A.15.1.1. Identificación de la legislación aplicable			
A.15.1.2. Derechos de propiedad intelectual			
A.15.1.3. Protección de los registros de la organización			
A.15.1.4 Protección de los datos y privacidad de la información personal			
A.15.1.5. Protección del uso inadecuado de los recursos de procesamiento de la información			
A.15.1.6. Reglamentación de los controles criptográficos			
A.15.2. Conformidad de Política de seguridad, norma y el cumplimiento técnico			

A.15.2.1. Conformidad de la política de seguridad y normas			
A.15.2.2. Verificación de conformidad técnico			
A.15.3. Consideraciones de Auditoria de Sistemas de Información			
A.15.3.1. Controles de auditoria de sistemas de información			
A.15.3.2. Protección de las herramientas de auditoria de sistemas de información			

Fuente: Autora del proyecto

VERIFICACIÓN DE AUDITORIA FÍSICA

Nombre de equipo	Excelente	Buena	Regular	Mínimo	No cumple

Fuente: Autora del proyecto

INFORME FINAL:

_____

_____