UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

FACULTAD DE CIENCIAS INFORMÁTICAS

TRABAJO DE TITULACIÓN: MODALIDAD PROYECTO DE INVESTIGACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA DEL PROYECTO:
SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO NORMAS ISO/IEC 27001

TAREA INVESTIGATIVA ASIGNADA:
"ELABORACIÓN DE LA PROPUESTA DE DECLARACIÓN DE APLICABILIDAD PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS BAJO LAS NORMAS ISO/IEC 27001: 2005"

AUTORA:

SRTA. DELGADO CHAVARRÍA KERLY NARCISA

DIRECTORA DE TRABAJO DE TITULACIÓN:

ING. VERA NAVARRETE DENISE SORAYA

MANTA-MANABÍ-ECUADOR

2018-2019

CERTIFICACIÓN

En calidad de docente tutor(a) de la Facultad de Ciencias Informáticas de la Universidad Laica "Eloy Alfaro" de Manabí, certifico:

Haber dirigido y revisado el trabajo de titulación, cumpliendo el total de 64 horas, bajo la modalidad de Proyecto de Investigación, cuyo tema del proyecto es "**Elaboración de Declaración de Aplicabilidad**", el mismo que ha sido desarrollado de acuerdo a los lineamientos internos de la modalidad en mención y en apego al cumplimiento de los requisitos exigidos por el Reglamento de Régimen Académico, por tal motivo CERTIFICO, que el mencionado proyecto reúne los méritos académicos, científicos y formales, suficientes para ser sometido a la evaluación del tribunal de titulación que designe la autoridad competente.

La autoría del tema desarrollado, corresponde a la Señorita **Kerly Narcisa Delgado Chavarría,** con cédula de identidad N° 131453154-0, estudiante de la carrera de Ingeniería en Sistemas, período académico 2017-2018, quien se encuentra apto para la sustentación de su trabajo de titulación.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

Manta, 08 de febrero del 2018.

Lo certifico,

Ing. Denise Vera Navarrete

Docente Tutor(a)

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

ELABORACIÓN DE LA PROPUESTA DE DECLARACIÓN DE APLICABILIDAD PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS BAJO LAS NORMAS ISO/IEC 27001: 2005"

Tribunal examinador que declara APROBADO el Grado de
INGENIERA EN SISTEMAS, de la señorita:
KERLY NARSICA DELGADO CHAVARRÍA

Dra. Dolores Muñoz Verduga (Presidenta Tribunal) _____
Dr. Johnny Larrea Plua (Miembro del tribunal) _____
Mg. Robert Moreira Centeno (Miembro del Tribunal) _____

Manta, 01 de marzo del 2019

DECLARACIÓN EXPRESA DE AUDITORÍA

Yo, DELGADO CHAVARRÍA KERLY NARCISA con Cédula de Identidad N° 131453154-0, declaro ser la responsable del contenido del presente Proyecto de Investigación, cuyo tema es "ELABRACIÓN DE LA DECLARACIÓN DE APLICABILIDAD PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS BAJO LAS NORMAS ISO/IEC 27001: 2005", y derechos patrimoniales a la Universidad Laica "Eloy Alfaro" de Manabí, en virtual de lo dispuesto en el Art. 15 de la Ley de Propiedad Intelectual.

Así mismo, autorizo a la Universidad Laica "Eloy Alfaro" de Manabí para que se realice la digitalización y publicación de este Proyecto de Investigación en el repositorio digital de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Además, la ejecución se respetó las disposiciones legales que protegen los derechos de autores vigentes. Por último la responsabilidad del contenido de este Proyecto de Investigación corresponde exclusivamente a mi autoría.

Lo Certifico:

Delgado Chavarría Kerly Narcisa

C.I: 131453154-0

DEDICATORIA

El presente trabajo investigativo lo dedico principalmente a Dios, por la bendición de la vida que me permite continuar este proceso de obtener uno de los anhelos más deseados.

A mis padres, por su amor incondicional, su educación y sobre todo, su trabajo y sacrificio en todos estos años, lo que me ha permitido llegar hasta aquí y convertirme en lo que soy.

A mis hermanos, que de una u otra manera siempre están ahí brindando el apoyo necesario.

A todos las personas que realmente me han apoyado y han hecho de este trabajo un éxito, especialmente a aquellos docentes que supieron compartir sus conocimientos.

Este nuevo logro es en gran parte de todos ustedes.

AGRADECIMENTO

Agradezco a Dios por acompañarme en el transcurso de la vida, brindándome paciencia y sabiduría para culminar con éxito este nuevo logro.

Gracias a mis padres: María y Carlos, por confiar, creer y apoyaren mis sueños, por los consejos, valores y principios inculcados desde muy pequeña.

Gracias a mis pequeños hermanos: Julexi y Jahir por demostrar lo buenos hermanos que son, y por tenerme como un ejemplo de hermana aunque no siempre sea así.

A mi amigo y pareja actual: Jairo, que me ha apoyado, acompañado y ayudado en todo este tiempo, y en el transcurso de la elaboración de este gran trabajo, brindándome la fortaleza y alegría necesaria en los momentos más difíciles, y la cordura y compañía en los más fáciles.

Finalmente agradezco a los docentes de la FACCI, esos docentes que realmente superan las expectativas y ayudan a sus estudiantes, no solo impartiendo sus conocimientos, si no mejorando todo lo que hacemos y apoyándonos a cumplir nuestros sueños.

RESUMEN

Este trabajo de investigación es una de muchas tareas que deben ser cumplidas para lograr el objetivo del "Sistema de Gestión de Seguridad de la Información bajo las normas ISO 27001", proyecto del cual forman parte y que se implementará en la facultad de Ciencias Informáticas en base al cumplimiento y finalización de las tareas.

Se realizó esta investigación no sólo para cumplir un parámetro del proyecto de seguridad informática a implementar en la Unidad académica, sino también, para dar a conocer el impacto de la declaración de aplicabilidad y las normas ISO usadas en el mismo, esto significa que, la gestión de la seguridad de la información en la Facultad se reduce a la declaración de aplicabilidad donde se encontraran todas las normas que estipuladamente se deben aplicar con su debida justificación y los documentos que lo corroboran.

Para poder elaborar la declaración de aplicabilidad se hicieron dos actividades previas enlazadas entre si y enlazadas a la declaración de aplicabilidad, tenemos como actividad inicial la "Evaluación y Tratamiento del Análisis de Riesgo de la Facultad de Ciencias Informáticas" tema investigado y elaborado por: "Guerrero Bravo Gema Lilibeth, y Mera Quintero Evelyn Janira". Y la "Instauración de un Plan de Contingencia y Continuidad de los Servicios Informáticos que brinda la FACCI" tema investigado y elaborado por "Domínguez Alvia Víctor Armando"

La mayoría de organizaciones empiezan a comprender que el activo más importante es la información que estas manejan, todo esto se puede perder fácilmente ante amenazas externas (desastres naturales, robos de equipos) y amenazas internas (desactualizaciones de so, virus, robo, ingeniería social), gracias a la falta de medidas y controles implementados.

Debido a que en Facultad de Ciencias Informáticas, esto ya ha ocurrido, se optó por un Sistema de Gestión de Seguridad de la Información bajo las normas ISO/IEC 27001:2005 para mantener a salvo su información conjuntamente con sus activos informáticos y de paso obtener certificaciones ISO a nivel de seguridad informática.

Este estudio se enfocado en la elaboración de la declaración de aplicabilidad, permitirá a la Unidad Académica adecuarse al seguimiento del proyecto a implementarse según los activos, los riesgos, y amenazas, logrando así la no obsolescencia del sistema de gestión de seguridad de la información y las debidas certificaciones requeridas y planteadas.

Abstract

This research work is one of many tasks that must be fulfilled to achieve the objective of the "Information Security Management System under the ISO 27001 standards", a project of which they are part and which will be implemented in the Faculty of Computer Science in based on compliance and completion of tasks.

This research was carried out not only to meet a parameter of the computer security project to be implemented in the academic unit, but also to publicize the impact of the declaration of applicability and the ISO standards used in it, this means that the Management of information security in the Faculty is reduced to the declaration of applicability where all the stipulative norms that should be applied with their due justification and the documents that corroborate it will be found.

In order to prepare the declaration of applicability, two previous activities linked to each other and linked to the declaration of applicability were made, we have as an initial activity the "Evaluation and Treatment of Risk Analysis of the Faculty of Computer Science" subject investigated and prepared by: “Guerrero Bravo Gema Lilibeth, and Mera Quintero Evelyn Janira ". And the "Establishment of a Contingency and Continuity Plan for Computer Services provided by the FACCI" theme investigated and prepared by "Dominguez Alvia Victor Armando"

Most organizations begin to understand that the most important asset is the information they handle, all this can easily be lost in the face of external threats (natural disasters, equipment thefts) and internal threats (outdated so, viruses, theft, social engineering), thanks to the lack of measures and controls implemented.

Because in Facultad de Ciencias Informáticas, this has already happened, we opted for an Information Security Management System under the ISO / IEC 27001: 2005 standards to keep your information safe with your IT assets and get ISO certifications at the computer security level.

This study focuses on the preparation of the declaration of applicability, will allow the Academic Unit to adapt to the monitoring of the project to be implemented according to assets, risks, and threats, thus achieving non-obsolescence of the information security management system and the required certifications required and raised.

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN 13
INTRODUCCIÓN 14
CAPÍTULO II: PLANTEAMIENTO DE LA INVESTIGACIÓN 15
2.1 Justificación de la Investigación 16
2.2 Antecedentes del tema 18
2.3 Planteamiento del problema 21
2.4 Objetivos del Tema Investigado 23
2.4.1 Objetivo General 23
2.4.2 Objetivo Específicos 23
CAPÍTULO III: MARCO TEÓRICO 24
3.1 Antecedentes 25
3.1.2 Análisis de activos 29
3.1.3 Análisis de Riesgos 33
3.1.4 Gestión de Riesgos 38
3.1.5 Selección de Objetivos de Control y Controles 45
3.2 Marco teórico – conceptual 46
3.2.1 Localización 46
3.2.2 Instrumento de Investigación 48
3.2.3 Análisis de los datos 52
CAPÍTULO IV: METODOLOGÍA 57
4.1 Metodología de Investigación 58
4.1.1 Tipo de Investigación 59
4.1.2 Método de Investigación 60
4.1.3 Herramientas de Investigación 60
4.2 Metodología Operativa 61
CAPÍTULO V: RESULTADOS 63
5.1 Desarrollo y Análisis de Propuesta de Declaración de Aplicabilidad 64
5.1.1 PROPUESTA DE DECLARACION DE APLICABILIDAD 65
5.2 Resultados Esperados 78
CAPÍTULO VI: CONCLUSIONES 79
CONCLUSIONES 80
REFERENCIAS BIBLIOGRÁFICAS 81
1. Referencias Bibliográficas 82

Bibliografía 82
ANEXOS 84

Ilustración 1: Utilidad de un SGSI .....
Ilustración 2: Diagrama-Marco de trabajo para la gestión de riesgos .....
Ilustración 3: Elementos del Análisis de Riesgos Potenciales .....
Ilustración 4: Diagrama del Proceso del Análisis de Riesgo .....
Ilustración 5: Proceso de Elaboración de un Plan de Contingencia para la FACCI .....
Ilustración 6: Facultad de Ciencias Informáticas .....
Ilustración 7: Ubicación FACCI .....
Ilustración 8: Organigrama Funcional FACCI .....
Ilustración 9: Componentes de la Declaración de Aplicabilidad .....
Ilustración 10: Contexto de la organización frente al SGSI .....
Ilustración 114: SGSI en la organización .....
Ilustración 12: Modelo PDCA aplicado a los procesos de un SGSI .....
Ilustración 13: Representación del Modelo "Plan/Do/Check/Act" .....

Tabla 1: Listado de activos Margerit 29
Tabla 2: Identificación de activos informáticos FACCI 31
Tabla 3: Dimensiones de seguridad para la identificación y valoración de amenazas en MARGERIT 37
Tabla 4: Medidas Preventivas en Hardware FACCI 40
Tabla 5: Afectación de Incidentes en Software 41
Tabla 6: Medidas Preventivas en Virus Informático FACCI 42
Tabla 7: Medidas Preventivas en Controles de Acceso FACCI 42
Tabla 8: Medidas Preventivas en Pérdida o Robo de Información 43
Tabla 9: A.5 Políticas de Seguridad 85
Tabla 10: A.6 Organización de la Seguridad de la Información 87
Tabla 11: A.7 Gestión de Activos 88
Tabla 12: A.8 Seguridad de los Recursos Humanos 90
Tabla 13: A.9 Seguridad Física y Ambiental 92
Tabla 14: A.10 Gestión de las Comunicaciones y Operaciones 97
Tabla 15: A.11 Control de Acceso 100
Tabla 16 A.12: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información 103
Tabla 17 A.13: Gestión de Incidentes en la Seguridad de la Información 104
Tabla 18: A.14 Gestión de la Continuidad Comercial 105
Tabla 19: A.15 Cumplimiento 107
Tabla 20: Controles Seleccionados Para Elaboración de Declaración de Aplicabilidad a aplicar en el SGSI de la FACCI 51

CAPÍTULO I: INTRODUCCIÓN

INTRODUCCIÓN

Este trabajo de titulación se enfoca en el desarrollo de la declaración de aplicabilidad para el "Sistema de Gestión de Seguridad de la Información bajo las normas ISO/IEC 27001" a implementarse en la FACULTAD DE CIENCIAS INFORMÁTICAS, el cual fue aprobado en el 2018, esta declaración de aplicabilidad se puede definir como uno de los pasos más importantes en este y en cualquier proyecto de seguridad informática a implantarse en una empresa u organización, ya que se trata del documento principal que define cómo se implementará una gran parte del sistema de seguridad. Este documento enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001, un conjunto de 133 controles agrupados en 11 objetivos de control.

La presente investigación se encamina a la elaboración de la declaración de aplicabilidad y está organizada y estructurada por capítulos de la siguiente manera. En el Capítulo I se describe de forma introductoria una visión general del presente trabajo, en el Capítulo II se describe el Planteamiento de la Investigación detallando así la Justificación de la Investigación, los Antecedentes y estado actual del tema, Planteamiento del problema y los Objetivos del Trabajo.

Luego, en el Capítulo III tenemos el Fondo Conceptual del Proyecto, donde se proporciona toda la información que sustenta el tema investigado, desde sus antecedentes hasta el desarrollo del mismo. Continuando, en el Capítulo IV tendremos la Metodología, aquí se indica el tipo de metodología, los métodos y herramientas usadas para llevar a cabo la tarea desarrollada, seguido a esto en el Capítulo V nos encontramos con los Resultados, se indica el resultado de este proyecto de investigación en base al cumplimiento del objetivo general del mismo.

Finalmente en el Capítulo VI se presentan las Concusiones del trabajo de investigación y de todo el proceso que incluyo el mismo.

Complementamos el trabajo de investigación detallando las referencias bibliográficas, y los Anexos del tema investigado.

CAPÍTULO II: PLANTEAMIENTO DE LA INVESTIGACIÓN

2.1 Justificación de la Investigación

La información se ha denominado como uno de los activos más preciados en una organización, por lo tanto definir políticas de seguridad en el manejo de la información y en el uso de las herramientas tecnológicas es vital, porque permite evitar incidentes que afecten el buen desempeño de las actividades académicas.

Proteger la información en una Institución de Educación Superior consiste en trabajar de manera proactiva, y es necesario resguardar todos los medios de acceso a la institución debido a que las últimas décadas el uso del Internet y los sistemas de información son más común, lo que convierte a una institución, cualquiera que sea su razón social, en vulnerable frente a los atacantes.

La FACCI al ser una Unidad Académica de formación en TIC, tiene una fama muy significativa, pero lamentablemente no cuenta con un Sistema de Gestión de Seguridad Informática, razón por la cual se ha visto en la necesidad de diseñar e implementar dicho sistema.

Consciente de esto, el presente trabajo forma parte de uno de los Proyectos de Investigación de la Facultad de Ciencias Informáticas de la Universidad Laica Eloy Alfaro de Manabí, el cual se denomina "Sistema de Gestión de Seguridad de la Información bajo las normas ISO/IEC 27001" cuyo objetivo principal es diseñar e implementar un Sistema de Gestión de la Seguridad de la Información bajo la Norma ISO/IEC 27001 en la Facultad de Ciencias Informáticas, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque informático o desastre natural.

Teniendo en consideración que nuestra Facultad pertenece a una Institución de Educación Superior Pública y nos rigen las leyes del Estado Ecuatoriano, el 19 de septiembre de 2013 se emitió el Acuerdo Ministerial No. 166, que dispone que las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID), la implementación del "Esquema Gubernamental de Seguridad de la Información EGSI", Norma Técnica Ecuatoriana INEN ISO/IEC 27002. Por tal motivo las leyes ecuatorianas también nos facultan para el desarrollo de este proyecto ambicioso pero necesario.

El proyecto se conforma de fases consecutivas denominadas tareas de investigación cuyos resultados deben aportar al cumplimiento del objetivo del proyecto principal y como insumo para la siguiente fase o tarea de investigación.

Para asegurar esto, es necesario utilizar estándares internacionales que garanticen los procedimientos y controles a emplear, es aquí donde interviene la "Elaboración de declaración de Aplicabilidad" que busca garantizar la seguridad en los procesos universitarios.

En Ecuador las Universidades están siendo evaluadas por parte de organismos superiores en todos sus procesos, y por la tanto deben garantizar seguridad en los mismos. Por lo cual la FACCI busca un mejoramiento continuo prestando un mejor servicio a la comunidad universitaria, adoptando herramientas de optimización, basadas en nuevas tecnologías y estableciendo políticas de seguridad de la información a fin de ir innovando en la calidad de la educación con la colaboración de las autoridades, docentes, estudiantes y personal administrativo.

2.2 Antecedentes del tema

La propuesta central para el desarrollo del proyecto de "SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO NORMAS ISO/IEC 27001" fue presentada al Departamento de Investigación de la Universidad con una fecha prevista de iniciación (Diciembre/2018). Sin embargo se presentaron avances significativos del mismo proyecto, tales como "SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001", "EVALUACIÓN Y TRATAMIENTO DEL RIESGO INFORMÁTICO DE LA FACULTAD DE CIENCIAS INFORMÁTICAS", e "INSTAURACIÓN DE UN PLAN DE CONTINGENCIA Y CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS QUE BRINDA LA FACCI", todos estos temas se encuentran ligados y dependientes uno de otros en el orden nombrado.

El desarrollo del sistema de gestión de seguridad de la información (SGSI) en la FACULTAD DE CIENCIAS INFORMÁTICAS, se enmarca, en la norma de seguridad de sistemas de información ISO/IEC 27001 en su versión 2005 que especifica los requisitos necesarios para establecer, implantar, mantener, y mejorar un SGSI.

Haremos énfasis en el uso de las norma ISO/IEC 27001 ya que es un estándar para la seguridad de la información (Information Tecnology-Security tecniques-Information security-management systems-Requirements) aprobado y publicado como estándar internacional el 15 octubre del 2005 por ISO (International Organization for Standardization) y por la comisión IEC (International Electrotechncal Commission). El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa.

La norma ISO 27001, está muy enfocada en la parte informática de la empresa, se encuentra muy ligada y tiene puntos en común con otras dos normas ISO: la ISO 22301 de continuidad del negocio y la ISO/IEC 20000, de gestión de servicios TI (Tecnología de la Información).

En su versión 2005, es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, y se encuentra desarrollada en base a la norma británica BS 7799-2:2002, creada por la entidad de normalización británica, la British Standards Institution (BSI), por lo cual es internacionalmente reconocida y usada para certificación.

Hoy en día nadie pone en duda la fortaleza de la norma ISO 27001 en materia de gestión de Seguridad de la Información. La norma ha ido ganando terreno cada vez más importante en el ajetreado mundo de la certificación. Y lo ha hecho de la mano de su guía de buenas prácticas ISO 27002, que sin ser certificable, es un compendio de recomendaciones para aquellos que se enfrentan a la ingente y exigente tarea de implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

No obstante, ISO 27001 está todavía muy lejos de alcanzar el grado de implantación a nivel mundial con respecto a otros estándares de gestión, como por ejemplo, el ampliamente conocido estándar que establece los requisitos de un sistema de Gestión de la Calidad: ISO 9001.

Viendo esa evolución que ha tenido ISO 9001 en todo el mundo desde que fuera publicada en 1987, y teniendo en cuenta que la sociedad en la que vivimos y las empresas que operan en el mercado dependen ya de una manera absoluta de la información, parece lógico pensar que ISO 27001 va a ir ganando peso progresivamente tanto en organizaciones de carácter público como de carácter privado.

Por ejemplo, en Perú la ISO/IEC 27002:2005 (la guía de buenas prácticas y no el estándar certificable) es de uso obligatorio en todas las instituciones públicas desde el año 2004, fijando así un estándar para las operaciones de la Administración, cuyo cumplimiento es supervisado por la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI.

Sin salir de Sudamérica, en Colombia la norma ISO 27001 es de cumplimiento obligatorio para algunos sectores. Es el caso de los operadores de información, que de conformidad con el Decreto 1931 de 2006 de aquél país, se hallan sujetos al cumplimiento del estándar.

Pero, sin duda, será el sector privado el que con mayor empuje pondrá a ISO 27001 en el lugar que le corresponde, debido al importante papel que puede desempeñar un SGSI en el ámbito del gobierno corporativo de las empresas en cuanto a gestión de riesgos se refiere.

La metodología de un SGSI y obviamente de éste, según ISO 27001 tiene una cadena de actuaciones basadas en PDCA (Plan, Do, Check, Act), Iniciando con Plan (Planificación), tenemos exactamente 7 actuaciones (tareas-requerimientos) que se deben. Entre estos requerimientos tenemos: Definición de política y objetivos, Determinación del Alcance,

Análisis de activos, Análisis de riesgos, Gestión de riesgos, Selección de objetivos de control y controles, y finalmente el último requerimiento: Declaración de Aplicabilidad.

La declaración de aplicabilidad es uno de los documentos principales e indispensables en todo Sistema de Gestión de Seguridad implementado en cualquier empresa u organización. Consiste en un documento que relaciona los controles que se aplican en el sistema de gestión, en su versión 2005 establece 133 puntos de control, y 11 secciones.

Una organización debe seleccionar aquellos controles que debe implantar y mantener en su sistema. El resultado de la elección de los controles forma parte del Plan de Tratamiento de riesgos, de modo que éste tiene como salida la declaración de aplicabilidad.

Esta declaración es uno de los documentos que tienen que ser redactados por exigencia de la norma ISO 27001, sin embargo en la mayoría de los casos se omite la elaboración de la misma gracias a la inopia o descuido de las organizaciones y de las personas a cargo de estos procedimientos, lo que retrasa los procesos de seguridad informáticos y en varios casos afecta a todo el SGSI hasta el punto de volver vulnerable al mismo, junto a la empresa u organización, por tanto en este trabajo de titulación enfatizaremos la importancia de la elaboración de la declaración de aplicabilidad en cualquier SGSI y en el SGSI FACCI del que somos parte.

2.3 Planteamiento del problema

La mayoría de las organizaciones hoy en día, sin importar su tipo o actividad comercial, están vinculadas de alguna manera con las Tecnologías de Información y Comunicación (TIC), y poseen una infraestructura que las soporta, en donde sostienen que la información es el activo de mayor valor que las sustentan. Sin embargo, los gerentes cuando elaboran planes estratégicos y plantean objetivos organizacionales usualmente no están conscientes que el ciberespacio está lleno de riesgos y amenazas, así como también los factores naturales que se puedan presentar; y esto conlleva a que no incluyan un presupuesto adecuado para implementar seguridad de la información en la empresa.

La Unidad Académica (FACCI) no tiene diseñado e implementado un Sistema de Gestión de la Seguridad de la Información, se expone a riesgos continuos que pueden incidir en pérdida, alteración o lectura no permitida de información, ocasionando retrasos en el normal funcionamiento de los procesos.

En la seguridad de la información existen las amenazas de carácter técnico, pero también influyen las amenazas de tipo humano, ya que muchos equipos informáticos que son conectados a la red son de uso personal y no institucional, los empleados no protegen o mantienen la confidencialidad de sus credenciales de acceso al dominio universitario, muchas veces utilizan sus correos electrónicos personales para la comunicación interinstitucional y se usan múltiples usuarios con múltiples contraseñas para acceder a diferentes servicios, ocasionando el frecuente olvido de sus datos de acceso.

Esto sin mencionar los riesgos en los equipos informáticos producidos por desastres naturales, justo como ocurrió en el terremoto del 16 de Abril en la ciudad de Manta, hubo pérdida de equipos informáticos, infraestructura, e información, en grandes masas.

De seguir con esta falta de seguridad en el manejo de la información, la Facultad continuará con problemas en los servicios en cualquier momento, no prestará un servicio óptimo a sus estudiantes, docentes, empleados y comunidad en general, se ralentizarán sus procesos institucionales ocasionando una mala imagen corporativa, deserción estudiantil y administrativa y robo o pérdida de información sensitiva, todo esto sumará un gasto financiero

implementando controles correctivos más que preventivos, lo cual puede incidir en graves pérdidas económicas y de información.

La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial y académica necesarios para lograr los objetivos de la organización y asegurar beneficios deseados.

Por lo antes mencionado, se debe contar con la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El siguiente gráfico nos da a conocer la utilidad de un Sistema de Gestión de seguridad Informática.

Ilustración 1: Utilidad de un SGSI
Fuente: *www.iso27000.es*
Obtenido de: *Proyecto de SGSI FACCI*

Por esos y tantos motivos más, el propósito de este proyecto es elaborar la declaración de aplicabilidad que se puede definir como uno de los pasos más importantes en este y en cualquier SGSI a implantarse en una empresa u organización, ya que se trata del documento que define cómo se implementará una gran parte del sistema se seguridad. Este documento enlista los controles de seguridad aplicables y no aplicables establecidos en el Anexo A del estándar ISO/IEC 27001:2005.

2.4 Objetivos del Tema Investigado

2.4.1 Objetivo General

Elaborar la propuesta de Declaración de Aplicabilidad bajo las normas ISO/IEC 27001: 2005 para el Sistema de Gestión de Seguridad de la Información en la Facultad de Ciencias Informáticas.

2.4.2 Objetivo Específicos

1. Identificar el estado actual de los trabajos previos realizados con el Inventario de activos de la FACCI y análisis de riesgos de los mismos activos.
2. Seleccionar el modelo de declaración de aplicabilidad a usar según la Normas ISO/IEC 27001:2005.
3. Detallar los motivos o razón para la selección por los que cada Control del Anexo A de la norma ISO 27001 se ha incluido en la Declaración e incluir de forma descriptica el o los documentos que se tomarán como evidencia a razón de cada control seleccionado a aplicar.
4. Presentar el modelo de declaración de aplicabilidad propuesto a implementarse en el SGSI en la FACULTAD.

CAPÍTULO III: MARCO TEÓRICO

3.1 Antecedentes

Entonces tenemos que el tema específico a investigar y cumplir es la "ELABORACIÓN DE LA DECLARACIÓN DE APLICABILIDAD PARA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS BAJO LAS NORMAS ISO/IEC 27001: 2005", pero para lograr su objetivo fue necesario elaborar actividades previas.

A continuación se muestra una cadena de acciones que se deben realizar en un SGSI desarrollado bajo las normas ISO/IEC 27001, el cual adopta el modelo: Plan Do Check Act, esta cadena de acciones es una manera de adentrarse al modelo PDCA para poder lograr el objetivo del SGSI de forma sistemática.

Tal como muestra la cadena de acciones en el ítem de "Plan" (color amarillo). Tenemos que las actividades previas a realizarse fueron: Definición de políticas, Determinación del Alcance, Análisis de activos y Análisis de riesgos (estos dos temas se pueden desarrollar como una sola tarea o como dos), Gestión de Riesgos, Selección de Objetivos de Control y Controles, y finalmente nuestra tarea a desarrollar "Declaración de Aplicabilidad"

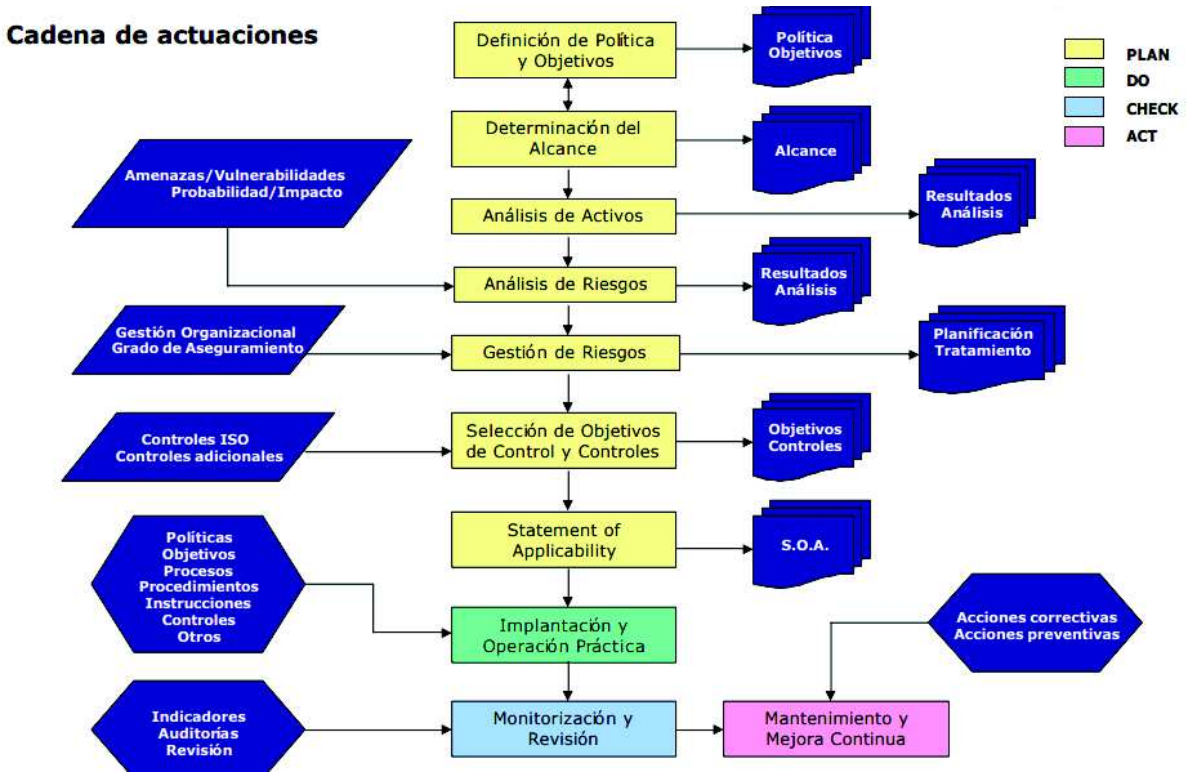

Ilustración 2: Metodología de un SGSI según ISO 27001

Fuente: *Zuccardi, G., & Gutiérrez, J. D. (2006). ISO 27001:2005. Obtenido de: pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001.doc*

3.1.1 Definición de política y objetivos

El diseño de políticas y objetivos, viene dado por el Objetivo General y Específicos del Proyecto de Investigación (**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO NORMAS ISO/IEC 27001**), los cuales se detallan a continuación.

Objetivo General

Diseñar e Implementar un Sistema de Gestión de la Seguridad de la Información bajo la Norma ISO/IEC 27001:2005 en la Facultad de Ciencias Informáticas, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque informático o desastre natural.

Objetivos Específicos

- Identificar riesgos de seguridad en el área informática a los que está expuesta la Facultad de Ciencias Informática.
- Definir las medidas de seguridad más apropiadas a aplicarse en este caso.
- Definir las políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información.
- Plantear un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la norma ISO/IEC 27001:2005 para la Facultad de Ciencias Informáticas que permita obtener confidencialidad, integridad y disponibilidad de la información.
- Implementar un SGSI para la Facultad de Ciencias Informáticas que permita proteger los recursos informáticos más valiosos; cómo la información el hardware y el software.

Determinación del alcance

De igual forma la Determinación del Alcance, viene dada, por el mismo alcance que tiene el proyecto de Investigación (**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO NORMAS ISO/IEC 27001)**

Este proyecto se va a realizar en la FACULTAD DE CIENCIAS INFORMÁTICAS (FACCI) de la UNIVERSIDAD LAICA ELOY ALFARO DE MANBÍ (ULEAM).

La Facultad de Ciencias Informáticas, a través del diseño e implementación de un SGSI busca minimizar los riesgos a los que se encuentra expuesta la información de la Facultad, proceso que se documenta paso a paso.

Para el desarrollo de la primera etapa se aplica la metodología Margerit con la cual se realiza el análisis de riesgos que es una de las principales actividades a cumplir ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales estamos expuestos identificando amenazas y vulnerabilidades.

Para el análisis de riesgos se realiza un inventario actualizado de activos, una valoración cualitativa de dichos activos, identificación de amenazas, definición de salvaguardas. También se atacará diversos entornos con la intención de descubrir fallos, vulnerabilidades, etc.

Una vez identificado claramente los activos que se encuentra en un riesgo inminente y que generaría mayor impacto en caso de que sufrieran un ataque, o con una alta probabilidad de que una amenaza informática o natural se materializara, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles considerados en la Norma ISO/IEC 27001:2005, de este proceso puede nacer la creación de planes integrales de prevención y mitigación de riesgo, como un plan de continuidad de los servicios y un plan de contingencia los cuales ayudaran a volver a la operatividad de las labores académicas si se concretara una amenaza natural.

3.1.2 Análisis de activos

El Análisis de Activos se llevó a cabo en el Trabajo de Titulación denominado "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" elaborado por: *Acosta Alvarado Nexar Jesús, y Carrillo Morán Fátima Guadalupe,* estudiantes graduados en la FACULTAD DE CIENCIAS INFORMATICAS.

Los estudiantes solicitaron a decanato la lista de todos los activos con los que cuenta la Facultad, luego realizaron un análisis de dichos activos, y, en base a eso, procedieron a desarrollar su Trabajo de Titulación.

A continuación, detallamos los puntos más importantes en cuanto a Análisis de Activos se refiere según el trabajo de titulación mencionado.

Activos: Los activos existentes son los bienes tanto tangibles como intangibles que son de importancia en la organización para lograr un mejor desempeño. Entre los activos se encuentran: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

En la siguiente tabla está el listado de los activos que se encuentra en el libro de MAGERIT:

[D]	Datos / Información
[K]	Claves Criptográficas
[S]	Servicios
[SW]	Aplicaciones
[HW]	Hardware
[COM]	Redes de comunicaciones
[Media]	Soporte de Información
[AUX]	Equipamiento Auxiliar
[L]	Instalaciones
[P]	Personal

Tabla 1: Listado de activos Margerit
Fuente: *Libro II Margerit v3 1*

Valoración de activos

Para determinar el valor de un activo se debe conocer la estimación del coste que causa la materialización de la amenaza sobre dicho activo.

Para realizar la valoración se debe considerar el daño total cuando la amenaza perjudica al activo y lo destroza completamente en cada dimensión, la destrucción parcial del valor se llama degradación, y proporciona estimar el impacto de la amenaza. La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles).

Identificación de los activos

Para llevar a cabo la identificación de los activos para el desarrollo del software, se solicitó el inventario de activos a la decana de la FACCI.

En la siguiente tabla se muestran la clasificación de los activos informáticos de la Facultad de Ciencias Informáticas.

ACTIVOS INFORMÁTICOS	
[DI] Datos/Información	Inventario general de los bienes
[S] Servicios	Red Intranet/Extranet
[SW] Software-Aplicaciones Informáticas	Ofimática
	Antivirus
	Sistema Operativa
	Otros tipos de software
[HW] Hardware-Equipamiento Informático	Ordenadores (Portátil/Escritorio)
	Impresoras
	Switch
	Router
	WAP (Punto de acceso inalámbrico)
[COM] Redes de Comunicaciones	Red WI-FI
	Red LAN
	Internet
[Media] Soportes de Información	CD
	Memorias USB
	Disco Duro Externo
[AUX] Equipamiento Auxiliar	Cámaras de seguridad
	Aires Acondicionados
[INST] Instalaciones	Instalaciones eléctricas
[PSL] Personal	Personal Administrativo
	Docentes
	Directivos

Tabla 2: Identificación de activos informáticos FACCI

Fuente: *"Propuesta de un Sistema de Gestión de Riesgos mediante la metodología Margerit aplicado a los activos informáticos. Caso de Aplicación FACCI"*

Análisis de los resultados

Análisis de resultados de encuesta a toda la comunidad de la FACCI

Al finalizar las estadísticas y análisis de cada una de las preguntas de la encuesta realizada dirigida a Docentes, estudiantes y personal administrativo y de servicio, se llegó a lo siguiente:

- Existe desconocimiento del plan de seguridad informática en los laboratorios de la FACCI, lo que perjudica al momento de ocurrir pérdidas de activos.
- La mano de obra en los laboratorios es especializada, pero carece de planificación en sus procesos.
- La FACCI carece de elementos de seguridad informática, según la encuesta y entrevista realizada al Jefe de laboratorios.
- Se conoce la obligatoriedad de las normas (SNAP).

Elaboración: Nexar, A., & Fátima, C. (2018). 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. Manta.

3.1.3 Análisis de Riesgos

El Análisis de Riesgos se detalla de forma explícita el Trabajo de Titulación denominado "EVALUACIÓN Y TRATAMIENTO DEL RIESGO INFORMÁTICO DE LA FACULTAD DE CIENCIAS INFORMÁTICAS" elaborado por: *Guerrero Bravo Gema Lilibeth, y Mera Quintero Evelin Janira,* estudiantes graduadas en la FACULTAD DE CIENCIAS INFORMATICAS.

A continuación detallaremos los puntos más importantes correspondientes al Análisis de Riesgos, según el trabajo realizado por: *Guerrero Bravo Gema Lilibeth, y Mera Quintero Evelin Janira.*

Metodología Margerit

Para llevar a cabo el análisis de riesgo, el equipo a cargo de este tema usó la metodología MARGERIT, una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados.

En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (Magerit-v3)

Pasos en la metodología

Ilustración 2: Diagrama-Marco de trabajo para la gestión de riesgos
Fuente: *(Margerit-v3.)*

Según (Magerit-v3, 2012) en su libro indica que MAGERIT sigue los siguientes pasos pautados:

- Determinar los activos relevantes para la Institución, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Los pasos indicados se detallan en la siguiente gráfica:

Ilustración 3: Elementos del Análisis de Riesgos Potenciales
Fuente: *(Margerit-v3, 2012))*

Análisis

En esta fase se identificarán los activos de la institución, identificando las relaciones que se establecen entre activos. De esta forma se obtiene el "catálogo de activos" que representan las distintas dependencias y relaciones entre activos, es decir, todos aquellos elementos que están "encadenados entre sí" en términos de seguridad. También se identifica el conjunto de amenazas, estableciendo para cada activo, cuál es la vulnerabilidad que presenta frente a dicha amenaza. Además, se cuantifica el impacto, para el caso en el que la amenaza se materializase. Analizar información generada en estudios de riesgos anteriores que permitan ajustar de forma más exacta las diferentes dependencias entre activos. Con toda esta información, tendremos una estimación del costo que podría producir la materialización de una amenaza sobre un activo. Teniendo en cuenta las relaciones funcionales y de dependencias entre activos, se hallan los valores de riesgo.

Tratamiento del Riesgo

El tratamiento de los riesgos es la fase del proceso de gestión de riesgos, que tiene como objetivo de tratar los riesgos disminuyendo su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable.

Al tratar el riesgo como esencial dentro del proceso se toman medidas para reducirlo, y también para establecer la forma de soportar las pérdidas que genera.

Gestión de Riesgos

En esta fase, se procede a la interpretación del riesgo. Una vez identificados los puntos débiles, debe seleccionarse el conjunto de funciones de salvaguarda que podrían ser usados para disminuir los niveles de riesgo a los valores deseados. Para ello, deberán especificarse los mecanismos de salvaguarda que se encuentran implantados hasta ese momento y cuál es su grado de cumplimiento. Este proceso es ayudado por la simulación.

Se van probando selecciones de diferentes mecanismos de salvaguarda y se estudia en qué medida reducen los niveles de riesgo a los márgenes deseados.

Selección de mecanismos de salvaguarda

Una vez obtenidos estos resultados, se establecen de nuevo reuniones con el equipo de la institución. De esta forma, se analizan los resultados obtenidos y se establece un plan de implantación de mecanismos.

Ilustración 4: Diagrama del Proceso del Análisis de Riesgo
Fuente: *(Margerit-v3, 2012)*

Características de Margerit

Clasifica el estado de seguridad de cada activo o grupo de activos de la siguiente manera según su estado de Autenticación, Confidencialidad, Integridad y Disponibilidad.

Dimensiones de Seguridad

DIMENSIÓN DE SEGURIDAD	NOMENCLATURA	DEFINICIÓN
Disponibilidad	D	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
Integridad	I	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004].
Confidencialidad	C	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007].
Autenticidad	A	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008].
Trazabilidad	T	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008].

Tabla 3: Dimensiones de seguridad para la identificación y valoración de amenazas en MARGERIT
Fuente: *(Vásquez, Aplicación de la metodología MARGERIT para el análisis y Gestión de Riesgos de la Seguridad de la Información, 2013)*

Análisis de Riesgo y Tratamiento de Riesgo

El cual pretende calificar los riesgos encontrados cuantificando sus consecuencias o determinando su importancia relativa, además permite controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación de activos, los controles, sus amenazas estimando el impacto y el riesgo al que puede estar expuestos cada uno de los activos.

3.1.4 Gestión de Riesgos

La Gestión de Riesgos, se llevó a cabo en el Trabajo de Titulación denominado INSTAURACIÓN DE UN PLAN DE CONTINGENCIA Y CONTINUIDAD DE LOS SERVICIOS INFORMÁTICOS QUE BRINDA LA FACCI" elaborado por: *Domínguez Alvia Víctor Armando,* estudiante graduado en la FACULTAD DE CIENCIAS INFORMATICAS.

El estudiante hizo uso de los trabajos de titulación realizados anteriormente, trabajos como el análisis de activos y análisis de riesgos, en base a eso, procedió a desarrollar su Trabajo de Titulación.

A continuación, detallamos los puntos más importantes, en cuanto a "Gestión de Riesgos" se refiere, según el trabajo de titulación elaborador por: *Domínguez Alvia Víctor Armando.*

Propuesta

Una vez obtenido el Análisis de Riesgo se empieza con la planificación del plan de contingencia cuya propuesta y pasos de elaboración la encontramos en la siguiente imagen.

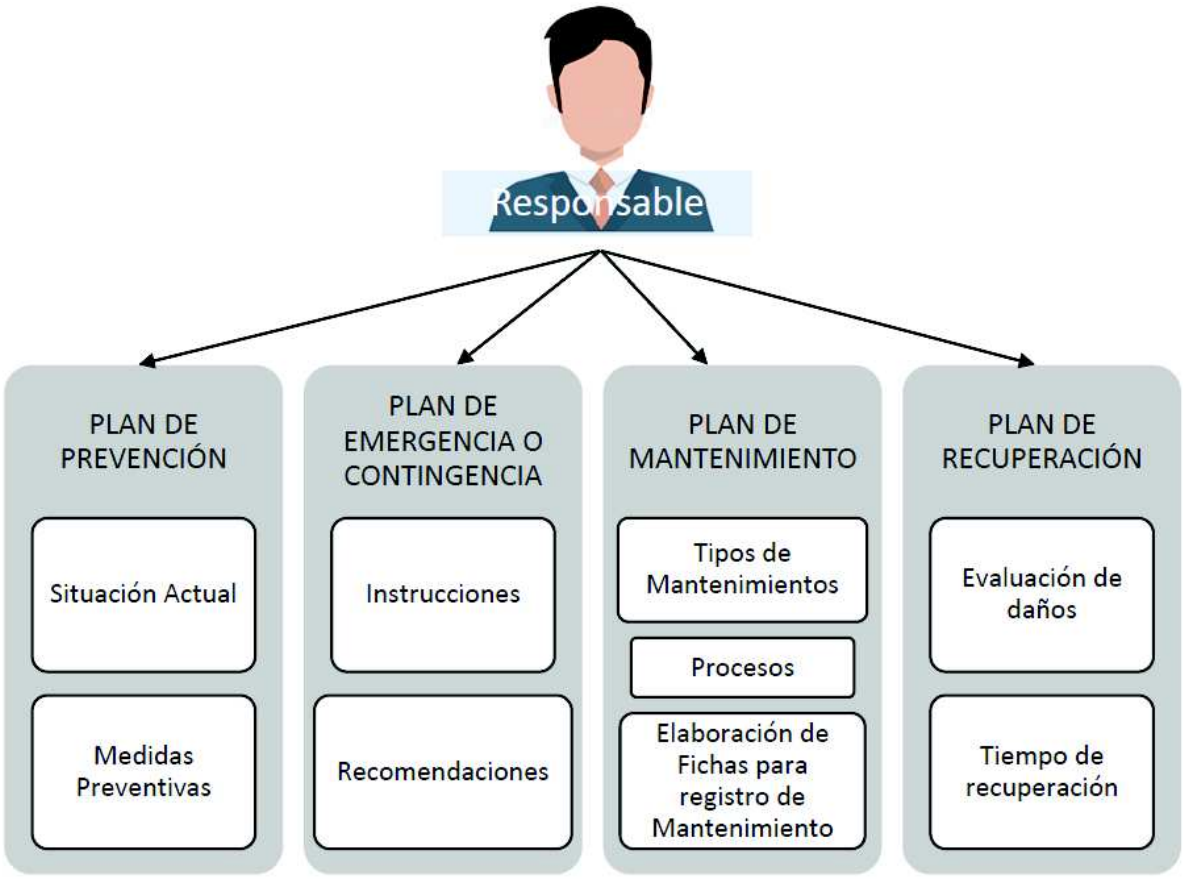

Ilustración 5: Proceso de Elaboración de un Plan de Contingencia para la FACCI
Fuente: *"Instauración de un Plan de Contingencia y Continuidad de los Servicios informáticos que brinda la FACCI" Domínguez 2018*

Plan de Respaldo o Prevención

Consiste en la verificación del estado actual de los recursos informáticos de la FACCI, e identificar el estado de vulnerabilidades, realizado anteriormente en el análisis de riesgo, y dar a conocer medidas preventivas y respaldos y que ayuden a la solución de estos riesgos.

Los mayores riesgos tomados en cuenta son:

- Incendio o Fuego.
- Fenómenos naturales.
- Inundaciones.
- Robo o pérdida de equipos informáticos.
- Falla en los equipos.
- Falta de respaldos y perdida de información.
- Daños provocados por virus informático.
- Accesos no autorizados.

MEDIDAS PREVENTIVAS EN HARDWARE FACCI	
SITUACIÓN ACTUAL	**MEDIDA PREVENTIVA**
Cuenta con la disponibilidad de equipos. Switch, Router y puntos de red.	Planificar mantenimientos preventivos y correctivos. Comunicarse con proveedores en caso de tener garantía en los equipos.
Uso de Microtik como servidor de internet. Ancho de banda de 5 Mb. Mantenimiento realizado por UCCI.	Aumentar acho de banda. Tener acceso y control del Microtik, que por el momento es manejado y controlado por UCCI.
Poco registro de activos que cuentan con garantía disponible.	Actualizar inventario de activos e identificar qué equipo cuenta con garantía vigente para llevar control del mantenimiento con los proveedores.
Propensos a robos.	Inspeccionar el laboratorio por parte del responsable que todo esté en orden. Cámaras de seguridad.
Reglas o indicaciones no visibles al ingresar al laboratorio.	Realizar indicaciones tanto para usuarios y técnicos de los laboratorios.
Cuenta con sistema de climatización.	Realizar mantenimientos preventivos y correctivos.
Daños por condiciones eléctricas regulares.	Coordinar mantenimientos con el departamento técnico de la ULEAM. Realizar inventario de componentes eléctricos. Implementar un sistema de alimentación interrumpida (SAI). Tener a disposición piezas de respaldo
Falta de lista de personas que ingresan al laboratorio en horario libre, con información de nombre, curso, hora, y unidad que ocupa el estudiante.	Control de ingreso de personas a los laboratorios (Bitácora).

Tabla 4: Medidas Preventivas en Hardware FACCI
Fuente: *"Instauración de un Plan de Contingencia y Continuidad de los Servicios informáticos que brinda la FACCI" Domínguez 2018*

Incidentes en Unidades Lógicas

Actualmente los equipos de la FACCI no dispone con un sistema operativo determinado a su uso, con la llegada de nuevos equipos la facultad ya dispone de laboratorios con Sistema Operativo Ubuntu, los cuales se tendrán que coordinar para el acceso a materias que utilizan este tipo de sistema, a más de eso también depende mucho, del uso de programas y características del computador.

Las afectaciones en software tienen graves consecuencias por los peligros que conllevan. Entre las cuales es provocada por: virus informático, pérdida o robo de información y claves o controles de acceso. A continuación mostramos la tabla de afectación que puede traer inconvenientes a la FACCI y luego mediante la situación actual plantea sugerencias o medidas preventivas que ayuden a solucionar los incidentes.

Afectación a la FACCI	
Grado de Negatividad	Grave
Frecuencia del Evento	Incierto
Grado de Impacto	Alto

Tabla 5: Afectación de Incidentes en Software
Fuente: *"Instauración de un Plan de Contingencia y Continuidad de los Servicios informáticos que brinda la FACCI" Domínguez 2018*

MEDIDAS PREVENTIVAS EN VIRUS INFORMATICO: FACCI	
SITUACIÓN ACTUAL	**ACCIÓN A REALIZAR**
Antivirus instalado y afectaciones en su sistema, utilizan freeze o congelador.	Realizar mantenimientos preventivos y correctivos de software.
Carecen de licencias en antivirus, SO, base de datos o leguajes de programación.	Analizar la colocación de licencias.
Reglas o indicaciones no visibles y dirigidas al uso de los equipos a nivel de software preferencia laboratorios.	Realizar indicaciones tanto para usuarios y técnicos de los laboratorios.

Manipulación de programas y sitios web infectados de virus.	Prevenir mediante el llamado de atención al estudiante.

Tabla 6: Medidas Preventivas en Virus Informático FACCI
Fuente: *"Instauración de un Plan de Contingencia y Continuidad de los Servicios informáticos que brinda la FACCI" Domínguez 2018*

MEDIDAS PREVENTIVAS EN CONTROLES DE ACCESO: FACCI	
SITUACIÓN ACTUAL	**ACCIÓN A REALIZAR**
Laboratorios con libre acceso.	Asegurar que estén realizando trabajos acorde a la materia impartida por el profesor caso contrario llamar la atención al estudiante.
Cuenta con controles de acceso solo en áreas críticas donde ningún estudiante o persona no autorizada puede manipular ningún activo.	En caso de que alguna persona ajena a la institución (pasantes) o estudiante este ayudando al profesor en alguna labor, verificar que se encuentre realizando su trabajo.
Ingreso a sitios web donde colocan usuario y contraseña.	Comprobar el cierre de sesión ya que sus datos e integridad pueden estar perjudicados ante una mala acción realizada por el hombre.

Tabla 7: Medidas Preventivas en Controles de Acceso FACCI
Fuente: *"Instauración de un Plan de Contingencia y Continuidad de los Servicios informáticos que brinda la FACCI" Domínguez 2018*

MEDIDAS PREVENTIVAS EN PÉRDIDA O ROBO DE INFORMACIÓN: FACCI	
SITUACIÓN ACTUAL	**ACCIÓN A REALIZAR**
Cuenta con respaldo Interno.	La información suelen estar respaldadas mediante dispositivo externos (USB, Disco Duro, o cuentas en la nube gratuitas de los usuarios.
Falta de respaldo de información masivo.	Implementar un sistema de respaldo de información (Nube, servidores, etc.) en áreas críticas ante un desastre mayor.
Tiene una brecha comunicación y alojamiento de poca información en la nube con UCCI.	Implementar un servicio en la nube propio de la facultad y controlada por el DTPO TI de la FACCI.

Tabla 8: Medidas Preventivas en Pérdida o Robo de Información
Fuente: *"Instauración de un Plan de Contingencia y Continuidad de los Servicios informáticos que brinda la FACCI" Domínguez 2018*

Plan de Recuperación

Todas las actividades de planeamiento, preparación, entrenamiento que se ejecutan deberán tener un seguimiento y monitoreo de aquellas actividades que se realizan, así como también trabajos y mantenimientos realizados con una respectiva documentación de acuerdo a la actividad realizada.

Por Cortes Eléctricos: En caso de cortes eléctricos la recuperación durará cuando regrese la energía eléctrica.

Por Daños de Equipos: Los daños de equipos se los recupera de forma inmediata ante un incidente leve, en caso de un daño más severo en donde no se disponga de piezas de respaldo máximo 2 días para su disposición.

Por Robo de Equipos: Revisión inmediata de las cámaras de seguridad, en busca de culpables, en caso de no encontrar comprobar garantía de equipos, y en caso de robo de activo de algún docente trabajar en la personal hasta que el Departamento TI asigne una nueva. Esto en gran parte dependerá de los recursos económicos que la FACCI dispone, pero la recuperación del equipo de trabajo debe ser lo más rápido posible.

Evaluación de Daños: Se da en un incidente severo como desastres naturales e incendio, e inmediatamente después que la contingencia ha concluido, se evaluará la magnitud de los daños producidos, estableciendo que sistemas están afectados, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc. Esto lo podemos evaluar mediante el plan de mantenimiento, además cuenta con la información del inventario y a la vez podemos solucionar problemas leves y poner en funcionamiento algunos equipos y luego se podrá calcular que porcentaje de equipos han sido afectados.

Adicionalmente se lanzará un pre-aviso a la institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha institución.

3.1.5 Selección de Objetivos de Control y Controles

Los objetivos de control y los controles se muestran enumeraros en ANEXOS, estos se derivan directamente de, y se alinean con, aquellos enumerados en BS ISO/IEC 17799:2005 (cláusulas del 5 al 15). Las listas de dichas tablas no son exhaustivas y una organización podría considerar que son necesarios objetivos de control y controles adicionales.

Los objetivos de control y los controles de las tablas deben seleccionarse como parte del proceso de SGSI especificado según los análisis e investigaciones previas realizadas en la Facultad.

El BS ISO/IEC 17799:2005 proporciona consulta y lineamientos para la implementación de las mejores prácticas en soporte de los controles especificados en las tabla (de A.5 al A.15)

3.2 Marco teórico – conceptual

3.2.1 Localización

El proyecto de investigación, **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO NORMAS ISO/IEC 27001**, se llevará a cabo en la FACULTAD DE CIENCIAS INFORMÁTICAS de la UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, por lo tanto, todos los requisitos, tareas previas, y trabajos de titulación vinculados al mismo proyecto, serán llevados a cabo en esta Unidad Académica.

La Elaboración de la Declaración de Aplicabilidad se realizará en la misma Unidad Académica.

Descripción de la empresa

La Facultad de Ciencias Informáticas FACCI, es una Unidad Académica de Educación 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: Facultad de Ciencias Informáticas
Fuente: *www.uleam.edu.ec*

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.

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.

Ubicación

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

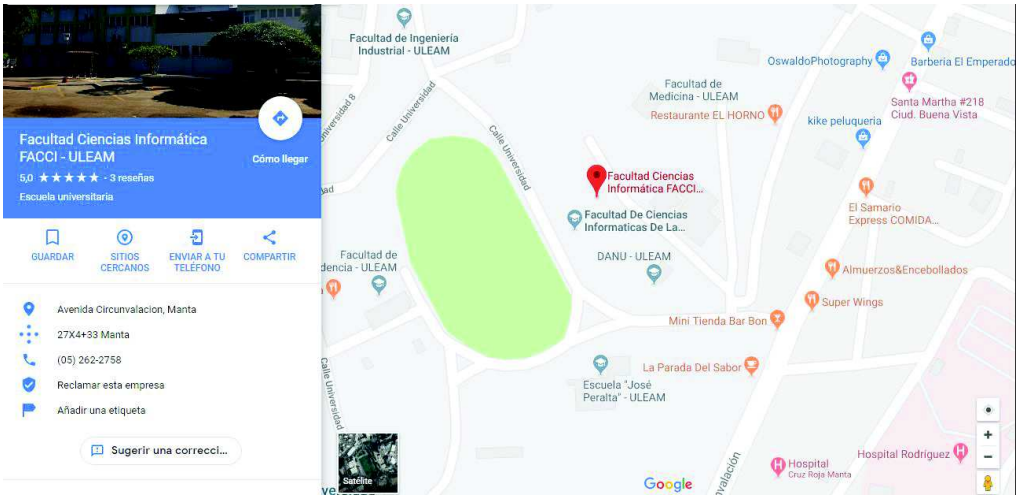

Ilustración 7: Ubicación FACCI
Fuente: *www.googlemaps.com*

Estructura Organizacional

- Decano: Lic. Dolores Muñoz.
- Coordinador de Carrera: Ing. Winter Molina.
- Coordinador de Académico: Ing. Fabricio Rivadeneira.
- D. Técnico: Ing. Gilbert Loor.

Organigrama Organizacional

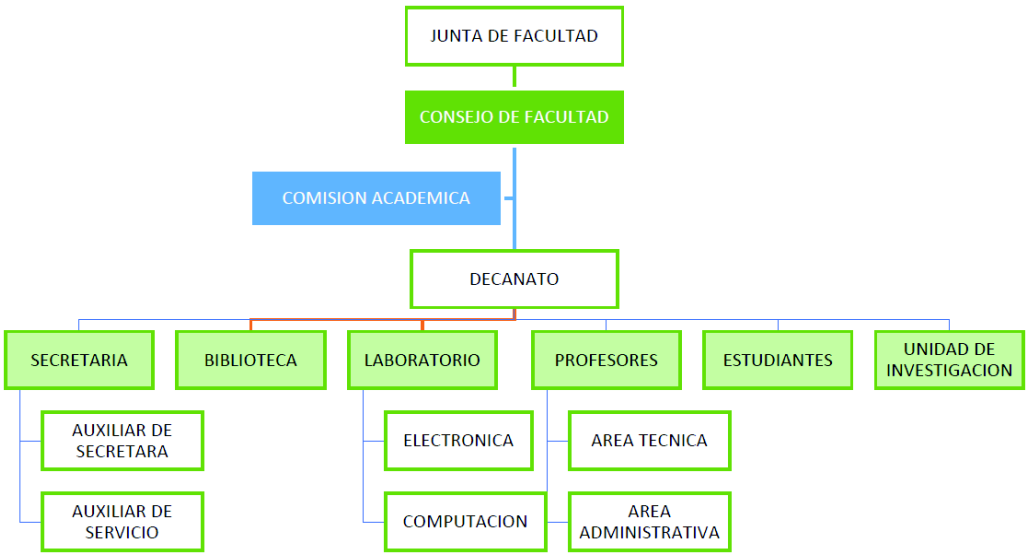

Ilustración 8: Organigrama Funcional FACCI
Fuente: *http://carreras.uleam.edu.ec/facci/datos-generales/estructura-organica/*

3.2.2 Instrumento de Investigación

Haremos uso de instrumentos de investigación como los trabajos de titulación enfocados en análisis de activos, análisis de riesgos, gestión de riesgos, entre otros.

Sin embargo el documento o instrumento principal para iniciar el proceso de investigación y elaboración de la Declaración de Aplicabilidad es: ***El ISO/IEC 27001 en su versión 2005*** con sus respectivas normas, enfatizando a las normas incluidas en el Anexo A de la misma.

En el Anexo A encontraremos ***Los Objetivos de Control y los Controles*** descritos en una tabla en el punto 6.1.6 de esta investigación. Si bien es cierto esa tabla detalla un conjunto de 133 controles agrupados en 11 objetivos de control, de los cuales seleccionaremos solo los controles aplicados en nuestro SGSI a implementarse en la Facultad.

Controles Seleccionados:

La Declaración de Aplicabilidad enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001, un conjunto de 133 controles agrupados en 11 objetivos de control.

Sin embargo, de los de 133 controles agrupados en 11 objetivos de control, solo se usan los que la empresa u organización considere aplicables dentro del SGSI, y si creen recomendable crear o seleccionar nuevos controles que sean necesarios aplicar, se hace, sustentado su motivo.

A continuación se muestran solo los controles seleccionados en la Declaración de Aplicabilidad para el SGSI a implementarse en la FACCI.

Numeral	**Dominio o descripción**
A.5	Políticas de seguridad
A.5.1.1	Documento de la política de seguridad de la información.
A.5.1.2	Revisión de la política de seguridad de la información.
A.6	Organización de la seguridad de la Información
A.6.1.1	Compromiso de la dirección con la seguridad de la información
A.6.1.2	Coordinación de la seguridad de la información.
A.6.1.3	Asignación de responsabilidades para la seguridad de la información.
A.6.1.4	Procesos de autorización para los servicios de procesamiento de información.
A.6.1.5	Acuerdos sobre confidencialidad
A.6.1.6	Contacto con las autoridades
A.6.1.7	Contacto con grupos de interés especiales
A.6.1.8	Revisión independiente de la seguridad de la información
A.6.2.1	Identificación de los riesgos relacionados con las partes externas
A.6.2.2	Consideraciones de la seguridad cuando se trata con los clientes
A.6.2.3	Consideraciones de la seguridad en los acuerdos con terceras partes
A.7	Gestión de activos
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.7.2.1	Directrices de clasificación
A.7.2.2	Etiquetado y manejo de información
A.8	Seguridad de los recursos humanos
A.8.1.2	Selección

A.8.2.2	Educación, formación y concientización sobre la seguridad de la información
A.8.2.3	Proceso disciplinario
A.8.3.1	Responsabilidades en la terminación
A.8.3.2	Devolución de activos
A.9	Seguridad física y ambiental
A.9.1.1	Perímetro de seguridad física
A.9.1.2	Controles de acceso físico
A.9.1.3	Seguridad de oficinas, recintos e instalaciones
A.9.1.4	Protección contra amenazas externas y ambientales
A.9.1.5	Trabajo en áreas seguras
A.9.1.6	Áreas de carga, despacho y acceso público
A.9.2.4	Mantenimiento de los equipos
A.9.2.6	Seguridad en la reutilización o eliminación de los equipos
A.10	Gestión de las comunicaciones y operaciones
A.10.1.1	Documentación de los procedimientos de operación
A.10.3.2	Aceptación del sistema
A.10.4.1	Controles contra códigos maliciosos
A.10.4.2	Controles contra códigos móviles
A.10.5.1	Respaldo de la información
A.10.7.1	Gestión de los medios removibles
A.10.7.3	Procedimientos para el manejo de la información
A.10.8.1	Políticas y procedimientos para el intercambio de la información
A.10.8.2	Acuerdos para el intercambio
A.10.8.4	Mensajería electrónica
A.10.10.1	Registro de auditorías
A.10.10.5	Registro de fallas
A.11	Control de acceso
A.11.1.1	Política de control de acceso
A.11.3.3	Política de escritorio despejado y de pantalla despejada
A.11.4.1	Política de uso de los servicios de red
A.11.7.1	Computación y comunicaciones móviles
A.12	Adquisición, desarrollo y mantenimiento de los sistemas de información

A.12.1.1	Análisis y especificación de los requisitos de seguridad
A.12.2.1	Validación de los datos de entrada
A.12.3.1	Política sobre el uso de controles criptográficos
A.12.5.1	Procedimientos de control de cambios
A.12.5.4	Fuga de información
A.12.5.5	Desarrollo de software contratado externamente
A.12.6.1	Control de vulnerabilidades técnicas
A.13	Gestión de incidentes de seguridad de la información
A.13.1.1	Reporte sobre los eventos de seguridad de la información
A.13.1.2	Reportes sobre las debilidades de la seguridad
A.13.2.1	Responsabilidades y procedimientos
A.14	Gestión de la continuidad del negocio
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información
A.15	Cumplimiento
A.15.1.1	Identificación de legislación aplicable
A.15.1.2	Derechos de propiedad intelectual (DPI)
A.15.1.4	Protección de los datos y privacidad de la información personal
A.15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información
A.15.2.1	Cumplimiento con las políticas y normas de seguridad
A.15.2.2	Verificación del cumplimiento técnico

Tabla 9: Controles Seleccionados Para Elaboración de Declaración de Aplicabilidad a aplicar en el SGSI de la FACCI

Fuente: *Elaboración propia*

3.2.3 Análisis de los datos

¿Qué es una declaración de Aplicabilidad y para qué sirve?

> "La declaración de aplicabilidad surge del tratamiento del riesgo y define los controles que debe implementar la organización para tratar los riegos. Estos controles pueden venir definidos por requisitos contractuales, legales, si fuese el caso, o por otros casos" *(Iranzo, 2015)*

> "Este documento es un requisito del estándar ISO/IEC 27001, pero puede ser utilizado para mantener registro y control de las medidas de seguridad aplicadas"
> *(Mendoza, 2015)*

> "Se trata del documento principal que define cómo usted implementará una gran parte de su sistemas de seguridad de la información. De hecho, la declaración de aplicabilidad es el nexo principal entre la evaluación y el tratamiento del riesgo y la implementación de su sistema de seguridad de la información"
> *(Kosutic, 2015)*

Entonces tenemos que, La Declaración de Aplicabilidad, es un documento que tiene una relación completa de Controles de Seguridad de la Información, donde se indica si cada uno de ellos resulta de aplicación o no a la organización, según la actividad de la misma. En cada caso, se deberán detallar los motivos por los que se aplica o no dicho Control, y tener información de su estado de implantación y referencia de los documentos que avalen lo mismo. El objetivo de este documento a más de definir qué controles son adecuados para implementar en la organización, cuáles son los objetivos de esos controles y cómo se implementan, es, aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados, gracias a la importancia y valor de la declaración de aplicabilidad este es uno de los tantos documentos que tienen que ser redactados por exigencia de la norma ISO27001.

La siguiente imagen nos muestra los Componentes que conforman la Elaboración de Declaración de Aplicabilidad.

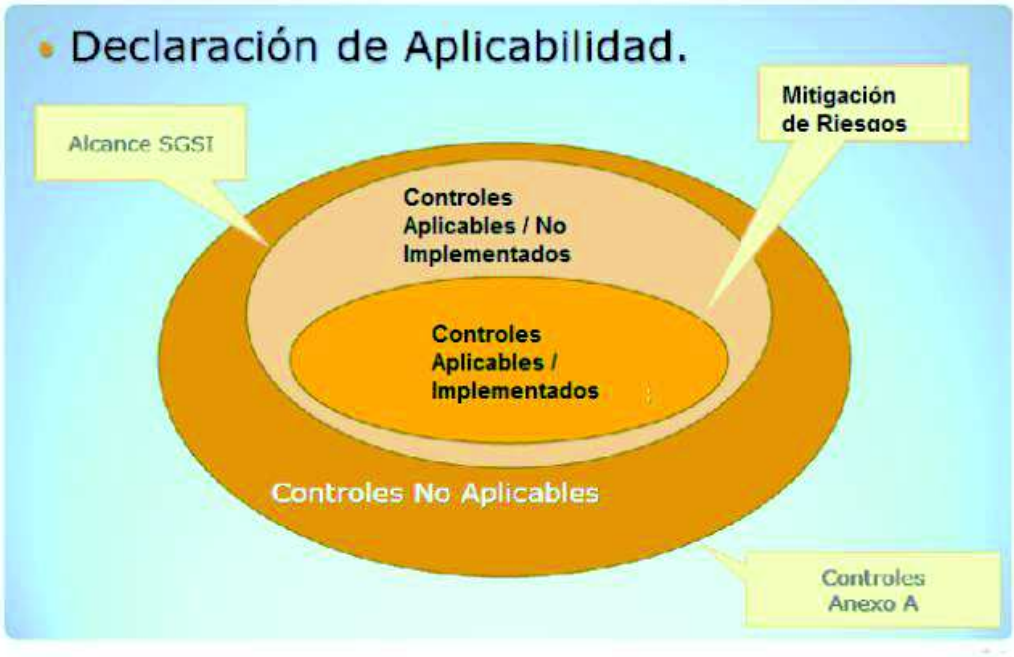

Ilustración 9: *Componentes de la Declaración de Aplicabilidad*

Razones más importantes en la elaboración de la Declaración de Aplicabilidad

1. Es un documento breve que sirve para presentar a la gerencia o auditores.
2. Sirve para documentar el estado actual de los controles aplicables como buenas prácticas en la organización.
3. Sirve para identificar controles necesarios por otras razones diferentes a las definidas en la matriz de riesgos, por ejemplo: motivos legales, requisitos contractuales, entre otros.
4. Redactando una buena declaración de aplicabilidad pueden disminuir la cantidad de otros documentos innecesarios y obtener buenos resultados de una evaluación de riesgos.
5. Sirve para hacer una auditoría, y para poder obtener una certificación de seguridad ISO27001,

(Mancera, 2013)

Impacto de la Declaración de Aplicabilidad en el SGSI

Basado en el ciclo de Deming (entendido como una estrategia de mejora continuada en cuatro pasos: planificar, hacer, comprobar y actuar y así de forma recurrente sin fin). Todo SGSI debe tener como cimientos la comprensión del contexto en que se desenvuelve la organización que lo implanta (en este caso la Facultad de Ciencias Informáticas). A partir de ese conocimiento el SGSI se sustentará en 3 pilares fundamentales: La Gestión de Riesgos, el seguimiento de acciones y la Declaración de Aplicabilidad.

Ilustración 10: *Contexto de la organización frente al SGSI*
Fuente: www.aspectosprofesionales.info/2017/10/integrar-la-norma-iso-27001-o-el.html

Los dos primeros pilares son comunes a cualquier sistema de gestión (desde el 2012), mientras que *la declaración de aplicabilidad únicamente se encuentra en aquellos Sistemas que dispongan de un catálogo de controles o medidas de seguridad en sus anexos.*

Si lo expresamos en un diagrama con mayor detalle, observamos que, además del contexto de la organización, las tres cajas azules corresponden a los tres pilares de un SGSI que acabamos de comentar.

La primera caja azul es la Gestión de riesgos, que se compone como ya hemos visto de un proceso de apreciación y otro de tratamiento de los riesgos identificados.

La segunda caja azul es el seguimiento de acciones. Si un SGSI es incapaz de generar acciones es que no está persiguiendo la mejora continua. Si todo el "tinglado" no es capaz de actuar, es que únicamente monitoriza y entonces se convierte en prescindible.

La tercera y última caja azul es la Declaración de Aplicabilidad, ésta consiste en, un documento que relaciona los controles que se aplican en el SGSI, se trata del documento principal que define cómo se implementará una gran parte del Sistema.

Si no se cuenta con este documento, se retrasaría los procesos de seguridad informáticos y en varios casos afectaría a todo el SGSI hasta el punto de volver vulnerable al mismo, junto a la empresa u organización.

Ilustración 114: *SGSI en la organización*
Fuente: www.aspectosprofesionales.info/2017/10/integrar-la-norma-iso-27001-o-el.html

Cómo elabora una declaración de aplicabilidad.

Para la elaboración de declaración de aplicabilidad necesitamos de otros documentos de planificación del SGSI en el que se trabaja, los mismos que son detallados en la cadena de acciones de la metodología PDCA (Capítulo III). Estos son:

- ✓ Definición de Política y Objetivos
- ✓ Determinación del Alcance
- ✓ Análisis de Riesgos
- ✓ Gestión de Riesgos

Y el requisito más importante y esencial, como lo es la "Selección de Objetivos de Control y Controles". Esa selección se hace en la norma ISO 27001 con la que se está trabajando. El resultado de la elección de los controles forma parte del Plan de Tratamiento de riesgos, de modo que éste tiene como salida la Declaración de aplicabilidad. Esta declaración es uno de los documentos que tienen que ser redactados por exigencia de la norma ISO 27001.

CAPÍTULO IV: METODOLOGÍA

4.1 Metodología de Investigación

La metodología de investigación es un ámbito de conocimiento disciplinar que versa sobre la forma de proceder en la ciencia y se ocupa específicamente de la manera de construir y desarrollar conocimiento.

. *(Sáez Alonso & Touriñan Lopez, 2014)*

La Metodología consiste entonces en un conjunto más o menos coherente y racional de técnicas y procedimientos cuyo propósito fundamental apunta a implementar procesos de recolección, clasificación y validación de datos y experiencias provenientes de la realidad, y a partir de los cuales pueda construirse el conocimiento científico.

La metodología surge a medida que las ciencias van desarrollándose, de donde se desprende que el conocimiento metodológico, el aprendizaje y experiencia de las técnicas opera como un proceso continuo, gradual y progresivo en el que el saber se construye y el modo de adquirirlo se configura con el paso de la experiencia.

Los aspectos generales que se tratan en este esquema de investigación son los siguientes:

- TIPO
- MÉTODO
- HERRMIENTAS

4.1.1 Tipo de Investigación

Investigación Exploratoria

Las investigaciones de tipo exploratorias ofrecen un primer acercamiento al problema que se pretende estudiar y conocer. Se realiza para conocer el tema que se abordará, lo que nos permita "familiarizarnos" con algo que hasta el momento desconocíamos.

Los resultados de este tipo de tipo de investigación nos dan un panorama o conocimiento superficial del tema, pero es el primer paso inevitable para cualquier tipo de investigación posterior que se quiera llevar a cabo.

Con este tipo de investigación o bien se obtiene la información inicial para continuar con una investigación más rigurosa, o bien se deja planteada y formulada una hipótesis.

Investigación Descriptiva

La investigación descriptiva es la que se utiliza, tal como el nombre lo dice, para describir la realidad de situaciones, eventos, personas, grupos o comunidades que se estén abordando y que se pretenda analizar.

En este tipo de investigación la cuestión no va mucho más allá del nivel descriptivo; ya que consiste en plantear lo más relevante de un hecho o situación concreta.

La investigación descriptiva no consiste únicamente en acumular y procesar datos. El investigador debe definir su análisis y los procesos que involucrará el mismo.

Investigación Explicativa o Documental

La investigación de tipo explicativa ya no solo describe el problema o fenómeno observado sino que se acerca y busca explicar y documentar la situación analizada.

En otras palabras, es la interpretación de una realidad o la explicación del por qué y para qué del objeto de estudio.

4.1.2 Método de Investigación

El método es un proceso de pasos a seguir para alcanzar una meta, y la técnica es el conjunto de procedimientos de los recursos de que se vale la ciencia para llegar a su fin, la técnica se puede repetir según el investigador lo considere para que su trabajo tenga validez.

Método Lógico Deductivo

Mediante ella se aplican los principios descubiertos a casos particulares, a partir de un enlace de juicios. El papel de la deducción en la investigación es doble.

Primero consiste en encontrar principios desconocidos, a partir de los conocidos.

También sirve para descubrir consecuencias desconocidas, de principios conocidos.

Método deductivo directo – inferencia o conclusión inmediata. Se obtiene el juicio de una sola premisa, es decir que se llega a una conclusión directa sin intermediarios.

Parte de lo general a lo particular.

4.1.3 Herramientas de Investigación

La observación consiste en saber seleccionar aquello que queremos analizar.

Para la observación lo primero es plantear previamente qué es lo que interesa observar. En definitiva haber seleccionado un objetivo claro de observación.

La observación científica "tiene la capacidad de describir y explicar el comportamiento, al haber obtenido datos adecuados y fiables correspondientes a conductas, eventos y /o situaciones perfectamente identificadas e insertas en un contexto teórico.

Las palabras claves de esta definición son: describir y explicar, datos adecuados y fiables, conductas perfectamente identificadas.

Piéron (1986).

4.2 Metodología Operativa

La metodología que vamos a utilizar para el desarrollo del proyecto será el de Planificar, Hacer, Comprobar, Actuar (Plan/Do/Check/Act)que es una serie de actividades documentadas ampliamente probadas en este campo, por parte de profesionales expertos, auditores de sistemas informáticos, peritos informáticos, informáticos forenses, oficiales de seguridad, etc.

Este modelo incluye la estructura, políticas, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

- Plan – Planificación
- Do – Hacer
- Check – Monitorear
- Act - Actuar

En las siguientes figuras podemos observar la metodología mencionada y sus componentes.

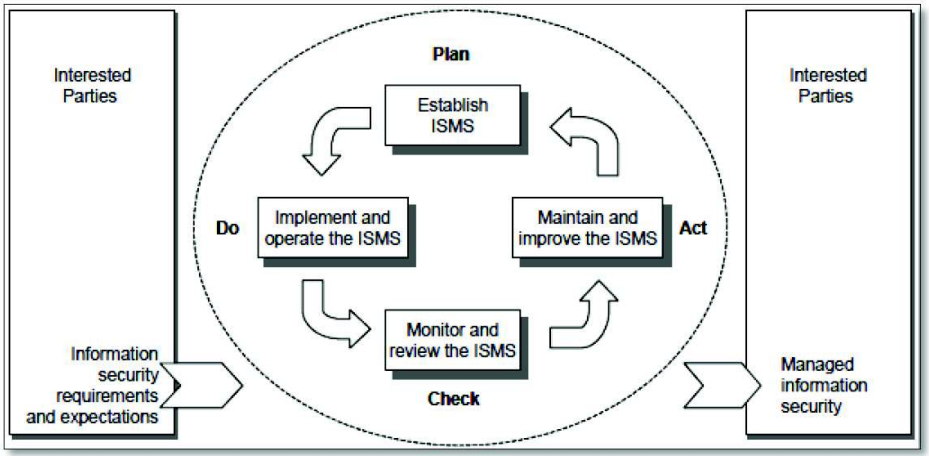

Ilustración 12: Modelo PDCA aplicado a los procesos de un SGSI

Fuentes: *ISO/IEC. International Standard ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary. Geneva: ISO Copyright Office. 2014.*

Ilustración 13: Representación del Modelo "Plan/Do/Check/Act"
***Fuente**: ISO27001.doc*

Finalmente la imagen que se mostrará a continuación muestra una cadena de acciones que se deben realizar en un SGSI desarrollado bajo las normas ISO/IEC 27001, el cual adopta el modelo: Plan Do Check Act, esta cadena de acciones es una manera de adentrarse al modelo PDCA para poder lograr el objetivo del SGSI de forma sistemática.

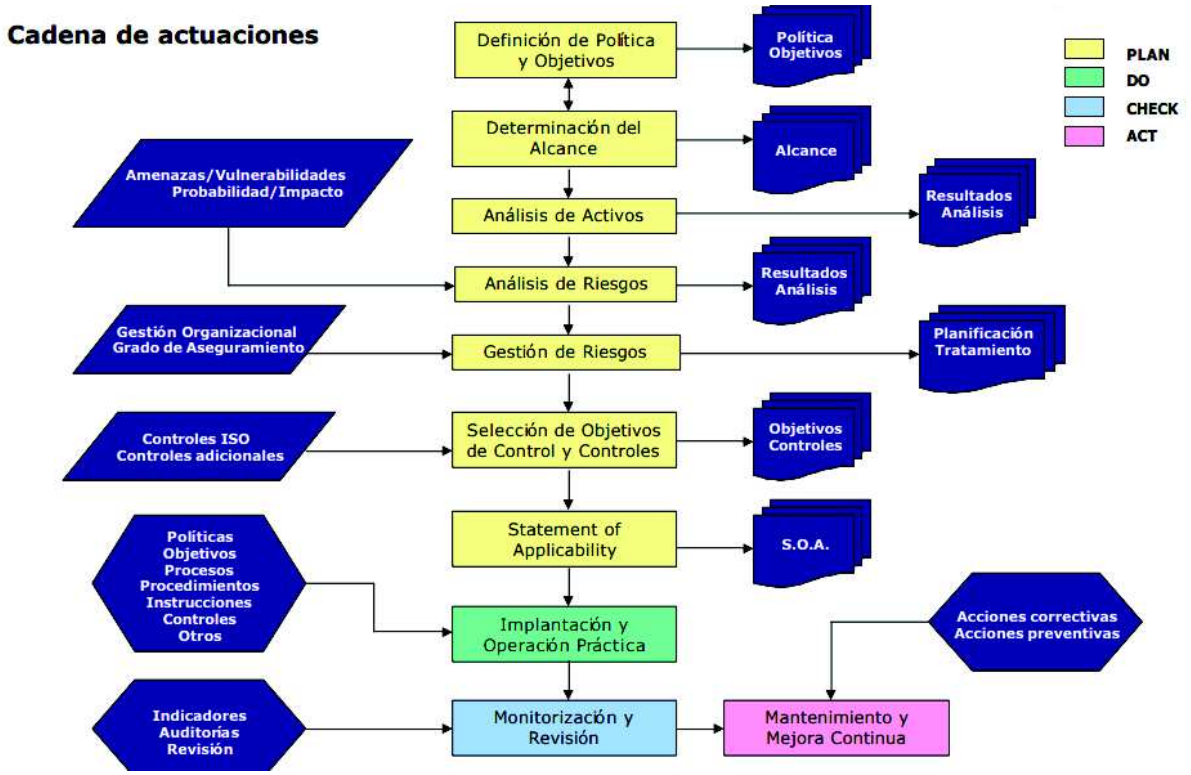

Ilustración 14: Metodología de un SGSI según ISO 27001
***Fuente:** Zuccardi, G., & Gutiérrez, J. D. (2006). ISO 27001:2005. Obtenido de: pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001.doc*

CAPÍTULO V:
RESULTADOS

5.1 Desarrollo y Análisis de Propuesta de Declaración de Aplicabilidad

Como se mencionó anteriormente, La Declaración de aplicabilidad es un documentos que tiene que ser redactado por exigencia de la norma ISO 27001, este documento consta de 133 controles agrupados en 11 objetivos de control, que viene ya definidos por ISO/IEC en su versión 2005, de los cuales sólo se selecciona los que aplican a la Institución, Empresa u organización con la que se esté trabajando, o en la que se esté aplicando el SGSI.

Los Objetivos de control y los controles enumerados a continuación se derivan y se alinean directamente, con aquellos enumerados en BS ISO/IEC 17799:2005 (Clausulas del 5 al 15). Una empresa u organización podría considerar que son necesarios objetivos de control y controles adicionales a las listas en estas tablas, sin embargo, en nuestra Investigación, solo se consideran necesarios 64 (de 133) controles, agrupados en los 11 objetivos de Control. Los Objetivos de Control y Controles de estas tablas deben seleccionarse como parte del proceso del SGSI a implementarse en la Facultad de Ciencias Informáticas.

El desarrollo de la Propuesta de Declaración de Aplicabilidad se muestra en el Capítulo de Resultados, en las tablas se muestra las Políticas (de la A5 a la A15), con sus respectivo Objetivos de Control detallado y Controles que lo conforman.

Cada Control cuenta con una columna donde se indica, si éste está entre los que SI aplica, o los que NO aplica, luego le preside una columna que indica la Razón de la selección de aplicabilidad, aquí se detalla, porque motivo dicho control aplica, caso contrario, se detalla porque motivo dicho control no aplica, seguido a esto, se encuentra la columna de Documento, en esta columna se describe con inexactitud(los nombres de los documentos pueden cambiar dentro de la Facultad) los documentos propuestos para validar la aplicabilidad o selección de un control, y Finalmente se encuentra la columna de Responsable, donde se indica, el departamento, la persona o el grupo de personas, dentro de la Facultad, que serán responsables de llevar a cabo el cumplimiento e información del control especificado.

Las celdas correspondientes a la columna de Documento y Responsable sólo contarán con información, cuando el control descrito en esa fila, SI aplique, caso contrario las celdas se encontrarán vacías. Tal como se muestra a continuación.

5.1.1 PROPUESTA DE DECLARACION DE APLICABILIDAD

Objetivo 1: A5 Políticas de Control

A5 POLÍTICAS DE SEGURIDAD						
A. 5.1		Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.5.1.1	**Políticas de seguridad de información**	Documentar las políticas de seguridad de la información.	SI	Tiene una aplicabilidad global en todo el SGSI gracias a las directrices establecidas por la alta dirección que funcionan como base para la implementación de las medidas de seguridad.	Documento de políticas debidamente aprobado y firmado por el honorable consejo de facultad, Actas de confirmación de publicación y socialización de las políticas a los empleados y departamentos de la FACCI	Docente o Departamento a cargo del control y seguimiento del SGSI
A.5.1.2		Revisión de las políticas de seguridad de la información.	SI	De manera periódica se debe realizar la revisión de las políticas de seguridad implementadas por si existen cambios o mejoras en las mismas, de ser el caso se debe documentar las acciones, para asegurar la continua idoneidad, eficiencia y efectividad.	Actas de revisión y validación periódica de políticas de seguridad implementadas.	Docente o Departamento a cargo del control y seguimiento del SGSI

Objetivo 2: A6 Organización de la Seguridad de la Información

A6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN						
A.6.1		Manejar la seguridad de la información dentro de la organización	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.6.1.1	**Organización Interna**	Compromiso de la dirección con la seguridad de la información	SI	Es fundamental, dado que el honorable consejo de facultad y decanato deben apoyar activamente la seguridad dentro de la organización y tienen la responsabilidad de aprobar el SGSI como última instancia.	Si la facultad no cuenta con un comité se SGSI se recomienda la creación de uno, de esta forma de pueden obtener las Actas de comité de los Contratos debidamente socializados y enfocados al SGSI. Caso contrario el trabajo debe ser hecho por el honorable consejo de facultad, decanato o un departamento o comisión asignados por las entidades nombradas anteriormente.	Honorable Consejo de Facultad/ Decanato
A.6.1.2		Coordinación de la seguridad de la información.	SI	Debe haber una o varias áreas que lideren la implementación del SGSI, así como su control, seguimiento y mantenimiento.	Estructura Organizacional de la FACCI. Documento de asignación de responsabilidades y roles dentro de la facultad. Los roles dentro de la facultad deben ser asignados por el comité de SGSI o en su defecto por el honorable consejo de facultad.	Docente o Departamento a cargo del control y seguimiento del SGSI
A.6.1.3		Asignación de responsabilidades para la seguridad de la información.	SI	A las áreas o departamentos existentes se les debe asociar responsabilidades frente al SGSI.	Documento de asignación de roles con la inclusión de las responsabilidades, en los cargos y comisiones en la facultad o en los procesos frente al SGSI.	Honorable Consejo de Facultad/ Decanato
A.6.1.4		Procesos de autorización para los servicios de procesamiento de información.	SI	Todo medio de procesamiento de información (Sistema de Información) dentro de la facultad debe contar con un proceso de aceptación mayor (HCF o decanato) antes de su funcionamiento.	Actas de proceso de aceptación de los sistemas de información debidamente autorizados por el decanato de la facultad	Honorable Consejo de Facultad/ Decanato

A.6.1.5		Acuerdos de confidencialidad	SI	La información dentro de la facultad es el activo más importante, por ende es fundamental su protección ante develado	Cláusulas contractuales, modelos de contratos con las cláusulas de confidencialidad. Acuerdos de no-divulgación.	Honorable Consejo de Facultad/ Decanato
A.6.1.6		Contacto con las autoridades	SI	Se debe mantener los contactos apropiados con las autoridades de la Universidad y departamentos de la misma tales como: rectorado, vicerrectorado, secretariado, UCCI, entre otros departamentos relevantes para reaccionar a tiempo frente a incidentes y permitir la reducción de riesgos. Asimismo contacto con autoridades policiales y de contra de la ciudad.	Matriz con los nombres de las autoridades de la universidad actuales con su respectivo cargo, número de contacto, lugar de contacto, correo, etc. De igual forma con las autoridades policiales y de control a cargo dentro de la ciudad o universidad	Secretaria FACCI/Decanato
A.6.1.7		Contacto con grupos de interés especiales	SI	Es necesario mantenerse informado sobre los acontecimientos en seguridad, más aun siendo la Facultad de Ciencias Informáticas de la Universidad, con ello, se puede retroalimentar el SGSI y los incidentes de seguridad que puedan ocasionarse en el mismo dentro de la facultad.	Convenios con entidades instituciones u organizaciones que brinden capacitaciones enfocadas a seguridad informática y comprobantes de inscripciones a grupos de interés en seguridad de la información, tales como Grupo Radical, RED CEDIA u otros y Certificaciones de asistencia a los mismos, y a foros de seguridad especializados.	Comisión de investigación/Docente o Departamento a cargo del control y seguimiento del SGSI
A.6.1.8		Revisión independiente de la seguridad de la información	SI	Las revisiones independientes o auditorías externas hacen más fuerte y transparente el proceso de implementación del SGSI	Contrato anual con revisores/auditoria externa de seguridad informática. Informe de evaluación de carrera.	Decanato/Docente o Departamento a cargo del control y seguimiento del SGSI
A.6.2	**Entidades Externas**	Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a los manejados por entidades externas	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.6.2.1		Identificación de los riesgos relacionados con entidades externas	SI	La facultad debe tener terceras partes o entidades externas que ayudan al objetivo del SGSI o a cumplir la misión de la misma facultad por lo cual es imprescindible implementar los controles apropiados antes de otorgar accesos o privilegios de accesos a estas entidades, o terceras personas.	Análisis de riesgos que evidencie la vulnerabilidad al momento de entregar información a empresas o personas externas con el respectivo mapa de riegos.	Decanato/Docente o Departamento a cargo del control y seguimiento del SGSI
A.6.2.2		Tratamiento de la seguridad cuando se trabaja con clientes	SI	Se debe tratar todos los requerimientos de seguridad identificados antes de otorgar a los estudiantes acceso a la información o activos de la Facultad	Socialización de procedimientos y manuales de seguridad como recomendaciones hacia los estudiantes	Decanato/Docente o Departamento a cargo del control y seguimiento del SGSI
A.6.2.3		Tratamiento de la seguridad en contratos con terceras partes	SI	Es imprescindible incluir los temas de seguridad en los contratos, debido a que existen acuerdos que involucran acceso de terceras personas a la información, y esto debe abarcar los requerimientos de seguridad necesarios relevantes.	Documento que detalle los controles que se debe tener en cuenta al momento de entregarle información de la facultad a entidades externas o personas.	Decanato

Objetivo 3: A7 Gestión de Activos

A7 GESTIÓN DE ACTIVOS						
A.7.1		Lograr y mantener la protección apropiada de los activos organizacionales	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.7.1.1	Responsabilidad por los activos	Inventario de activos	SI	Para una adecuada gestión de riesgos y tratamiento de estos, es necesario conocer los activos de información de la FACCI.	Inventario actualizado con todos los activos de la FACCI organizados por departamentos y áreas.	Departamento técnico FACCI
A.7.1.2		Propiedad de los activos	SI	Cada activo de información dentro de la facultad debe tener un responsable que esté a cargo del mismo.	Listado de los activos de información con el responsable a cargo del mismo. Actas de responsabilidades de los activos asignados a cada docente o personal administrativo	Departamento técnico FACCI
A.7.1.3		Uso aceptable de los activos	SI	Se debe identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información	Actas de capacitación sobre el uso adecuado de recursos informáticos. Controles para el uso adecuado de la información y los activos asociados a la misma, dirigidos a estudiantes, docentes, y personal administrativo.	Departamento técnico FACCI
A.7.2		Asegurar que la información reciba un nivel de protección apropiado	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.7.2.1	Clasificación de la información	Lineamientos de clasificación	SI	La información debe protegerse, por ello es necesario clasificarla en términos de valor, requerimientos legales, confidencialidad y grado crítico para la organización.	Documento con los niveles de clasificación de la información debidamente aprobada por el honorable consejo de facultad.	Decanato
A.7.2.2		Etiquetado y manejo de información	SI	Se debe implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con la clasificación	Documento con los niveles de clasificación y procedimiento para etiquetado debidamente aprobado por el consejo de facultad	Secretaria FACCI/Decanato

Objetivo 4: A8 Seguridad de los Recursos Humanos

A8 SEGURIDAD DE LOS RECURSOS HUMANOS						
A.8.1		Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.8.1.1	**Antes del empleo**	Roles y responsabilidades	NO	Los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en la Universidad en general frente a un SGSI u otro, es asignado por las autoridades de la Universidad, específicamente el departamento de Recursos Humanos. No la FACCI.		NO ASIGANDO
A.8.1.2		Selección	SI	Desde los procesos iniciales de ingreso del personal, se debe establecer parámetros de seguridad, como chequeo de verificación de antecedentes, proporcionales a los requerimientos e información a la cual se va a tener acceso y los riesgos percibidos.	Inclusión de elementos de seguridad sobre los procesos de selección de personal en la entrevista realizada por decanato cuando ingresa personal nuevo en la facultad.	Decanato
A.8.1.3		Términos y condiciones laborales	NO	Los términos y condiciones del contrato de empleo, que debe establecer las responsabilidades del contratado y las de la Facultad para la seguridad y protección de la información es asignado u otorgado por la autoridades de la Facultad, específicamente el departamento de Recursos Humanos de la Universidad. No la FACCI.		NO ASIGANDO

A.8.2		Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.8.2.1	**Durante el empleo**	Gestión de responsabilidades	NO	Las autoridades de la Universidad son las que deben requerir que los empleados apliquen la seguridad en concordancia con algún SGSI, no la Facultad.		NO ASIGANDO
A.8.2.2		Capacitación y educación en seguridad de la información	SI	Ser competitivos es de gran importancia para la implementación y mantenimiento del SGSI, esto implica tener planes de capacitación frente a los temas de seguridad	Informe de Plan de capacitación y registros de participación de personal docente, administrativo y estudiantes.	Miembro/s del proyecto de SGSI FACCI a cargo
A.8.2.3		Proceso disciplinario	SI	El control es fundamental, y las faltas de los empleados deben ser investigadas y sancionadas con un debido proceso disciplinario formal.	Inclusión de elementos de seguridad sobre los procesos de selección de personal. Informe de la comisión de ética y disciplina en casos de vulneración de información en la facultad	Comisión Académica/Decanato
A.8.3		Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.8.3.1	**Terminación o cambio del empleo**	Responsabilidades de terminación	SI	Se debe definir y asignar claramente las responsabilidades para realizar la terminación del empleo	Documento de asignación de roles con la inclusión de las responsabilidades, en los cargos o en los procesos frente al SGSI	Decanato
A.8.3.2		Devolución de activos	SI	A las áreas deben asociarse las responsabilidades frente al SGSI, dentro de éstas, la devolución de activos y accesos que le fueron asignados.	Procedimiento para el retiro de equipos informáticos. Actas de entrega-recepción	Departamento técnico FACCI/ Decanato
A.8.3.3		Eliminación de derechos de acceso	NO	El proceso de eliminación de derechos de acceso, es llevado por la UCCI		NO ASIGANDO

Objetivo 5: A9 Seguridad Física y Ambiental

A9 SEGURIDAD FÍSICA Y AMBIENTAL						
A.9.1		Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.9.1.1	**Áreas seguras**	Perímetro de seguridad física	SI	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Documento en donde se detallan las medidas físicas de seguridad, perímetro, accesos, personal, etc., debidamente autorizado y aprobado por el honorable consejo de facultad	Decanato/Honorable Consejo de Facultad
A.9.1.2		Controles de entrada físicos	SI	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Documento en donde se detallan las medidas físicas de seguridad, perímetro, accesos, personal, etc., debidamente autorizado y aprobado por el honorable consejo de facultad	Decanato/Honorable Consejo de Facultad
A.9.1.3		Seguridad de oficinas, habitaciones y medios	SI	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Documento en donde se detallan las medidas físicas de seguridad, perímetro, accesos, personal, etc., debidamente autorizado y aprobado por el honorable consejo de facultad	Decanato/Honorable Consejo de Facultad

A.9.1.4		Protección contra amenazas externas y ambientales	SI	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Documento en donde se detallan las medidas físicas de seguridad, perímetro, accesos, personal, etc., debidamente autorizado y aprobado por el honorable consejo de facultad	Decanato/Honorable Consejo de Facultad
A.9.1.5		Trabajo en áreas seguras	SI	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Documento en donde se detallan las medidas físicas de seguridad, perímetro, accesos, personal, etc., debidamente autorizado y aprobado por el honorable consejo de facultad	Decanato/Honorable Consejo de Facultad
A.9.1.6		Áreas de acceso público, entrega y carga	SI	Los sistemas de cómputo, los recursos y la personas deben estar adecuadamente protegidas contra amenazas físicas y ambientales	Implementación de medidas físicas y procedimentales. Documento en donde se detallan las medidas físicas de seguridad, perímetro, accesos, personal, etc., debidamente autorizado y aprobado por el honorable consejo de facultad	Decanato/Honorable Consejo de Facultad
A.9.2		Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.9.2.1		Ubicación y protección de los equipos	NO	La protección de los sistemas de cómputo, los recursos y la personas contra amenazas físicas y ambientales son responsabilidad de la Universidad o el departamento que esta asigné, pero no es responsabilidad ni obligación de la Facultad.		NO ASIGNADO
A.9.2.2		Servicios públicos	NO	La protección de los sistemas de cómputo, los recursos y la personas contra amenazas físicas y ambientales son responsabilidad de la Universidad o el departamento que esta asigné, pero no es responsabilidad ni obligación de la Facultad.		NO ASIGNADO
A.9.2.3		Seguridad en el cableado	NO	La protección de los sistemas de cómputo, los recursos y la personas contra amenazas físicas y ambientales son responsabilidad de la Universidad o el departamento que esta asigné, pero no es responsabilidad ni obligación de la Facultad.		NO ASIGNADO
A.9.2.4	**Seguridad del equipo**	Mantenimiento de equipos	SI	Los sistemas de cómputo, y hardware en general deben estar adecuadamente protegidas contra amenazas físicas y ambientales, lo que se logra hacer con los mantenimientos preventivos y correctivos.	Plan de mantenimiento correctivo y preventivo aprobado por el honorable consejo de facultad, con cronograma semestral de aplicación del plan. Contratos sobre equipos informáticos.	Departamento técnico FACCI
A.9.2.5		Seguridad de los equipos fuera de las instalaciones	NO	La protección de los sistemas de cómputo, los recursos y la personas contra amenazas físicas y ambientales son responsabilidad de la Universidad o el departamento que esta asigné, pero no es responsabilidad ni obligación de la Facultad.		NO ASIGNADO
A.9.2.6		Seguridad en la reutilización o eliminación de los equipos	SI	Los sistemas de cómputo y los recursos existentes en la facultad deben estar adecuadamente actualizados en el respectivo inventario.	Presentación del inventario actualizado con equipos dados de baja con su respectiva justificación. Procedimientos de borrado seguro de información sin recuperación	Departamento técnico FACCI
A.9.2.7		Traslado de activos	NO	La protección de los sistemas de cómputo, los recursos y la personas contra amenazas físicas y ambientales son responsabilidad de la Universidad o el departamento que esta asigné, pero no es responsabilidad ni obligación de la Facultad.	procedimientos para el ingreso y retiro de equipos tecnológicos a las instalaciones	NO ASIGNADO

Objetivo 6: A10 Gestión de las Comunicaciones y Operaciones

A10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES						
A.10.1		Asegurar la operación correcta y segura de los medios de procesamiento de la información	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.1.1	**Procedimientos y responsabilidades operacionales**	Procedimientos de operación documentados	SI	Todos los procedimientos operativos deben estar documentados por la Unidad Académica, en este caso la FACCI.	Documentos y manuales de operación, Plan de mantenimiento preventivo y correctivo.	Secretaria FACCI/Decanato
A.10.1.2		Gestión de cambio	NO	Todos los procedimientos operativos de cualquier SI son realizados, supervisados y controlados por la UCCI y no por la Facultad.		NO ASIGNADO
A.10.1.3		Segregación de deberes	NO	Todos los procedimientos operativos de cualquier SI son realizados, supervisados y controlados por la UCCI y no por la Facultad.		NO ASIGNADO
A.10.1.4		Separación de los medios de desarrollo, y operacionales	NO	Todos los procedimientos operativos de cualquier SI son realizados, supervisados y controlados por la UCCI y no por la Facultad.		NO ASIGNADO
A.10.2		Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.2.1	**Gestión de la entrega del servicio de terceros**	Entrega o prestación del servicio	NO	La seguridad de la información y controles de los SI y entrega del servicio en línea o contratos de entrega del servicio de terceros es manejado y controlado por la UCCI y las autoridades de la Universidad no por la Facultad.		NO ASIGNADO
A.10.2.2		Monitoreo y revisión de los servicios de terceros	NO	La seguridad de la información y controles de los SI y entrega del servicio en línea o contratos de entrega del servicio de terceros es manejado y controlado por la UCCI y las autoridades de la Universidad no por la Facultad.		NO ASIGNADO
A.10.2.3		Manejo y Gestión en los servicios de terceras	NO	La seguridad de la información y controles de los SI y entrega del servicio en línea o contratos de entrega del servicio de terceros es manejado y controlado por la UCCI y las autoridades de la Universidad no por la Facultad.		NO ASIGNADO
A.10.3		Minimizar el riesgo de fallas en los sistemas	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.3.1	**Planeación y aceptación del sistema**	Gestión de la capacidad	NO	La UCCI es quien monitorear y realizar proyecciones del uso de los recursos, para asegurar el desempeño de los sistemas requeridos. No la Facultad		NO ASIGNADO
A.10.3.2		Aceptación del sistema	SI	Todo sistema informático debe contar con procedimientos de aceptación de los sistemas antes de su funcionamiento.	Proceso de aceptación en gestión de calidad de los sistemas en la facultad, producto de: proyectos integradores de saberes, proyectos de titulación o sistemas que se adquieran a terceros.	Decanato/Comisión académica/HCF
A.10.4		Proteger la integridad del software y la información	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.4.1	**Protección contra software malicioso y código móvil**	Controles contra software malicioso	SI	Se debe implementar controles de detección, prevención y recuperación, para protegerse de códigos maliciosos.	Documento en donde se detallan las medidas lógicas de seguridad contra códigos maliciosos. Debidamente autorizado y aprobado por el honorable consejo de facultad.	Docente o Departamento a cargo del control y seguimiento del SGSI
A.10.4.2		Controles contra códigos móviles	SI	Se debe controlar de manera adecuada los códigos maliciosos, asegurándose que los códigos móviles autorizados operen de acuerdo a las políticas de seguridad definidas.	Políticas de seguridad contra códigos maliciosos. Autorizaciones para uso de códigos móviles.	Docente o Departamento a cargo del control y seguimiento del SGSI
A.10.5		Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.5.1	**Respaldo (back-up)**	Respaldo de la información	SI	Ante eventos de seguridad, es necesario contar con backup que permitan la recuperación de la información.	Procedimientos para el respaldo de la información debidamente autorizado por el Honorable Consejo de Facultad	Docente o Departamento a cargo del control y seguimiento del SGSI

A.10.6		Asegurar la protección d ella información en redes y la protección de la infraestructura de soporte	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.6.1	**Gestión de seguridad de redes**	Controles de las red	NO	El control de acceso a las redes el cual debe permitir la reducción de los riesgos es hecho por la UCCI y no por la Facultad.		NO ASIGNADO
A.10.6.2		Seguridad de los servicios de red	NO	El control de acceso a las redes el cual debe permitir la reducción de los riesgos es hecho por la UCCI y no por la Facultad.		NO ASIGNADO
A.10.7		Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.7.1		Gestión de los medios removibles	SI	Se debe tener control y planes de sensibilización con respecto a los medios removibles	Procedimientos y políticas en la red para el uso de medios removibles	Departamento técnico FACCI/Decanato
A.10.7.2	**Gestión de medios**	Eliminación de los medios	NO	Quien debe tener control y planes de sensibilización con respecto a los medios removibles es la UCCI no la Facultad		NO ASIGNADO
A.10.7.3		Procedimientos de manejo de la información	SI	Se deben establecer los procedimientos para el manejo y almacenamiento de la información protegiéndola de divulgación no autorizada o mal uso de la misma	Documento con niveles de clasificación y ejecución de planes de sensibilización de la información.	Miembro/s del proyecto de SGSI FACCI a cargo
A.10.7.4		Seguridad de documentación del sistema	NO	UCCI es quien debe proteger la documentación de un acceso no autorizado, no la Facultad		NO ASIGNADO
A.10.8		Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.8.1		Políticas y procedimientos de información y software	SI	Se debe establecer políticas, procedimientos y controles de intercambio formales para proteger la información.	Procedimiento para el intercambio de información con niveles de clasificación de la misma entre departamentos, comisiones, etc. Donde se indique cómo debe ser el flujo de información, verificaciones y autorizaciones.	Decanato/Comisión académica/HCF
A.10.8.2	**Intercambio de información**	Acuerdos de intercambio	SI	Tanto la clasificación como los planes de sensibilización fortalecen la reducción de riesgos sobre el inadecuado manejo de la información.	Documento con niveles de clasificación, ejecución de planes de sensibilización y procedimientos para el intercambio de información. herramientas técnicas para la protección de la documentación	Miembro/s del proyecto de SGSI FACCI a cargo
A.10.8.3		Medios físicos en tránsito	NO	La UCCI es quien debe tener control y planes de sensibilización con respecto a los accesos no-autorizados, mal uso o corrupción durante el transporte de la información, no la Facultad		NO ASIGNADO
A.10.8.4		Mensajería electrónica	SI	Las áreas o departamentos hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello se debe proteger	procedimientos para el control de acceso sobre la mensajería, criptografía e implementación de sistemas Anti malware	Docente o Departamento a cargo del control y seguimiento del SGSI
A.10.8.5		Sistemas de información comercial	NO	La Facultad no cuenta con sistemas de información comercial, por lo cual es innecesario proteger información asociada con la interconexión de los sistemas de información comercial, ya que esto no existe		NO ASIGNADO
A.10.9	**Servicios de comercio electrónico**	Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**

A.10.9.1		Comercio electrónico	NO	La Facultad no cuenta con servicios de comercio electrónico o un SI vinculado a esto, por lo cual es información involucrada en el comercio electrónico, debido a que no existe.		NO ASIGNADO
A.10.9.2		Transacciones en línea	NO	La Facultad no cuenta con servicios de comercio electrónico o un SI vinculado a esto, por lo cual es información involucrada en el comercio electrónico, debido a que no existe.		NO ASIGNADO
A.10.9.3		Información disponible al público	NO	La Facultad no cuenta con servicios de comercio electrónico o un SI vinculado a esto, por lo cual es información involucrada en el comercio electrónico, debido a que no existe.		NO ASIGNADO
A.10.10		Detectar actividades de procesamiento de información no autorizadas	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.10.10.1		Registro de auditorías	SI	Se deben producir registros de las actividades de auditoría para ayudar en investigaciones futuras y monitorear el control de acceso	Registros de auditorías internas y externas.	Decanato/HCF/Docente o Departamento a cargo del control y seguimiento del SGSI
A.10.10.2		Monitoreo del uso del sistema	NO	Los sistemas son monitoreados de manera regular por la UCCI no por la Facultad		NO ASIGNADO
A.10.10.3	**Monitoreo**	Protección de la información del registro	NO	Los logs y registros son configurados y protegidos para validaciones, monitores y manejo de incidentes de seguridad por la UCCI no por la Facultad		NO ASIGNADO
A.10.10.4		Registros del administrador y del operador	NO	Las actividades del administrador y operador de los sistemas son registrados dentro de la UCCI no por la Facultad.		NO ASIGNADO
A.10.10.5		Registro de fallas	SI	Las fallas de deben registrar, analizar y se debe tomar la acción apropiada	Documento de análisis de fallas. Acciones contra fallas. Lo ideal sería implementar un sistemas de registro de incidentes de seguridad informática, O en su defecto contratar los servicios de RED CEDIA como el CSIRT	Docente o Departamento a cargo del control y seguimiento del SGSI/Departamento técnico FACCI
A.10.10.6		Sincronización de relojes	NO	El tiempo es fundamental en los sistemas y más aún en las aplicaciones de tiempo real (Online).	Procedimiento para la configuración de NTP.	NO ASIGNADO

Objetivo 7: A11 Control de Acceso

A11 CONTROL DE ACCESO						
A.11.1	**Requerimiento comercial para el control del acceso**	Controlar acceso a la información	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.1.1		Política de control de acceso	SI	Tiene una aplicabilidad global en todo el SGSI	Documento de políticas de control firmado y aprobado por el honorable consejo de facultad	Docente o Departamento a cargo del control y seguimiento del SGSI
A.11.2		Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.2.1	**Gestión del acceso del usuario**	Registro de usuarios	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos y otorgados por la UCCI no por la Facultad.		NO ASIGNADO
A.11.2.2		Gestión de privilegios	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos y otorgados por la UCCI no por la Facultad.		NO ASIGNADO

A.11.2.3		Gestión de contraseñas para usuario	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos y otorgados por la UCCI no por la Facultad.		NO ASIGNADO
A.11.2.4		Revisión de los derechos de acceso de los usuarios	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos y otorgados por la UCCI no por la Facultad.		NO ASIGNADO
A.11.3		Controlar acceso a la información	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.3.1	**Responsabilidades del usuario**	Uso de contraseñas	NO	La UCCI es quien debe requerir que los estudiantes, personal docente y administrativo de la Universidad en general sigan buenas prácticas de seguridad en la selección y uso de claves, no la Facultad.		NO ASIGNADO
A.11.3.2		Equipo de usuario desatendido	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos por la UCCI no por la Facultad.		NO ASIGNADO
A.11.3.3		Política de pantalla y escritorio limpio	SI	La información sensible debe estar coherentemente resguardada	Planes de sensibilización sobre la protección de la información e implementación de políticas para resguardar la información en escritorios de las PCs	Miembro/s del proyecto de SGSI FACCI a cargo
A.11.4		Evitar el acceso no-autorizado a los servicios en red.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.4.1		Política sobre el uso de servicios en red	SI	Los usuarios sólo deben tener acceso a los servicios en red que les fueron autorizados para permitir la reducción de los riesgos	Procedimientos para el control de acceso (creación, bloqueo, modificación, aprovisionamiento). Plan de sensibilicen de control de acceso a las redes a los estudiantes, docentes y personal administrativo	Departamento técnico FACCI
A.11.4.2		Autenticación del usuario para conexiones externas	NO	La Facultad no cuenta con métodos de autenticación para controlar el acceso de usuarios remotos.		NO ASIGNADO
A.11.4.3		Identificación del equipos en red	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos por la UCCI no por la Facultad.		NO ASIGNADO
A.11.4.4	**Control de acceso a redes**	Protección del puerto de diagnóstico remoto	NO	La UCCI es quien controla el acceso físico y lógico a los puertos de diagnóstico y configuración, no la Facultad		NO ASIGNADO
A.11.4.5		Separación en las redes	NO	UCCI es quien controla y separa de manera adecuada los servicios de información, usuarios y sistemas de información en las redes de modo que se reduzcan los errores operativos, no la Facultad.		NO ASIGNADO
A.11.4.6		Control de conexión a las redes	NO	UCCI es quien restringe la capacidad de conexión de los usuarios en las redes, para cumplir con la política de control de acceso y la reducción de los riesgos (11.1), no la Facultad		NO ASIGNADO
A.11.4.7		Control de enrutamiento en la red	NO	UCCI es quien debe implementar controles "routing" en las redes para asegurar las conexiones y que no infrinja la política de control de acceso de las aplicaciones comerciales en caso de que exista, no la Facultad.		NO ASIGNADO
A.11.5		Evitar el acceso no-autorizado a los sistemas operativos.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.5.1		Procedimientos de registros en el terminal	NO	Los procedimientos de registro seguro controlan el acceso a los servicios operativos, proceso hecho por la UCCI no por la Facultad.		NO ASIGNADO
A.11.5.2	**Control de acceso al sistema de operación**	Identificación y autenticación de usuarios	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos. Por la UCCI no por la Facultad.		NO ASIGNADO
A.11.5.3		Sistema de gestión de contraseñas	NO	Es la UCCI quien debe asegurar la calidad de las claves por medio de sistemas de manejo de claves y accesos. No la Facultad		NO ASIGNADO

A.11.5.4		Uso de las utilidades del sistema	NO	La UCCI es quien restringe y controla el uso de los programas de utilidad, y no la Facultad		NO ASIGNADO
A.11.5.5		Sesión inactiva	NO	Las sesiones inactivas deben cerrarse después de un periodo. Proceso hecho por la UCCI no por la Facultad		NO ASIGNADO
A.11.5.6		Limitación del tiempo de conexión	NO	Todos los usuarios y sistemas deben identificarse, autenticarse y autorizarse acorde a los accesos permitidos. Por la UCCI no por la Facultad.		NO ASIGNADO
A.11.6	**Control de acceso a la aplicación e información**	Evitar el acceso no-autorizado a la información mantenida en los sistemas de aplicación	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.6.1		Restricción de acceso a la información	NO	Se debe restringir el acceso al sistema de información de acuerdo a las políticas de control de acceso establecida y puestas en prácticas por la UCCI no por la Facultad.		NO ASIGNADO
A.11.6.2		Aislamiento de sistemas sensibles	NO	Los sistemas sensibles deben tener un nivel de seguridad más alto. Proceso realizado por la UCCI no por la Facultad		NO ASIGNADO
A.11.7	**Computación móvil y tele-trabajo**	Asegurar la seguridad de la información cuando se utilice medios de computación móvil y tele-trabajo.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.11.7.1		Computación y comunicaciones móviles	SI	La movilidad es fundamental en las organizaciones, por ello, se deben adoptar las medidas de seguridad apropiadas para la reducción de riesgos.	Documento en donde se detallan las medidas lógicas de seguridad, contra códigos maliciosos. Debidamente autorizado y aprobado por el honorable consejo de facultad	Docente o Departamento a cargo del SGSI/Decanato/HCF
A.11.7.2		Tele-trabajo (trabajo remoto)	NO	Aunque el tele-trabajo es fundamental en la mayoría de organizaciones. La Facultad no se ha acogido a esto formalmente.		NO ASIGNADO

Objetivo 8: A12 Adquisición, Desarrollo y Manteniendo de los Sistemas de Información

A12 ADQUISICIÓN. DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN						
A.12.1	**Requerimientos de seguridad de los sistemas**	Asegurar que la seguridad sea una parte integral de los sistemas de información	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.12.1.1		Análisis y especificación de los requisitos de seguridad	SI	Las mejoras o requerimientos para sistemas existentes o nuevos son un foco de vulnerabilidades, por lo cual se deben especificar los requerimientos de los controles de seguridad.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) que incluya los controles de seguridad en base a los requerimientos. Y Aplicación anual de análisis de riesgo informático en la FACCI	Docente o Departamento a cargo del SGSI/Decanato/HCF
A.12.2	**Procesamiento correcto en las aplicaciones**	Evitar errores, pérdida, modificación no-autoriza o mal uso de la información en las aplicaciones	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.12.2.1		Validación de los datos de entrada	SI	Los datos de entrada pueden incluir contenido erróneo, inapropiado o infectado, por ello dichos datos deben ser validados correctamente.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones que incluya la validación de datos de entrada. Enfocado a la gestión de la calidad de software para proyectos integradores.	Docente o Departamento a cargo del SGSI/Decanato/HCF
A.12.2.2		Control de procesamiento interno	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.		NO ASIGNADO
A.12.2.3		Integridad del mensaje	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.		NO ASIGNADO
A.12.2.4		Validación de los datos de salida	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.		NO ASIGNADO

A.12.3		Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.12.3.1	**Controles criptográficos**	Política sobre el uso de controles criptográficos	SI	Los controles criptográficos permiten proteger la información en todo SGSI. Información confidencial.	Políticas de controles criptográficos y el uso de los mismos para información confidencial en decanato y Honorable consejo de facultad.	Docente o Departamento a cargo del SGSI
A.12.3.2		Gestión de llaves	NO	La Facultad no crea controles criptográficos para proteger la información en el SGSI. Usa otros métodos		NO ASIGNADO
A.12.4		Garantizar la seguridad de los archivos del sistema	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.12.4.1		Control del software operativo	NO	Quien mantiene la seguridad de los archivos del sistema tales como como control de software operativo, protección de los datos de pruebas, y control de acceso a código fuente, es la UCCI no la Facultad.		NO ASIGNADO
A.12.4.2	**Seguridad de los archivos del sistema**	Protección de los datos de prueba del sistema	NO	Quien mantiene la seguridad de los archivos del sistema tales como como control de software operativo, protección de los datos de pruebas, y control de acceso a código fuente, es la UCCI no la Facultad.		NO ASIGNADO
A.12.4.3		Control de acceso al código fuente del programa	NO	Quien mantiene la seguridad de los archivos del sistema tales como como control de software operativo, protección de los datos de pruebas, y control de acceso a código fuente, es la UCCI no la Facultad.		NO ASIGNADO
A.12.5		Mantener la seguridad del software e información del sistema de aplicación	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.12.5.1		Procedimientos de control de cambios	SI	La implementación de cambios trae consigo riesgo de infiltración de malware en la información. Los cuales se deben controlar de forma adecuada ya tiempo.	Procedimientos formales de control de cambios.	Decanato/HCF/Docente o Departamento a cargo del control y seguimiento del SGSI
A.12.5.2	**Seguridad en los procesos de desarrollo y soporte**	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	NO	Los cambios de SO, u otros paquetes de software que se hagan en la Facultad o Universidad está a cargo de la UCCI en conjunto con las autoridades de la Universidad.		NO ASIGNADO
A.12.5.3		Restricciones sobre los cambios en los paquetes de software	NO	Los cambios de SO, u otros paquetes de software que se hagan en la Facultad o Universidad está a cargo de la UCCI en conjunto con las autoridades de la Universidad.		NO ASIGNADO
A.12.5.4		Filtración o fuga de información	SI	La filtración de información es una de las causas principales de ataque en los sistemas, es un riesgo innato que debe ser mitigado.	Planes de sensibilización sobre la protección de la información e Ingeniería social.	Miembro/s del proyecto de SGSI FACCI a cargo
A.12.5.5		Desarrollo de software contratado externamente (outsourced)	SI	El desarrollo de software que ha sido contratado externamente debe ser supervisado y monitoreado por la organización.	Documento con los requisitos mínimos de seguridad para el desarrollo de aplicaciones (línea base) outsourced.	Decanato/HCF
A.12.6		Reducir los riegos resultantes de la explotación de vulnerabilidades técnicas publicadas.	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.12.6.1	**Gestión de vulnerabilidad técnica**	Control de vulnerabilidades técnicas	SI	Para tener un control de los riesgos en los sistemas, es fundamental conocer de manera técnica qué tipo de vulnerabilidades se tienen, tanto en las redes, como en los SI y las aplicaciones.	Documento de planeación y diseño de las pruebas de seguridad periódicas a realizar.	Departamento técnico FACCI/Docente o departamento a cargo del SGSI

Objetivo 9: A13 Gestión de Incidentes en la Seguridad de la Información

A13 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN						
A.13.1	**Reporte de eventos y debilidades en la seguridad de la información**	Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.13.1.1		Reporte de eventos en la seguridad de la información	SI	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad de la información y la gestión sobre éstos, por ello se deben reportar adecuadamente y rápidamente.	Herramienta para la documentación de Incidentes de seguridad y Reportes.	Departamento técnico FACCI/Docente o departamento a cargo del SGSI
A.13.1.2		Reportes sobre las debilidades en la seguridad	SI	Parte fundamental de la gestión de riesgos es las fuentes de incidentes de seguridad y la gestión sobre éstos, por ello se deben reportar adecuadamente	Herramienta para la documentación de Incidentes de seguridad y Reportes.	Departamento técnico FACCI/Docente o departamento a cargo del SGSI
A.13.2	**Gestión de incidentes y mejoras en la seguridad de la información**	Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.13.2.1		Responsabilidades y procedimientos	SI	Se debe establecer las responsabilidades y procedimientos gerenciales de forma efectiva y acertada, para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información	Documento de políticas de seguridad, documento con las responsabilidades de las áreas frente a los incidentes de seguridad.	Decanato/Honorable Consejo de Facultad
A.13.2.2		Aprendizaje de los incidentes de seguridad de la información	NO	Es la UCCI quien debe recopilar los incidentes en la seguridad de la información que permitir aprender de los mismos para mitigar las vulnerabilidades encontradas, y no la Facultad		NO ASIGNADO
A.13.2.3		Recolección de evidencia	NO	La recolección de la evidencia en un incidente de seguridad de la información es fundamental para presentarla en las acciones legales y dar seguimiento a las mismas. Proceso realizado por la UCCI y no por la Facultad.		NO ASIGNADO

Objetivo 10: A14 Gestión de la Continuidad Comercial

A14 GESTIÓN DE LA CONTINUIDAD COMERCIAL						
A.14.1	**Aspectos de la seguridad de la información de la gestión de la continuidad comercial.**	Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.14.1.1		Inclusión de la seguridad de la información en el proceso de gestión de continuidad comercial.	NO	Los aspectos de la seguridad de la información de la gestión de la continuidad comercial, no se toman en cuenta debido a que la Facultad no realiza procesos de continuidad comercial.		NO ASIGNADO
A.14.1.2		Continuidad comercial y evaluación de riesgos	NO	Los aspectos de la seguridad de la información de la gestión de la continuidad comercial, no se toman en cuenta debido a que la Facultad no realiza procesos de continuidad comercial.		NO ASIGNADO
A.14.1.3		Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.	SI	La recuperación ante desastres y los planes de contingencia son fundamentales y dentro de estos, es necesario asegurar la información impulsando el desarrollo del Plan de Continuidad	Plan de contingencia y continuidad. Seguimiento por parte del Honorable Consejo de Facultad.	Docente o departamento a cargo de del SGSI/Decanato/HCF
A.14.1.4		Marco referencial (estructura) para la planificación de la continuidad comercial.	NO	Los aspectos de la seguridad de la información de la gestión de la continuidad comercial, no se toman en cuenta debido a que la Facultad no realiza procesos de continuidad comercial.		NO ASIGNADO
A.14.1.5		Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	NO	Los aspectos de la seguridad de la información de la gestión de la continuidad comercial, no se toman en cuenta debido a que la Facultad no realiza procesos de continuidad comercial.		NO ASIGNADO

Objetivo 11: A15 Cumplimiento

A15 CUMPLIMIENTO						
A.15.1		Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad	APLICA	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.15.1.1	**Cumplimiento con requerimientos legales.**	Identificación de legislación aplicable	SI	Es necesario conocer las reglamentaciones de seguridad a nivel Ecuador y de la Universidad que aplican para el sector de las telecomunicaciones y sistemas informáticos.	Documento con las normas/leyes que aplican al SGSI en Ecuador y la ULEAM.	Docente o departamento a cargo de del SGSI/Decanato/HCF
A.15.1.2		Derechos de propiedad intelectual (DPI)	SI	Es necesario conocer las reglamentaciones de los Derechos de propiedad intelectual a nivel Ecuador que aplican para el sector de las telecomunicaciones y sistemas informáticos.	Documento con las normas/leyes que aplican al SGSI en Ecuador. Derechos de Propiedad Intelectual para TICS. Plan de sensibilización en el cual se brinde capacitación en las políticas propiedad intelectual dadas en el ecuador en el iepi en el caso de sistemas informáticas	Miembro/s del proyecto de SGSI FACCI a cargo/Decanato/HCF
A.15.1.3		Protección de los registros de la organización	NO	Tanto los log, como las herramientas de auditoría y monitoreo deben ser protegidos contra accesos no autorizados, por la UCCI no por la Facultad.		NO ASIGNADO
A.15.1.4		Protección de los datos y privacidad de la información personal	SI	Se debe asegurar la protección y privacidad tal como se requiere en la legislación de Ecuador.	Documento con las normas/leyes de protección y privacidad de los datos y la información.	Docente o departamento a cargo de del SGSI
A.15.1.5		Prevención del uso inadecuado de medios de procesamiento de información	SI	Se deben implementar controles persuasivos y disuasivos en los sistemas/plataformas para que no se utilicen de forma no-autorizado	Documento con los planes de cultura y sensibilización, procedimientos de configuración de los sistemas. Políticas de control de acceso y privilegios. capacitaciones a la comunidad académica en controles persuasivos y disuasivos en los sistemas o plataformas	Miembro/s del proyecto de SGSI FACCI a cargo
A.15.1.6		Regulación de los controles criptográficos	NO	Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes en el Ecuador. Proceso realizado por la UCCI en conjunto con las autoridades de la Universidad.		NO ASIGNADO
A.15.2		Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.15.2.1	**Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico**	Cumplimiento con las políticas y normas de seguridad	SI	Es fundamental tener planes de auditoria, que validen y ajusten los objetivos del SGSI y que se cumplan.	Documento con la planeación de auditorías anuales, incluyendo auditorias técnicas. Verificación de cumplimiento de la declaración de aplicabilidad	Decanato/HCF
A.15.2.2		Verificación del cumplimiento técnico	SI	Es fundamental tener planes de auditoria, que validen y ajusten los objetivos del SGSI	Documento con la planeación de auditorías anuales, incluyendo auditorias técnicas internas y externas. Plantillas de Mantenimiento correctivo y preventivo.	Decanato/HCF
A.15.3		Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad	**APLICA**	**RAZÓN PARA LA SELECCIÓN**	**DOCUMENTO**	**RESPONSABLE**
A.15.3.1	**Consideraciones de auditoría de los sistemas de información**	Controles de auditoría de los sistemas de información	NO	Los log y registros del sistema son fundamentales para el monitoreo y control de la seguridad, así como para investigaciones. Proceso realizado por la UCCI y no por la Facultad.		NO ASIGNADO
A.15.3.2		Protección de las herramientas de auditoría de los sistemas de información	NO	Tanto los log, registros así como las herramientas de auditoría y monitorea deben ser protegidas contra accesos no autorizados. Proceso realizado por la UCCI y no por la Facultad.		NO ASIGNADO

5.2 Resultados Esperados

La declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información a implementarse en la Facultad de Ciencias Informáticas, cuenta con un docente responsable, que es quien se hará cargo del desarrollo de todo el estudio, y del seguimiento del mismo.

Con respecto a los resultados esperados después de presentar el modelo de declaración de aplicabilidad a implementarse en el SGSI en la FACCI, el monitoreo, se va a llevar a cabo por las auditorías internas que se implementaran en el proyecto de investigación (SGSI), quienes verificaran los controles de las normas ISO/IEC a las cuales hace referencia este proyecto. Además de esto, dentro de la Declaración de Aplicabilidad, se suma la columna de Responsable, que es donde se encontrará a la persona a cargo del monitoreo de cada uno de los controles implementados, cumpliendo así los objetivos planteados.

CAPÍTULO VI: CONCLUSIONES

CONCLUSIONES

Una vez finalizado este Trabajo de Titulación correspondiente a la modalidad de Proyecto de Investigación, enfocado en la Elaboración de la Declaración de Aplicabilidad de un SGSI para la FACCI. Podemos concluir lo siguiente:

- Las empresas u organizaciones que manejan cualquier tipo de información valiosa y cuentan con equipos tecnológicos deben someterse a la implementación de un Sistema de Gestión de Seguridad Informática, no solo para proteger sus equipos o su información de cualquier incidente, también para saber qué hacer para proteger resguardada, y hasta recuperar sus activos en caso de pérdida.
- La Elaboración de la Declaración de Aplicabilidad está sometida y depende de otros procesos para poder ser desarrollada, por tal motivo el SGSI usa la metodología PCDA, ésta indica de forma concreta e ilustrativa que procesos llevar a cabo antes de otras, y, qué se necesita para llevarlo a ejecución.
- La Declaración de Aplicabilidad o también conocida como SOA, es denominada uno de los documentos más importantes dentro de un SGSI, sin embargo algunas empresas desconocen de la existencia del mismo, y si la conocen, no le toman la importancia necesaria, esto origina una elaboración de un SGSI incompleto e ineficaz , y por ende lleva a la perdida de activos, por el simple hecho de que se desconocen que controles se deben aplicar en la empresa, en base a que se aplican, y quien es el responsable.
- Si la Facultad u otra empresa u organización quisiera obtener una Certificación ISO/IEC 27001 es indiscutible que se necesita de forma obligatoria el SOA, mismo documento que es solicitado en cualquier auditoria o proceso de Certificación donde intervenga las TIC.

REFERENCIAS BIBLIOGRÁFICAS

1. Referencias Bibliográficas

Bibliografía

Iranzo, M. (2015). *Adaptando a la ISO 27001:2013- Declaración de aplicabilidad.*

Kosutic, D. (s.f.). *La importancia de la Declaración de aplicabilidad para la norma ISO 27001.*

Mancera, G. (2013). *Declaración de Aplicabilidad.*

Mendoza, M. Á. (2015). ¿Qué es una declaración de Aplicabilidad (SoA) y para qué sirve? *WeLiveSecurity*.

Zuccardi, G., & Gutiérrez, J. D. (2006). *ISO 27001:2005.* Obtenido de: pegasus.javeriana.edu.co/~edigital/Docs/ISO27001/ISO27001.doc

Ávila, T.M. (14 de Septiembre del 2012). ¿Qué es la Declaración de Aplicabilidad, en un SGSI sobre ISO 27001?. Recuperado de: http://www.doitsmart.es/wiki/que-es-la-declaracion-de-aplicabilidad-en-un-sgsi-sobre-iso-27001/

Fernández, J.M. (2006). Sistema de Gestión de Seguridad de la Información según ISO 27001: 2005. Obtenido de: https://es.slideshare.net/jhonny14/iso27001-norma-e-implantacion-sgsi?from_action=save

Díaz, M. (sf). ISO 27001: ¿Hacia un cumplimiento obligatorio? Obtenido de: http://www.iso27000.es/download/ISO_27001_cumplimiento.pdf

ISOTOOLS (sf.). Sistemas de Gestión de Riesgos y Seguridad. Obtenido de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO Tools Excellence. (sf). Comparativa entre la ISO 27001:2013 y la ISO 27001:2005. Obtenido de: https://www.pmg-ssi.com/2015/02/comparativa-entre-la-iso-270012013-y-la-iso-270012005/

ISO Tools. (sf). La Gestión de la Seguridad de la Información, más ágil que nunca. Obtenido de: https://www.isotools.org/software/riesgos-y-seguridad/iso-27001

Advisera. (sf). ¿Qué es norma ISO 27001? Obtenido de: https://advisera.com/27001academy/es/que-es-iso-27001/

BSIGroup. (sf). Norma ISO/IEC 27001- Gestión de la Seguridad de la Información. Obtenido de: https://www.bsigroup.com/es-ES/Seguridad-de-la-Informacion-ISOIEC-27001/

Wikipedia. (sf). ISO/IEC 27001. Obtenido de: https://es.wikipedia.org/wiki/ISO/IEC_27001

Mancera, G. (2013). Declaración de Aplicabilidad. Obtenido de: https://prezi.com/j1dsa2a6jkct/declaracion-de-aplicabilidad/

ISO Tools. (2013). La importancia de la Declaración de Aplicabilidad en un SGSI. Obtenido de: https://www.isotools.org/2013/05/29/la-importancia-de-la-declaracion-de-aplicabilidad-en-un-sgsi/

Iranzo, M. (2015). Adaptando a la ISO 27001:2013 – Declaración de aplicabilidad. Obtenido de: https://www.securityartwork.es/2015/05/18/adaptando-a-la-iso-270012013-declaracion-de-aplicabilidad/

ISO Win. (sf). La Declaración de Aplicabilidad en la norma ISO 27001 2017. Obtenido de: https://isowin.org/blog/declaracion-aplicabilidad-ISO-27001/

Mendoza, M.A. (2015). ¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve? Obtenido de: https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

ANEXOS

ANEXO 1: **Objetivo de Control y Controles (3.1.5)**

A.5 Política de seguridad		
A.5.1 Política de seguridad de información Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.

Tabla 10: A.5 Políticas de Seguridad
Fuente: www.iso27000.es

A.6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo*:* Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.

A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.
A.6.2 Entidades externas Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.

A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.

Tabla 11: A.6 Organización de la Seguridad de la Información
Fuente: www.iso27000.es

A.7 Gestión de Activos		
A.7.1 Responsabilidad por los activos Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad'3 de una parte designada de la organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

A.7.2 Clasificación de la información Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.

Tabla 12: A.7 Gestión de Activos
Fuente: www.iso27000.es

A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo[4] Objetivo*:* Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 Durante el empleo Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros

		deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de Derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.

Tabla 13: A.8 Seguridad de los Recursos Humanos
Fuente: www.iso27000.es

A.9 Seguridad física y ambiental		
A.9.1 Áreas seguras Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.

A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 Seguridad del equipo Objetivo*:* Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del- local	Control Se debe aplicar seguridad al equipo fuera-del- local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o

		sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.

T**abla 14:** A.9 Seguridad Física y Ambiental
Fuente: www.iso27000.es

A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Control Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4	Separación de los medios de Desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		

A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.
A.10.2.3	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la re-evaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 Protección contra software malicioso y código móvil Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.

A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
A.10.5 Respaldo (back-up) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	*Back-up o respaldo de la información*	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 Gestión de seguridad de redes Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestión de medios Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.

A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema	Control Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		
A.10.8.1	Procedimientos y políticas de Información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		

A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en - línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o re-envío no-autorizado del mensaje.
A.10.9.3	Información disponible públicamente	Control Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	*Registro de auditoria*	Control Se deben producir registros de la actividades de auditoria, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	*Uso del sistema de monitoreo*	Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.

A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.

Tabla 15: A.10 Gestión de las Comunicaciones y Operaciones
Fuente: www.iso27000.es

A.11 Control de acceso		
A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		
A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de Pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control de conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de 'routing' de redes	Control Se deben implementar controles 'routing' para las redes para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de

		inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y tele-trabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y tele-trabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.

Tabla 16: A.11 Control de Acceso
Fuente: www.iso27000.es

A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de Procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

A.12.3.2	Gestión clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del software e información del sistemade aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.

A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

Tabla 17 A.12: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
Fuente: www.iso27000.es

A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo*:* Asegurar que la información de loseventos y debilidades en la seguridad dela información asociados con los sistemas deinformación sea comunicada de una manera que permita tomar una acción correctiva oportuna.		
A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		

A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.

Tabla 18 A.13: Gestión de Incidentes en la Seguridad de la Información
Fuente: www.iso27000.es

A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el procesode gestión de continuidad comercial	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y Evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de

		dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.

Tabla 19: A.14 Gestión de la Continuidad Comercial
Fuente: www.iso27000.es

A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo*:* Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación aplicable	Control Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.

A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	*Cumplimiento con las políticas y estándares de seguridad*	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	*Chequeo de cumplimiento técnico*	Control Los sistemas de información deben chequearse

		regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoria de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría de los sistema de información.		
A.15.3.1	Controles de auditoria de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorias que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoria de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

Tabla 20: A.15 Cumplimiento
Fuente: www.iso27000.es