UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ

FACULTAD DE CIENCIAS INFORMÁTICAS

TRABAJO 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 LA NORMA ISO 27001"

TAREA INVESTIGATIVA:

"PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN PARA MINIMIZAR LOS RIESGOS INFORMÁTICOS EN LA FACULTAD DE CIENCIAS INFORMÁTICAS"

AUTORAS:

Rodríguez Zambrano Joselyne Elizabeth

Sánchez Montes Diana Fernanda

DIRECTOR: Ing. Larrea Plua Johnny, PhD

CO-DIRECTOR: Ing. Bazurto Roldán José, PhD

MANTA – MANABI – ECUADOR

2019

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
Creada el 13 de noviembre de 1985 mediante Decreto Ley No.10, publicado en el Registro Oficial No. 313
FACULTAD DE CIENCIAS INFORMÁTICAS
Creada, Resolución H. Consejo Universitario del 11 de Julio del 2001

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

"PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN PARA MINIMIZAR LOS RIESGOS INFORMÁTICOS EN LA FACULTAD DE CIENCIAS INFORMÁTICAS"

Tribunal examinador que declara APROBADO el Grado de INGENIERA EN SISTEMAS, de las señoritas: RODRÍGUEZ ZAMBRANO JOSELYNE ELIZABETH y SÁNCHEZ MONTES DIANA FERNANDA

Dra. Dolores Muñoz Verduga _____

Dr. Jorge Herrera Tapia _____

Ing. Juan Carlos Sendón _____

Manta, 28 de febrero de 2019

CERTIFICACIÓN

En nuestra condición de Director y Co-Director de tesis, certificamos que el Trabajo de Investigación presentado por las señoritas: Rodríguez Zambrano Joselyne Elizabeth y Sánchez Montes Diana Fernanda, cuyo tema es: **"PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN PARA MINIMIZAR LOS RIESGOS INFORMÁTICOS EN LA FACULTAD DE CIENCIAS INFORMÁTICAS"** ha sido desarrollado de acuerdo a las normativas vigentes para el desarrollo de una investigación.

Damos fe que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación y evaluación por parte del jurado examinador que se designe.

Atentamente:

_____

Ing. Johnny Larrea Plúa
Director

_____

Ing. José Bazurto Roldán
Co-Director

DEDICATORIA

Este proyecto de titulación se lo dedico a esas personas, que me han apoyado durante todo este proceso y son especiales en mi vida, quiero dedicarles esto a ellos por ser parte este sueño tan importante.

Principalmente a mis padres Eliana Zambrano y Yoffre Rodríguez que con amor y rigor han sabido guiarme, amarme, consentirme, sacrificando todo sin dudarlo, sin ellos no fuera la persona que soy en este punto de mi vida.

A mi abuelita Zoila Loor y mi tía Tania Zambrano que son mis consejeras, mis cómplices y son mi pilar de apoyo muy especial.

A mi hermano Joffre Rodríguez ya que, por ser su ejemplo, su guía necesito ser mejor cada día y demostrarle que se puede mientras se quiera.

A mis padrinos tíos, Mariuxi Moreira y Antonio Zambrano que me han inspirado a superarme, me han brindado todo su amor y ayuda sin importar cuando o donde.

A toda mi familia por enseñarme como es la vida, porque con sus consejos y palabras de aliento hicieron de mí una mejor persona, así poder cumplir todos mis sueños.

A mi compañera de este gran proyecto Diana Sánchez que ella hizo esto posible, dándome el hombro y brindándome aliento durante todo este camino lleno de sorpresas, ahora estamos juntas cumpliendo esta meta importante en nuestras vidas.

A mi compañero especial David Cedeño gracias por su cariño y apoyo incondicional durante todo este proceso, brindándome su compañía en los momentos llenos de lágrimas, risas, derrotas y triunfos, siendo cómplices durante el proceso de titulación.

Si querer olvidarme de nadie le dedico esto a aquellas personas que pasaron por mi vida y dejaron una gran huella, a mis profesores, a mis amigos(as), a mis compañeros(as), a mis compadres y comadres por apoyarme cuando más lo necesite, por enseñarme y demostrarme que la vida es fácil cuando se tiene a gente con quien compartirla. Por eso este triunfo es para ustedes.

Siempre los llevare en mi corazón.

Joselyne Elizabeth Rodríguez Zambrano

DEDICATORIA

El presente trabajo investigativo está dedicado a mi madre, por su amor, sacrificio en todos en estos años y en especial, por haber sido una guía a lo largo de mi carrera universitaria y de mi vida.

A mis profesores, por su tiempo y por la sabiduría transmitida en el desarrollo de mi formación profesional. A mi compañera por el equipo que formamos logramos llegar hasta el final del camino.

A todas las personas que me han apoyado acompañándome en esta etapa y han hecho que este trabajo se realice con éxito, principalmente a aquellos que me abrieron las puertas y compartieron sus conocimientos.

Diana Fernanda Sánchez Montes

AGRADECIMIENTO

En primer lugar, le agradezco a dios por permitirme ser parte de este proceso, por prestarme vida, paciencia y fuerzas para llegar a cumplir esta meta.

A toda mi familia por confiar en mí, por sus consejos y palabras de aliento que fueron mi motor en este proceso.

Mi profundo agradecimiento a todos lo que hicieron parte de este grupo de investigación en especial a él Ing. Johnny Larrea y él Ing. José Basurto quienes con su enseñanza de sus valiosos conocimientos hicieron posible el desarrollo y éxito de este proyecto, muchas gracias por su paciencia, apoyo incondicional y amistad.

A Diana Sánchez mi dupla perfecta, con su compresión y apoyo incondicional formamos un grupo excelente de trabajo integrando conocimientos, aptitudes y destrezas para hacer posible este proyecto.

De igual manera mis agradecimientos a las Universidad Laica Eloy Alfaro de Manabí, a toda la Facultad de Ciencias Informáticas por brindarme la guía y el conocimiento necesario para ser de mi un gran profesional, de manera especial a los decanos que fueron mis consejeros, a mis profesores por impulsar mis fortalezas y el personal administrativo por permitirme disfrutar de tantas oportunidades y anécdotas, eternamente agradecida de ser parte de la familia FACCI.

Joselyne Elizabeth Rodríguez Zambrano

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos los que formamos el grupo de investigación. Por ello agradezco a mis directores de trabajo de titulación, quienes con su experiencia, conocimiento y motivación nos orientaron en la investigación.

A mi compañera Elizabeth con cada una de sus valiosas aportaciones hicieron posible la realización de este proyecto y por la gran calidad humana. Y demás compañeros de clases por su amistad desinteresada.

A mi madre por confiar y creer mis expectativas, por los consejos, valores y principios que me ha inculcado.

Un eterno agradecimiento a esta prestigiosa universidad la cual abre sus puertas a jóvenes como yo, preparándonos para un futuro competitivo y formándonos como personas de bien.

A la Facultad de Ciencias Informáticas por haberme brindado tantas oportunidades, enriquecerme en conocimiento y concluir con una etapa de mi vida, y en especial, por dejarme pertenecer a esta gran familia FACCI.

A los docentes por haber compartido sus conocimientos a lo largo de la preparación de mi profesión. Gracias a todas las personas que fueron partícipes de este proceso, ya sea de manera directa o indirecta.

De igual forma agradezco a quien lee este apartado y más de este trabajo de titulación, por permitir a mis experiencias, investigaciones y conocimiento, sean parte de su formación. Finalmente, gracias a la vida por este nuevo triunfo.

Diana Fernanda Sánchez Montes

ÍNDICE

RESUMEN 17
ABSTRACT 18
CAPÍTULO I: INTRODUCCIÓN 19
CAPÍTULO II: PLANTEAMIENTO DE LA INVESTIGACIÓN 22
2.1. Justificación de la investigación 23
2.2. Problema de investigación 24
2.2.1. Preguntas de investigación 25
2.3. Objetivos 26
2.3.1. Objetivo general 26
2.3.2. Objetivos específicos 26
CAPÍTULO III: REVISIÓN DE LITERATURA 27
4.1. Antecedentes 28
4.2. Marco teórico - conceptual 29
4.2.1. Riesgos, amenazas y vulnerabilidades 29
4.2.2. Normas ISO 33
4.2.3. Políticas de seguridad 36
4.2.4. Sistema de Gestión de Seguridad de la Información (SGSI) 38
4.2.5. Estrategias de Seguridad Informática 38
4.2.6. Sensibilización 43
4.2.7. Comunicación 44
4.2.8. Capacitación 47
4.2.9. Diferencia Sensibilización, Comunicación y Capacitación 48
4.2.10. Beneficios de la Sensibilización, Comunicación y Capacitación 49
CAPÍTULO IV: METODOLOGÍA 50
4.1. Preliminar 51
4.2. Diseño 51
4.3. Población 58
4.4. Métodos e instrumentos de investigación 58
4.4.1. Métodos 58
4.4.2. Instrumentos de investigación 60
4.5. Análisis de los datos 61
CAPÍTULO V: RESULTADOS 64
3.1. Análisis de resultados previo a la propuesta 65
3.1.1. Análisis de Riesgo de los Activos Informáticos 65
3.1.1.1. Riesgos generales por activos informáticos 65
3.1.1.2. Riesgos por Áreas 66
3.1.1.3. Riesgos por Laboratorios 67

3.1.1.4. Riesgo por Aulas 68
3.1.2. Análisis de la Declaración de Aplicabilidad 68
3.1.2.1. Análisis Declaración de Aplicabilidad: Riesgos generales por activos informáticos 69
3.1.2.2. Riesgos por Áreas 70
3.1.2.3. Riesgos por Laboratorios 71
3.1.2.4. Riesgos por Aulas 72
3.1.3. *Medidas de Control de los Activos Informáticos de la FACCI* 73
3.1.3.1. Riesgos generales por activos informáticos 74
3.1.3.1. *Riesgos por Áreas* 89
3.1.3.2. Riesgos por Laboratorios 98
3.1.3.3. Riesgos por Aulas 110
3.2. Plan de Sensibilización, Comunicación y Capacitación 113
3.2.1. Introducción 113
3.2.2. Justificación 113
3.2.3. Objetivo 114
3.2.3.1. Objetivo General 114
3.2.3.2. Objetivos Específicos 114
3.2.4. Metas 114
3.2.5. Destinatarios 115
3.2.6. Estrategias y actividades 116
3.2.6.1. Comunicación Interna 117
3.2.6.2. Responsable de comunicación 120
3.2.7. Herramientas 121
3.2.8. Presupuesto 129
3.2.9. Cronograma 130
3.2.10. Seguimiento y evaluación de resultados 133
3.2.11. Aspectos legales 134
3.2.12. Glosario 135
CAPÍTULO VI: CONCLUSIONES, LIMITACIONES Y RECOMENDACIONES 138
6.1. Conclusiones 139
6.2. Limitaciones 140
6.3. Recomendaciones 141
REFERENCIAS BIBLIOGRÁFICAS 143
ANEXOS 146

LISTA DE TABLAS

Tabla 1. *Análisis de vulnerabilidad con valoración* 32
Tabla 2. *Análisis de riesgo de los activos informáticos: Riesgos generales de los activos informáticos* 65
Tabla 3. *Análisis de riesgo de los activos informáticos: Áreas* 66
Tabla 4. *Análisis de riesgo de los activos informáticos: Laboratorios* 67
Tabla 5. *Análisis de riesgo de los activos informáticos: Aulas* 68
Tabla 6. *Análisis del informe: declaración de aplicabilidad por riesgos generales de los activos informáticos* 69
Tabla 7. *Análisis del informe: declaración de aplicabilidad por Áreas* 70
Tabla 8. *Análisis del informe: declaración de aplicabilidad por Laboratorios* 71
Tabla 9. *Análisis del informe: declaración de aplicabilidad por Aulas* 72
Tabla 10. *Medidas de control de los activos informáticos de la FACCI por Riesgos generales de los activos informáticos* 74
Tabla 11. *Medidas de control de los activos informáticos de la FACCI por Áreas* 89
Tabla 12. *Medidas de control de los activos informáticos de la FACCI por Laboratorios* 98
Tabla 13. *Medidas de control de los activos informáticos de la FACCI por Aulas* 110
Tabla 14. *Tabla de alcance de objetivos* 114
Tabla 15. *Estrategias y actividades para cumplir objetivos* 117
Tabla 16. *Documento Medidas de Seguridad de SGSI* 123
Tabla 17. *Documento Plan de Mantenimiento* 123
Tabla 18. *Documento Plan de Continuidad* 123
Tabla 19. *Documento Plan de Contingencia* 124
Tabla 20. *Documento Lineamientos del Buen Uso de Activos* 124
Tabla 21. *Documento Procedimientos de Control* 124
Tabla 22. *Documento Requisitos para el desarrollo de aplicaciones y sistemas* 125
Tabla 23. *Documento Pruebas e Informes de Seguridad* 125
Tabla 24. *Documento Inventario de Activos* 126
Tabla 25. *Documento Seguridad Física* 126
Tabla 26. *Documento Procedimientos Generales para el Manejo, Almacenamiento y Comunicación de Información* 127
Tabla 27. *Documento Registro de Actividades* 127
Tabla 28. *Documento Informe de Auditoría* 128
Tabla 29. *Documento Procesos Disciplinarios* 128
Tabla 30. *Presupuesto para las actividades del Plan* 129
Tabla 31. *Cronograma de Sensibilización* 130
Tabla 32. *Cronograma de Talleres de Capacitación* 131
Tabla 33. *Tabla para el seguimiento y evaluación de resultados del Plan* 133

LISTA DE ILUSTRACIONES

Ilustración 1. Ejemplos de Activos 30
Ilustración 2. Clasificación de normas ISO 34
Ilustración 3. Diseño de la investigación. 53
Ilustración 4. Fases y etapas de la investigación cualitativa 55
Ilustración 5. Diseños de la investigación-acción 58
Ilustración 6. Directrices del análisis cualitativo 62
Ilustración 7. Destinatarios 115
Ilustración 8. Herramientas del Plan 121

SIGLAS

ULEAM: Universidad Laica Eloy Alfaro de Manabí

FACCI: Facultad de Ciencias Informáticas

SGSI: Sistema de Gestión de la Seguridad de la Información:

TIC: Tecnologías de la Información y la Comunicación

ISO: International Organization for Standardization / Organización Internacional de Estandarización

IEC: International Electrotechnical Commission / Comisión Electrotécnica Internacional

GLOSARIO

A

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]

Análisis: Descomposición de un todo en sus partes para su estudio.

Aplicación: Programa que realiza una serie de funciones y con el cual trabajamos en el ordenador.

B

Backup: Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información o ficheros en varios disquetes y que además la comprime.

C

Clasificación: Distribución de los datos en grupos según su tipo: cualitativos y cuantitativos.

Control de acceso: Definido como los medios para asegurar que el acceso a los bienes está autorizado y restringido a los requisitos de seguridad de la empresa.

Correo electrónico: Mensajes, documentos, archivos que se envían personas a través de Internet o de una red.

CPU (Unidad Central de Proceso): Carcasa donde van montados los principales componentes del ordenador. Puede ser de sobremesa, minitorre, semitorre y torre.

D

Declaración de aplicabilidad: Se refiere a los resultados de las evaluaciones de riesgos de la información y, en particular, a las decisiones sobre el tratamiento de dichos riesgos. Puede tomar la forma de una matriz que identifica varios riesgos de información en un eje y opciones de tratamiento del riesgo en el otro. También muestra cómo se deben tratar los riesgos, y quién es responsable de los mismos.

Disponibilidad: Definido como la información accesible y utilizable bajo solicitud de un organismo autorizado para ello.

Documento: Soporte material de una información que constituye una fuente de consulta.

E

Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente. [CE 052]

Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos. [CE 052]

Entrenamiento: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.

Evaluación de riesgos: Identificación, análisis y evaluación de riesgos de todo el proceso.

F

Frecuencia: Tasa de ocurrencia de una amenaza.

G

Gestión de riesgos: Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos. [Magerit:1997]

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [Guía ISO/IEC 73:2002]

H

Hacker: Informáticos que utilizan sus grandes conocimientos para traspasar cualquier barrera informática.

I

Indicadores: o medidores "Conjunto de mediciones realizadas al proceso para medir tanto las actividades como los resultados del proceso. Los indicadores suelen enfocarse en los aspectos de eficacia y eficiencia".

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro. [ArCert]

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento. [17799:2002]

Integridad de la información: debe ser precisa, coherente y completa desde su creación hasta su destrucción. [CE 052]

Impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

L

Línea de investigación: Área temática amplia o problemática general de la cual se derivan proyectos de investigación que se relacionan por complementariedad y secuencia temporal.

M

Metodología: Término que posee distintas acepciones:

- Estudio o tratado de método.
- Conjunto de métodos empleados.
- Serie de técnicas, instrumentos y procedimientos utilizados en una investigación. Esta última acepción es la adoptada en esta guía.

O

Ofimática: Dícese de la informática y la tecnología aplicada a la oficina.

P

Política: Declaraciones de alto nivel que expresan los objetivos a cumplir de la Entidad respecto a algún tema en particular.

Programa: Grupo de instrucciones que sirven para realizar determinadas tareas. También llamadas aplicaciones.

Protocolo: Conjunto de normas que los equipos utilizan para comunicarse entre sí a través de una red y poder hablar el mismo idioma.

R

Regulador de voltaje: Es un dispositivo que tiene varios enchufes, se encarga de mantener el voltaje estabilizado y libre de variaciones (el voltaje es la fuerza con que son impulsados los electrones a través de los cables de la red eléctrica), ello porque comúnmente la electricidad llega con variaciones que provocan desgaste de los elementos electrónicos a largo plazo en las fuentes de alimentación de las computadoras y elementos electrónicos. Lo que el regulador hace es estabilizar la electricidad a un nivel promedio constante para que no provoque daños en los equipos.

Riesgo: Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

Routers: Dispositivos de red cuya misión principal es encaminar los paquetes de información que reciben en la dirección adecuada para que alcancen su destino.

Ruta de acceso (Path - Camino o Trayectoria): Forma para llegar hasta un lugar o una ubicación determinada, partiendo de una unidad específica, por carpetas y nombre de archivo.

S

Seguridad informática: La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Seguridad de la información: La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información. se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Sensibilización: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

Servidor DHCP: Es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responderá a dichas peticiones proporcionando los parámetros que permitan a los clientes auto-configurarse. Para que un PC solicite la configuración a un servidor, en la configuración de red de los PC's hay que seleccionar la opción 'Obtener dirección IP automáticamente'.

Sistema: Conjunto formado por el hardware y software que componen la parte esencial del ordenador.

Sistema operativo: Programa primario que debe tener un ordenador para que las demás aplicaciones puedan funcionar.

Software: Partes blandas de un ordenador o soportes donde se almacenarán los datos generados con éste.

T

Tarjeta de red: Hardware que se inserta en un equipo para conectarlo a una red.

TCP/IP: Protocolo de Internet (Protocolo de Control de Transmisión/Protocolo Internet) que especifica cómo se transmiten los datos en Internet para que todos los sistemas hablen el mismo idioma en Internet.

U

Unidad: Dispositivo físico de almacenamiento de los datos. Por lo general se les nombra mediante una etiqueta o nombre (A: C: D:).

Unidad Central de Proceso (CPU): Carcasa donde van montados los principales componentes del ordenador.

Usuario remoto: Persona que se conecta a una red mediante un módem y Acceso telefónico a redes.

Utilidad: Programa que complementa o mejora las funciones de un sistema operativo o de un programa concreto.

V

Virus: Programas informáticos diseñados con mala intención, ya que se convierten en parásitos capaces de infectar a otros para incluir una copia evolucionada de sí mismos.

RESUMEN

El presente trabajo forma parte de una de las tareas investigativas del proyecto, "Sistema de Gestión de Seguridad de la Información bajo Normas ISO/IEC 27001", implementado en la Facultad de Ciencias Informáticas de la Universidad Laica Eloy Alfaro de Manabí.

Esta investigación para su desarrollo se usó como insumos, la información de las otras tareas previas realizadas por estudiantes investigadores, tales como los resultados obtenidos del análisis de riesgos informáticos y la declaración de aplicabilidad. Una de las finalidades de la implementación del SGSI es minimizar la materialización de estos aspectos a través de la definición e implementación de controles, medidas y políticas fundamentadas en las normas ISO.

La falta de medidas y controles contribuyen a la deficiencia de la gestión de seguridad informática, por lo que, a través del desarrollo de propuestas de medidas se propone mitigar los riesgos informáticos de la FACCI.

Para la reducción y mitigación de los riesgos informáticos a nivel de hardware, software e información esta investigación desarrolló un Plan de Sensibilización, Comunicación y Capacitación dirigido a la comunidad de la FACCI con la finalidad de implementar una serie de medidas y controles que deben ser ejecutados y supervisados técnicamente.

Para el logro de los objetivos de esta investigación se identificaron los riesgos, amenazas y vulnerabilidades, posterior a esto se clasificaron y analizaron para ver su aplicabilidad de acuerdo con las normas ISO/IEC. El resultado de esta actividad es la que nos proporcionó la información para la elaboración de nuestro Plan de Sensibilización, Comunicación y Capacitación con sus respectivos lineamientos técnicos para el buen uso de los activos informáticos.

Palabras claves: riesgos informáticos, medidas de seguridad, normas ISO, plan, sensibilización, comunicación, capacitación

ABSTRACT

The present work is part of one of the research tasks of the project, "Information Security Management System under ISO/IEC 27001 Standards", implemented in the Faculty of Computer Science of the "Laica Eloy Alfaro de Manabí" University.

This research for its development used as inputs the information of the other previous tasks carried out by student researchers, such as the results obtained from the analysis of computer risks and the declaration of applicability. One of the purposes of the implementation of the ISMS is to minimize the materialization of these aspects through the definition and implementation of controls, measures and policies based on ISO standards.

The lack of measures and controls contribute to the deficiency of information security management, which is why, through the development of proposed measures, it is proposed to mitigate the IT risks of the FACCI.

For the reduction and mitigation of computer risks at the hardware, software and information level, this research developed a Plan of Awareness, Communication and Training directed to the FACCI community with the purpose of implementing a series of measures and controls that must be executed and technically supervised.

To achieve the objectives of this research, the risks, threats and vulnerabilities were identified, after which they were classified and analyzed to see their applicability in accordance with ISO / IEC standards. The result of this activity is the one that provided us with the information for the elaboration of our Awareness, Communication and Training Plan with its respective technical guidelines for the proper use of computer assets.

Keywords: computer risks, security measures, ISO standards, plan, awareness, communication, training

CAPÍTULO I:
INTRODUCCIÓN

INTRODUCCIÓN

En el año 2018, la Facultad de Ciencias Informáticas, recibió la aprobación de uno de los proyectos de investigación denominado: Sistema de Gestión de la Seguridad de la Información, bajo la Norma ISO/IEC 27001. Una de las tareas finales de este proyecto es la elaboración de un Plan de Sensibilización de seguridad, que permita minimizar los riesgos informáticos en la FACCI con la finalidad de proteger de manera adecuada los activos informáticos de la Facultad mediante la implementación y difusión de controles, medidas y políticas basadas en normativas internacionales.

La propuesta del plan se basa en la planificación estratégica y eficaz de las actividades y/o, herramientas de comunicación y difusión divididas en temáticas acordes a la seguridad del hardware y software, primordiales para el desempeño de las labores académicas y administrativas, salvaguardando la información generada en ambos aspectos.

La falta de medidas y controles de seguridad, inciden en una posible materialización de riesgos informáticos que pueden ser provocados por personas o de índole natural. Estas vulnerabilidades o debilidades de los activos informáticos pueden causar una afectación o daño en estos, por ende, perjudicar las actividades académicas, administrativas y de servicios en la Facultad.

Esta tarea investigativa es parte del proyecto de Sistema de Gestión de la Seguridad de la Información, bajo la Norma ISO/IEC 27001, los insumos para la elaboración del plan, se consideraron los resultados obtenidos de tareas investigativas previas realizadas por otros investigadores (Docentes y estudiantes), tales como como el análisis de riesgos y la Declaración Aplicabilidad según las normas ISO.

La fundamentación teórica de esta tarea se basa en aspectos relacionados con la seguridad informática tal como recursos literarios de trabajos con similitud al presentado, así como de las normativas internacionales. Debido a la naturaleza documental, en el marco de la metodología se adoptó un diseño de investigación con un enfoque cualitativo, aplicando técnicas, instrumentos y estrategias proporcionados por dicho enfoque.

Una de las limitantes presentadas en el desarrollo de la investigación, ocurrió al inicio de ésta, ya que la temática sufrió variaciones debido a que no tenía aporte investigativo, lo que ocasionó que el tema de la tarea investigativa sufriera variantes.

La estructura de trabajo está divida en capítulos. En el número I, se describe a manera introductoria una visión general de esta tarea investigativa; en el capítulo II se describe la problemática, se justifica y se plantean los objetivos de posible solución de la tarea de investigación. En el capítulo III, se proporciona información científica que sustenta nuestra tarea investigativa.

Continuando, en el capítulo IV se indica la Metodología que incluye aspectos relacionados con el paradigma investigativo, métodos y la estrategia investigativa para conseguir los objetivos; en el capítulo V muestra los Resultados que son producto de la realización de actividades tales como recogida de los datos, análisis y el tratamiento. Finalmente, en el capítulo VI se presentan las Conclusiones, Limitaciones y Recomendaciones dirigidas a las autoridades, personal académico y administrativo de la Facultad de Ciencias Informáticas.

CAPÍTULO II:

PLANTEAMIENTO DE LA INVESTIGACIÓN

2.1. Justificación de la investigación

Debido al avance de la tecnología en la actualidad, se requieren nuevos mecanismos de seguridad informática que permitan su desarrollo e implementación, la misma que, se va convirtiendo en una necesidad cada vez más latente en las instituciones de educación superior.

Consciente de aquello, 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, denominado "Sistema de Gestión de Seguridad de la Información bajo 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 FACCI, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque informático o desastre natural.

El proyecto se conforma de fases consecutivas denominadas tareas de investigación cuyos resultados deben ser validados y aportan insumos para la siguiente fase investigativa. El presente trabajo corresponde a una de las últimas fases dentro del proyecto, el cual se enfoca en el desarrollo de un Plan de Sensibilización, Comunicación y Capacitación dirigido a la comunidad FACCI.

El plan en cuestión busca, mediante la sociabilización de resultados de ésta e investigaciones anteriores, las cuales involucran: análisis de riesgos, planes de Contingencia y Continuidad, y Declaración de Aplicabilidad, dar a conocer las medidas, políticas y controles de seguridad basadas en la Norma ISO y la Metodología MAGERIT, implementadas en la Facultad con el fin de aportar un nuevo enfoque de responsabilidad tecnológica en cuanto al uso y protección adecuado de los recursos informáticos y por parte del colectivo de la Unidad Académica.

A su vez, este plan brinda toda la información necesaria con respecto al estado actual de la entidad, además de los lineamientos y medidas de control que se deben aplicar para mejorar la seguridad y mitigar los riesgos informáticos dentro de la misma.

La importancia del plan dentro del proyecto de investigación es tomar las vulnerabilidades de mayor riesgo y elaborar propuestas que mitiguen estos riesgos dentro de

la Facultad, específicamente en el sector de seguridad informática, dando a conocer los intereses a implementar con este proyecto, además del cumplimiento con las normativas internacionales.

Al proponer medidas de esta índole, se contribuye a mejorar la gestión del proceso interno de la seguridad informática evitando la materialización de diferentes tipos de riesgos a los que se encuentren expuestos tanto el hardware, software, como la información e incluso el personal como tal. Así mismo, la preparación es un factor crucial en el marco de la seguridad, por lo que, teniendo el personal capacitado e idóneo para manejar estos temas se podría identificar a tiempo dichos riesgos y llevar a cabo la ejecución apropiada de los planes elaborados dentro del proyecto en general.

2.2. Problema de investigación

La Seguridad Informática implica el proceso de proteger contra intrusos el uso de los recursos informáticos con intenciones maliciosas e incluso la posibilidad de acceder a ellos por accidente, misma que, abarca una serie de medidas de seguridad con las cuales se busca minimizar y controlar el riesgo latente al que, dichos recursos se encuentran expuestos.

El proyecto de Seguridad Informática que se está implementando en la FACCI, Sistema de Gestión de la Seguridad de la Información bajo Normas ISO/IEC 27001, permite la protección de la infraestructura computacional, de manera especial a uno de los activos más importantes, como es la información.

Este proyecto se desarrolla mediante la ejecución de diversas tareas de investigación, una de ellas, es la evaluación y tratamiento del riesgo informático de la FACCI y tiene como propósito analizar las amenazas que podemos encontrar en los activos con el fin de prevenir los altos riesgos que se pueden convertir en problemas o imprevistos.

Luego de la detección de las vulnerabilidades, amenazas y riesgos que afectan a los activos informáticos de la Unidad Académica, se comparará con las normas ISO 27001 y se verifica su aplicabilidad a la misma.

Como parte final del proyecto, una de las tareas a implementar es la elaboración de un plan de sensibilización, comunicación y capacitación de seguridad informática dirigida a los usuarios con la finalidad de concientizar sobre las diferentes normativas y acciones a tomar ante los riesgos encontrados y ante cualquier eventual riesgo que se presente.

La falta de medidas de seguridad informática contribuye a que se genere una deficiencia en la gestión del proceso de seguridad, ocasionando que el hardware, software e información sean vulnerables ante cualquier tipo de riesgo informático, así como, robo o pérdida de equipos hardware o la manipulación de los sistemas de software e incluso al mismo personal, que permita el acceso a información confidencial.

Otra problemática de inseguridad informática se debe al gran avance de la tecnología que requiere nuevos mecanismos de seguridad. De igual manera, la falta de personal idóneo que permita identificar los riesgos informáticos. Así mismo, estar preparado para hacer uso del plan de acción que permita mitigar dichos riesgos de acuerdo con las normas ISO 27001.

2.2.1. Preguntas de investigación

General

- ¿Cuál será el impacto que tendrá en la FACCI, el desarrollo e implementación del plan de sensibilización, comunicación y capacitación en la seguridad informática?
- ¿Por qué es importante sociabilizar las medidas, políticas y controles que minimicen los riesgos informáticos en la Facultad de Ciencias Informáticas?

Específicas

1. ¿Cuál es la situación actual de los riesgos, amenazas y vulnerabilidades informáticas en la FACCI?
2. ¿Cuáles son las políticas de la Norma ISO 27001 y medidas de seguridad aplicables para la Facultad?
3. ¿La FACCI, requiere de un plan de sensibilización que concientice a los diversos usuarios?

2.3. Objetivos

2.3.1. Objetivo general

Desarrollar un plan de sensibilización, comunicación y capacitación de Seguridad Informática, que minimice los riesgos informáticos en la Facultad de Ciencias Informáticas.

2.3.2. Objetivos específicos

1. Identificar el estado actual de los riesgos, amenazas y vulnerabilidades de los recursos informáticos de la Facultad de Ciencias Informáticas.
2. Analizar los resultados de los objetivos de control de las normas ISO 27001.
3. Desarrollar el plan de sensibilización, comunicación y capacitación de seguridad informática basadas en las normas ISO 27001.
4. Desarrollar una propuesta de lineamientos para el buen uso de los activos informáticos.

CAPÍTULO III: REVISIÓN DE LITERATURA

4.1. Antecedentes

La presente investigación se enmarca en un proyecto factible de seguridad informática, enfocada en el desarrollo de un plan de sensibilización, comunicación y capacitación para minimizar los riesgos informáticos en la FACCI. De acuerdo con la naturaleza consecutiva del proyecto en general, el cual se encuentra conformado por diversas tareas de investigación, las mismas que han servido como insumos para la elaboración del presente trabajo.

La primera tarea de investigación dentro del proyecto fue realizada por Guerrero Bravo Gema y Mera Evelyn (2018), es: "Evaluación y Tratamiento del Análisis de Riesgos de la Facultad de Ciencias Informáticas" … En este trabajo se revelaron los riesgos y vulnerabilidades existentes, la búsqueda se realizó en base a las normas ISO 27001:2005 y Magerit. Reafirmando que la institución no cuenta con la adecuada seguridad informática que debe ser implementada.

La segunda tarea de investigación fue realizada por Domínguez Víctor (2018), es: "Instauración de un Plan de Contingencia y Continuidad de los Servicios Informáticos que brinda la FACCI" … Este trabajo se trata de la realización de diversos planes que apoya a la continuidad del proyecto, en la cual se desarrolló materiales (tipo formulario), lo cual favorece al control de activos dentro de la institución. Logrando resultados eficientes y así mejorar las condiciones internas de la Facultad.

La tercera tarea de investigación dentro del proyecto realizada por Delgado Kerly (2018), es: "Declaración de Aplicabilidad" … En el desarrollo de este trabajo se consideró de interés establecer las normas que dentro del estudio aplican positivamente para ser implementadas dentro de la institución, estas normas están establecidas en base a la ISO 27001:2005. Para ello es necesario conocer las circunstancias que interceden en el proceso y que favorecen positivamente a la seguridad informática de la Facultad.

Mediante la investigación de María Fernanda Chaparro Ronderos (2016), en su Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones a través de su trabajo de investigación: "Elaboración de un Plan de

Implementación de la ISO/IEC 27001:2013 para la unidad de GST", realiza un plan que pretende reunir la definición de las políticas y los objetivos de seguridad, el análisis diferencial en base a la ISO/IEC 27001:2013 e ISO/IEC 27002.

Donde identifica el valor corporativo de los activos para la metodología de análisis de riesgos y termina con una evaluación de madurez y nivel existente dentro del área de TI de la sede principal de una universidad de Colombia, con el objetivo de establecer las bases de un SGSI teniendo en cuenta que lo que interesa son los Sistemas de Información que dan soporte a actividades y servicios de dicha área. (Chaparro Ronderos, 2016)

4.2. Marco teórico - conceptual

4.2.1. Riesgos, amenazas y vulnerabilidades

A continuación, se identifican y se describen todos los riesgos, amenazas y vulnerabilidades.

Riesgo

Según la Norma ISO 90012 riesgo es el efecto de la incertidumbre en un resultado esperado y se caracteriza a menudo por referencia a potenciales "eventos" y "consecuencias", o una combinación de éstos. De acuerdo con (PÉREZ, 2018), riesgo es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según (ISO Guía 73:2002): es la combinación de la probabilidad de un evento y sus consecuencias. El riesgo se lo puede expresar mediante una fórmula matemática en donde:

$$Riesgo = Amenaza\ x\ Vulnerabilidad$$

Esto nos quiere decir que si estamos en la presencia de una amenaza (peligro) y surge una vulnerabilidad (humana) asociada ante la misma, entonces existe un riesgo. (Soldano, 2008) Sin embargo, los riesgos pueden reducirse o manejarse. Si somos cuidadosos en nuestra relación con el ambiente, y si estamos conscientes de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, podemos tomar medidas para asegurarnos de que las amenazas no se conviertan en desastres.

Riesgos informáticos

Es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control que puedan evaluar el desempeño del entorno informático. (Galeon, 2010)

Elementos del Riesgo

Activos: Un Activo es un objeto o recurso de valor empleado en una empresa u organización. Activo informático es cualquier dato, dispositivo u otro componente del entorno que apoya actividades relacionadas con la información. Los activos incluyen generalmente hardware (servidores y switches), software (por ejemplo, aplicaciones de misión crítica y sistemas de apoyo) e información confidencial. (SO/IEC 13335-1, 2004).

Ejemplo

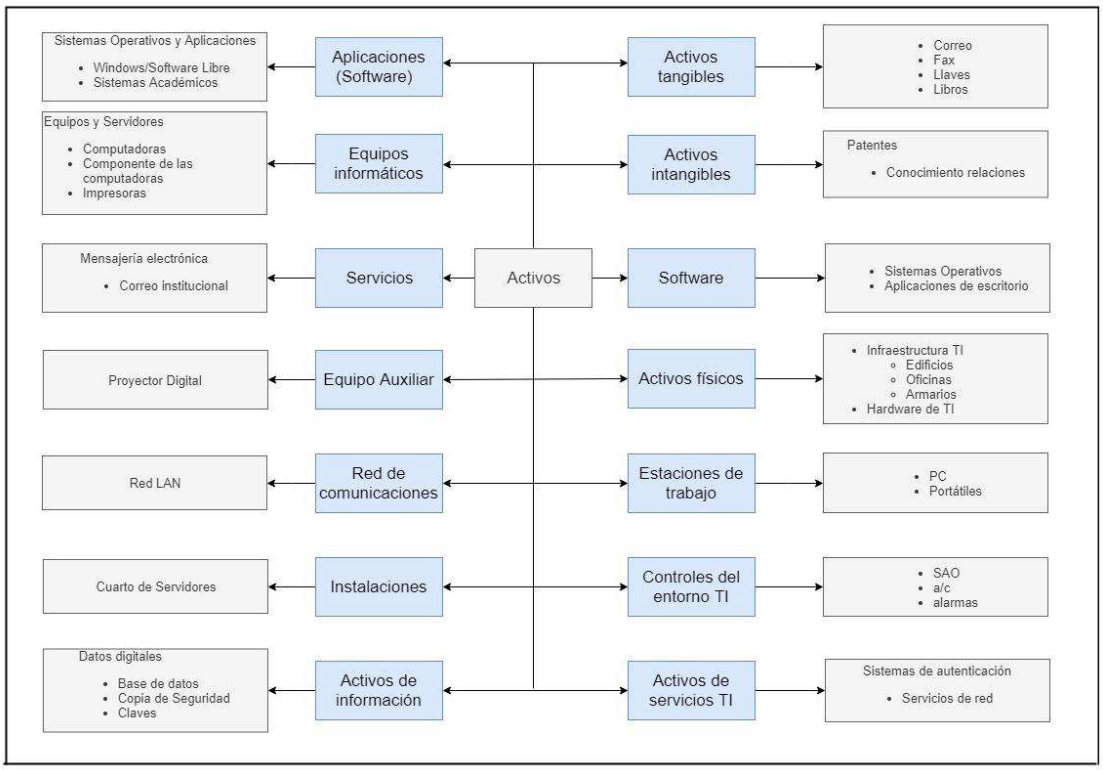

Ilustración 1. Ejemplos de Activos

Ilustración 1.- Se muestra ejemplos de activos.
Fuente: Las autoras de la investigación.

Vulnerabilidad

Una vulnerabilidad es la debilidad de un activo o un conjunto de activos que pueden ser explotado por una amenaza o varias amenazas a un activo. (ISO/IEC 13335-1, 2004)

En cambio, en la ISO 27001:2005 refiriéndose a vulnerabilidad en "Identificar riesgos" nos dice identificar las vulnerabilidades bajo las que podría actuar dichas amenazas. Se entiende que la vulnerabilidad nunca es la consecuencia de la amenaza, sino una situación existente que pudiera ser aprovechada (explotada) por una determinada amenaza. (PÉREZ, 2018)

Ejemplo

En un laboratorio hay 20 las computadoras y están conectadas a Internet, dónde además todas tiene configurada la misma cuenta de correo electrónico a través de la que recibe mensajes diariamente de publicidades (SPAM). También tienen instalado un antivirus que es capaz de chequear los mensajes electrónicos, incluidos los archivos que están adjuntos. Pero el antivirus fue instalado en una versión gratuita y no lo ha vuelto a actualizar en más de un año.

En este caso los equipos son vulnerables a los virus más recientes que puedan llegar mediante el correo electrónico, ya que el antivirus no está actualizado y no sabe que éstos nuevos virus existen.

Pero una cosa sí que es cierta, que exista una vulnerabilidad no significa que se produzca un daño a un equipo de forma automática. Es decir, la computadora tiene un punto flaco, pero no por eso va a fallar, lo único que ocurre es que es posible que alguien ataque el equipo aprovechando ese punto débil**.**

Amenaza

Es un evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.

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

Potencial ocurrencia de eventos o acciones que violentan la integridad, disponibilidad y confidencialidad de la información, que pueden desencadenar un incidente en las personas y/o en la plataforma de una organización, ocasionando pérdidas humanas, daños materiales o pérdidas materiales de sus activos. (Misión Sucre, s.f.)

Ejemplo

En la Facultad de Ciencias Informáticas se necesita analizar un servidor donde se obtuvieron los siguientes datos:

Ubicación inadecuada, y a la vista de todos los que entran a secretaria, pero debería estar en un lugar seguro. La secretaria cuenta con dos ventiladores de techo el cual no abastece para la temperatura necesaria que es entre 17°C y 21°C. Mantenimiento cada ciclo académico.

Sin planta de emergencia al momento de suspenderse la luz en el edificio el servidor dejara de funcionar inmediatamente y podría dañar su contenido.

Con los datos obtenemos la siguiente tabla de vulnerabilidad teniendo en cuenta que 1 es nivel de vulnerabilidad nulo; 2 es nivel de vulnerabilidad bajo; 3 es nivel de vulnerabilidad Medio; 4 es nivel de vulnerabilidad Alto:

Tabla 1. *Análisis de vulnerabilidad con valoración*

Activo	Vulnerabilidad	Nivel de Vulnerabilidad
Servidor de Usuarios	Mala ubicación	3
	Temperatura inadecuada	2
	Mantenimiento constante	2
	Ausencia de planta de energía	4

En la tabla 1 se presenta el análisis de vulnerabilidad estableciendo valoración que va desde la más alta siendo la de mayor gravedad.
Fuente: Las autoras de la investigación

Diferencia entre riesgos, vulnerabilidad y amenaza

La diferencia entre estos términos radica en que la vulnerabilidad se presenta como una debilidad de un sistema o activo informático en cuanto a seguridad, sin que se produzca un daño de forma automática, mientras que un riesgo se lo define como la posibilidad de que se efectúe un ataque a dicho sistema o activo informático, a través de acciones (internas o externas), aprovechando así, ese punto débil existente para causar daño o pérdidas a una organización específica.

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Siendo una combinación de probabilidad de un evento y sus consecuencias. (Universidad Nacional de Luján, 2010)

4.2.2. Normas ISO

ISO (International Organization for Standardization / Organización Internacional de Estandarización) crea documentos que proporcionan requisitos, especificaciones, pautas o características que se pueden usar de manera consistente para garantizar que los materiales, productos, procesos y servicios sean adecuados para su propósito. (ISO.ORG, n.d.)

El objetivo perseguido por las normas ISO es asegurar que los productos y/o servicios alcanzan la calidad deseada. Para las organizaciones son instrumentos que permiten minimizar los costos, ya que hacen posible la reducción de errores y sobre todo favorecen el incremento de la productividad.

Para la sociedad, las normas ISO también son importantes. Existen más de 19.500 normas que ayudan a casi todos los aspectos del día a día de una persona, como aquellas destinadas a garantizar la seguridad vial o la seguridad de los juguetes. Si un producto y/o servicio cumple con alguna de estas normativas, la sociedad puede estar segura de que son fiables y que cuentan con la calidad exigida a nivel mundial. La clasificación de estas normas es:

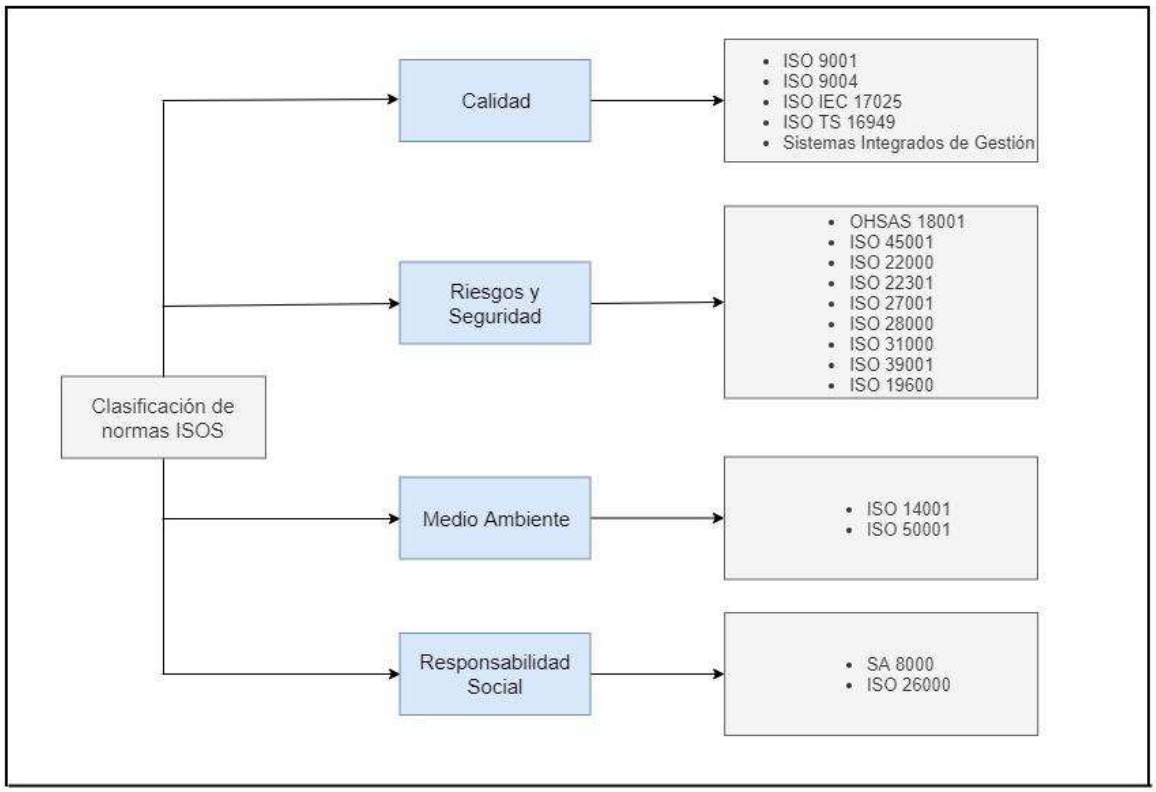

Ilustración 2. Clasificación de normas ISO

Ilustración 2.- Se muestra la clasificación de las normas ISO.
Fuente: Las autoras de la investigación.

En este proyecto usaremos la norma de Riesgos y Seguridad específicamente la ISO 27001 y 17799.

ISO/IEC: 27001

La norma internacional ISO-27001 marca las pautas que se deben de seguir para proceder a la correcta implantación de un SGSI, de manera sistemática, documentada y comunicada a toda la organización. Algunas de las utilidades de un SGSI:

- Asegura la confidencialidad, integridad y disponibilidad de información sensible de la organización.
- Minimiza la incertidumbre por el conocimiento de los riesgos e impactos asociados.
- Mejora periódicamente la gestión de la seguridad de la información.
- Garantizar la continuidad del negocio.
- Incrementa los niveles de confianza de clientes y partners.

- Aumenta la competitividad, lo que supone mejoras en la imagen corporativa.
- Incrementa la confianza de los stakeholders.
- Aumenta la rentabilidad, gracias al control de los riesgos.
- Mejora del cumplimiento legal en materia de seguridad de la información.
- Reducción de las vulnerabilidades que puedan existir.
- Evitar virus informáticos, fraudes, espionajes, vandalismo, etc.
- Mejoran las oportunidades de negocio.

Resumiendo, la implantación de un SGSI según la norma ISO 27001, permite conocer aquellos riesgos a los que esté sometida la organización. De manera que es posible asumirlo y trabajar para minimizarlos y controlarlos de manera ordenada, para seguir en el camino de la mejora continua. (ISOTools Excellence Perú, 2013)

Porque se implementa la ISO 27001

Concretamente, este estándar internacional, nos ayuda a gestionar la seguridad de la información en una organización, sea cual sea el tamaño de esta o su carácter público o privado, dado que ofrece a ésta la metodología necesaria para implantar la seguridad en la gestión de la información.

ISO/IEC:17799

La norma define la seguridad como la preservación de la confidencialidad, integridad y disponibilidad de la información, siendo necesario para ello no solo medidas técnicas sino también políticas y organizativas. Según (Colinas, 2004), para alcanzarla define diez áreas de control:

1. Políticas de seguridad
2. Organización de la seguridad
3. Clasificación y control de activos
4. Seguridad del personal
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones

7. Control de accesos
8. Desarrollo y mantenimiento de sistemas
9. Gestión de la continuidad
10. Conformidad

Cubriendo todo el ámbito de gestión de la seguridad planteando sobre ellas 36 objetivos de control y un total de 127 controles que nos pueden servir para validar el grado de adecuación a la norma. En cualquier caso, es importante darse cuenta de que será una labor prioritaria adaptar la ISO 17799, y más concretamente el peso que se da de queda una de las áreas de la norma, a las características concretas del ámbito de aplicación. (Marín, 2006)

Porque se implementa la ISO 17799

Según (Thorp, 2004), las ventajas observadas de implementar ISO 17799 incluyen:

- Un acceso rápido a la información requiere una documentación clara y un enfoque coherente en las tareas.
- Inculca disciplinas tales como la gestión del riesgo y el mantenimiento de registros, que pueden convertirse en ventajas.
- El ser humano trabaja de forma natural más eficientemente en un marco ordenado y estructurado, al reducirse las suposiciones y la duplicación de esfuerzos y facilitarse el intercambio de información.
- Proporciona herramientas y métodos para que la gerencia y los usuarios compartan una parte de la responsabilidad sobre sus acciones.
- Aporta la base para defender el uso de buenas prácticas

4.2.3. Políticas de seguridad

Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de

una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital. De esta forma mantendremos nuestra organización alejada de cualquier ataque externo peligroso. (Emprende Pyme, 2016)

Políticas de Seguridad Informáticas

Cualquier política de seguridad debe incorporar y contemplar elementos claves como la integridad de los programas, su disponibilidad, la privacidad de las operaciones y los archivos y, finalmente, ejercer un control eficaz y efectivo, garantizar la autenticidad de las comunicaciones y los protocolos y ser útil, pues ninguna medida coercitiva se justifica a sí misma si no es en virtud del principio de utilidad. (Segurode, 2017)

Para que la implementación de unas políticas de seguridad sea exitosas y aceptadas por todos es necesario es que procedamos a realizar una especie de estrategia de mercadeo para hacerles entender al personal las razones por la que se quieren implementar las políticas, los beneficios que podemos obtener y sobre todo involucrar a todo el personal.

De igual manera estas políticas deberían ser integradas en las estrategias de la organización para que los altos ejecutivos reconozcan la importancia de estas y estén en las proyecciones de las organizaciones. (DUARTE.)

Fundamentos de Seguridad Informática

El propósito de la protección de seguridad de la información es proteger los recursos valiosos de una organización, tales como información, hardware y software. A través de la selección y aplicación de candados o protecciones, la seguridad ayuda en la misión de la organización por la protección de sus recursos físicos y financieros, la reputación, la posición legal, empleados y otros activos tangibles e intangibles.

Las normas y procedimientos de seguridad no son elegidos no existen por comodidad, sino que se ponen en marcha para proteger los activos importantes y por lo tanto apoyar los objetivos de negocio. La seguridad es el estado de bienestar de la información e infraestructuras donde se mantiene la posibilidad de no detectada, de que sea manipulada, robada o alterada. (Domanda, Inserimento, Di, & Del, 2012)

La seguridad es un estado de bienestar de las infraestructuras de información y en el que se mantiene la posibilidad de robo de éxito aún no detectada, templado, y la alteración de la información y servicios de baja o tolerable.

- La seguridad se basa en la confidencialidad, autenticidad, integridad y disponibilidad
- Confidencialidad: es el ocultamiento de información o recursos.
- Autenticidad: es la identificación y la garantía de origen de la información
- Integridad: se refiere a la confiabilidad de los datos o recursos en términos de prevenir cambios no autorizados e impropios
- Disponibilidad: se refiere a la capacidad de utilizar la información o recurso deseado

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

Según el artículo (Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001) publicado por la revista tecnológica de la SPOL nos dice que el SGSI, "tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad.

El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados.

4.2.5. Estrategias de Seguridad Informática

Las medidas actuales de seguridad no están diseñadas para realizar un verdadero "Seguimiento de intrusiones", por lo tanto, se debe plantear una nueva línea de pensamiento. Lo crítico, es el absoluto desconocimiento del adversario de lo que surge el

primer desbalance de fuerzas En las operaciones defensivas a lo largo de la historia no se tienen antecedentes de una fortaleza invulnerable. (Estrada & Somolinos, 2011)

Soluciones de prevención

Hay una gran diversidad de ataques y ciberataques que tienen como objetivo dañar, robar o dejar inutilizable la información. Virus, troyanos, spyware y ransomware son sólo algunos ejemplos de ataques directos a la información. (Tecno XXI, 2017)

Es importante, además de generar concientización en seguridad informática, llevar a cabo medidas de prevención contra daños al valioso recurso como:

- No abrir archivos adjuntos de correo electrónicos de direcciones desconocidas
- No enviar o recibir archivos por plataformas de mensajería instantánea
- No conectar a la red empresarial dispositivos de uso personal
- No usar USB desconocidas en los equipos de la compañía
- No hacer clic en ventanas pop – up sospechosas
- No buscar instalar software ajeno al autorizado por la empresa
- Es muy importante usar contraseñas seguras
- Bloquear los equipos cuando no se está en el lugar de trabajo
- No habilitar la opción de "Recordar contraseña"

El seguir estos consejos e implementar más medidas de prevención de seguridad podemos establecer una capa de seguridad extra y es mucho menos probable que se pierda control sobre los recursos de la institución.

Soluciones de control

La seguridad computacional a menudo se divide en tres categorías maestras distintas, comúnmente llamadas controles:

- Físico
- Técnico
- Administrativo

Estas tres amplias categorías definen los objetivos principales de una implementación de seguridad apropiada. Dentro de estos controles hay subcategorías que detallan aún más los controles y como estos se implementan.(Burke, 2005)

Controles físicos

El control físico es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial. Ejemplos de los controles físicos son:

- Cámaras de circuito cerrado
- Sistemas de alarmas térmicos o de movimiento
- Guardias de seguridad
- Identificación con fotos
- Puertas de acero con seguros especiales
- Biométrica (incluye huellas digitales, voz, rostro, iris, escritura a mano y otros métodos automatizados utilizados para reconocer individuos)

Controles técnicos

Los controles técnicos utilizan la tecnología como una base para controlar el acceso y uso de datos confidenciales a través de una estructura física y sobre la red. Los controles técnicos son mucho más extensos en su ámbito e incluyen tecnologías tales como:

- Encriptación
- Tarjetas inteligentes
- Autenticación a nivel de la red
- Listas de control de acceso
- Software de auditoría de integridad de archivos

Controles administrativos

Los controles administrativos definen los factores humanos de la seguridad. Incluye todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso a qué recursos e información usando medios tales como:

- Entrenamiento y conocimiento
- Planes de recuperación y preparación para desastres
- Estrategias de selección de personal y separación
- Registro y contabilidad de personal

Soluciones de Mitigación

Mediante la fase de tratamiento se busca mitigar riesgos. Esto consiste en definir los controles para aquellos riesgos identificados en la evaluación, buscando disminuir la probabilidad de que suceda el riesgo o al menos reducir los impactos que pudieran originar.

Partiendo de la base de que los recursos disponibles en las organizaciones son limitados, debemos comenzar centrando la atención en aquellos riesgos identificados como no aceptables, de manera que se establezca un orden de prioridad a la hora de mitigar riesgos. (ISOTools, 2016)

Por supuesto que no todos los riesgos se generan de la misma forma y no todos tienen el mismo impacto. El objetivo del tratamiento de riesgos es determinar la importancia y el impacto del riesgo, y de esta forma, optar por una de las siguientes formas de mitigar.

Reducir el riesgo

Aplicar controles de seguridad, según el Anexo A de la ISO 27001, para reducir el riesgo. Es la opción más utilizada, e incluye la implementación de medidas de seguridad como cámaras de vigilancia, sensores de movimiento, de fuego, de humo, y por supuesto, instalación de firewall.

Compartir o transferir el riesgo

El ejemplo más común, es la suscripción de una póliza de seguros, con cobertura para el riesgo que se desea compartir. Contratar una compañía de seguridad, que asuma el compromiso de velar por la integridad de la información es otra forma de compartir el riesgo, cuando el contrato especifica una penalidad en caso de que se presente un incidente.

En cualquier caso, estas son medidas que no conjuran la ocurrencia del incidente, ya que tan solo se transfiere el riesgo financiero a otra organización, pero pueden resultar efectivas si se utilizan en conjunto con una o varias de las otras opciones de mitigación en el tratamiento de riesgos según ISO 27001.

Eliminar el riesgo

Se logra eliminando una actividad, un procedimiento o un proceso que puede ser la causa del incidente, o modificándolos de tal forma que se elimine el riesgo. Un ejemplo de ello es el uso de ordenadores portátiles fuera de las instalaciones de la organización. Prohibir esta práctica, elimina la posibilidad de ocurrencia de muchos incidentes, generadores de riesgos de alto impacto.

Aceptar el riesgo

Cuando las acciones necesarias para eliminar un riesgo tienen un coste demasiado alto o superior a las consecuencias previstas de la ocurrencia del incidente, conviene pensar en la posibilidad de convivir con el riesgo, y minimizar su impacto.

Para estos casos, resulta ideal utilizar esta opción, en conjunto con la de compartir el riesgo, adquiriendo una póliza de seguros. La seguridad en la información tiene importancia capital para cualquier organización y para asegurar la continuidad del negocio en todo momento. Ahora tiene 4 opciones para el tratamiento de riesgos según ISO 27001. Sin olvidar que puede hacer uso de una o todas, incluso algunas de ellas en conjunto. (ISOTools, 2017)

4.2.6. Sensibilización

La sensibilización puede fomentarse gracias a la realización de una serie de actividades para concienciar a las personas sobre una determinada situación, en este caso de estudio fomentaremos el buen uso de los activos informáticos en la FACCI.

Según el comité de la agencia de refugiados españoles de la ONU nos dice que "la sensibilización tiene por objetivo la concienciación de las personas y, para ello, se pueden realizar acciones de diversa índole: charlas, conferencias, exposiciones, talleres, formación de grupos, concursos, juegos, mercadillos, eventos deportivos o acciones directas en la calle". (ACNUR, 2018)

Criterios para llevar a cabo la sensibilización

Duración

Tiene una duración de máxima de 30 horas y es intensiva. (En caso de no poder hacer las 30 horas, se podrían hacer 20 o 10 en las que se desarrollan las bases teóricas fundamentales de comunidades de aprendizaje, mediante actividades. Lo ideal es poder hacer lecturas de la información que se quiere sensibilizar y debatirla entre los asistentes durante la sensibilización.). (Learning Communities.)

Asistentes

Debe contar con la presencia de todo el claustro y pueden participar todos los miembros de la unidad académica (personal administrativo, estudiantes y profesores). (Learning Communities.)

Otros participantes

Se valora como un elemento importante la participación de una persona certificada y capacitada del tema en funcionamiento brindando así información efectiva. Sus aportaciones desde la práctica suponen un enriquecimiento en el proceso de formación y transformación.(Learning Communities.)

Figura de coordinación

Contar con una persona coordinadora durante la sensibilización que se encargue de recoger los intereses, percepciones y dudas que vayan surgiendo en el proceso de sensibilización.

En este caso de investigación figuraría como coordinadora la líder del proyecto de SGSI. Esto permite dar más continuidad, en la medida en que establece un puente entre las diferentes personas que exponen en cada una de las sesiones y el auditorio conjunto con otras personas participantes de la sensibilización. Las tareas concretas serán:

- Recoger notas con aquellas ideas, reflexiones que se expongan en los diferentes debates, así como sugerencias, dudas o temas no resultados en cada una de las sesiones.
- Hacer de enlace entre las diferentes personas que exponen en cada una de las sesiones, situándoles en el momento en el que se encuentra el debate, informándoles sobre las aportaciones que se han dado en sesiones anteriores, etc.
- Recoger todas las dudas, sugerencias, reflexiones o temas pendientes de resolver para que se puedan abordar en la sesión de cierre.(Learning Communities.)

4.2.7. Comunicación

La UNESCO en su proyecto de Comunicación nos habla que "La comunicación es el intercambio de ideas, mensajes e información. Puede revestir formas diversas y recurrir tanto a medios de comunicación social tradicionales (radio y televisión, por ejemplo) como a medios más modernos (internet, entre otros).

Gracias a la comunicación, las personas expresan sus ideas, conocimientos y capacidades creativas y las comparten con otros individuos o públicos, nacionales o extranjeros. En efecto, la comunicación presupone la participación y el diálogo, y también desempeña un papel fundamental en la salvaguardia del pluralismo al posibilitar que las personas expresen sus ideas y las pongan al alcance de los demás". (UNESCO, 2014)

Teorías contextuales de la información

Comunicación Intrapersonal

Millar y Rogers (1976) establecen un análisis muy interesante de la complementariedad y la simetría mediante el estudio de la variable denominada control.

Axiomas de la comunicación

- Un individuo no puede no comunicar.
- Toda comunicación tiene un contenido y un aspecto relacional denominado metacomunicación.
- Las unidades o sintagmas de la comunicación no son una suma de elementos aislados.
- Los seres humanos pueden comunicarse de formas analógica y digital.
- Las interacciones pueden ser simétricas o complementarias. (Ongallo, 2007)

Comunicación Grupal

Para Lewin, los seres humanos tienen un espacio vital, un campo de juego psíquico en el que se desarrollan. Cada persona se mueve en un espacio vital, que según Lewin también consta de elementos grupales. Los individuos no pueden prescindir de los grupos humanos a los que pertenecen y con los que se identifican.

Por extensión, los grupos también tienen un espacio vital. En esta afirmación nace la dinámica grupal, que engloba desde los grupos más pequeños (la familia), a los grandes grupos de trabajo. El análisis incluye un gran número de grupos humanos, desde instituciones hasta comunidades.

Es necesario añadir que cada persona puede ser miembro de uno o varios grupos simultáneamente, con lo que el peso de cada uno de dichos grupos de pertenencia en su espacio vital será menor en tanto en cuanto dicho individuo pertenezca a mayor número de grupos. El espacio vital propio se verá sometido, por así decirlo, a tensiones creadas por los distintos grupos, que influirán en las acciones de dicha persona.

Se llega así a uno de los puntos más importantes de la teoría de Lewin, que es el impacto de los grupos en la vida de los individuos, según los puntos siguientes:

- El grupo proporciona estabilidad a la vida de la persona.
- El grupo es un vehículo para lograr los objetivos vitales del individuo.
- Los valores y actitudes de los individuos son influidos enormemente por los valores y actitudes del grupo.
- Como parte del espacio vital, la persona busca lograr los objetivos del grupo, llegar a ellos y hacer de ellos parte de sus logros.

  (Ongallo, 2007)

Comunicación de Masas

La comunicación de masas el proceso por el que se elaboran y transmiten mensajes al gran público. Los denominados medios de comunicación de masas o mass-media son los encargados de llevar a cabo dicha tarea.

De todos los tipos de comunicación estudiados, la comunicación de masas es el más difícil de conceptualizar, debido precisamente a su ubicuidad: en la actualidad, los medios de comunicación de masas, la publicidad masiva y todos los elementos de comunicación social (marketing electoral, internet, etc.) están alcanzando las mayores cotas de protagonismo de la historia.

Es preciso destacar que muchos de los denominados medios de comunicación de masas son utilizados como instrumentos válidos de comunicación interna en las organizaciones, si bien sus públicos objetivos son cuantitativamente menores (empleados, socios o voluntarios). Ejemplo de ello pueden ser los canales internos de televisión para los empleados de una empresa, o la revista o periódico de la organización, así como otros medios adaptados a los socios y colaboradores.(Ongallo, 2007)

4.2.8. Capacitación

Capacitación o desarrollo de personal, es toda actividad realizada en una organización, respondiendo a sus necesidades, que busca mejorar la actitud, conocimiento, habilidades o conductas de su personal.

Concretamente, la capacitación: busca perfeccionar al colaborador en su puesto de trabajo, en función de las necesidades de la empresa, en un proceso estructurado con metas bien definidas. (Edgardo Frigo, 2016)

Técnicas de capacitación

Es por ello por lo que es imprescindible el uso de capacitación del personal para maximizar su productividad y hacer crecer potencialmente a la empresa.

"El aprendizaje […] es una actitud, una cultura, una predisposición crítica que alimenta la reflexión que ilumina la acción" menciona Ernesto Gore en su libro "La Educación en la Empresa" además de que "la capacitación es un agente de cambio y de productividad en tanto sea capaz de ayudar a la gente a interpretar las necesidades del contexto y a adecuar la cultura, la estructura y la estrategia (en consecuencia, el trabajo) a esas necesidades". (Tecnológico de Monterrey, 2017)

Técnica actual

- **Videoconferencias:** Es una forma sencilla si las personas se encuentran en distintos lugares para reunirlos en un solo lugar y hay interacción al momento.
- **Cursos en línea:** No hay necesidad de ir a clases y hay flexibilidad de horario, así como de interacción. Además de un apoyo invaluable de gráficos, videos y textos. (Tecnológico de Monterrei, 2017)

Tipología de capacitación

Los tipos de capacitación son bastantes variables y se pueden clasificar de la siguiente forma:

Capacitación técnica

Es aquella formación para el puesto de trabajo. Se divide en programas, talleres o formación en el puesto. Es la formación que se necesita para el desempeño: desde aprender a dominar un programa informático, procesos internos, el funcionamiento de una máquina, u otra formación requerida para el puesto. (Recursos Humanos.)

Capacitación conductual

Es aquella formación necesaria para liderar equipos o también llamada formación en valores. Esta formación está destinada a mandos medios (jefes y Gerentes) formación en valores corporativos, habilidades para la comunicación, pensamiento estratégico, inteligencia emocional, gestión del conocimiento, manejo de equipos, etc. Son temas más abstractos que aquellos que forman la capacitación técnica, pero que impactan mucho en la función.

Para no crear brechas entre poblaciones de empresa, cada vez más empresas dictan formación en valores a todos los empleados sin importar el rango o el puesto que ocupen. (Recursos Humanos.)

4.2.9. Diferencia Sensibilización, Comunicación y Capacitación

La diferencia entre estos tres conceptos es el objetivo que plantea cada uno para un fin particular el conocimiento. La sensibilización permite preparar a las personas a un entendimiento y ser parte de una misma comunidad permitiendo una relación bidireccional empleado - empresa y viceversa.

La comunicación permite utilizar medios para un fin que ayuda a diagnosticar situaciones, permitiendo establecer una conexión directa con el empleado y evitar malentendidos. La capacitación permite evitar la obsolescencia de los conocimientos del personal, que ocurre generalmente entre los empleados más antiguos si no han sido reentrenados.

4.2.10. Beneficios de la Sensibilización, Comunicación y Capacitación

Sensibilizar

A través del proceso de sensibilización la empresa crea y transmite su cultura, entendida ésta como el conjunto de valores, políticas, normas y tradiciones relativamente estables en el tiempo y que distinguen a cada institución, así como cada individuo tiene una personalidad propia, también cada empresa desarrolla una cultura distintiva. Se puede transmitir y refrescar información mediante seminarios y conferencias a realizarse en ocasiones especiales, como cursos de entrenamiento. (Meiras, 2017)

Comunicar

Aprender técnicas de comunicación nos permite, entre otras cosas, entendernos mejor y comunicarnos con nuestro entorno con mayor nivel de conciencia y eficacia. La capacidad de comunicarnos permite la evolución de los seres humanos y de sus actividades. Cuanto mejor sea la comunicación, mayor será el desarrollo como comunidad o grupo de trabajo. (Monika Suso.)

Capacitar

Disminuye la tasa de rotación de personal, y permite entrenar sustitutos que puedan ocupar nuevas funciones rápida y eficazmente. Por ello, las inversiones en capacitación redundan en beneficios tanto para la persona entrenada como para la empresa que la entrena. Y las empresas que mayores esfuerzos realizan en este sentido, son las que más se beneficiarán en los mercados hipercompetitivos que llegaron para quedarse. (Edgardo Frigo, 2016)

CAPÍTULO IV: METODOLOGÍA

4.1. Preliminar

La investigación como proceso dinámico, conlleva distintos niveles de complejidad de los cuales se obtienen conocimientos acordes con la finalidad planteada en ella. En este apartado se detallan los aspectos metodológicos de la presente investigación, tales como el diseño, la población, los métodos e instrumentos utilizados y la descripción de las técnicas para el análisis de los datos.

Por la modalidad corresponde a una tarea investigativa encaminada a la planificación de una sociabilización de medidas, políticas y controles de seguridad informática, a través de una organización y esquematización de temáticas, dirigidas a un grupo específico.

En términos generales, se ha considerado al trabajo, como documental puesto que la obtención de la información proviene de material impreso y de otro tipo de documentos, a su vez, se encuentra enmarcada en un enfoque de carácter cualitativo debido a su flexibilidad, por lo que, se ha ido complementando y precisando de forma simultánea conforme se ha desarrollado la investigación con el objetivo de que ésta sea sensible a aquello que busca describir y comprender.

De acuerdo con el alcance del estudio se determina como tipo descriptivo ya que se han detallado las características, cualitativas y cuantitativas fundamentales de la postura actual manejada por la Facultad frente a los riesgos informáticos con criterios sistemáticos para mostrar su estructura y comportamiento.

4.2. Diseño

El diseño metodológico implica definir los procedimientos y estrategias que ayuden a alcanzar los objetivos estipulados, para lo cual se ha desarrollado un plan de acción a seguir durante la ejecución de la presente investigación y así, llegar a la obtención de los resultados.

Para la construcción del marco teórico de la investigación se hizo una exhaustiva revisión de la literatura, que complementa una etapa más del proceso, desde el planteamiento del problema hasta la obtención de los resultados.

Los instrumentos utilizados en el proceso de la investigación se enmarcaron en la técnica de investigación documental (sistematización bibliográfica), principalmente, la técnica de fichaje (resumen de información), fuentes de datos secundarios (investigaciones previas) y observación cualitativa.

En el proceso de validación y esquematización de la información se utilizaron métodos para ordenar y sistematizar los resultados, entendiendo el entorno y teniendo una visión clara de la situación actual de la gestión del proceso de seguridad informática en la Facultad. Los métodos fueron: sintético (síntesis bibliográfica), analítico e inductivo.

Para el procesamiento y análisis de información, de acuerdo con el enfoque dado, se cuenta con estrategias para ello que permiten ordenar e interpretar dicha información con base a los planteamientos teóricos, sustento del estudio realizado.

Con el análisis y la utilización de las estrategias de procesamiento de la información se estructura todo el cuerpo del trabajo, que le da sentido a la investigación, para lo cual en la obtención de los resultados se da a conocer lo obtenido en las investigaciones previas de forma sistematizada a través de matrices resumen para su comprensión (análisis de riesgos y declaración de aplicabilidad), además de la propuesta de un plan de Sensibilización, Comunicación y Capacitación en seguridad informática.

Sin embargo, el diseño definido a continuación, no puede permanecer estático puesto que, en el transcurso de la evolución de la investigación puede variar en función de las acciones que se lleven a cabo.

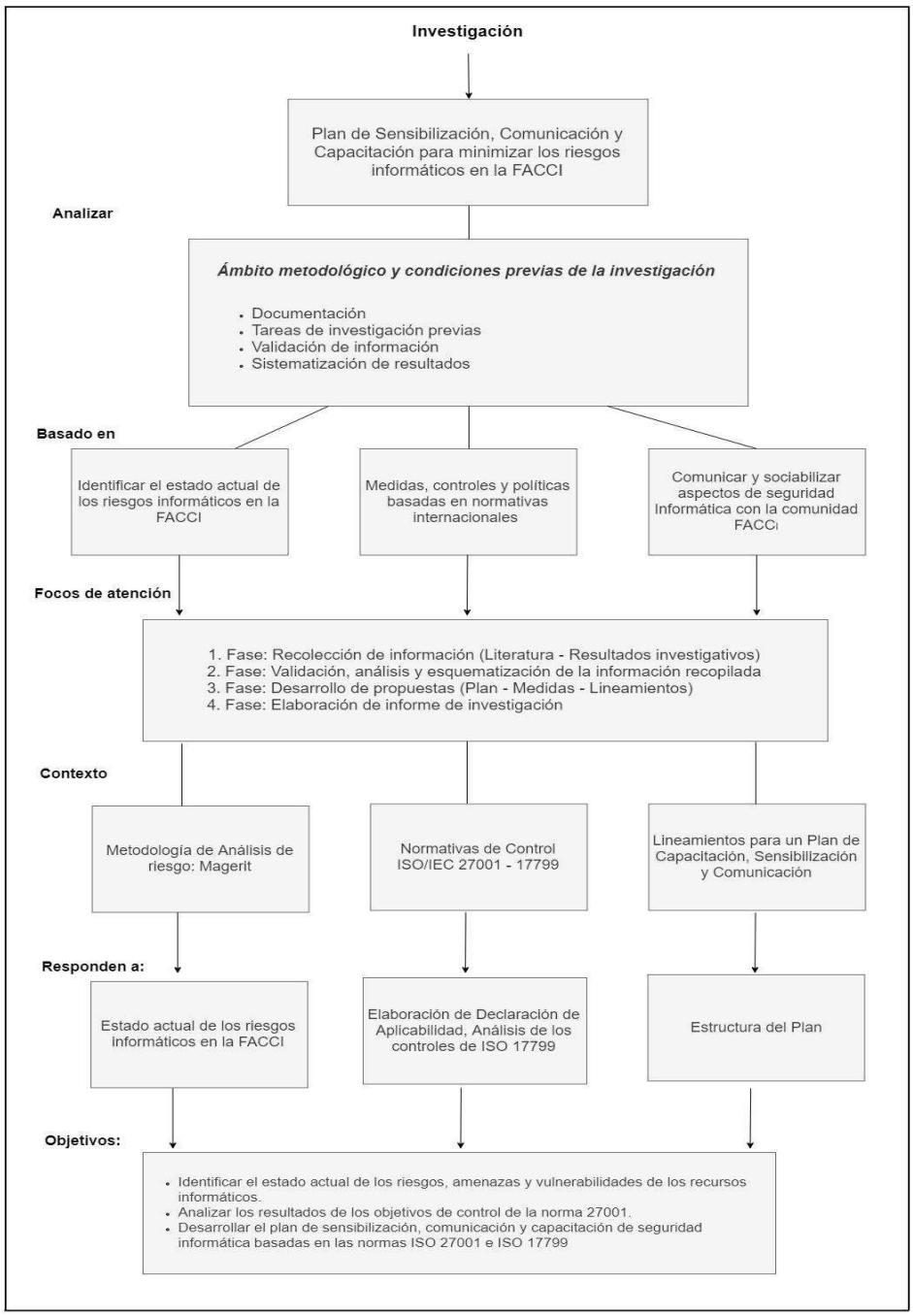

Ilustración 3. Diseño de la investigación.

Ilustración 3.- Muestra el diseño adoptado para el desarrollo de la investigación.
Fuente: Las autoras de la investigación basada en (Moreno Flórez, n.d., p. 179)

Con respecto al alcance del estudio realizado, se lo ha catalogado como descriptivo puesto que, con base a la información obtenida, de la literatura y del análisis de los

resultados de investigaciones previas, se presenta los hechos y eventos que caracterizan la postura de la Facultad frente al proceso de la seguridad de la información.

En base a lo definido por varios autores, conceptualmente se tiene, según (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, p. 92), "los estudios descriptivos busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis".

Para (Monje Álvarez, 2011, p. 95), "la descripción permite reunir los resultados de la observación en una exposición relacionada de los rasgos del fenómenos que se estudia de acuerdo con criterios que le den coherencia y orden a la presentación de los datos." También señala que, "la descripción se ocupa principalmente de la información sobre cantidad, ubicación, capacidad, tipo y situación general del problema".

Aplicando al caso de estudio, permite describir e interpretar la realidad de las personas, en este caso, la situación actual de la gestión del proceso de seguridad informática en la Facultad. De acuerdo con el tipo de problema de investigación (una problemática necesita resolverse), se seleccionó como estrategia de este enfoque a la investigación – acción, para lo cual se presenta una propuesta de un Plan para minimizar riesgos informáticos dirigido a la comunidad FACCI.

De acuerdo con (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014, p. 7), el enfoque cualitativo "utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación. La acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación."

Este mismo autor, (Hernández Sampieri et al., 2014, p. 8), enuncia que "las *investigaciones cualitativas* se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas), van de lo particular a lo general."

Para la representación gráfica del proceso cualitativo, se ha tomado como referencia a (Monje Álvarez, 2011, p. 35), el cual, lo desarrolla a través de cuatro fases en las que se

distinguen etapas, donde, en cada una de éstas el investigador tendrá que ir tomando opciones entre las diferentes alternativas que se vayan presentando.

En la *Ilustración 4* se puede observar las fases: preparatoria, trabajo de campo, analítica e informativa, que van precediendo una a la otra, es decir cada fase se superpone con siguiente y la anterior. De esta forma se destaca que el proceso se desarrolla de una forma sutil. Cuando aún no se ha finalizado una fase ya se comienza con la anterior. Este mismo hecho se contempla en la representación gráfica de las etapas de cada fase. (Monje Álvarez, 2011, p. 34).

A continuación, se presenta la representación.

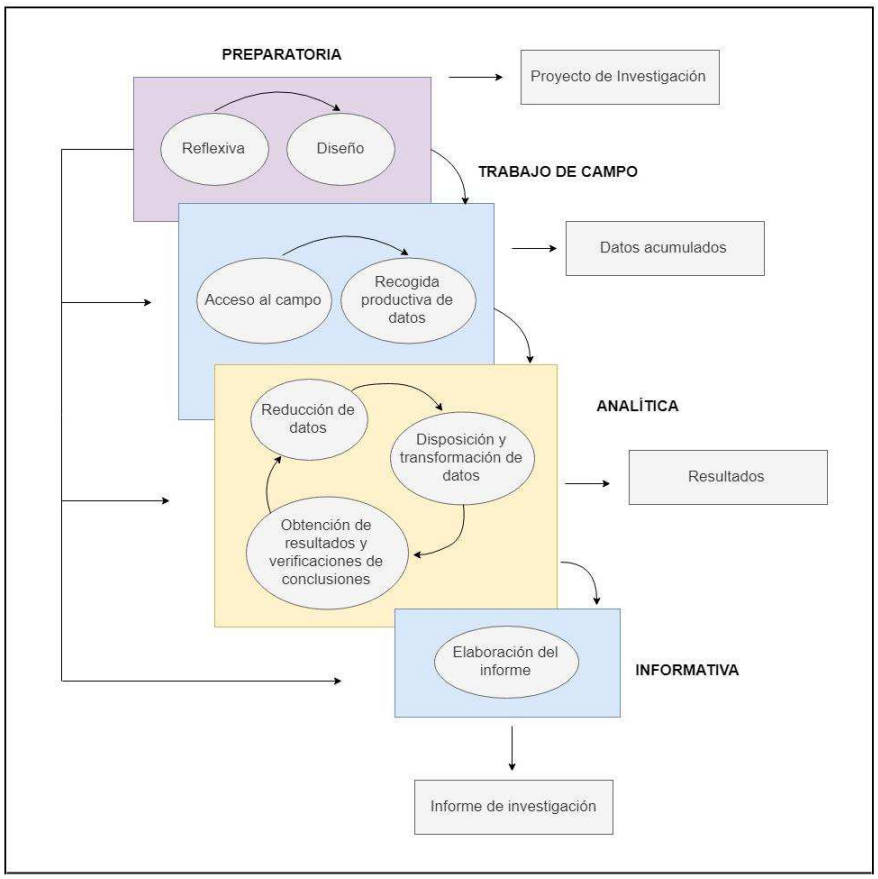

Ilustración 4. Fases y etapas de la investigación cualitativa

Ilustración 4.- Muestra las fases y etapas de la investigación cualitativa
Fuente: (Monje Álvarez, 2011, p. 35)

Por lo tanto, adaptando ese modelo al presente trabajo se tiene:

- Fase *preparatoria* se diferencian dos etapas:

  1. La reflexiva o reflexión teórica en la que se toma como base la propia formación, conocimientos, experiencias e ideologías para guiar y orientar el desarrollo de la tarea investigativa, identificando las temáticas, marco teórico – conceptual, a tratar en el trascurso de ésta, considerado como una herramienta para orientar el proceso de recogida y análisis de datos.

  2. En la etapa de diseño se enfoca en la planificación de las actividades ejecutadas posteriormente que suelen estructurarse a partir de las preguntas de investigación. Se trata de determinar hasta qué punto se cuenta con los recursos, métodos y técnicas de recogida de información, necesarios para realizar el estudio.

- Fase *trabajo de campo* en esta fase se toman en cuenta las etapas del acceso al campo y la recogida productiva de datos.

  1. Acceso al campo, en ésta se accede progresivamente a la información fundamental para el trabajo a través de la compresión del entorno en que se desenvuelve la investigación haciendo uso de la observación y la elaboración de esquemas.

  2. Recogida productiva de los datos, para recolección de la información se utilizan métodos para el manejo de datos, donde es preciso asegurar el rigor de la investigación, refiriéndose a la cantidad de información recogida y a la selección, de ésta, en base a las necesidades teóricas del estudio.

- Fase *analítica* se eligen unas series de tareas u operaciones que constituyen el proceso analítico básico, que serían: reducción de datos, disposición y transformación de datos; y obtención de resultados y verificación de conclusiones, entre las cuales, no siempre se establece una sucesión en el tiempo y pueden ocurrir de forma simultánea.

- Fase *informativa*, en ésta se involucra la presentación y difusión de los resultados, en caso mediante la presentación de un informe de investigación donde muestren los principales hallazgos y resultados obtenidos apoyados en las conclusiones.

Dentro del enfoque cualitativo se encuentra diversas tipologías de los diseños, de los cuales se ha seleccionado el diseño de investigación – acción cuya finalidad es comprender y resolver problemáticas específicas de una comunidad vinculada a un ambiente, tal como lo define (Hernández Sampieri et al., 2014, p. 496).

El mismo autor señala que, el precepto básico, de la investigación acción, es que debe conducir a cambiar y por tanto este cambio debe incorporarse en el propio proceso de investigación. Se indaga al mismo tiempo que se interviene. (Hernández Sampieri et al., 2014, p. 496)

Entonces de acuerdo a lo anterior, se puede determinar que esta tipología, se centra en propiciar un cambio social y transformar la realidad educativa, alcanzando que cada uno de los usuarios de la FACCI tome conciencia de su papel en proceso de la gestión de seguridad, para lograr aquello, es necesaria la colaboración de todos los involucrados en: la detección de las necesidades de la Facultad en dicho proceso y la implementación de una campaña de sensibilización y capacitación de medidas, controles y políticas para minimizar los riesgos informáticos.

En éste, se destacan dos diseños fundamentales, los cuales son el práctico y participativo, en la *Ilustración 5* se presenta el esquema. En base a ello, se ha determinado que la investigación se enmarca en el diseño práctico, en general, se estudia las prácticas de la FACCI sobre la seguridad de la información centrándose en el desarrollo y aprendizaje de los usuarios, a su vez, implementa un plan de acción para resolver el problema que genere un cambio.

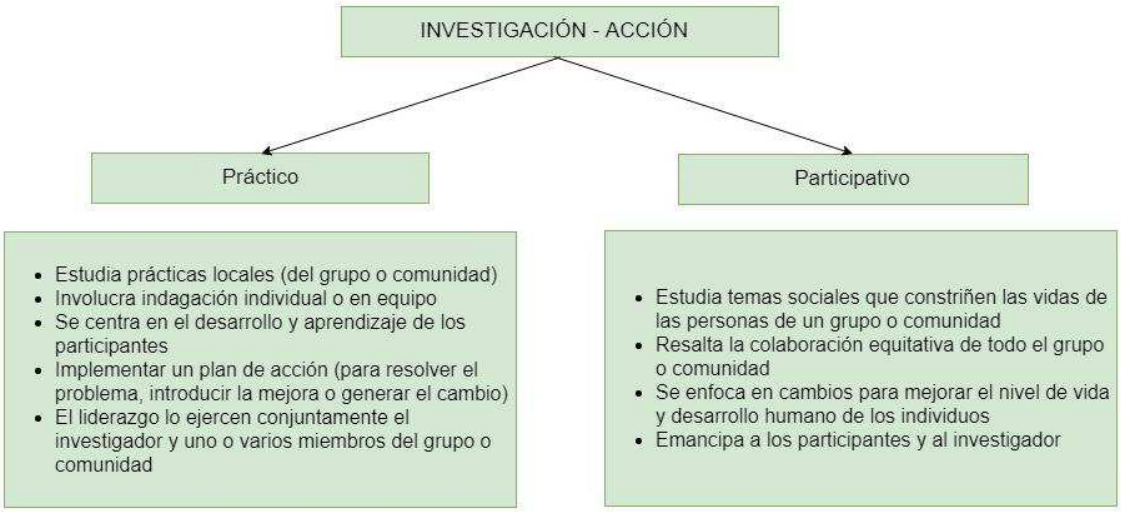

Ilustración 5. Diseños de la investigación-acción

Ilustración 5.- Muestra el diseño de la investigación – acción
Fuente: (Hernández Sampieri et al., 2014, p. 498)

4.3. Población

La población se encuentra seleccionada en la comunidad FACCI que comprende: el personal administrativo – docentes y estudiantes

4.4. Métodos e instrumentos de investigación

En este apartado se detallan los métodos e instrumentos utilizados para la tarea investigativa. El método hace referencia a los caminos a tomar para acercarse a la realidad, al fenómeno u objeto a estudiar. En cuanto a los instrumentos equivale a las acciones para recolectar la información necesaria y pertinente para el trabajo investigativo. A continuación, se describen cada uno de estos aspectos.

4.4.1. Métodos

Según (Del Cid, Méndez, & Sandoval, 2011, p. 20), están disponibles diversas perspectivas metodológicas, distintas formas de ver y acercarse a los fenómenos. Estos autores los denomina *procesos lógicos*, entendiéndolo como la forma en que se utiliza la razón para relacionar datos.

Para efecto de estudio se ha utilizado el método analítico, sintético e inductivo, textualmente se tiene:

1. **Método Analítico. -** El método analítico consiste precisamente en descomponer un objeto en sus partes constitutivas. La ventaja al hacer esto es que se puede enfocar el estudio, una por una, en cada parte, comprendiéndola con detalle y profundidad. (Del Cid et al., 2011, pp. 20–21)

2. **Método Sintético. -** En una investigación practicamos el método sintético cuando nos preguntamos qué conclusiones podemos sacar del estudio, cuando queremos condensar en unas pocas, pero importantes ideas todo el esfuerzo realizado. También es sintético preguntarse qué podemos recomendar a la institución que auspició el estudio. Al realizar un ejercicio de síntesis practicamos lo que se denomina formular generalizaciones. (Del Cid et al., 2011, p. 21)

3. **Método Inductivo. -** Consiste en una operación lógica que va de lo particular a lo general. El método inductivo supone tener datos parciales confiables para, a partir de ellos, concluir que hay características que se repiten una y otra vez. Supone atención en los datos, en lo observado. La práctica cuidadosa de los fenómenos de una misma especie es la que permite practicar la inducción. (Del Cid et al., 2011, pp. 21–22)

El primer método es aplicable al estudio, en base a la teoría, se ha descompuesto a la comunidad FACCI en tres grupos (personal docente, personal administrativo y estudiantes) para la aplicación de procesos en la gestión de la seguridad informática que le correspondería a cada uno de ellos como actores principales.

También se ha seccionado a la Facultad en tres partes: Laboratorios, Aulas y Áreas, en donde, para cada uno de éstos, se tiene riesgos y amenazas que pudiesen materializarse en sus activos. Por último, dichos activos se los ha dividido en:

hardware, software e información. Todo esto para tener una visión clara de la situación actual de la FACCI en cada aspecto mencionado.

Mediante el segundo método se condensa los resultados del análisis de riesgo dividido en las secciones, antes mencionadas, y por cada activo definido, dando a conocer dichos resultados mediante matrices de resumen. De igual forma se realiza la síntesis de las normas ISO aplicables de acuerdo con la Declaración de Aplicabilidad para cada uno de esos riesgos detectados.

En este último método lleva el paso a la generalización, el cual, a partir de los resultados obtenidos de la investigación, se puede concluir las características que se repiten, es decir, observar los temas referentes al proceso de seguridad, que serán propuestos en el Plan de Capacitación y Sensibilización, en los que se encuentran mayor debilidad para conocer qué tipo de medidas y controles informáticos minimicen aquella debilidad.

4.4.2. Instrumentos de investigación

En este paso de la investigación consiste en seleccionar técnicas e instrumentos que permitan llegar a las fuentes para obtener la información necesaria. Según (Del Cid et al., 2011, p. 111), existe una gran variedad de técnicas para las cuales hay múltiples clasificaciones, que se utilizarán según los intereses de la investigación.

También afirma que, las técnicas dependen de la naturaleza del conocimiento disponible, de los requisitos o exigencias de precisión, así como de la inteligencia y la habilidad del investigador encargado de aplicar la técnica.(Del Cid et al., 2011, p. 111)

En base a lo anterior se describen los instrumentos utilizados de acuerdo con la presente, la investigación documental ha sido la base para el desarrollo de ésta ya que se ha previsto de información en relación con el tema y la obtención de resultados previas, así como, el uso de técnicas para resumir dicha información. A través de la observación se logra entender las características importantes de la seguridad informática en la Facultad. Conceptualmente se tiene:

Técnica de investigación documental. – Estas técnicas se orientan a obtener información que otros han escrito sobre el tema estudiado. Éstas recurren a fuentes secundarias de información. (Del Cid et al., 2011, p. 112). Puede darse en dos niveles, el primer nivel involucra teorías generales y elementos teóricos sobre lo que se estudia. (libros, tratados, etc.) El segundo nivel implica el análisis de información secundaria o proveniente de distintas fuentes. (Publicaciones, mapas, etc.)

Técnica de fichaje. – Esta técnica consiste en extraer segmentos de información de fuentes documentales. La principal utilidad es la reducción de información resultante que posteriormente, se podrá organizar. (Del Cid et al., 2011, p. 112)

Técnica de resumen. - Facilita al investigador el registro de información presentada en distintos documentos; es una forma de sintetizar. El resumen permite concentrar información extraída de documentos completos, es decir, abarca una mayor cantidad de información. Y hace uso de una tabla preliminar, en este caso:

- Técnica de elaboración de mapas. - son los que se elaboran como producto de la lectura analítica de documentos. (Del Cid et al., 2011, pp. 114–117)

Observación cualitativa. – según (Hernández Sampieri et al., 2014, p. 399), uno de los propósitos comprender procesos, vinculaciones entre personas y sus situaciones, experiencias o circunstancias, los eventos que suceden al paso del tiempo y los patrones que se desarrollan.

4.5. Análisis de los datos

En este apartado se describe las técnicas para el análisis de los datos, cabe mencionar que en la investigación cualitativa los pasos de recolección y el análisis ocurren prácticamente en paralelo, tal como lo enuncia (Hernández Sampieri et al., 2014, p. 418), la acción esencial, de este paso, consiste en que recibimos datos no estructurados, a los cuales se les proporciona una estructura.

En la, *Ilustración 6* se presenta una guía general para el análisis, del lazo izquierdo se incluyen 3 acciones en paralelo que están relacionadas: recolección de los datos, tareas analíticas y resultados. Las flechas en dos sentidos indican que se puede regresar a las etapas previas y las fecha sin direccionalidad muestran actividades asociadas.

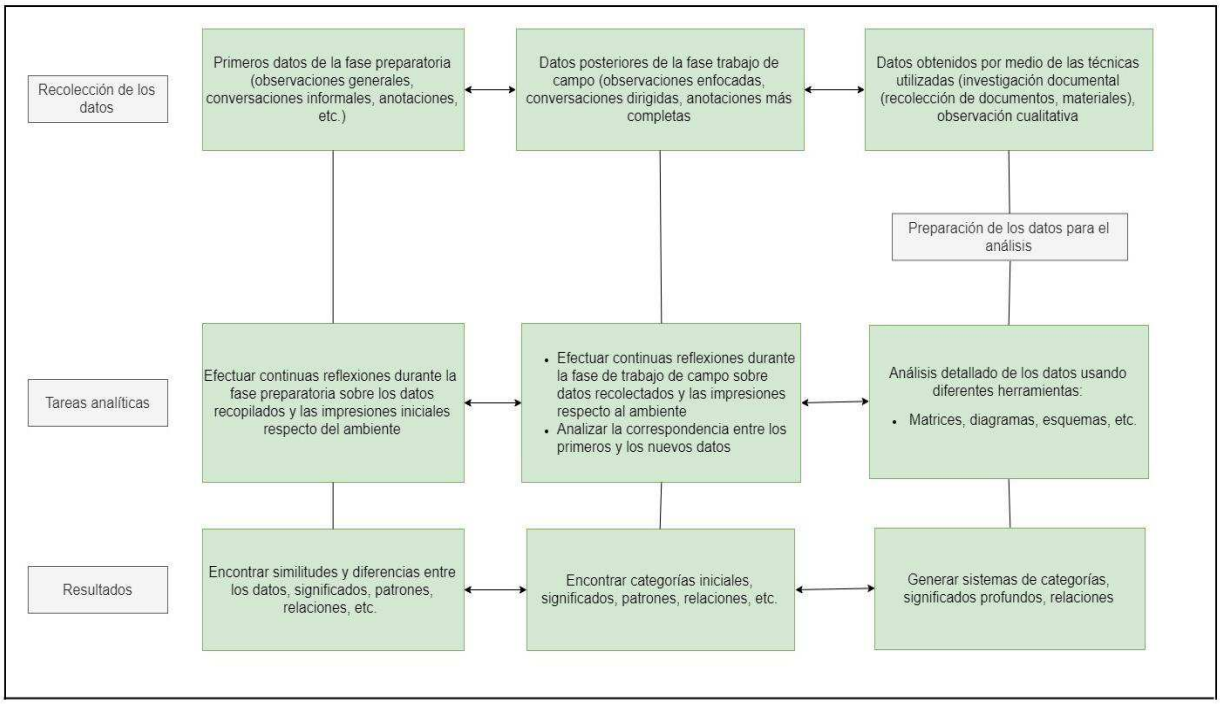

Ilustración 6. Directrices del análisis cualitativo

Ilustración 6.- Muestra una guía general para el análisis de datos de la investigación
Fuente: Las autoras de la investigación basada en (Hernández Sampieri et al., 2014, p. 498)

Ahora se describen las tareas analíticas y los resultados.

- **Reflexiones durante la fase preparatoria.** – durante esta fase se realiza observaciones del entorno, se conversa con los miembros del grupo del proyecto, se recaba documentos y otros materiales, entre otras actividades con el fin de reflexionar y evaluar el problema de investigación.

- **Reflexiones durante la fase de trabajo de campo. –** en este proceso se recopilan más datos, las observaciones se enfocan en responder al planteamiento. De forma inductiva surgen categorías iniciales, significados, patrones del fenómeno a estudiar.

- **Análisis detallado de los datos. –** para esta actividad, de acuerdo con el diseño de investigación – acción, se dispone de diversas herramientas para llevar a cabo el análisis una vez lograda la claridad conceptual y recopilación de información, usando la técnica de *Matrices,* se realizó una matriz para representar el análisis de riesgos a manera de resumen, indicando los riesgos altos y muy altos, es decir, los que representan una mayor debilidad, especificando por secciones de la Facultad y por activos.

De manera similar, se elaboró una matriz mostrando el análisis de las normas ISO aplicables, en base a la Declaración de aplicabilidad, para minimizar cada riesgo detectado. Finalmente, a partir de esas normas, se realizó una matriz determinando las medidas para implementarlas a través de controles, políticas, manuales, normas para mejorar la gestión del proceso de la seguridad informática.

Después de los datos se hayan analizado, se efectuó el desarrollo del plan de sensibilización y capacitación que incorpore las temáticas de seguridad basada en las medidas definidas anteriormente, además de la respectiva planificación para la comunicación efectiva, con la comunidad FACCI, de temarios por grupo específico y de esta manera generar un cambio de concientización con respecto a la seguridad de los activos.

CAPÍTULO V:

RESULTADOS

3.1. Análisis de resultados previo a la propuesta

3.1.1. Análisis de Riesgo de los Activos Informáticos

El análisis de riesgos fue realizado por medio de la tarea de investigación "Evaluación y Tratamiento del análisis de riesgos informáticos de la FACCI", elaborado por las Ing. Gema Guerrero y Evelyn Mera. Mediante el análisis de riesgos que se realizó a la Facultad de Ciencias Informáticas se pueden visualizar las amenazas en que se ven afectados los activos, e introduciendo la probabilidad y el impacto de cada uno de ellos se puede observar la gravedad en que afectaría a estos. Las cuales se dividieron en:

- Riesgos generales por activos informáticos
- Riesgos por Áreas
- Riesgos por Laboratorios
- Riesgos por Aulas

Cabe destacar que los resultados que mostraremos de la investigación anterior han sido verificados, analizados por criterio de expertos y por las investigadoras, siendo adaptados a las necesidades del presente estudio.

3.1.1.1.Riesgos generales por activos informáticos

Tabla 2. *Análisis de riesgo de los activos informáticos: Riesgos generales de los activos informáticos*

RIESGOS GENERALES POR ACTIVOS INFORMÁTICOS - FACCI			
Activo	**Descripción**	**Amenaza**	**Impacto**
1.1. Datos e Información	**1.1.1. Copias de Seguridad**	1.1.1.1. Directrices deficientes para el proceso de backups	Alto
		1.1.1.2. Acceso a respaldos por usuarios no autorizados	Medio
		1.1.1.3. Deficientes mecanismos de cifrado	Alto
	1.1.2. *Contratos - *Historial Académico - *Historial Laboral	1.1.2.1. Gran cantidad de archivos sin organizar archivísticamente, sin tablas de valoración documental	Medio
		1.1.2.2. Insuficientes procedimientos para la preservación de documentos de archivos: tradicionales y digital	Medio
		1.1.2.3. Fácil acceso a información, personal y confidencial	Alto
1.2. Servicios	**1.2.1. Correo Electrónico**	1.2.1.1. Proliferación de "malware" o "malicious software"- Acciones de "ingeniería social" malintencionada: "phishing" - Correo no deseado - Noticias falsas	Alto
		1.2.1.2. Insuficiente definición de políticas referentes al cumplimiento de directrices sobre el intercambio de información a través de correo electrónico	Alto
		1.2.1.3. Manejo inadecuado de contraseñas (inseguras, compartidas)	Alto
1.3. Soft ware	**1.3.1. Gestores de Bases de Datos**	1.3.1.1. Manejo inadecuado de datos críticos (Datos sensibles mal gestionados: alteración, destrucción, etc.)	Alto

		1.3.1.2. Pérdidas de datos por errores del administrador	Medio
		1.3.1.3. Abuso de privilegios de acceso asignados - Privilegios excesivos e inutilizados	Alto
		1.3.1.4. Deficiencia en el sistema de encriptación	Medio
	1.3.2. Utilitarios de Ofimática - Sistemas Operativo - Antivirus	1.3.2.1. Falla de actualización del software - licencias no vigentes	Medio
	1.3.3. Programas para aplicaciones específicas, Gestor de Base de datos, máquinas virtuales, entre otros	1.3.3.1. Licencias no vigentes	Bajo
	1.3.4. Sistemas Operativo	1.3.4.1. Abuso de privilegios de acceso al SO	Muy Alto
1.4. Hardware	**1.4.1. Dispositivos de respaldo**	1.4.1.1. Exposición de los medios de almacenamiento para backups (intromisión por usuarios no autorizados, daños al HW)	Medio
		1.4.1.2. Afectación en los elementos informáticos a causa de catástrofes naturales: inundaciones, incendios, sismos, etc.	Alto
		1.4.1.3. Fallos en el hardware ocasionando pérdida de información relevante	Medio
	1.4.2. Servidores	1.4.2.1. Administración débil del servidor	Medio
		1.4.2.2. Deficiencia en el borrado de datos en equipos reciclados	Alto
		1.4.2.3. Accesos no autorizados	Alto
	1.4.3. Unidad Central de Proceso - Switch - Teclado - Monitor - Mouse - Proyector - Impresora - Computadora Portátil - Router	1.4.3.1. Fallo del equipo por corte de suministro eléctrico	Medio
		1.4.3.2. Insuficiente ejecución de mantenimientos preventivo y correctivo	Alto
		1.4.3.3. Robo de equipo y periféricos	Alto
		1.4.3.4. Uso inadecuado del activo por parte del personal (Errores voluntarios o involuntarios en el uso de la tecnología)	Medio
		1.4.3.5. Planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas	Alto
	1.4.4. Unidad Central de Proceso 1.4.5 Computadora portátil	1.4.4.1. Infección de sistemas a través de unidades portables. 1.4.5.1. Fallo en el software que posee el recurso informático a causa de virus	Medio
	1.4.6. Monitor	1.4.6.1. Acceder a información sin medio visual.	Bajo
	1.4.7. Switch	1.4.7.1. Abuso de privilegios de acceso al switch	Medio
1.5. Comunicaciones	**1.5.1. Servicio de internet: Red inalámbrica**	1.5.1.1. Cambios continuos en configuración de la red	Alto
		1.5.1.2. Cracking de contraseña WIFI	Alto
	1.5.2. Equipos de la Red Cableada e Inalámbrica - Patch Cord - Puntos de red - Switch Core	1.5.2.1. Cableado expuesto al acceso no autorizado	Medio
		1.5.2.2. Robo de equipo	Medio
		1.5.2.3. Insuficiente mantenimiento en los equipos y periféricos	Medio
1.6. Equipo Auxiliar	**1.6.1. Fuente de Alimentación**	1.6.1.1. Afectación en los elementos informáticos a causa de catástrofes naturales: inundaciones, incendios, sismos, etcétera.	Alto
	1.6.2. Cableado eléctrico	1.6.2.1. Insuficiente mantenimiento preventivo y correctivo	Alto
		1.6.2.2. Red cableada expuesta para el acceso no autorizado	Medio

En la tabla 2 se muestra los resultados del análisis de riesgos generales por activos clasificados por su impacto en la Facultad. Fuente: Ing. Gema Guerrero, Ing. Evelyn Quinteros y las autoras de la investigación.

3.1.1.2.Riesgos por Áreas

Tabla 3. *Análisis de riesgo de los activos informáticos: Áreas*

ANÁLISIS DE RIESGO DE LOS ACTIVOS INFORMÁTICOS: ÁREAS			
Activo	**Descripción**	**Amenaza**	**Impacto**
2.1. Software	**2.1.1. Sistema Operativo**	2.1.1.1. Limitada disponibilidad de licencias y recursos financieros para activar el software	Bajo
	2.1.2. Antivirus	2.1.2.1. Probabilidad de baja detección de virus.	Alto
	2.1.3. Programas para aplicaciones específicas, Gestor de Base de datos, máquinas virtuales, etc.	2.1.3.1. Carecen de licencia (Lenguajes de programación)	Bajo
		2.1.3.2. Errores de mantenimiento y/o actualización de programas.	Medio

2.2. Hardware	**2.2.1.Servidor DHCP y equipos de redes y telecomunicaciones**	2.2.1.1. Inadecuada configuración y/o fuera de servicio; probabilidad de robo de datos, probabilidades de Cracking de contraseña Wi-Fi, colocación del malware, probabilidades de acceso remoto.	Muy Alto
	2.2.2. Tarjeta Inalámbrica de las PC	2.2.2.1. Uso inapropiado e ilegal, Robo de datos, Cracking de contraseña Wi-Fi, colocación del malware.	Medio
	2.2.3. Unidad Central de Procesos (CPU´S de áreas de trabajo)	2.2.3.1. Corte de suministro eléctrico externo y/o fallos del sistema eléctrico accidental o por maniobras maliciosas	Medio
		2.2.3.2. Daños del hardware y software por falla eléctrica	Alto
		2.2.3.3.Insuficiente ejecución de mantenimientos preventivo y correctivo	Alto
		2.2.3.5. Corte de suministro eléctrico internos y/o fallos de reguladores de voltaje de forma accidental o por maniobras maliciosas	Muy Alto
		2.2.3.6. Infección del sistemas operacional por el uso de unidades portables	Alto
	2.2.4. Computadora portátil	2.2.4.1. Falla de aplicativos o sistemas a causa de virus	Alto
	2.2.5. Computadora portátil - Teclado - Impresora	2.2.5.1.Incorrecto uso del software por parte del personal	Alto
	2.2.6. Impresora - Monitor	2.2.6.1. Corte de suministro eléctrico internos y/o fallos de reguladores de voltaje de forma accidental o por maniobras maliciosas	Medio

En tabla 3 se muestra los resultados del análisis de riesgos de activos por las áreas de trabajo clasificados por su impacto en la Facultad. Fuente: Ing. Gema Guerrero, Ing. Evelyn Quinteros y las autoras de la investigación

3.1.1.3.Riesgos por Laboratorios

Tabla 4. *Análisis de riesgo de los activos informáticos: Laboratorios*

ANÁLISIS DE RIESGO DE LOS ACTIVOS INFORMÁTICOS: LABORATORIOS			
Activo	**Descripción**	**Amenaza**	**Impacto**
3.1. Software	**3.1.1. Sistemas Operativo**	3.1.1.1. Abuso de privilegios de acceso al SO	Muy Alto
		3.1.1.2. Limitada disponibilidad de licencias y recursos financieros para activar el software	Muy Alto
	3.1.2. Utilitarios de Ofimática	3.1.2.1. Errores de mantenimiento / actualización del paquete de OFFICE (software)	Bajo
	3.1.3. Antivirus	3.1.3.1. No disponen de licencia	Muy Alto
		3.1.3.2. Probabilidad de baja detección de virus.	Medio
	3.1.4. Programas para aplicaciones específicas, Gestor de Base de datos, máquinas virtuales, etc.	3.1.4.1. Carecen de licencia (Lenguajes de programación)	Bajo
		3.1.4.2. Errores de mantenimiento y/o actualización de programas.	Medio
3.2. Hardware	**3.2.1. Servidor DHCP y equipos de redes y telecomunicaciones**	3.2.1.1. Inadecuada configuración y/o fuera de servicio; probabilidad de robo de datos, probabilidades de Cracking de contraseña Wi-Fi, colocación del malware, probabilidades de acceso remoto.	Muy Alto
	3.2.2. Tarjeta Inalámbrica de las PC	3.2.2.1. Uso y manipulación inapropiada de la tarjeta.	Medio
	3.2.3. Unidad Central de Procesos (CPU´S de laboratorios de informática)	3.2.3.1. Corte de suministro eléctrico externo y/o fallos del sistema eléctrico accidental o por maniobras maliciosas	Medio
		3.2.3.2. Insuficiente ejecución de mantenimientos preventivo y correctivo	Alto
		3.2.3.3. Robo de equipo por personal no autorizado	Muy Alto
		3.2.3.4. Insuficiente actualización de Software (procesos y recursos)	Alto
	3.2.4. Teclados	3.2.4.1. Robos de periférico	Medio
		3.2.4.2. Derrame de líquidos, fluidos o alimentos sobre el periférico.	Medio
	3.2.5. Monitores de PC	3.2.5.1. Robos de periférico	Medio
		3.2.5.2. Manipulación de configuración del periférico	Baja
		3.2.5.3. Acceder a información sin medio visual.	Medio
		3.2.5.4. Errores de configuración	Bajo

	3.2.6. Mouse	3.2.6.1. Robo de equipo.	Muy Alto
		3.2.6.2. Fallos por averías o pérdida de vida útil.	Baja
	3.2.7. Proyector	3.2.7.1. Corte de suministro eléctrico externo y/o fallos del sistema eléctrico accidental o por maniobras maliciosas	Medio
		3.2.7.2. Insuficiente mantenimiento preventivo-correctivo y/o reposición de lámpara	Alto
		3.2.7.3. Robo o sustracción	Alto
	3.2.8. Switch (Redes)	3.2.8.1. Ingreso de contraseñas por personal no autorizado	Medio
		3.2.8.2. Compartir privilegios de acceso a usuarios no autorizados	Muy Alto
		3.2.8.3. Corte de suministro eléctrico externo y/o fallos del sistema eléctrico accidental o por maniobras maliciosas	Medio

En la tabla 4 se muestra los resultados del análisis de riesgos de activos por los laboratorios, clasificados por su impacto en la Facultad. Fuente: Ing. Gema Guerrero, Ing. Evelyn Quinteros y las autoras de la investigación

3.1.1.4.Riesgo por Aulas

Tabla 5. *Análisis de riesgo de los activos informáticos: Aulas*

ANÁLISIS DE RIESGO DE LOS ACTIVOS INFORMÁTICOS: AULAS			
Activo	**Descripción**	**Amenaza**	**Impacto**
4.1. Hardware	**4.1.1. Proyector**	4.1.1.1. Robo de periférico	Alto
		4.1.1.2. Corte de suministro eléctrico externo y/o fallos del sistema eléctrico accidental o por maniobras maliciosas	Medio
		4.1.1.3. Insuficiente mantenimiento preventivo-correctivo y/o reposición de lámpara	Alto
		4.1.1.4. Fallo de equipo por manipulación incorrecta del personal	Medio
4.2. Comunicaciones	**4.2.1. Red inalámbrica**	4.2.1.1. Cambios continuos en configuración de la red	Alto
		4.2.1.2. Cracking de contraseña WIFI	Alto

En la tabla 5 se muestra los resultados del análisis de riesgos de activos por las aulas, clasificados por su impacto en la Facultad. Fuente: Ing. Gema Guerrero, Ing. Evelyn Quinteros y las autoras de la investigación

3.1.2. Análisis de la Declaración de Aplicabilidad

El análisis de la declaración de aplicabilidad fue realizado por medio de la tarea de investigación "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", elaborado por las Egda. Kerly Delgado. Mediante el análisis de la aplicabilidad que se realizó a la Facultad de Ciencias Informáticas se pueden visualizar las políticas que nos ayudan con las amenazas existentes en los activos. Implementando la ISO 17799 como refuerzo para las amenazas que no tenían implementadas políticas de seguridad. Las cuales se dividieron en:

- Riesgos generales por activos informáticos
- Riesgos por Áreas
- Riesgos por Laboratorios

- Riesgos por Aulas

Cabe destacar que los resultados que presentamos de la investigación anterior han sido verificados, analizados por criterio de expertos y por las investigadoras, siendo adaptados a las necesidades del presente estudio.

3.1.2.1.Análisis Declaración de Aplicabilidad: Riesgos generales por activos informáticos

Tabla 6. *Análisis del informe: declaración de aplicabilidad por riesgos generales de los activos informáticos*

ANÁLISIS DEL INFORME: DECLARACIÓN DE APLICABILIDAD			
#	A quien aplica	Políticas ISO 27001:2005 - ISO 17799:2005	
		Sección	Descripción del control
1.1.1.1	Personal administrativo/área técnica	A.10.5.1	Respaldo de la información
		A.10.1.1	Procedimientos de operación documentados
1.1.1.2	Personal administrativo/área técnica	A.9.1.2	Controles de entrada físico
		A.9.1.3	Seguridad de oficinas, habitaciones y medios
1.1.1.3	Personal administrativo/área técnica	A.12.3.1	Política sobre el uso de controles criptográficos
1.1.2.1	Decana (contratos) – Secretaria de la Facultad (Historial académico y laboral)	A.7.2.1	Lineamientos de clasificación
1.1.2.2	Decana (contratos) – Secretaria de la Facultad (Historial académico y laboral)	A.10.7.3	Procedimientos de manejo de la información
1.1.2.3	Decana (contratos) – Secretaria de la Facultad (Historial académico y laboral)	A.11.1.1	Política de control de acceso
		A.11.3.3	Política de pantalla y escritorio limpio
1.2.1.1	Personal docente, personal administrativo, estudiantes	A.8.2.2	Capacitación y educación en seguridad de la información
		A.7.1.3	Uso aceptable de los activos
1.2.1.2	Personal docente, personal administrativo, estudiantes	A.10.8.4	Mensajería electrónica
		A.10.8.1	Políticas y procedimientos de intercambio de información
1.2.1.3	Personal docente, personal administrativo, estudiantes	11.3.1	Uso de claves secretas
1.3.1.1	Personal administrativo/área técnica	A.10.7.3	Procedimientos de manejo de la información
1.3.1.2	Personal administrativo/área técnica	A.10.5.1	Respaldo de la información
1.3.1.3	Personal administrativo/área técnica	A.11.1.1	Política de control de acceso
		11.2.2	Gestión de privilegios
1.3.1.4	Personal administrativo/área técnica	A.12.3.1	Política sobre el uso de controles criptográficos
1.3.2.1	Personal administrativo/área técnica	A.7.1.1	Inventario de activos
		A.12.5.1	Procedimientos de control de cambios
		A.15.1.2	Derechos de propiedad intelectual (DPI)
1.3.3.1	Personal docente, estudiantes		
1.3.4.1	Personal administrativo/área técnica	A.11.1.1	Política de control de acceso
1.4.1.1	Personal administrativo/área técnica	A.9.1.2	Controles de entrada físico
		A.10.7.1	Gestión de los medios removibles
1.4.1.2	Personal administrativo/área técnica	A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información
1.4.1.3	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipo
		A.10.5.1	Respaldo de la información
1.4.2.1	Personal administrativo/área técnica	A.7.1.3	Uso aceptable de los activos
1.4.2.2	Personal administrativo/área técnica	A.9.2.6	Seguridad en la reutilización o eliminación de los equipos
1.4.2.3	Personal administrativo/área técnica	A.11.1.1	Política de control de acceso

1.4.3.1	Personal administrativo/área técnica	9.2.2	Servicios públicos de soporte
	Personal administrativo/área técnica	A.12.6.1	Control de vulnerabilidades técnicas
1.4.3.2	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipo
1.4.3.3	Personal administrativo/área técnica	A.9.1.3	Seguridad de oficinas, habitaciones y medios
		9.2.1	Ubicación y protección del equipo
1.4.3.4	Personal docente, personal administrativo, estudiantes	A.7.1.3	Uso aceptable de los activos
		A.8.2.2	Capacitación y educación en seguridad de la información
1.4.3.5	Personal administrativo/área técnica	A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información
1.4.4.1 1.4.5.1	Personal docente, personal administrativo, estudiantes	A.10.4.1	Controles contra software malicioso
1.4.6.1	Personal docente, estudiantes	A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
1.4.7.1	Personal administrativo/área técnica	A.11.1.1	Política de control de acceso
1.5.1.1	Personal administrativo/área técnica	10.6.1	Controles de redes
1.5.1.2	Personal docente, estudiantes	A.11.4.1	Política sobre el uso de servicios en red
1.5.2.1	Personal administrativo/área técnica	9.2.3	Seguridad del cableado
1.5.2.2	Personal administrativo/área técnica	9.2.1	Ubicación y protección del equipo
1.5.2.3	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipos
1.6.1.1	Personal administrativo/área técnica	A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información
1.6.2.1	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipo
1.6.2.2	Personal administrativo/área técnica	9.2.3	Seguridad del cableado

Leyenda	
	Norma ISO 27001:2005
	Norma ISO 17799:2005

En la tabla 6 se muestra los resultados del análisis de la declaración de aplicabilidad generales por activos clasificados por su impacto en la Facultad. Fuente: Srta. Kerly Delgado y las autoras de la investigación.

3.1.2.2.Riesgos por Áreas

Tabla 7. *Análisis del informe: declaración de aplicabilidad por Áreas*

ANÁLISIS DEL INFORME: DECLARACIÓN DE APLICABILIDAD			
#	A quien aplica	Políticas ISO 27001:2005 - ISO 17799:2005	
		Sección	Descripción del control
2.1.1.1	Personal administrativo, aso de estudiantes y docentes	A.15.2.2	Verificación del cumplimiento técnico
2.1.2.1	Personal administrativo, aso de estudiantes y docentes	A.10.4.1	Controles contra software malicioso
2.1.3.1	Personal administrativo, aso de estudiantes y docentes	A.12.6.1	Control de vulnerabilidades técnicas
		A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
2.2.1.1	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipos
		A.9.2.6	Seguridad en la reutilización o eliminación de los equipos
		A.10.7.1	Gestión de los medios removibles
		A.10.10.5	Registro de fallas
		A.12.5.4	Filtración o fuga de información
		A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
2.2.2.1	Personal administrativo/área técnica	A.7.1.3	Uso aceptable de los activos
		A.9.2.4	Mantenimiento de equipos
		A.10.4.1	Controles contra software malicioso
2.2.3.1	Personal administrativo/área técnica	A.9.1.3	Seguridad de oficinas, habitaciones y medios
		A.9.1.5	Trabajo en áreas seguras
		A.13.1.2	Reportes sobre las debilidades en la seguridad
2.2.3.2		A.12.6.1	Control de vulnerabilidades técnicas
2.2.3.3		A.9.2.4	Mantenimiento de equipos
2.2.3.4		A.12.6.1	Control de vulnerabilidades técnicas

	Personal administrativo/área técnica	A.13.1.2	Reportes sobre las debilidades en la seguridad
2.2.3.5		A.9.1.3	Seguridad de oficinas, habitaciones y medios
		A.9.1.5	Trabajo en áreas seguras
		A.12.6.1	Control de vulnerabilidades técnicas
2.2.3.6	Personal administrativo, aso de estudiantes y docentes	A.9.1.1	Perímetro de seguridad física
		A.9.1.2	Controles de entrada físicos
		A.9.1.3	Seguridad de oficinas, habitaciones y medios
		A.10.4.1	Controles contra software malicioso
		A.10.4.2	Controles contra códigos móviles
		A.10.7.1	Gestión de los medios removibles
		A.12.5.4	Filtración o fuga de información
		A.13.1.2	Reportes sobre las debilidades en la seguridad
2.2.4.1	Personal administrativo, aso de estudiantes y docentes	A.10.4.1	Controles contra software malicioso
		A.10.4.2	Controles contra códigos móviles
		A.10.7.1	Gestión de los medios removibles
		A.12.5.4	Filtración o fuga de información
		A.12.6.1	Control de vulnerabilidades técnicas
		A.13.1.2	Reportes sobre las debilidades en la seguridad
2.2.5.1	Personal administrativo, aso de estudiantes y docentes	A.8.2.2	Capacitación y educación en seguridad de la información
		A.8.2.3	Proceso disciplinario
2.2.6.1	Personal administrativo, aso de estudiantes y docentes	9.2.3	Seguridad del cableado
		A.13.1.2	Reportes sobre las debilidades en la seguridad

Leyenda	
	Norma ISO 27001:2005
	Norma ISO 17799:2005

En la tabla 7 se muestra los resultados del análisis de la declaración de aplicabilidad generales por áreas clasificados por su impacto en la Facultad. Fuente: Srta. Kerly Delgado y las autoras de la investigación

3.1.2.3.Riesgos por Laboratorios

Tabla 8. *Análisis del informe: declaración de aplicabilidad por Laboratorios*

ANÁLISIS DEL INFORME: DECLARACIÓN DE APLICABILIDAD			
#	A quien aplica	Políticas ISO 27001:2005 - ISO 17799:2005	
		Sección	Descripción del control
3.1.1.1	Personal docente, personal administrativo, estudiantes	A.6.2.3	Tratamiento de la seguridad en contratos con terceras partes
		A.11.1.1	Política de control de acceso
3.1.1.2	Personal docente, personal administrativo, estudiantes	A.12.1.1	Análisis y especificación de los requisitos de seguridad
		A.12.6.1	Control de vulnerabilidades técnicas
		A.15.1.2	Derechos de propiedad intelectual (DPI)
		A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
3.1.2.1	Personal administrativo/área técnica	A.15.1.2	Derechos de propiedad intelectual (DPI)
3.1.3.1	Personal docente, personal administrativo, estudiantes	A.10.4.1	Controles contra software malicioso
		A.12.6.1	Control de vulnerabilidades técnicas
3.1.3.2		A.15.1.2	Derechos de propiedad intelectual (DPI)
3.1.4.1	Docente, estudiantes	A.10.3.2	Aceptación del sistema
3.1.4.2	Personal administrativo/área técnica	A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
		A.15.2.2	Verificación del cumplimiento técnico
3.2.1.1	Personal administrativo/área técnica	A.7.1.3	Uso aceptable de los activos
		A.9.2.4	Mantenimiento de equipos
		A.9.2.6	Seguridad en la reutilización o eliminación de los equipos

		A.10.4.1	Controles contra software malicioso
		A.10.5.1	Respaldo de la información
		A.12.5.1	Procedimientos de control de cambios
		A.12.6.1	Control de vulnerabilidades técnicas
3.2.2.1	Personal administrativo/área técnica	A.7.1.3	Uso aceptable de los activos
		A.7.2.2	Etiquetado y manejo de información
		A.9.2.4	Mantenimiento de equipos
		A.10.4.1	Controles contra software malicioso
3.2.3.1	Personal administrativo/área técnica	A.9.1.1	Perímetro de seguridad física
		A.9.1.2	Controles de entrada físicos
		A.9.1.3	Seguridad de oficinas, habitaciones y medios
3.2.3.2	Personal administrativo/área técnica	A.9.1.4	Protección contra amenazas externas y ambientales
		A.9.1.5	Trabajo en áreas seguras
3.2.3.3	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipos
3.2.3.4	Personal administrativo/área técnica	10.1.2	Gestión del cambio
		10.1.3	Segregación de los deberes
3.2.4.1	Personal docente, personal administrativo, estudiantes	A.9.1.1	Perímetro de seguridad física
		A.9.1.2	Controles de entrada físicos
		A.9.1.3	Seguridad de oficinas, habitaciones y medios
		10.1.3	Segregación de los deberes
		A.10.7.1	Gestión de los medios removibles
3.2.4.2	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipos
		A.12.6.1	Control de vulnerabilidades técnicas
3.2.5.1	Personal docente, personal administrativo, estudiantes	A.9.1.1	Perímetro de seguridad física
		A.9.1.2	Controles de entrada físicos
		A.9.1.3	Seguridad de oficinas, habitaciones y medios
3.2.5.2	Personal docente, personal administrativo, estudiantes	10.1.3	Segregación de los deberes
3.2.5.3	Personal docente, personal administrativo, estudiantes	A.12.5.4	Filtración o fuga de información
		A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
3.2.5.4	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipos
		A.10.10.6	Sincronización de relojes
3.2.6.1	Personal docente, personal administrativo, estudiantes	A.9.1.1	Perímetro de seguridad física
		A.9.1.2	Controles de entrada físicos
		A.9.1.3	Seguridad de oficinas, habitaciones y medios
3.2.6.2		10.1.3	Segregación de los deberes
		A.15.1.5	Prevención del uso inadecuado de medios de procesamiento de información
3.2.7.1	Personal docente, personal administrativo, estudiantes	A.9.1.3	Seguridad de oficinas, habitaciones y medios
		A.9.1.4	Protección contra amenazas externas y ambientales
3.2.8.1	Personal administrativo/área técnica	A.9.1.4	Protección contra amenazas externas y ambientales
3.2.8.2		A.11.1.1	Política de control de acceso
3.2.8.3		A.12.6.1	Control de vulnerabilidades técnicas

Leyenda	
	Norma ISO 27001:2005
	Norma ISO 17799:2005

En la tabla 8 se muestra los resultados del análisis de la declaración de aplicabilidad generales por laboratorios clasificados por su impacto en la Facultad. Fuente: Srta. Kerly Delgado y las autoras de la investigación

3.1.2.4.Riesgos por Aulas

Tabla 9. *Análisis del informe: declaración de aplicabilidad por Aulas*

ANÁLISIS DEL INFORME: DECLARACIÓN DE APLICABILIDAD			
#	A quien aplica	Políticas ISO 27001:2005 - ISO 17799:2005	
		Sección	Descripción del control
4.1.1.1	Personal docente, estudiantes	A.9.1.3	Seguridad de oficinas, habitaciones y medios
		9.2.1	Ubicación y protección del equipo
4.1.1.2	Personal administrativo/área técnica	9.2.2	Servicios públicos de soporte

4.1.1.3	Personal administrativo/área técnica	A.9.2.4	Mantenimiento de equipos
4.1.1.4	Personal docente, estudiantes	A.7.1.3	Uso aceptable de los activos
4.2.1.1	Personal administrativo/área técnica	10.6.1	Controles de redes
4.2.1.2	Personal docente, estudiantes	A.11.4.1	Política sobre el uso de servicios en red

Leyenda	
	Norma ISO 27001:2005
	Norma ISO 17799:2005

En la tabla 9 se muestra los resultados del análisis de la declaración de aplicabilidad generales por aulas clasificados por su impacto en la Facultad. Fuente: Srta. Kerly Delgado y las autoras de la investigación

3.1.3. *Medidas de Control de los Activos Informáticos de la FACCI*

Las medidas de control de los activos Informáticos fueron realizadas por medio de la tarea de investigación "Plan de Sensibilización, Comunicación y Capacitación para minimizar los riesgos informáticos en la FACCI". Elaborado por las Srta. Elizabeth Rodríguez y Srta. Diana Sánchez.

Mediante el análisis de la aplicabilidad y de los riesgos informáticos que se realizó a la Facultad de Ciencias Informáticas se pueden visualizar las medidas de implementación de diferentes controles aplicados para minimizar los riesgos existentes. Las cuales se dividieron en:

- Riesgos generales de los activos informáticos
- Riesgos por Áreas
- Riesgos por Laboratorios
- Riesgos por Aulas

Cabe destacar que los resultados que mostraremos de la investigación anterior han sido verificados, analizados por criterio de expertos y por las investigadoras, siendo adaptados a las necesidades del presente estudio.

3.1.3.1.Riesgos generales por activos informáticos

Tabla 10. *Medidas de control de los activos informáticos de la FACCI por Riesgos generales de los activos informáticos*

MEDIDAS DE CONTROL DE LOS ACTIVOS INFORMÁTICOS DE LA FACCI						
#	**Descripción del control adoptado a la FACCI**	**Medidas de implementación del control**	**Acciones (Cómo)**	**Quienes (responsable)**	**Tiempo**	**Documento a generar (Evidencia)**
1.1.1.1	Establecer los procedimientos de rutina para implementar la política de respaldo	1.- Determinar manual de procedimientos para el respaldo de información	1.- Establecer manual de procedimientos de rutina para implementar una política de respaldo de la información. 2.- Establecer cronograma de planificación de los backups, así como responsables a cargo de este proceso. 3.- Establecer modelo de formatos para el control de respaldos. 4.- Establecer cronograma de planificación de pruebas de los respaldos realizados cada cierto período de tiempo y asignar un responsable para ello. 5.-Redactar un informe a modo de reporte de las actividades realizadas en el proceso de respaldo e informe de pruebas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada semana	1.- Manual de procedimientos de rutina para respaldos 2.- Cronograma de planificación de los backups 3.- Modelo de formatos para el control de respaldos. 4.- Cronograma de planificación de pruebas de los respaldos realizados cada cierto período de tiempo 5.-Informe de reporte de las actividades de backups y de pruebas de seguridad.
	Preparar, mantener e informar procedimientos de operación para las actividades de copias de seguridad	1.- Documentar manual procedimientos de operación para las actividades de copias de seguridad de la información.	1.- Establecer manual de procedimientos internos para el proceso de realización de respaldos. 2.- Establecer cronograma de sensibilización con el personal del área técnica. 3.- Elaborar informe de actividades.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada período académico	1.- Manual de procedimientos internos para el proceso de realización de respaldos. 2.- Cronograma de sensibilización con el personal del área técnica. 3.- Informe
1.1.1.2	Establecer la protección de las áreas mediante controles de ingreso apropiado	1.- Determinar manual de instrucciones sobre los requerimientos de seguridad de ingreso al área	1.- Establecer manual de instrucciones de seguridad para el ingreso a las áreas restringidas. 2.- Modelo de ficha de registro de la fecha y hora de entrada y salida de los visitantes, supervisado por personal del administrativo/área técnica. 3.- Realizar informes diarios de los ingresos suscitados y anomalías previstas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Manual de instrucciones de seguridad para el ingreso a las áreas restringidas. 2.- Modelo de ficha de registro de visitantes. 3.- Informes

	Establecer la seguridad de oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Determinar procedimientos para la seguridad física para las aulas. 2.- Determinar controles de acceso físico	1.- Establecer procedimientos de seguridad para la protección física en las áreas de la Facultad. 2.- Elaborar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Realizar controles de acceso de físico 4.- Preparar y comunicar informes periódicos	1. Personal Administrativo/Decana RESPONSABLE 2. Personal Administrativo/Área Técnica 3. Docentes - Usuario interno y externo	Periódico: Revisar y actualizar cada año	1. - Procedimientos de seguridad para la protección física en las áreas. 2. - Manual de funciones y responsabilidades para usuarios internos y externos. 3. - Controles de acceso físico. 4. - Informes
1.1.1.3	Establecer políticas acerca del uso de controles criptográficos para proteger la información	1.- Determinar manual de políticas sobre el uso de controles criptográficos en el proceso de respaldo de seguridad de la información	1.- Establecer manual de políticas sobre el uso de controles criptográficos en base al enfoque administrativo de la institución, al análisis de riesgos y el impacto de utilizar información codificada. 2.- Establecer manual de funciones para usuarios internos del área técnica. 3.- Establecer cronograma para realizar pruebas de seguridad 4.- Realizar y comunicar informe de pruebas e implementación.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada período	1.- Manual de políticas sobre el uso de controles criptográficos 2.- Manual de funciones para usuarios internos del área técnica. 3.- Cronograma para realizar pruebas de seguridad 4.- Informes
1.1.2.1	Establecer pautas para la clasificación de la información para indicar la necesidad, prioridades y grado de protección basado en lo que determina UCCI	1.- Determinar manual de procedimientos para la clasificación de información	1.- Establecer manual de procedimientos para la clasificación de la información de acuerdo con los lineamientos establecidos en UCCI, las necesidades de la Facultad, control de acceso del personal que maneja información generada a través de sus funciones. 2.- Establecer cronograma de sensibilización al personal de secretaría. 3.- Informes de las actividades de la socialización de las pautas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI	Periódico: Revisar y actualizar cada año	1.- Manual de procedimientos para la clasificación de la información. 2.- cronograma de sensibilización 3.- Informes
1.1.2.2	Establecer procedimientos para el manejo, almacenaje y comunicación de la información consistente con su clasificación	1.- Determinar manual de procedimientos para el manejo y almacenaje de información consistente con su clasificación. 2.- Desarrollar y mantener un modelo de registro formal de los usuarios autorizados a acceder a la información	1.- Establecer manual de procedimientos para el manejo y almacenaje de la información en base a las restricciones de acceso, manipuleo y etiquetado de medios, y otras especificaciones. 2.- Elaborar un modelo de registro formal de las personas autorizadas al acceso de la información. 3.- Disponer un cronograma de capacitación periódico. 4.- Desarrollar e implementar una planificación de control de protección y permisos 5.- Elaborar y sociabilizar informes periódicos.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI	Periódico: Revisar y actualizar cada período	1.- Manual de procedimientos para el manejo y almacenaje de la información. 2.- Modelo de registro formal de las personas autorizadas al acceso de la información. 3.- Cronograma de capacitación periódico. 4.- Planificación de control de protección y permisos 5.- Informes

1.1.2.3	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	Desarrollar la política general de seguridad de acceso a la información de los contratos e historiales generados por los procesos de la Facultad	1.- Establecer manual de políticas generales de seguridad de acceso para cada usuario o grupos de usuario que maneje información. 2.- Establecer un cronograma para la revisión periódica de los controles de acceso. 3.- Determinar manual de uso de activos. 4.- Establecer modelo de revocación de derechos de acceso. (Cuando sea el caso) 5.- Desarrollar e implementar Planificación de control de seguridad y acceso. 6.- Establecer cronograma de sensibilización con el personal interesado 7.-Establecer manual de funciones y responsabilidades para usuarios internos. 8.- Elaborar y socializar informes periódicos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Personal de Secretaría 4.- Miembros del SGSI	Periódico: Revisar y actualizar cada período	1.- Manual de políticas generales de seguridad de acceso. 2.- Cronograma para la revisión periódica de los controles de acceso. 3.- Manual de uso de activos. 4.- Modelo de revocación de derechos de acceso. 5.- Planificación de control de seguridad y acceso. 6.- Cronograma de sensibilización 7.-Manual de funciones y responsabilidades para usuarios internos 8.- Informes
	Establecer políticas de escritorio y pantalla limpia para los medios de procesamiento de la información	1.- Determinar manual de políticas de escritorio limpio y de pantalla limpia para el personal administrativo	1.- Establecer manual de políticas de escritorio limpio y pantalla limpia en base a la clasificación de la información, riesgos detectados, requerimientos de la unidad académica, requerimientos legales. 2.- Establecer políticas de seguridad de confiabilidad y acceso. 3.- Crear manual de funciones y responsabilidades para personal administrativo 4.- Determinar manual de uso de activos. 5.- Elaborar y socializar informes periódicos.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Personal de Secretaría	Periódico: Revisar y actualizar cada período académico	1.- Manual de políticas de escritorio limpio y pantalla limpia. 2.- Manual de políticas de seguridad de confiabilidad y acceso. 3.- Manual de funciones y responsabilidades para personal administrativo 4.- Manual de uso de activos. 5.- Informes.
1.2.1.1	Proporcionar a los empleados, estudiantes y terceras personas una adecuada capacitación en procedimientos de seguridad y uso adecuado de los activos informáticos	1.- Elaborar propuesta de plan de educación y capacitación continua en aspectos de seguridad informática. 2.-Establecer manual de procesos disciplinarios por uso inadecuado de activos	1.- Establecer cronograma para el proceso de capacitación y comunicación de los procesos de seguridad implementados en la Facultad. 2.- Elaborar propuesta de capacitación, sensibilización y comunicación. 3.- Establecer manual de procesos disciplinarios de acuerdo con el activo y grado de incumplimiento. 4.- Elaborar modelos para los medios informativos para llevar a cabo la sociabilización de los procesos de seguridad. 5.- Elaborar modelo de certificado de participación a los asistentes y firmas de actas. 6.- Realizar un informe de las actividades.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período académico	1.- Cronograma para el proceso de capacitación y comunicación. 2.- Propuesta de capacitación, sensibilización y comunicación. 3.- Manual de procesos disciplinarios de acuerdo con el activo y grado de incumplimiento. 4.- Modelo de medios informativos 5.- Modelo de certificado de participación y actas. 6.- Informes

	Establecer propuesta de lineamientos para el uso adecuado de los activos informáticos de la Facultad	1.- Determinar manual de guía de uso de activos. 2.- Desarrollar plan de educación y capacitación.	1.- Establecer manual de uso de activos. 2.- Instaurar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Fijar un plan de sensibilización y capacitación. 4.- Disponer un cronograma de capacitación periódico. 5.- Elaborar certificado de participación a los asistentes y firmas de actas. 6.- Formar y sociabilizar informes de las capacitaciones.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período	1.- Manual de uso de activos. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Plan de sensibilización y capacitación. 4.- Cronograma de capacitación periódico. 5.- Certificado de participación a los asistentes y firmas de actas. 6.- Informes
1.2.1.2	Establecer la protección adecuada de a información involucrada en mensajes electrónicos en base a parámetros de seguridad establecidos	1.- Determinar la implementación de política de uso del servicio de correo electrónico 2.- Desarrollar plan de educación y capacitación.	1.- Elaborar cronograma para sensibilizar con el personal las políticas de uso del servicio de correo electrónico. 2.- Elaborar modelo de plantilla de acuerdo de intercambio de ejemplo cuando se requiera el envío por correo electrónico de información sensible para la Facultad. 3.- Crear manual de funciones y responsabilidades para usuarios internos y externos. 4.- Realizar un informe de las actividades.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes	Periódico: Revisar y actualizar cada período	1.- Cronograma para sensibilizar 2.- Modelo de plantilla de acuerdo de intercambio de información. 3.- Manual de funciones y responsabilidades para usuarios internos y externos. 4.- Informes
	Establecer procedimientos y controles para el intercambio formal de la información a través del uso de correo electrónico	1.- Determinar manual de procedimientos y controles a seguir cuando se utiliza el correo electrónico para el intercambio de información	1.- Establecer manual de procedimientos y controles para el intercambio de información. 2.- Elaborar plantilla de acuerdo de confidencialidad. 3.- Establecer cronograma para sensibilizar los ejemplos de procedimientos y controles generales a seguir a la comunidad FACCI. 4.- Crear un informe de las actividades realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes	Periódico: Revisar y actualizar cada período	1.- Manual de procedimientos y controles para el intercambio de información. 2.- Plantilla de acuerdo de confidencialidad. 3.- Cronograma para sensibilizar 4.- Informes
1.2.1.3	Instruir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de claves secretas	1.- Desarrollar plan de educación y capacitación para sensibilizar las políticas generales de contraseña segura para los sistemas institucionales definido por la UCCI	1.- Establecer cronograma para sensibilización de las políticas a la comunidad FACCI. 2.- Disponer un cronograma de capacitación periódico. 3.- Elaborar certificado de participación a los asistentes y firmas de actas. 4.- Formar y sociabilizar informes de las capacitaciones.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes	Periódico: Revisar y actualizar cada período	1.- Establecer cronograma para sensibilización de las políticas a la comunidad FACCI. 2.- Cronograma de capacitación periódico. 3.- Modelo de certificado de participación y actas. 4.- Informes. 5.- Políticas de Contraseña, elaborado por la UCCI

1.3.1.1	Establecer procedimientos para el manejo, almacenaje y comunicación de la información consistente con su clasificación	1.- Determinar manual de procedimientos para el manejo y almacenaje de información consistente con su clasificación. 2.- Desarrollar y mantener un modelo de registro formal de los usuarios autorizados a acceder a la información	1.- Establecer manual de procedimientos para el manejo y almacenaje de la información en base a las restricciones de acceso, manipuleo y etiquetado de medios, y otras especificaciones. 2.- Elaborar un modelo de registro formal de las personas autorizadas al acceso de la información. 3.- Disponer un cronograma de capacitación periódico. 4.- Desarrollar e implementar una planificación de control de protección y permisos 5.- Elaborar y sociabilizar informes periódicos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI	Periódico: Revisar y actualizar cada período	1.- Manual de procedimientos para el manejo y almacenaje de la información. 2.- Modelo de registro formal de las personas autorizadas al acceso de la información. 3.- Cronograma de capacitación periódico. 4.- Planificación de control de protección y permisos 5.- Informes
1.3.1.2	Establecer los procedimientos de rutina para implementar la política de respaldo	1.- Determinar manual de procedimientos para el respaldo de información	1.- Establecer manual de procedimientos de rutina para implementar una política de respaldo de la información. 2.- Establecer cronograma de planificación de los backups, así como responsables a cargo de este proceso. 3.- Establecer modelo de formatos para el control de respaldos. 4.- Establecer cronograma de planificación de pruebas de los respaldos realizados cada cierto período de tiempo y asignar un responsable para ello. 5.-Redactar un informe a modo de reporte de las actividades realizadas proceso de respaldo e informe de pruebas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada semana	1.- Manual de procedimientos de rutina para respaldos 2.- Cronograma de planificación de los backups 3.- Modelo de formatos para el control de respaldos. 4.- Cronograma de planificación de pruebas de los respaldos realizados cada cierto período de tiempo 5.-Informe de reporte de las actividades de backups y de pruebas de seguridad.
1.3.1.3	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	1.- Determinar un manual de políticas para la seguridad al acceso lógico al gestor de BD 2.-Determinar controles de acceso físico al área restringida	1.- Establecer manual de políticas de control de acceso, lógicos y físicos. 2.- Establecer un cronograma para la revisión periódica de los controles de acceso. 3.-Establecer manual de funciones y responsabilidades para usuarios internos y externos. 4.- Establecer modelo de revocación de derechos de acceso. (Cuando sea el caso) 5.- Determinar manual de uso de activos. 6.- Elaborar informes periódicos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Usuario interno y externo	Periódico: Revisar y actualizar cada año	1.- Manual de políticas de control de acceso: lógico y físico 2.- Cronograma para la revisión periódica de los controles de acceso. 3.-Manual de funciones y responsabilidades para usuarios internos y externos. 4.- Modelo de revocación de derechos de acceso. 5.- Manual de uso de activos. 6.- Informes

	Establecer la restricción y control de la asignación y uso de los privilegios en base a las funciones del empleado	1.- Determinar manual para el control de la asignación de privilegios a través de un proceso de autorización formal	1.- Establecer manual de pasos para el control de la asignación de privilegios a través de autorización formal. 2.- Elaborar un modelo de proceso de autorización y registro de privilegios en caso de que se requiera otorgan dichos privilegios. 3.- Disponer de un cronograma de sensibilización de las políticas con el personal del Personal Administrativo/Área Técnica. 4.- Elaborar informe de las actividades realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada período	1.- Manual de pasos para el control de la asignación de privilegios a través de autorización formal 2.- Modelo de proceso de autorización y registro de privilegios 3.- Cronograma de sensibilización de las políticas 4.- Informes
1.3.1.4	Establecer políticas acerca del uso de controles criptográficos para proteger la información	1.- Determinar manual de políticas sobre el uso de controles criptográficos en el proceso de respaldo de seguridad de la información	1.- Establecer manual de políticas sobre el uso de controles criptográficos en base al enfoque administrativo de la institución, al análisis de riesgos y el impacto de utilizar información codificada. 2.- Establecer manual de funciones para usuarios internos del área técnica. 3.- Establecer cronograma para realizar pruebas de seguridad 4.- Realizar y comunicar informe de pruebas e implementación.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada período	1.- Manual de políticas sobre el uso de controles criptográficos 2.- Manual de funciones para usuarios internos del área técnica. 3.- Cronograma para realizar pruebas de seguridad 4.- Informes
1.3.2.1	Elaborar y mantener actualizado un inventario de todos los activos informáticos de la Facultad	1.- Determinar modelo de inventario del catálogo de software existente en la Facultad	1.- Establecer la implementación de formato de inventario del software existente en la Facultad, con las especificaciones técnicas requeridas para incluirlo en el plan de actualizaciones. 2.- Establecer manual de funciones y responsabilidades para el personal del área técnica. 3.- Informes de las actividades realizadas	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada período	1.- Modelo de formato de inventario del software existente en la Facultad 2.- Manual de funciones y responsabilidades para el personal del área técnica. 3.- Informes
	Establecer la segregación de deberes y áreas de responsabilidad de funciones del departamento técnico	1.- Determinar manual de plan de actualizaciones para el software. 2.- Determinar modelo de registro de control del cambio de software. 3.- Determinar manual de funciones y responsabilidades	1.- Establecer manual del plan de actualizaciones para el software. 2.- Desarrollar e implementar manual de políticas sobre el cumplimiento de derechos de propiedad intelectual. 3.- Establecer manual de funciones y responsabilidades para el personal del área técnica. 4.- Establecer manual de procedimientos para detectar e instalar actualizaciones. 5.- Establecer manual de procedimientos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Cada vez que se realice una actualización del software	1.- Manual del plan de actualizaciones para el software. 2.- Manual de políticas sobre el cumplimiento de derechos de propiedad intelectual. 3.- Manual de funciones y responsabilidades para el personal del área técnica. 4.- Manual de procedimientos para detectar e instalar

			para deshacer cambios 6.- Establecer modelo de registro de control de los cambios realizados al software. (Los cambios deben ser autorizados por la decana y continuamente por UCCI para su ejecución) 7.- Elaborar y socializar informes periódicos			actualizaciones. 5.- Manual de procedimientos para deshacer cambios 6.- Modelo de registro de control de los cambios de SW 7.- Informes
1.3.3.1	Establecer la implementación de normas generales sobre el uso de material con respecto a los cuales pueda existir derechos de propiedad intelectual y uso de productos software patentado	1.- Determinar manual de procedimientos para asegurar que se cumpla con la Ley de Propiedad Intelectual	1.- Establecer manual de procedimientos para el cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos software. 2.- Establecer manual de controles de adquisición de software solo a través de fuentes conocidas y acreditados. 3.- Establecer manual de política para mantener las condiciones de licencias apropiadas. 4.- Elaborar cronograma para pruebas de verificaciones de la instalación de software autorizados y productos con licencia. 5.- Establecer cronograma para sensibilizar las políticas con la comunidad FACCI. 6.- Realizar un informe de las actividades realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Docentes 4.- Estudiantes	Periódico: Revisar y actualizar cada período	1.- Manual de procedimientos para el cumplimiento de los derechos de propiedad intelectual 2.- Manual de controles de adquisición de software 3.- Manual de política para mantener las condiciones de licencias apropiadas. 4.- Cronograma para pruebas de verificaciones de la instalación de software 5.- Cronograma para sensibilizar las políticas con la comunidad FACCI. 6.- Informes
1.3.4.1	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	1.- Determinar un manual de políticas para la seguridad al acceso lógico al SO 2.-Determinar controles de acceso físico al área	1.- Establecer manual de políticas de control de acceso, lógicos y físicos. 2.- Establecer un cronograma para la revisión periódica de los controles de acceso. 3.-Establecer manual de funciones y responsabilidades para usuarios internos y externos. 4.- Establecer modelo de revocación de derechos de acceso. (Cuando sea el caso) 5.- Determinar manual de uso de activos. 6.- Desarrollar e implementar Planificación de control de seguridad y acceso 7.- Elaborar y socializar informes periódicos preventivos y de fin de períodos.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Usuario interno y externo	Periódico: Revisar y actualizar cada año	1.- Manual de políticas de control de acceso: lógico y físico 2.- Cronograma para la revisión periódica de los controles de acceso. 3.- Manual de funciones y responsabilidades para usuarios internos y externos. 4.- Modelo de revocación de derechos de acceso. 5.- Manual de uso de activos. 6.- Planificación de control de seguridad y acceso 7.- Informes

1.4.1.1	Establecer la protección de las áreas mediante controles de ingreso apropiado	1.- Determinar manual de instrucciones sobre los requerimientos de seguridad de ingreso al área	1.- Establecer manual de instrucciones de seguridad para el ingreso a las áreas restringidas. 2.- Modelo de ficha de registro de la fecha y hora de entrada y salida de los visitantes, supervisado por personal del administrativo/área técnica. 3.- Realizar informes diarios de los ingresos suscitados y anomalías previstas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Manual de instrucciones de seguridad para el ingreso a las áreas restringidas. 2.- Modelo de ficha de registro de visitantes. 3.- Informes
	Establecer procedimientos para la gestión de medios removibles	1.- Determinar manual de políticas para controlar y proteger los medios removibles	1.- Establecer manual de políticas de seguridad a los medios removibles. 2.- Crear manual de funciones y responsabilidades para usuarios internos y externos. 3.- Establecer modelo de ficha para llevar el control del registro de eliminación de los dispositivos. 4.- Desarrollar e implementar una planificación de control de protección y permisos 5.- Elaborar y socializar informes periódicos.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3. Usuario interno y externo	Periódico: Revisar y actualizar cada período académico	1.- Manual de políticas de seguridad a los medios removibles. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Modelo de ficha para llevar el control del registro de eliminación de los dispositivos. 4.- Planificación de control de protección y permisos 5.- Informes
1.4.1.2	Establecer el desarrollo e implementación de planes para mantener/restaurar los servicios prestados y asegurar la disponibilidad de la información en el nivel requerido	1.- Determinar la implementación de los planes de continuidad y contingencia formulados 2.- Desarrollar plan de educación y capacitación.	1.- Elaborar cronograma para sensibilizar con el personal de los procedimientos y procesos de recuperación/acción. 2.- Crear manual de funciones y responsabilidades para usuarios internos y externos. 3.- Crear un cronograma para realizar pruebas de los planes como una simulación. 4. Realizar un informe donde se detallen las actividades de la puesta en marcha de los planes.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Cronograma para sensibilizar con el personal de los procedimientos y procesos de recuperación/acción. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Cronograma para realizar pruebas de los planes 4. Informes.

1.4.1.3	Establecer procedimientos de mantenimiento del equipo para asegurar su continua disponibilidad e integridad	1.- Determinar procedimientos de mantenimiento preventivo y correctivo de equipos y periféricos. 2.- Determinar controles apropiados para guiar el programa de mantenimiento de los equipos y periféricos. 3.- Determinar modelo de solicitud para el retiro de equipos y periféricos.	1.- Establecer procedimientos de mantenimiento de equipos y periféricos. 2.- Elaborar controles apropiados cuando se programa el equipo para mantenimiento 3.- Generar un cronograma de mantenimiento periódico. 4.- Utilizar plantilla de mantenimiento de hardware. 5.- Implantar una plantilla modelo de solicitud para el retiro formal del equipo y periférico. 6.- Diseñar un modelo de registro de las fallas internas encontradas en el soporte. 7.- Elaborar y comunicar informes del mantenimiento realizado.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Procedimientos de mantenimiento de equipos y periféricos. 2.- Controles para mantenimiento 3.- Cronograma de mantenimiento periódico. 4.- Plantilla de mantenimiento de hardware. 5.- Modelo de solicitud para el retiro formal del equipo y periférico. 6.- Modelo de registro de las fallas internas. 7.- Informes
	Establecer los procedimientos de rutina para implementar la política de respaldo	1.- Determinar manual de procedimientos para el respaldo de información	1.- Establecer manual de procedimientos de rutina para implementar una política de respaldo de la información. 2.- Establecer cronograma de planificación de los backups, así como responsables a cargo de este proceso. 3.- Establecer modelo de formatos para el control de respaldos. 4.- Establecer cronograma de planificación de pruebas de los respaldos realizados cada cierto período de tiempo y asignar un responsable para ello. 5.-Redactar un informe a modo de reporte de las actividades realizadas proceso de respaldo e informe de pruebas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada semana	1.- Manual de procedimientos de rutina para respaldos 2.- Cronograma de planificación de los backups 3.- Modelo de formatos para el control de respaldos. 4.- Cronograma de planificación de pruebas de los respaldos realizados cada cierto período de tiempo 5.-Informe de reporte de las actividades de backups y de pruebas de seguridad.
1.4.2.1	Establecer propuesta de lineamientos para el uso adecuado de los activos informáticos de la Facultad	1.- Determinar manual de guía de uso de activos. 2.- Desarrollar plan de educación y capacitación.	1.- Establecer manual de uso de activos. 2.- Instaurar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Fijar un plan de sensibilización y capacitación. 4.- Disponer un cronograma de capacitación periódico. 5.- Elaborar certificado de participación a los asistentes y firmas de actas. 6.- Formar y sociabilizar informes de las capacitaciones.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período	1.- Manual de uso de activos. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Plan de sensibilización y capacitación. 4.- Cronograma de capacitación periódico. 5.- Certificado de participación a los asistentes y firmas de actas. 6.- Informes

1.4.2.2	Establecer procedimientos en la eliminación seguro o re-uso del equipo en redes.	1.- Determinar manual de normativas enfocadas al borrado de datos en equipos reciclados	1.- Establecer manual de normativas para el borrado de datos en equipos reciclados. 2.- Establecer modelo de seguimiento de los dispositivos. 3.- Documentar cualquier operación realizada sobre los dispositivos que almacenan información: mantenimiento, reparación, sustitución, etc. 4.- Establecer manual de procesos de eliminación de información para la reutilización de equipos electrónicos en buen estado. 5.- Establecer manual de procesos de eliminación de la información antes de deshacerse de los soportes de almacenamiento. 6.- Elaborar informe del proceso de borrado.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Manual de normativas para el borrado de datos en equipos reciclados. 2.- Modelo de seguimiento 3.- Documento de operación realizada sobre los dispositivos que almacenan información. 4.- Manual de procesos de eliminación de información para la reutilización de equipos electrónicos en buen estado. 5.- Manual de procesos de eliminación de la información antes de deshacerse de los soportes de almacenamiento. 6.- Informes
1.4.2.3	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	1.- Determinar un manual de políticas para la seguridad al acceso lógico al switch. 2.-Determinar controles de acceso físico al área asignada para switch	1.- Establecer manual de políticas de control de acceso, lógicos y físicos. 2.- Establecer un cronograma para la revisión periódica de los controles de acceso. 3.-Establecer manual de funciones y responsabilidades para usuarios internos y externos. 4.- Establecer modelo de revocación de derechos de acceso. (Cuando sea el caso) 5.- Determinar manual de uso de activos. 6.- Desarrollar e implementar Planificación de control de seguridad y acceso 7.- Elaborar y socializar informes periódicos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Usuario interno y externo	Periódico: Revisar y actualizar cada año	1.- Manual de políticas de control de acceso. 2.- Cronograma para la revisión periódica de los controles de acceso. 3.-Manual de funciones y responsabilidades para usuarios internos y externos. 4.- Modelo de revocación de derechos de acceso. 5.- Manual de uso de activos. 6.- Planificación de control de seguridad y acceso 7.- Informes
1.4.3.1	Establecer protección del equipo y periféricos ante posibles interrupciones de fallas de energía de los equipos	1.- Desarrollar protecciones generales para los equipos de posibles fallas de energía.	1.- Establecer procedimientos de protección general para los equipos y periféricos informáticos ante las posibles fallas de energía en el suministro eléctrico. 2.- Crear un cronograma para inspecciones (mantenimiento) periódicas del sistema eléctrico. 3.- Utilizar plantilla de mantenimiento del sistema eléctrico. 4.- Elaborar modelo de registro de las fallas internas encontradas en mantenimiento. 5.- Generar y comunicar informes de las inspecciones realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Procedimientos de protección general para los equipos y periféricos. 2.- Cronograma para inspecciones del sistema eléctrico. 3.- Plantilla de mantenimiento. 4.- Modelo de registro de fallas internas. 5.- Informes

	Control de vulnerabilidades técnicas respecto a las fallas en el hardware	1.- Determinar manual para el proceso de gestión efectivo para las vulnerabilidades técnicas. 2.- Determinar cronograma para pruebas de seguridad	1.- Establecer manual para el proceso de gestión de vulnerabilidades técnicas de los activos informáticos 2.- Establecer manual de funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica para el personal del área. 3.- Mantener un inventario actualizado y completo de los activos de la FACCI. 4.- Establecer cronograma para pruebas de seguridad 5.- Preparar y comunicar informes periódicos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Manual para el proceso de gestión de vulnerabilidades técnicas de los activos informáticos 2.- Manual de funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica 3.- Inventario actualizado 4.- Cronograma para pruebas de seguridad 5.- Informes
1.4.3.2	Establecer procedimientos de mantenimiento del equipo para asegurar su continua disponibilidad e integridad	1.- Determinar procedimientos de mantenimiento preventivo y correctivo de equipos y periféricos. 2.- Determinar controles apropiados para guiar el programa de mantenimiento de los equipos y periféricos. 3.- Determinar modelo de solicitud para el retiro de equipos y periféricos.	1.- Establecer procedimientos de mantenimiento de equipos y periféricos. 2.- Elaborar controles apropiados cuando se programa el equipo para mantenimiento 3.- Generar un cronograma de mantenimiento periódico. 4.- Utilizar plantilla de mantenimiento de hardware. 5.- Implantar una plantilla modelo de solicitud para el retiro formal del equipo y periférico. 6.- Diseñar un modelo de registro de las fallas internas encontradas en el soporte. 7.- Elaborar y comunicar informes del mantenimiento realizado.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Procedimientos de mantenimiento de equipos y periféricos. 2.- Controles para mantenimiento 3.- Cronograma de mantenimiento periódico. 4.- Plantilla de mantenimiento de hardware. 5.- Modelo de solicitud para el retiro formal del equipo y periférico. 6.- Modelo de registro de las fallas internas. 7.- Informes
1.4.3.3	Establecer la seguridad de oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Determinar procedimientos para la seguridad física para las aulas. 2.- Determinar controles de acceso físico	1.- Establecer procedimientos de seguridad para la protección física en las áreas. 2.- Elaborar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Realizar controles de acceso de físico 4.- Preparar y comunicar informes periódicos	1. Personal Administrativo/Decana RESPONSABLE 2. Personal Administrativo/Área Técnica 3. Docentes – Usuarios internos y externos	Periódico: Revisar y actualizar cada año	1. - Procedimientos de seguridad para la protección física en las áreas. 2. - Manual de funciones y responsabilidades para usuarios internos y externos. 3. - Controles de acceso físico. 4. - Informes
	Establecer pautas para la ubicación y protección de los equipos informáticos de la Facultad	1.- Determinar manual de directrices para la ubicación y protección de los proyectores en las aulas.	1.- Establecer manual de directrices para la ubicación y protección adecuada del activo dentro del área de acuerdo con las especificaciones del espacio. 2.- Realizar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Elaborar y comunicar informes periódicos	1. Personal Administrativo/Decana RESPONSABLE 2. Personal Administrativo/Área Técnica 3. Docentes- Usuario interno y externo	Periódico: Revisar y actualizar cada año	1.- Manual de directrices para la ubicación y protección adecuada del activo. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Informes

1.4.3.4	Establecer propuesta de lineamientos para el uso adecuado de los activos informáticos de la Facultad	1.- Determinar manual de guía de uso de activos. 2.- Desarrollar plan de educación y capacitación.	1.- Establecer manual de uso de activos. 2.- Instaurar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Fijar un plan de sensibilización y capacitación. 4.- Disponer un cronograma de capacitación periódico. 5.- Elaborar certificado de participación a los asistentes y firmas de actas. 6.- Formar y sociabilizar informes de las capacitaciones.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período	1.- Manual de uso de activos. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Plan de sensibilización n y capacitación. 4.- Cronograma de capacitación periódico. 5.- Certificado de participación a los asistentes y firmas de actas. 6.- Informes
	Proporcionar a los empleados, estudiantes y terceras personas una adecuada capacitación en procedimientos de seguridad y uso adecuado de los activos informáticos	1.- Elaborar propuesta de plan de educación y capacitación continua en aspectos de seguridad informática. 2.-Establecer manual de procesos disciplinarios por uso inadecuado de activos	1.- Establecer cronograma para el proceso de capacitación y comunicación de los procesos de seguridad implementados en la Facultad. 2.- Elaborar propuesta de capacitación, sensibilización y comunicación. 3.- Establecer manual de procesos disciplinarios de acuerdo con el activo y grado de incumplimiento. 4.- Elaborar modelos para los medios informativos para llevar a cabo la sociabilización de los procesos de seguridad. 5.- Elaborar modelo de certificado de participación a los asistentes y firmas de actas. 6.- Realizar un informe de las actividades realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período académico	1.- Cronograma para el proceso de capacitación y comunicación. 2.- Propuesta de capacitación, sensibilización y comunicación. 3.- Manual de procesos disciplinarios de acuerdo con el activo y grado de incumplimiento. 4.- Modelo de medios informativos 5.- Modelo de certificado de participación y actas. 6.- Informes
1.4.3.5	Establecer el desarrollo e implementación de planes para mantener/restaurar los servicios prestados y asegurar la disponibilidad de la información en el nivel requerido	1.- Determinar la implementación de los planes de continuidad y contingencia formulados 2.- Desarrollar plan de educación y capacitación.	1.- Elaborar cronograma para sensibilizar con el personal de los procedimientos y procesos de recuperación/acción. 2.- Crear manual de funciones y responsabilidades para usuarios internos y externos. 3.- Crear un cronograma para realizar pruebas de los planes como una simulación. 4. Realizar un informe donde se detallen las actividades de la puesta en marcha de los planes.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Cronograma para sensibilizar con el personal de los procedimientos y procesos de recuperación/acción. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Cronograma para realizar pruebas de los planes 4. Informes.

1.4.4.1 1.4.5.1	Establecer controles y medidas de seguridad físicas y lógicas contra códigos maliciosos	1.- Determinar manual de controles contra software malicioso en los activos informáticos	1.- Establecer manual de controles contra código malicioso apropiados para los activos informáticos según su uso (Laboratorios, Aulas, Medios visuales, Dpto. Docentes, Dpto. Administrativos) 2.- Elaborar manual controles de medidas lógicas y físicas de seguridad. 3.- Elaborar plan de sensibilización y capacitación. 4.- Establecer un cronograma de capacitación periódico. 5.- Realizar informe de actividades realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período académico	1.- Manual de controles contra código malicioso apropiados para los activos informáticos según su uso 2.- Manual controles de medidas lógicas y físicas de seguridad. 3.- Plan de sensibilización y capacitación. 4.- Cronograma de capacitación periódico. 5.- Informes
1.4.6.1	Comunicar a los usuarios sobre la prevención del uso de los medios de procesamiento de la información para propósitos no autorizados	1.- Elaborar propuesta de plan de educación y capacitación continua en aspectos de seguridad informática. 2.-Establecer manual de procesos disciplinarios por uso inadecuado de activos	1.- Establecer cronograma para el proceso de capacitación y comunicación de los procesos de seguridad implementados en la Facultad. 2.- Elaborar propuesta de capacitación, sensibilización y comunicación. 3.- Establecer manual de procesos disciplinarios de acuerdo con el activo y grado de incumplimiento. 4.- Elaborar modelos para los medios informativos para llevar a cabo la sociabilización de los procesos de seguridad. 5.- Elaborar modelo de certificado de participación a los asistentes y firmas de actas. 6.- Realizar un informe de las actividades realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período académico	1.- Cronograma para el proceso de capacitación y comunicación. 2.- Propuesta de capacitación, sensibilización y comunicación. 3.- Manual de procesos disciplinarios de acuerdo con el activo y grado de incumplimiento. 4.- Modelo de medios informativos 5.- Modelo de certificado de participación y actas. 6.- Informes
1.4.7.1	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	1.- Determinar un manual de políticas para la seguridad al acceso lógico al switch. 2.-Determinar controles de acceso físico al área asignada para switch	1.- Establecer manual de políticas de control de acceso, lógicos y físicos. 2.- Establecer un cronograma para la revisión periódica de los controles de acceso. 3.-Establecer manual de funciones y responsabilidades para usuarios internos y externos. 4.- Establecer modelo de revocación de derechos de acceso. (Cuando sea el caso) 5.- Determinar manual de uso de activos. 6.- Desarrollar e implementar Planificación de control de seguridad y acceso 7.- Elaborar y socializar informes periódicos	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Docentes 4.- Usuario interno y externo	Periódico: Revisar y actualizar cada año	1.- Manual de políticas de control de acceso: lógico y físico 2.- Cronograma para la revisión periódica de los controles de acceso. 3.-Manual de funciones y responsabilidades para usuarios internos y externos. 4.- Modelo de revocación de derechos de acceso. 5.- Manual de uso de activos. 6.- Planificación de control de seguridad y acceso 7.- Informes

1.5.1.1	Establecer controles para la seguridad de la red	1.- Determinar manual de seguridad con los controles estándares para la red	1.- Establecer manual de seguridad con los controles estándares para la red. 2.- Instaurar manual de funciones y responsabilidades para el personal administrativo/área técnica. 3.- Realizar informes	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	periódico: Revisar y actualizar cada año	1.- Manual de seguridad con los controles estándares para la red. 2.- Manual de funciones y responsabilidades para el personal administrativo/área técnica. 3.- Informes
1.5.1.2	Establecer políticas sobre el uso de las redes y los servicios de la red	1. - Determinar manual normativas internas para el uso de los servicios de la red inalámbrica. 2.- Desarrollar plan de educación y capacitación	1.- Establecer manual normativas internas para el uso de los servicios de la red inalámbrica de acuerdo con la política de uso de internet elaborado por UCCI. 2.- Instaurar manual de funciones y responsabilidades para usuarios internos y externos 3.- Elaborar plan de sensibilización y capacitación. 4.- Establecer un cronograma de capacitación periódico. 5.- Realizar informe de actividades realizadas	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	periódico: Revisar y actualizar cada período	1.- Manual de normativas internas para el uso de los servicios de la red inalámbrica 2.- Manual de funciones y responsabilidades para usuarios internos y externos 3.- Plan de sensibilización y capacitación. 4.- Cronograma de capacitación periódico. 5.- Informe
1.5.2.1	Establecer protección contra la interceptación o daño del cableado de energía y de telecomunicaciones que dan soporte a los servicios de la Facultad	1.- Determinar manual de lineamientos para la seguridad del cableado de energía. 2.- Determinar manual de buenas prácticas para la instalación de cables (energía y telecomunicaciones)	1.- Establecer manual de lineamientos para la seguridad del cableado de telecomunicaciones. 2.- Establecer manual de buenas prácticas para la instalación de cables. 3.- Desarrollar e implementar una planificación de control para revisiones periódicas de las conexiones de red y de energía. 4.- Elaborar y socializar informes periódicos.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	periódico: Revisar y actualizar cada año	1.- Manual de lineamientos para la seguridad del cableado de telecomunicaciones. 2.- Manual de buenas prácticas para la instalación de cables. 3.- Planificación de control para revisiones periódicas 4.- Informes
1.5.2.2	Establecer pautas para la ubicación y protección de los equipos informáticos de la Facultad	1.- Determinar directrices para la ubicación y protección de los equipos de soporte para la red	1.- Establecer manual de directrices para la ubicación y protección adecuada de los equipos de soporte de red de acuerdo con las especificaciones del espacio. 2.- Realizar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Elaborar y comunicar informes periódicos preventivos, asertivos y de fin de períodos.	1. Personal Administrativo/Decana RESPONSABLE 2. Personal Administrativo/Área Técnica 3. Docentes 4. Usuario interno y externo	periódico: Revisar y actualizar cada año	1.- Manual de directrices para la ubicación y protección adecuada del activo. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Informes
1.5.2.3	Establecer procedimientos de mantenimiento de equipo y periféricos para	1.- Determinar procedimientos de mantenimiento preventivo y correctivo de equipos y	1.- Establecer procedimientos de mantenimiento de equipos y periféricos. 2.- Elaborar controles apropiados cuando se programa el equipo para mantenimiento	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal	periódico: Revisar y actualizar cada año	1.- Procedimientos de mantenimiento de equipos y periféricos. 2.- Controles para

	asegurar su continua disponibilidad e integridad	periféricos. 2.- Determinar controles apropiados para guiar el programa de mantenimiento de los equipos y periféricos. 3.- Determinar modelo de solicitud para el retiro de equipos y periféricos.	3.- Generar un cronograma de mantenimiento periódico. 4.- Utilizar plantilla de mantenimiento de hardware. 5.- Implantar una plantilla modelo de solicitud para el retiro formal del equipo y periférico. 6.- Diseñar un modelo de registro de las fallas internas encontradas en el soporte. 7.- Elaborar y comunicar informes del mantenimiento realizado.	Administrativo/Área Técnica		mantenimiento 3.- Cronograma de mantenimiento periódico. 4.- Plantilla de mantenimiento de hardware. 5.- Modelo de solicitud para el retiro formal del equipo y periférico. 6.- Modelo de registro de las fallas internas. 7.- Informes
1.6.1.1	Establecer el desarrollo e implementación de planes para mantener/restaurar los servicios prestados y asegurar la disponibilidad de la información en el nivel requerido	1.- Determinar la implementación de los planes de continuidad y contingencia formulados 2.- Desarrollar plan de educación y capacitación.	1.- Elaborar cronograma para sensibilizar con el personal de los procedimientos y procesos de recuperación/acción. 2.- Crear manual de funciones y responsabilidades para usuarios internos y externos. 3.- Crear un cronograma para realizar pruebas de los planes como una simulación. 4. Realizar un informe donde se detallen las actividades de la puesta en marcha de los planes.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	periódico: Revisar y actualizar cada año	1.- Cronograma para sensibilizar con el personal de los procedimientos y procesos de recuperación/acción. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Cronograma para realizar pruebas de los planes 4. Informes.
1.6.2.1	Establecer procedimientos de mantenimiento de equipo y periféricos para asegurar su continua disponibilidad e integridad	1.- Determinar procedimientos de mantenimiento preventivo y correctivo de equipos y periféricos. 2.- Determinar controles apropiados para guiar el programa de mantenimiento de los equipos y periféricos. 3.- Determinar modelo de solicitud para el retiro de equipos y periféricos.	1.- Establecer procedimientos de mantenimiento de equipos y periféricos. 2.- Elaborar controles apropiados cuando se programa el equipo para mantenimiento 3.- Generar un cronograma de mantenimiento periódico. 4.- Utilizar plantilla de mantenimiento de hardware. 5.- Implantar una plantilla modelo de solicitud para el retiro formal del equipo y periférico. 6.- Diseñar un modelo de registro de las fallas internas encontradas en el soporte. 7.- Elaborar y comunicar informes del mantenimiento realizado.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	periódico: Revisar y actualizar cada año	1.- Procedimientos de mantenimiento de equipos y periféricos. 2.- Controles para mantenimiento 3.- Cronograma de mantenimiento periódico. 4.- Plantilla de mantenimiento de hardware. 5.- Modelo de solicitud para el retiro formal del equipo y periférico. 6.- Modelo de registro de las fallas internas. 7.- Informes

1.6.2.2	Establecer protección contra la interceptación o daño del cableado de energía y de telecomunicaciones que dan soporte a los servicios de la Facultad	1.- Determinar manual de lineamientos para la seguridad del cableado de energía. 2.- Determinar manual de buenas prácticas para la instalación de cables (energía y telecomunicaciones)	1.- Establecer manual de lineamientos para la seguridad del cableado de energía. 2.- Establecer manual de buenas prácticas para la instalación de cables. 3.- Elaborar planos del sistema eléctrico 4.- Desarrollar e implementar una planificación de control para revisiones periódicas de las conexiones de red y de energía. 5.- Elaborar y socializar informes periódicos.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	periódico: Revisar y actualizar cada año	1.- Manual de lineamientos para la seguridad del cableado de energía. 2.- Manual de buenas prácticas para la instalación de cables. 3.- Planos del sistema eléctrico 4.- Planificación de control para revisiones periódicas 5.- Informes

En la tabla 10 se muestra los resultados medidas de control para los activos informáticos definido por riesgos generales de los activos, de acuerdo a la aplicabilidad de las normas ISOS y amenazas detectadas. Fuente: Las autoras de la investigación

3.1.3.1.*Riesgos por Áreas*

Tabla 11. *Medidas de control de los activos informáticos de la FACCI por Áreas*

MEDIDAS DE CONTROL DE LOS ACTIVOS INFORMÁTICOS DE LA FACCI						
#	**Descripción del control adoptado a la FACCI**	**Medidas de implementación del control**	**Acciones (Cómo)**	**Quienes (responsable)**	**Tiempo**	**Documento a generar (Evidencia)**
2.1.1.1	Control de políticas y estándares de seguridad establecidos a los programas usados en la facultad.	1.- Requisitos de funcionamiento para los sistemas a implementar en la Facultad realizados por estudiantes o terceros.	1.- Elaborar y Sociabilizar política de seguridad 2.- Elaborar e Implementar el cronograma de pruebas 3.- Cumplir con los requerimientos, políticas y configuraciones solicitados y establecidos por la Facultad 4.- Elaborar y Sociabilizar Informe de funcionalidad	_Personal Administrativo/Área Técnica RESPONSABLE	1 año	1.- Requisitos para implementar sistemas o aplicativos 2.- Informes
2.1.2.1	Establecer controles de detección, prevención y recuperación contra códigos maliciosos en la facultad	1.- Directivas físicas y lógicas 2.- Enfoques reactivos y proactivos para la prevención de virus y malware 3.- Implementar estrategias para reducir el malware	1.-Implementar Seguridad física 2.- Implementar Seguridad Lógica 3.- Procedimientos y directivas proactivas frente a reactivas 4.- Elaborar y sociabilizar informes de Actividades	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.-Informes

2.1.3.1	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica en la facultad.	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos.	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes
	Comunicar la prevención del uso de los medios de procesamiento de la información para propósitos no autorizados en la facultad	1.- Plan de Capacitación y Prevención a los usuarios y personal de la facultad.	1.- Planificar y ejecutar el Plan de Capacitación y Prevención. 2.- Supervisar el cumplimiento del cronograma de actividades. 3.- Informe de Actividades 4.- Definir y Socializar las Acciones de Prevención.	_Encargado del Plan de Capacitación, sensibilización y del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica (Asignación de privilegios) _Docentes - Estudiantes	6 meses	1.- Plan de Capacitación y Prevención. 2.- Informes 4.- Acciones de Prevención.

2.2.1.1	Procedimientos de mantenimiento preventivo y correctivo del equipo asegurando la disponibilidad e integridad	1.- Plan de Mantenimiento 2.- Plan de Continuidad	1.- Elaborar e implementar el cronograma mantenimiento preventivo. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informe de mantenimiento, con su historial. 3.- Implementar el Plan de continuidad.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3.- Informes
	Procedimientos en la eliminación seguro o re-uso del equipo en redes utilizado en la facultad.	1.- Procedimientos de eliminación y re-uso de activos (Redes) 2.- Actualización de Inventario	1.- Inventario actualizado al día y supervisado por la autoridad competente. 2.- Realizar análisis de riesgo 3.- Los activos que no se encuentren en funcionalidad deben tener justificación evidenciada para ser suspendidos o dados de baja. 4.- Realizar el seguimiento a los activos de almacenamiento.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Inventario de Nativos 2.- Análisis de Riesgo

	Establecer procedimientos para la gestión de medios removibles	1.- Políticas guías para controlar y proteger los medios removibles. 2.- Sociabilizar las políticas a todo el personal de la facultad. 3.- Control de Activos	1.- Establecer políticas de seguridad a los medios removibles. 2.- Sociabilizar y ejecutar las políticas. 3.- Llevar un registro de movimiento de los activos informáticos en el inventario. 4.- Determinar Manual de uso de activos. 5.- Elaborar y Sociabilizar el informe de actividades.	Personal Administrativo/Área Técnica	6 meses	1.-Políticas de control y protección de medios removibles 2.- Plan de sensibilización, Comunicación y Capacitación. 3.-Inventario de Activos
	Detección en fallas de la seguridad en activos informáticos	1.- Análisis y seguimiento de fallas en activos informáticos 2.- Plan de continuidad	1.- Detección de fallas en activos informáticos, por parte del personal y estudiantes de la facultad. 2.- Análisis de las fallas encontradas en los activos informáticos. 3.- Brindar tratamiento a las fallas encontradas. 4.- Seguimiento de las fallas y toma de decisiones. 5.- Elaborar y sociabilizar informe de actividades.	_Personal Administrativo/Área Técnica RESPONSABLE	Cada vez que se realice un mantenimiento	1.- Medidas de Seguridad Física y lógica del SGSI 2.- Plan de Mantenimiento 3.- Informes
	Capacitar al personal y estudiantes sobre la seguridad de la información.	1.- Política de filtración o fuga de información 2.- Plan de Capacitación sobre la seguridad e infiltración de la información	1.- Desarrollar modelos de Acuerdos de Confidencialidad y de intercambio de información entre la institución y empleados o terceras personas. 2.- Definir política de filtración o fuga de información 3.- Apoyar las campañas de UCCI para la seguridad de la información. 4.- Comunicar las métricas básicas para prevenir la infiltración de la información.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	6 meses	1.- Modelos de Confidencialidad en el Intercambio de Información. 2.- Política de Filtración o Fuga de información. 3.- Plan de sensibilización, Comunicación y Capacitación.
	Comunicar la prevención del uso de los medios de procesamiento de la información para propósitos no autorizados en la facultad	1.- Plan de Capacitación y Prevención a los usuarios y personal de la facultad.	1.- Planificar y ejecutar el Plan de Capacitación y Prevención. 2.- Supervisar el cumplimiento del cronograma de actividades. 3.- Informe de Actividades 4.- Definir y Socializar las Acciones de Prevención.	_Encargado del Plan de Capacitación, sensibilización y del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica (Asignación de privilegios) _Docentes _Estudiantes	6 meses	1.- Plan de Capacitación y Prevención. 2.- Informes 4.- Acciones de Prevención.

	Propuesta de lineamientos o reglas para el uso adecuado de los activos informáticos de la Facultad	1.- Capacitar sobre el buen uso de los activos informáticos como parte del Plan de Sensibilización, Comunicación y Capacitación.	1.- Elaborar los lineamientos para el buen uso de los activos informáticos 2.- Los lineamientos para el buen uso deben estar basado al reglamento interno de la Universidad 3.- Elaborar e Implementar el cronograma de capacitación 4.- Elaborar y Sociabilizar informe de sensibilización	_Encargado del Plan de Capacitación, sensibilización del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica (Asignación de privilegios)	6 meses	1.-Lineamientos o reglas para el uso adecuado de los activos informáticos FACCI 2.- Plan de Sensibilización, Comunicación y Capacitación. 3.- Informes
2.2.2.1	Procedimientos de mantenimiento preventivo y correctivo del equipo asegurando la disponibilidad e integridad	1.- Plan de Mantenimiento 2.- Plan de Continuidad	1.- Elaborar e implementar el cronograma mantenimiento preventivo. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informe de mantenimiento, con su historial. 3.- Implementar el Plan de continuidad.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3.- Informes
	Establecer controles de detección, prevención y recuperación contra códigos maliciosos en la Facultad	1.- Directivas físicas y lógicas 2.- Enfoques reactivos y proactivos para la prevención de virus y malware 3.- Implementar estrategias para reducir el malware	1.-Implementar Seguridad física 2.- Implementar Seguridad Lógica 3.- Procedimientos y directivas proactivas frente a reactivas 4.- Elaborar y sociabilizar informes de Actividades	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.-Informes
2.2.3.1	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
	Asegurar las condiciones en las áreas de trabajo académico en la facultad	1.- Implementar condiciones de trabajo segura de accidentes eléctricos. 2.- Lineamientos del buen uso de activos informáticos.	1.- Definir las protecciones físicas, acordes a la necesidad de los activos. 2.- Delimitar los de perímetros de seguridad. 3.- Establecer y ejecutar las medidas seguridad y de acceso en las áreas de trabajo. 4.- Cumplir con los parámetros del lineamiento del buen uso de activos informáticos.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimientos de seguridad Física. 2.- Medidas de Seguridad 3.- Lineamiento del Buen Uso de Activos Informáticos.

	Medidas de prevención a las debilidades que afectan a los activos informáticos de la facultad.	1.- Pruebas de Seguridad Informática 2.- Plan de capacitación sobre los reportes existente para avisar las debilidades en la seguridad	1.- Elaborar e implementar cronograma de pruebas de seguridad a los activos informáticos. 2.- Brindar tratamiento a las fallas encontradas 3.- Elaborar y sociabilizar informe de actividades 4.- Capacitar al personal docente administrativo y estudiantil a reportar las debilidades o problemas existente en los activos informáticos.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que sea observado este tipo de debilidades	1.- Pruebas e Informes de Seguridad 2.- Plan de Mantenimiento 3.- Informes 4.- Plan de sensibilización, Comunicación y Capacitación.
2.2.3.2	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica en la facultad.	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos.	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes
2.2.3.3	Procedimientos de mantenimiento preventivo y correctivo del equipo asegurando la disponibilidad e integridad	1.- Plan de Mantenimiento 2.- Plan de Continuidad	1.- Elaborar e implementar el cronograma mantenimiento preventivo. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informe de mantenimiento, con su historial. 3.- Implementar el Plan de continuidad.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3.- Informes
2.2.3.5	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
	Asegurar las condiciones en las áreas de trabajo académico en la facultad	1.- Implementar condiciones de trabajo segura de accidentes eléctricos. 2.- Lineamientos del buen uso de activos informáticos.	1.- Definir las protecciones físicas, acordes a la necesidad de los activos. 2.- Delimitar los de perímetros de seguridad. 3.- Establecer y ejecutar las medidas seguridad y de acceso en las áreas de trabajo. 4.- Cumplir con los parámetros del lineamiento del buen uso de activos informáticos.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimientos de seguridad Física. 2.- Medidas de Seguridad 3.- Lineamiento del Buen Uso de Activos Informáticos.

	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica en la facultad.	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos.	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes
2.2.3.6	Implementación de perímetros de seguridad física en los activos de la facultad.	1.- Gestión de Seguridad en la información 2-Establecer Perímetros de Seguridad Física correspondiente al sistema eléctrico que entra en contacto con los CPU's 2.- Protección física contra los accesos que no estén autorizados.	1.- Identificar los riesgos 2.- Detallar el lugar donde estará le cableado de la energía eléctrica dependiendo de los requisitos de seguridad del activo de formación entre el perímetro y los resultados de la evaluación de riesgos del SGSI. 3.- Establecer perímetros de peligro dentro de las áreas de trabajo que dieron como resultado de la evaluación de riesgos del SGSI. 4.- Instalación de un área de recepción manual y otros medios de control de acceso físico a las instalaciones. El acceso se puede restringir sólo al personal que esté autorizado. 5.- Asignar las salidas de emergencias	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Gestión de Seguridad en la información 2.- Modelo de procedimientos de seguridad física
	Protección de las áreas mediante controles de ingreso apropiado en la facultad	1.- Controles físicos correspondiente al sistema eléctrico que están en contacto con los CPU's	1.- Definir controles de entradas en las áreas de trabajo 2.- Garantizar el acceso al personal terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible. 3.-Medidas de prevención en activos de suministro eléctricos	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física

	Establecer controles de detección, prevención y recuperación contra códigos maliciosos en la facultad	1.- Directivas físicas y lógicas 2.- Enfoques reactivos y proactivos para la prevención de virus y malware 3.- Implementar estrategias para reducir el malware	1.-Implementar Seguridad física 2.- Implementar Seguridad Lógica 3.- Procedimientos y directivas proactivas frente a reactivas 4.- Elaborar y sociabilizar informes de Actividades	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.-Informes
	Controles contra malware para evitar el acceso a las laptops	1.- Implementar controles contra alteraciones por infecciones. 2.- Comunicar los controles a ejecutarse	1.- Ejecutar controles para los activos informáticos según su uso (Laboratorios, Dpto. Docentes, Dpto. Administrativos, etc.) 2.- Establecer normas de seguridad físicas 3.- Comunicar a todo el personal y estudiantes de las medidas a implementarse.	_Personal Administrativo/Área Técnica RESPONSABLE _Docentes _Estudiantes	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.- Plan de sensibilización, Comunicación.
	Establecer procedimientos para la gestión de medios removibles	1.- Políticas guías para controlar y proteger los medios removibles. 2.- Sociabilizar las políticas a todo el personal de la facultad. 3.- Control de Activos	1.- Establecer políticas de seguridad a los medios removibles. 2.- Sociabilizar y ejecutar las políticas. 3.- Llevar un registro de movimiento de los activos informáticos en el inventario. 4.- Determinar Manual de uso de activos. 5.- Elaborar y Sociabilizar el informe de actividades.	Personal Administrativo/Área Técnica	6 meses	1.-Políticas de control y protección de medios removibles 2.- Plan de sensibilización, Comunicación y Capacitación. 3.-Inventario de Activos
	Capacitar al personal y estudiantes sobre la seguridad de la información.	1.- Política de filtración o fuga de información 2.- Plan de Capacitación sobre la seguridad e infiltración de la información	1.- Desarrollar modelos de Acuerdos de Confidencialidad y de intercambio de información entre la institución y empleados o terceras personas. 2.- Definir política de filtración o fuga de información 3.- Apoyar las campañas de UCCI para la seguridad de la información. 4.- Comunicar las métricas básicas para prevenir la infiltración de la información.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	6 meses	1.- Modelos de Confidencialidad en el Intercambio de Información. 2.- Política de Filtración o Fuga de información. 3.- Plan de sensibilización, Comunicación y Capacitación.

	Medidas de prevención a las debilidades que afectan a los activos informáticos de la facultad.	1.- Pruebas de Seguridad Informática 2.- Plan de capacitación sobre los reportes existente para avisar las debilidades en la seguridad	1.- Elaborar e implementar cronograma de pruebas de seguridad a los activos informáticos. 2.- Brindar tratamiento a las fallas encontradas 3.- Elaborar y sociabilizar informe de actividades 4.- Capacitar al personal docente administrativo y estudiantil a reportar las debilidades o problemas existente en los activos informáticos.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que sea observado este tipo de debilidades	1.- Pruebas e Informes de Seguridad 2.- Plan de Mantenimiento 3.- Informes 4.- Plan de sensibilización, Comunicación y Capacitación.
2.2.4.1	Establecer controles de detección, prevención y recuperación contra códigos maliciosos en la facultad	1.- Directivas físicas y lógicas 2.- Enfoques reactivos y proactivos para la prevención de virus y malware 3.- Implementar estrategias para reducir el malware	1.-Implementar Seguridad física 2.- Implementar Seguridad Lógica 3.- Procedimientos y directivas proactivas frente a reactivas 4.- Elaborar y sociabilizar informes de Actividades	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.-Informes
	Controles contra malware para evitar el acceso a las laptops	1.- Implementar controles contra alteraciones por infecciones. 2.- Comunicar los controles a ejecutarse	1.- Ejecutar controles para los activos informáticos según su uso (Laboratorios, Dpto. Docentes, Dpto. Administrativos, etc.) 2.- Establecer normas de seguridad físicas 3.- Comunicar a todo el personal y estudiantes de las medidas a implementarse.	_Personal Administrativo/Área Técnica RESPONSABLE _Docentes _Estudiantes	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.- Plan de sensibilización, Comunicación.
	Establecer procedimientos para la gestión de medios removibles	1.- Políticas guías para controlar y proteger los medios removibles. 2.- Sociabilizar las políticas a todo el personal de la facultad. 3.- Control de Activos	1.- Establecer políticas de seguridad a los medios removibles. 2.- Sociabilizar y ejecutar las políticas. 3.- Llevar un registro de movimiento de los activos informáticos en el inventario. 4.- Determinar Manual de uso de activos. 5.- Elaborar y Sociabilizar el informe de actividades.	Personal Administrativo/Área Técnica	6 meses	1.-Políticas de control y protección de medios removibles 2.- Plan de sensibilización, Comunicación y Capacitación. 3.-Inventario de Activos
	Capacitar al personal y estudiantes sobre la seguridad de la información.	1.- Política de filtración o fuga de información 2.- Plan de Capacitación sobre la seguridad e infiltración de la información	1.- Desarrollar modelos de Acuerdos de Confidencialidad y de intercambio de información entre la institución y empleados o terceras personas. 2.- Definir política de filtración o fuga de información 3.- Apoyar las campañas de UCCI para la seguridad de la información. 4.- Comunicar las métricas básicas para prevenir la infiltración de la información.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	6 meses	1.- Modelos de Confidencialidad en el Intercambio de Información. 2.- Política de Filtración o Fuga de información. 3.- Plan de sensibilización, Comunicación y Capacitación.

	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica en la facultad.	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos.	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes
	Medidas de prevención a las debilidades que afectan a los activos informáticos de la facultad.	1.- Pruebas de Seguridad Informática 2.- Plan de capacitación sobre los reportes existente para avisar las debilidades en la seguridad	1.- Elaborar e implementar cronograma de pruebas de seguridad a los activos informáticos. 2.- Brindar tratamiento a las fallas encontradas 3.- Elaborar y sociabilizar informe de actividades 4.- Capacitar al personal docente administrativo y estudiantil a reportar las debilidades o problemas existente en los activos informáticos.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que sea observado este tipo de debilidades	1.- Pruebas e Informes de Seguridad 2.- Plan de Mantenimiento 3.- Informes 4.- Plan de sensibilización, Comunicación y Capacitación.
2.2.5.1	Capacitación en procedimientos de seguridad y uso adecuado de los activos informáticos	1.- Capacitar al personal y estudiantes sobre los lineamientos del buen uso de activos informáticos	1.- Establecer y ejecutar el cronograma el del Plan de Sensibilización, Comunicación y Capacitación 2.- Elaborar y autorizar los lineamientos del buen uso de activos informáticos. 3.- Elaborar y sociabilizar informe de actividades	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	6 meses	1.- Plan de Sensibilización Comunicación y Capacitación 2.- Lineamientos del Buen Uso de Activos Informáticos 4.- Informes
	Implementar procesos disciplinarios en el SGSI de la facultad.	1.- Gestión de controles del proceso disciplinario	1.- Definir cláusula de cumplimiento del buen uso de los activos informáticos. 2.- Sociabilizar las violaciones de la seguridad informática que no se deben realizar. 3.- Determinar las sanciones por cometer violaciones a la seguridad informática. 4.- Elaborar y sociabilizar informe de actividades	_Honorable Consejo de Facultad _Personal Administrativo/Área Técnica _ Personal Administrativo _Estudiantes	Cada vez que se cometa una sanción	1.- Medidas de seguridad de SGSI 2.- Plan de sensibilización, Comunicación y Capacitación 3.-Samciones 4.- Informes
2.2.6.1	Protección contra la interceptación o daño del cableado de energía y de telecomunicaciones que dan soporte a los servicios de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Obtener los planos de energía eléctrica de la facultad 3.- Establecer medidas físicas de las habitaciones donde funcionan los activos informáticos para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE)	Cada que haya una reestructuración física, cambio de localidad, reorganización del espacio en las áreas	1.- Modelo de procedimiento de seguridad física 2.- Planos eléctricos de la facultad.

	Medidas de prevención a las debilidades que afectan a los activos informáticos de la facultad.	1.- Pruebas de Seguridad Informática 2.- Plan de capacitación sobre los reportes existente para avisar las debilidades en la seguridad	1.- Elaborar e implementar cronograma de pruebas de seguridad a los activos informáticos. 2.- Brindar tratamiento a las fallas encontradas 3.- Elaborar y sociabilizar informe de actividades 4.- Capacitar al personal docente administrativo y estudiantil a reportar las debilidades o problemas existente.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que sea observado este tipo de debilidades	1.- Pruebas e Informes de Seguridad 2.- Plan de Mantenimiento 3.- Informes 4.- Plan de sensibilización, Comunicación y Capacitación.

En la tabla 11 se muestra los resultados medidas de control de los activos informáticos definido por áreas, de acuerdo a las normas ISOS aplicables y amenazas detectadas. Fuente: Las autoras de la investigación

3.1.3.2.Riesgos por Laboratorios

Tabla 12. *Medidas de control de los activos informáticos de la FACCI por Laboratorios*

MEDIDAS DE CONTROL DE LOS ACTIVOS INFORMÁTICOS DE LA FACCI						
#	**Descripción del control adoptado a la FACCI**	**Medidas de implementación del control**	**Acciones (Cómo)**	**Quienes (responsable)**	**Tiempo**	**Documento a generar (Evidencia)**
3.1.1.1	Realizar tratamiento de la seguridad para la intervención de usuarios internos o externos en contratos de la FACCI.	1.- Determinar políticas para uso del SO de parte de los usuarios internos y externos aplicando controles y privilegios de acceso.	1.- Establecer políticas de seguridad de confiabilidad y acceso. 2.- Crear manual de funciones y responsabilidades para usuarios internos y externos. 3.- Determinar manual de uso de activos. 4.- Desarrollar e implementar una planificación de control de protección y permisos 5.- Elaborar y socializar informes periódicos	_Personal Administrativo/Decana RESPONSABLE _Personal Administrativo/Área Técnica _Docentes (Supervisión del cumplimiento de accesos) _Estudiantes - Usuario ext	Periódico: Revisar y actualizar cada año	1.- Políticas de seguridad de confiabilidad y acceso. 2.-Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Manual de uso de activos. 4.- Planificación de control de seguridad y acceso 5.- Informes.
	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	1.- El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos y política de seguridad establecidos en el contrato de trabajo. 2.- Los servicios accedidos por terceros acatarán las disposiciones generales de acceso a servicios por el personal interno	1.- Definir la política de seguridad por parte del SGSI. 2.- Compartir e implementar la política de seguridad. 3.- Asignar supervisor del control de acceso 4.- Establecer sanciones para el incumplimiento de la política de seguridad.	_Líder del Proyecto SGSI, RESPONSABLE _Personal Administrativo/Área Técnica (Asignación de privilegios) _Docentes _Estudiantes	1 año	1.- Política de seguridad de acceso a la información. 3.- Asignar supervisor del control de acceso 4.- Procesos Disciplinarios

3.1.1.2	Análisis y especificación de los requerimientos de seguridad especificados por la facultad	1.- Requerimientos de seguridad necesarios especificados por la Facultad	1.- Definir los requisitos que debe cumplir un sistema o aplicativo para ser aceptado y ejecutado en la unidad académica. 2.- Asignar a un Docente responsable. 3.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos. 4.-Actualizar los requerimientos cada ciclo académico.	_Personal Administrativo/Área Técnica (Asignación de privilegios) _Docentes RESPONSABLE (Por materia)	6 meses	1.- Requisitos para el desarrollo y ejecución de aplicativos o sistemas. 2.- Asignar responsable supervisor. 3.- Informes. 4.-Actualización de requerimientos.
	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica en la facultad.	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos.	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes
	Implementar procesos apropiados del uso de software patentado por la facultad	1.- Gestiones extracurriculares para el uso académico de software patentado	1.- Elaborar y Sociabilizar política de seguridad de protocolo de uso de software patentado. 2.- Usar gestiones extracurriculares para facilitar el uso de software patentado. 3.- Elaborar y sociabilizar informes Gestión Extracurriculares. 4.- Utilizar software libre como alternativa.	_Docentes o Estudiantes RESPONSABLE (Por Gestión Extracurricular)	1 año	1.- Gestión de marca de software 2.- Informes
	Comunicar la prevención del uso de los medios de procesamiento de la información para propósitos no autorizados en la facultad	1.- Plan de Capacitación y Prevención a los usuarios y personal de la facultad.	1.- Planificar y ejecutar el Plan de Capacitación y Prevención. 2.- Supervisar el cumplimiento del cronograma de actividades. 3.- Informe de Actividades 4.- Definir y Socializar las Acciones de Prevención.	_Encargado del Plan de Capacitación, sensibilización del Proyecto SGSI (RESPONSABLE) _P. Administrativo/Área Técnica Docentes - Estudiantes	6 meses	1.- Plan de Capacitación y Prevención. 2.- Informes 4.- Acciones de Prevención.
3.1.2.1	Implementar procesos apropiados del uso de software patentado por la facultad	1.- Gestiones extracurriculares para el uso académico de software patentado	1.- Elaborar y Sociabilizar política de seguridad de protocolo de uso de software patentado. 2.- Usar gestiones extracurriculares para facilitar el uso de software patentado. 3.- Elaborar y sociabilizar informes Gestión Extracurriculares. 4.- Utilizar software libre como alternativa.	_Docentes o Estudiantes RESPONSABLE (Por Gestión Extracurricular)	1 año	1.- Gestión de marca de software 2.- Informes

3.1.3.1	Establecer controles de detección, prevención y recuperación contra códigos maliciosos en la facultad	1.- Directivas físicas y lógicas 2.- Enfoques reactivos y proactivos para la prevención de virus y malware 3.- Implementar estrategias para reducir el malware	1.-Implementar Seguridad física 2.- Implementar Seguridad Lógica 3.- Procedimientos y directivas proactivas frente a reactivas 4.- Elaborar y sociabilizar informes de Actividades	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica	6 meses	1.- Medidas de Seguridad Física y lógica del SGSI 2.-Informes
	Control de vulnerabilidades técnicas de antivirus utilizados por la facultad	1.- Seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática constante.	1.-Asignar responsable del control de vulnerabilidades técnicas de Antivirus. 2.- Establecer herramienta de gestión de vulnerabilidades y definir el cronograma de control de parches de seguridad 3.- Configurar la actualización automática 4.- Elaborar y sociabilizar informes de Actividades	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.-Pruebas e Informes de Seguridad en Antivirus 2.- Informes
3.1.3.2	Implementar procedimientos sobre el uso de productos software patentado en la facultad	1.- Gestiones extracurriculares para el uso académico de software patentado	1.- Elaborar y Sociabilizar política de seguridad de protocolo de uso de software patentado. 2.- Usar gestiones extracurriculares para facilitar el uso de software patentado. 3.- Elaborar y sociabilizar informes Gestión Extracurriculares. 4.- Utilizar software libre como alternativa.	_Docentes o Estudiantes RESPONSABLE (Por Gestión Extracurricular)	1 año	1.- Gestión de marca de software 2.- Informes
3.1.4.1	Protocolo de aceptación de sistemas o aplicativos en la Facultad	1.- Pruebas de Aceptación de Sistemas	1- Realizar el Plan de prueba 2.- Establecer el cronograma de pruebas 3.- Elaborar y sociabilizar los resultados e informe de las pruebas	_Personal Administrativo/Área Técnica RESPONSABLE	1 año	1.- Requisitos para implementar sistemas o aplicativos 2.- Informes
3.1.4.2	Control de políticas y estándares de seguridad establecidos a los programas usados en la facultad.	1.- Requisitos de funcionamiento para los sistemas a implementar en la Facultad realizados por estudiantes o terceros.	1.- Elaborar y Sociabilizar política de seguridad 2.- Elaborar e Implementar el cronograma de pruebas 3.- Cumplir con los requerimientos, políticas y configuraciones solicitados y establecidos por la Facultad 4.- Elaborar y Sociabilizar Informe de funcionalidad	_Personal Administrativo/Área Técnica RESPONSABLE	1 año	1.- Requisitos para implementar sistemas o aplicativos 2.- Informes

3.2.1.1	Propuesta de lineamientos o reglas para el uso adecuado de los activos informáticos de la Facultad	1.- Capacitar sobre el buen uso de los activos informáticos como parte del Plan de Sensibilización, Comunicación y Capacitación.	1.- Elaborar los lineamientos para el buen uso de los activos informáticos 2.- Los lineamientos para el buen uso deben estar basado al reglamento interno de la Universidad 3.- Elaborar e Implementar el cronograma de capacitación 4.- Elaborar y Sociabilizar informe de sensibilización	_Encargado del Plan de Capacitación, sensibilización del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica (Asignación de privilegios)	6 meses	1.-Lineamientos o reglas para el uso adecuado de los activos informáticos FACCI 2.- Plan de Sensibilización, Comunicación t Capacitación. 3.- Informes
	Procedimientos de mantenimiento preventivo y correctivo del equipo asegurando la disponibilidad e integridad	1.- Plan de Mantenimiento 2.- Plan de Continuidad	1.- Elaborar e implementar el cronograma mantenimiento preventivo. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informe de mantenimiento, con su historial. 3.- Implementar el Plan de continuidad.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3.- Informes
	Procedimientos en la eliminación seguro o re-uso del equipo en redes utilizado en la facultad.	1.- Procedimientos de eliminación y re-uso de activos (Redes) 2.- Actualización de Inventario	1.- Inventario actualizado al día y supervisado por la autoridad competente. 2.- Realizar análisis de riesgo 3.- Los activos que no se encuentren en funcionalidad deben tener justificación evidenciada para ser suspendidos o dados de baja. 4.- Realizar el seguimiento a los activos de almacenamiento.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Inventario de activos 2.- Análisis de Riesgo
	Establecer controles y medidas de seguridad físicas y lógicas contra códigos maliciosos	1.- Seguimiento constante de software malicioso	1.- Definir y ejecutar acciones de prohibición 2.- Designar a un administrador de control. 3.- Utilizar herramienta de gestión de vulnerabilidades, implementando el cronograma de control. 4.- Elaborar y sociabilizar el Informe de Actividades	_Personal Administrativo/Área Técnica RESPONSABLE	2 meses	1.- Lineamientos del Buen Uso de Activos Informáticos 2.-Pruebas e Informes de Seguridad 3.- Informes
	Implementar la política de respaldo de información de la facultad	1.- Gestión de Seguridad en la información 2.- Procedimientos de respaldo de información que se genera en la unidad académica 3.- Plan de Continuidad	1.- Establecer e implementar la política de seguridad 2.- Elaborar y cumplir con el cronograma del respaldo de la información 3.- Elaborar y sociabilizar los Reportes de las actividades 4.- Implementar el Plan de Continuidad	_Personal Administrativo/Área Técnica RESPONSABLE	Cada semana	1.- Gestión de Seguridad en la información 2.- Procedimientos Generales para el Proceso, respaldo de la Información 3.- Plan de Continuidad 4.- Reportes

	Protocolo para el cambio de equipos de redes utilizado en la Facultad	1.- Protocolo de cambios en equipos 2.- Plan de Mantenimiento	1.-Revisión por el Área Técnica 2.-Solicitud de cambios en el equipo dirigido al Decano(a) con su correcta justificación 3.- Acta de entrega y recepción del activo para el cambio respectivo	_Personal Administrativo/Área Técnica RESPONSABLE _Decano(a)	1 año	1.- Medidas de seguridad de SGSI 2.- Acta de cambio
	Control de vulnerabilidades técnicas en equipo de redes utilizados por la facultad	1.- Seguimiento constante de parches de seguridad mediante herramientas de gestión de vulnerabilidades y/o actualización automática constante.	1.-Asignar responsable del control de vulnerabilidades técnicas de Antivirus. 2.- Establecer herramienta de gestión de vulnerabilidades y definir el cronograma de control de parches de seguridad 3.- Configurar la actualización automática 4.- Elaborar y sociabilizar informes de Actividades	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.-Pruebas e Informes de Seguridad en Antivirus 2.- Informes
3.2.2.1	Propuesta de lineamientos o reglas para el uso adecuado de los activos informáticos de la Facultad	1.- Capacitar sobre el buen uso de los activos informáticos como parte del Plan de Sensibilización, Comunicación y Capacitación.	1.- Elaborar los lineamientos para el buen uso de los activos informáticos 2.- Los lineamientos para el buen uso deben estar basado al reglamento interno de la Universidad 3.- Elaborar e Implementar el cronograma de capacitación 4.- Elaborar y Sociabilizar informe de sensibilización	_Encargado del Plan de Capacitación, sensibilización del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica (Asignación de privilegios)	6 meses	1.-Lineamientos o reglas para el uso adecuado de los activos informáticos FACCI 2.- Plan de Sensibilización, Comunicación t Capacitación. 3.- Informes
	Protocolo para el etiquetado y manejo de la información de acuerdo al el esquema de clasificación adoptado	1.- Etiquetado y control del registro e inventario de información y activos informáticos	1.- Verificar el código único del activo establecido por la Universidad y por la facultad 2.- La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de esta, clasificándola y etiquetándola en los mismos niveles establecidos en clasificación de la información. 3.- Elaborar y Sociabilizar informe	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Inventario de Activos 2.- Informe
	Procedimientos de mantenimiento del equipo para asegurar su continua disponibilidad e integridad	1.- Disponibilidad y procesamiento óptimo de los activos informáticos de redes 2.- Plan de Continuidad	1.- Establecer e Implementar un cronograma de tareas de mantenimiento preventivo se realizarán de acuerdo con los intervalos de servicio y especificaciones de la Facultad. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informes de mantenimiento con su historial.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3. Informes

	Establecer controles y medidas de seguridad físicas y lógicas contra códigos maliciosos	1.- Seguimiento constante de software malicioso	1.- Definir y ejecutar acciones de prohibición 2.- Designar a un administrador de control. 3.- Utilizar herramienta de gestión de vulnerabilidades, implementando el cronograma de control. 4.- Elaborar y sociabilizar el Informe de Activ.	_Personal Administrativo/Área Técnica RESPONSABLE	2 meses	1.- Lineamientos del Buen Uso de Activos Informáticos 2.-Pruebas e Informes de Seguridad 3.- Informes
3.2.3.1	Implementación de perímetros de seguridad física en los activos de la facultad.	1.- Gestión de Seguridad en la información 2-Establecer Perímetros de Seguridad Física correspondiente al sistema eléctrico que entra en contacto con los CPU's 2.- Protección física contra los accesos que no estén autorizados.	1.- Identificar los riesgos 2.- Detallar el lugar donde estará le cableado de la energía eléctrica dependiendo de los requisitos de seguridad del activo de formación entre el perímetro y los resultados de la evaluación de riesgos del SGSI. 3.- Establecer perímetros de peligro dentro de las áreas de trabajo que dieron como resultado de la evaluación de riesgos del SGSI. 4.- Instalación de un área de recepción manual y otros medios de control de acceso físico a las instalaciones. 5.- Asignar las salidas de emergencias	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Gestión de Seguridad en la información 2.- Modelo de procedimientos de seguridad física
	Protección de las áreas mediante controles de ingreso apropiado en la facultad	1.- Controles físicos correspondiente al sistema eléctrico que están en contacto con los CPU's	1.- Definir controles de entradas en las áreas de trabajo 2.- Garantizar el acceso al personal terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible. 3.-Medidas de prevención en activos de suministro eléctricos	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
3.2.3.2	Análisis de amenazas externas y ambientales, estableciendo medidas de protección para su mitigación.	1.-Establecer las amenazas externas y ambientales que se es vulnerable. 2.- Analizar el impacto de las amenazas en los activos informáticos. 3.- Definir medidas de protección para las amenazas.	1.- Definir probabilidad de las amenazas que está expuesta la facultad. 2.- Determinar la protección física contra estas amenazas. 3.- Implementar el Plan de Contingencia. 4.- Asignar al personal que a cargo de las situaciones de riesgo. 5.- Elaborar y sociabilizar el Informe de actividades	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física 2.- Plan de Contingencia 3.- Informes

	Asegurar las condiciones en las áreas de trabajo académico en la facultad	1.- Implementar condiciones de trabajo segura de accidentes eléctricos. 2.- Lineamientos del buen uso de activos informáticos.	1.- Definir las protecciones físicas, acordes a la necesidad de los activos. 2.- Delimitar los de perímetros de seguridad. 3.- Establecer y ejecutar las medidas seguridad y de acceso en las áreas de trabajo. 4.- Cumplir con los parámetros del lineamiento del buen uso de activos informáticos.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimientos de seguridad Física. 2.- Medidas de Seguridad 3.- Lineamiento del Buen Uso de Activos Informáticos.
3.2.3.3	Procedimientos de mantenimiento del equipo para asegurar su continua disponibilidad e integridad	1.- Disponibilidad y procesamiento óptimo de los activos informáticos de redes 2.- Plan de Continuidad	1.- Establecer e Implementar el cronograma de tareas de mantenimiento preventivo se realizarán de acuerdo con los intervalos de servicio y especificaciones de la Facultad. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informes de mantenimiento con su historial. 4.- Implementar Plan de continuidad	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3. Informes
3.2.3.4	Gestión de cambios en los medios y sistemas de procesamiento de información.	1.- Actualización de los sistemas en activos informáticos	1.- Establecer e Implementar el cronograma de actualización o cambios. 2.- Decidir si la ejecución lo realiza el personal técnico de facultad o los pasantes que estén residiendo en la Facultad. 3.- Elaborar y Sociabilizar informes por cada actualización o cambio a realizarse en los activos informáticos para llevar un historial.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3. Informes
	Asignar deberes y áreas de responsabilidad en el departamento técnico	1.-Delegar al personal responsabilidades de los activos existentes. 2.- Sociabilizar las decisiones con todo el personal.	1.-Establecer un responsable general por cada área de actividad de la facultad. 2.- Sociabilizar las responsabilidades del docente, mientras ejerce sus responsabilidades dentro de las áreas. 3.- Elaborar y Sociabilizar informes de actividades en las áreas de la facultad.	_Personal Administrativo/Área Técnica RESPONSABLE _Docentes	6 meses	1.-Modelo de procedimientos de seguridad Física 2.- Plan de sensibilización, Comunicación y Capacitación 3.- Informes
3.2.4.1	Implementación de perímetros de seguridad física en los activos de la facultad.	1.- Gestión de Seguridad en la información 2-Establecer Perímetros de Seguridad Física correspondiente al sistema eléctrico que entra en contacto con los CPU's 2.- Protección física contra los accesos que no estén autorizados.	1.- Identificar los riesgos 2.- Detallar el lugar donde estará le cableado de la energía eléctrica dependiendo de los requisitos de seguridad del activo de formación entre el perímetro y los resultados de la evaluación de riesgos del SGSI. 3.- Establecer perímetros de peligro dentro de las áreas de trabajo que dieron como resultado de la evaluación de riesgos del SGSI. 4.- Instalación de un área de recepción	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Gestión de Seguridad en la información 2.- Modelo de procedimientos de seguridad física

			manual y otros medios de control de acceso físico a las instalaciones. El acceso se puede restringir sólo al personal que esté autorizado. 5.- Asignar las salidas de emergencias			
	Protección de las áreas mediante controles de ingreso apropiado en la facultad	1.- Controles físicos correspondiente al sistema eléctrico que están en contacto con los CPU's	1.- Definir controles de entradas en las áreas de trabajo 2.- Garantizar el acceso al personal terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible. 3.-Medidas de prevención en activos de suministro eléctricos	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes - Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio	1.- Modelo de procedimiento de seguridad física
	Asignar deberes y áreas de responsabilidad en el departamento técnico	1.-Delegar al personal de la facultad responsabilidades de los activos existentes. 2.- Sociabilizar las decisiones con todo el personal	1.-Establecer un responsable general por cada área de actividad de la facultad. 2.- Sociabilizar las responsabilidades del docente, mientras ejerce sus responsabilidades dentro de las áreas. 3.- Elaborar y Sociabilizar informes de actividades en las áreas de la facultad.	_Personal Administrativo/Área Técnica RESPONSABLE _Docentes	6 meses	1.-Modelo de procedimientos de seguridad Física 2.- Plan de sensibilización, Comunicación y Capacitación 3.- Informes
	Establecer procedimientos para la gestión de medios removibles	1.- Políticas guías para controlar y proteger los medios removibles. 2.- Sociabilizar las políticas a todo el personal de la facultad. 3.- Control de Activos	1.- Establecer políticas de seguridad a los medios removibles. 2.- Sociabilizar y ejecutar las políticas. 3.- Llevar un registro de movimiento de los activos informáticos en el inventario. 4.- Determinar Manual de uso de activos. 5.- Elaborar y Sociabilizar el informe de actividades.	Personal Administrativo/Área Técnica	6 meses	1.-Políticas de control y protección de medios removibles 2.- Plan de sensibilización, Comunicación y Capacitación. 3.-Inventario de Activos
3.2.4.2	Procedimientos de mantenimiento del equipo para asegurar su continua disponibilidad e integridad	1.- Disponibilidad y procesamiento óptimo de los activos informáticos de redes 2.- Plan de Continuidad	1.- Establecer e Implementar un cronograma de tareas de mantenimiento preventivo se realizarán de acuerdo con los intervalos de servicio y especificaciones de la Facultad. 2.- Personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informes de mantenimiento con su historial. 4.- Implementar Plan de continuidad	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3. Informes

	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica en la facultad.	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos preventivos, alarmantes y de fin de períodos.	_Personal Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes
3.2.5.1	Implementación de perímetros de seguridad física en los activos de la facultad.	1.- Gestión de Seguridad en la información 2-Establecer Perímetros de Seguridad Física correspondiente al sistema eléctrico que entra en contacto con los CPU's 2.- Protección física contra los accesos que no estén autorizados.	1.- Identificar los riesgos 2.- Detallar el lugar donde estará le cableado de la energía eléctrica dependiendo de los requisitos de seguridad del activo de formación entre el perímetro y los resultados de la evaluación de riesgos del SGSI. 3.- Establecer perímetros de peligro dentro de las áreas de trabajo que dieron como resultado de la evaluación de riesgos del SGSI. 4.- Instalación de un área de recepción manual y otros medios de control de acceso físico a las instalaciones. El acceso se puede restringir sólo al personal que esté autorizado. 5.- Asignar las salidas de emergencias	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Gestión de Seguridad en la información 2.- Modelo de procedimientos de seguridad física
	Protección de las áreas mediante controles de ingreso apropiado en la facultad	1.- Controles físicos correspondiente al sistema eléctrico que están en contacto con los CPU's	1.- Definir controles de entradas en las áreas de trabajo 2.- Garantizar el acceso al personal terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible. 3.-Medidas de prevención en activos de suministro eléctricos	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física
	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio	1.- Modelo de procedimiento de seguridad física
3.2.5.2	Asignar deberes y áreas de responsabilidad en el departamento técnico	1.-Delegar al personal de la facultad responsabilidades de los activos existentes. 2.- Sociabilizar las decisiones con todo el personal de la facultad.	1.-Establecer un responsable general por cada área de actividad de la facultad. 2.- Sociabilizar las responsabilidades del docente, mientras ejerce sus responsabilidades dentro de las áreas. 3.- Elaborar y Sociabilizar informes de actividades en las áreas de la facultad.	_Personal Administrativo/Área Técnica RESPONSABLE _Docentes	6 meses	1.-Modelo de procedimientos de seguridad Física 2.- Plan de sensibilización, Comunicación y Capacitación 3.- Informes

3.2.5.3	Capacitar al personal y estudiantes sobre la seguridad de la información.	1.- Política de filtración o fuga de información 2.- Plan de Capacitación sobre la seguridad e infiltración de la información	1.- Desarrollar modelos de Acuerdos de Confidencialidad y de intercambio de información entre la institución y empleados o terceras personas. 2.- Definir política de filtración o fuga de información 3.- Apoyar las campañas de UCCI para la seguridad de la información. 4.- Comunicar las métricas básicas para prevenir la infiltración de la información.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	6 meses	1.- Modelos de Confidencialidad en el Intercambio de Información. 2.- Política de Filtración o Fuga de información. 3.- Plan de sensibilización, Comunicación y Capacitación.
	Comunicar la prevención del uso de los medios de procesamiento de la información para propósitos no autorizados en la facultad	1.- Plan de Capacitación y Prevención a los usuarios y personal de la facultad.	1.- Planificar y ejecutar el Plan de Capacitación y Prevención. 2.- Supervisar el cumplimiento del cronograma de actividades. 3.- Informe de Actividades 4.- Definir y Socializar las Acciones de Prevención.	_Encargado del Plan de Capacitación, sensibilización del Proyecto SGSI (RESPONSABLE) _P. Administrativo/Área Técnica - Docentes - Estudiantes	6 meses	1.- Plan de Capacitación y Prevención. 2.- Informes 4.- Acciones de Prevención.
3.2.5.4	Procedimientos de mantenimiento del equipo para asegurar su continua disponibilidad e integridad	1.- Disponibilidad y procesamiento óptimo de los activos informáticos de redes 2.- Plan de Continuidad	1.- Establecer e Implementar un cronograma de tareas de mantenimiento preventivo se realizarán de acuerdo con los intervalos de servicio y especificaciones de la Facultad. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informes de mantenimiento con su historial. 4.- Implementar Plan de continuidad	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3. Informes
	Controlar la sincronización de relojes en los equipos informáticos.	1.- Sincronización de relojes en los activos existentes. 2.- Lineamientos del buen uso de activos informáticos.	1.-Ejecutar los lineamientos en todos los activos informáticos. 2.- Elaborar y Sociabilizar informes de cumplimiento.	_Personal Administrativo/Área Técnica RESPONSABLE	Esporádico	1.- Modelo de procedimientos de seguridad Física 2.- Lineamientos del Buen Uso de Activos Informáticos. 3.- Informes.
3.2.6.1	Implementación de perímetros de seguridad física en los activos de la facultad.	1.- Gestión de Seguridad en la información 2-Establecer Perímetros de Seguridad Física correspondiente al sistema eléctrico que entra en contacto con los CPU's 2.- Protección física contra los accesos que no estén autorizados.	1.- Identificar los riesgos 2.- Detallar el lugar donde estará le cableado de la energía eléctrica dependiendo de los requisitos de seguridad del activo de formación entre el perímetro y los resultados de la evaluación de riesgos del SGSI. 3.- Establecer perímetros de peligro dentro de las áreas de trabajo que dieron como resultado de la evaluación de riesgos del SGSI. 4.- Instalación de un área de recepción manual y otros medios de control de acceso físico a las	_Líder del Proyecto SGSI (RESPONSABLE) _Personal Administrativo/Área Técnica _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Gestión de Seguridad en la información 2.- Modelo de procedimientos de seguridad física

			instalaciones. 5.- Asignar las salidas de emergencias			
	Protección de las áreas mediante controles de ingreso apropiado en la facultad	1.- Controles físicos correspondiente al sistema eléctrico que están en contacto con los CPU's	1.- Definir controles de entradas en las áreas de trabajo 2.- Garantizar el acceso al personal terceras personas hacia las áreas de seguridad o los recursos de los procesos de información sensible. 3.-Medidas de prevención en activos de suministro eléctricos	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio	1.- Modelo de procedimiento de seguridad física
	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes- Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio	1.- Modelo de procedimiento de seguridad física
3.2.6.2	Asignar deberes y áreas de responsabilidad en el departamento técnico	1.-Delegar al personal de la facultad responsabilidades de los activos existentes. 2.- Sociabilizar las decisiones con todo el personal	1.-Establecer un responsable general por cada área de actividad de la facultad. 2.- Sociabilizar las responsabilidades del docente, mientras ejerce sus responsabilidades dentro de las áreas. 3.- Elaborar y Sociabilizar informes de actividades en las áreas	_Personal Administrativo/Área Técnica RESPONSABLE _Docentes	6 meses	1.-Modelo de procedimientos de seguridad Física 2.- Plan de sensibilización, Comunicación y Capacitación 3.- Informes
	Comunicar la prevención del uso de los medios de procesamiento de la información para propósitos no autorizados	1.- Plan de Capacitación y Prevención a los usuarios y personal de la facultad.	1.- Planificar y ejecutar el Plan de Capacitación y Prevención. 2.- Supervisar el cumplimiento del cronograma de actividades. 3.- Informe de Actividades 4.- Definir y Socializar las Acciones de Prevención.	_Encargado del Plan de Capacitación, sensibilización del Proy. SGSI (RESPONSABLE) _P. Administrativo/Área Técnica - Docentes _Estudiantes	6 meses	1.- Plan de Capacitación y Prevención. 2.- Informes 4.- Acciones de Prevención.
3.2.7.1	Seguridad en oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Perímetros de Seguridad Física laboral correspondiente al sistema eléctrico que entra en contacto con los CPU's	1.- Disponer la ubicación de los activos para el área de trabajo 2.- Establecer medidas físicas de las habitaciones donde funcionan los laboratorios para una mejor organización y optimización de espacio.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización	1.- Modelo de procedimiento de seguridad física
	Procedimientos de mantenimiento preventivo y correctivo del equipo asegurando la disponibilidad e integridad	1.- Plan de Mantenimiento 2.- Plan de Continuidad	1.- Elaborar e implementar el cronograma mantenimiento preventivo. 2.- Solo el personal de autorizado puede brindar mantenimiento y realizar reparaciones. 3.- Elaborar y sociabilizar informe de mantenimiento, con su historial.	_Personal Administrativo/Área Técnica RESPONSABLE	6 meses	1.- Plan de Mantenimiento 2.- Plan de Continuidad 3.- Informes

	Análisis de amenazas externas y ambientales, estableciendo medidas de protección para su mitigación.	1.-Establecer las amenazas externas y ambientales que se es vulnerable. 2.- Analizar el impacto de las amenazas en los activos informáticos. 3.- Definir medidas de protección para las amenazas.	1.- Definir probabilidad de las amenazas que está expuesta la facultad. 2.- Determinar la protección física contra estas amenazas. 3.- Implantar el Plan de Contingencia. 4.- Asignar al personal que a cargo de las situaciones de riesgo. 5.- Elaborar y sociabilizar el Informe de Actv.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio	1.- Modelo de procedimiento de seguridad física 2.- Plan de Contingencia 3.- Informes
3.2.8.1	Análisis de amenazas externas y ambientales, estableciendo medidas de protección para su mitigación.	1.-Establecer las amenazas externas y ambientales que se es vulnerable. 2.- Analizar el impacto de las amenazas en los activos informáticos. 3.- Definir medidas de protección para las amenazas.	1.- Definir probabilidad de las amenazas que está expuesta la facultad. 2.- Determinar la protección física contra estas amenazas. 3.- Implantar el Plan de Contingencia. 4.- Asignar al personal que a cargo de las situaciones de riesgo. 5.- Elaborar y sociabilizar el Informe de Act.	_Personal Administrativo/Área Técnica (RESPONSABLE) _Docentes _Estudiantes	Cada vez que se realice un cambio de localidad o reorganización del espacio de trabajo	1.- Modelo de procedimiento de seguridad física 2.- Plan de Contingencia 3.- Informes
3.2.8.2	Establecer la política de control de acceso a la información en base a los requerimientos de la Facultad	1.- El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos y política de seguridad establecidos en el contrato de trabajo. 2.- Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno	1.- Definir la política de seguridad por parte del SGSI. 2.- Compartir e implementar la política de seguridad. 3.- Asignar supervisor del control de acceso 4.- Establecer sanciones para el incumplimiento de la política de seguridad.	_Líder del Proyecto SGSI, RESPONSABLE _P. Administrativo/Área Técnica (Asignación de privilegios) _Docentes (Supervisión del cumplimiento de accesos) _Estudiantes	1 año	1.- Política de seguridad de acceso a la información. 3.- Asignar supervisor del control de acceso 4.- Procesos Disciplinarios
3.2.8.3	Control de vulnerabilidades técnicas respecto a los sistemas operativos utilizados por la Facultad	1.- Implementar gestión de vulnerabilidad técnica	1.- Asignar responsable del control de vulnerabilidades técnicas en los Sistemas Operativos. 2.- Desarrollar pruebas de seguridad 3.- Establecer el cronograma de ejecución de pruebas. 4.- Elaborar y socializar informes periódicos	_P. Administrativo/Área Técnica RESPONSABLE (Asignación de privilegios)	1 año	1.- Planificación de Pruebas e Informes de Seguridad 4.- Informes

En la tabla 12 se muestra los resultados de las medidas de control de los activos informáticos definido por laboratorios, de acuerdo a la aplicabilidad de las normas ISO y amenazas detectadas. Fuente: Las autoras de la investigación

3.1.3.3.Riesgos por Aulas

Tabla 13. *Medidas de control de los activos informáticos de la FACCI por Aulas*

MEDIDAS DE CONTROL DE LOS ACTIVOS INFORMÁTICOS DE LA FACCI						
#	**Descripción del control adoptado a la FACCI**	**Medidas de implementación del control**	**Acciones (Cómo)**	**Quienes (Responsable)**	**Tiempo**	**Documento a generar (Evidencia)**
4.1.1.1	Establecer la seguridad de oficinas, aulas, laboratorios, medios visuales y demás dependencias de la Facultad	1.- Determinar procedimientos para la seguridad física para las aulas. 2.- Determinar controles de acceso físico	1.- Establecer procedimientos de seguridad para la protección física en las aulas. 2.- Elaborar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Realizar controles de acceso de físico 4.- Preparar y comunicar informes periódicos.	1. Personal Administrativo/Decana RESPONSABLE 2. Personal Administrativo/Área Técnica 3. Docentes - Usuario interno y externo	Periódico: Revisar y actualizar cada año	1. - Procedimientos de seguridad para la protección física en las aulas. 2. - Manual de funciones y responsabilidades para usuarios internos y externos. 3. - Controles de acceso físico. 4. - Informes
	Establecer pautas para la ubicación y protección de los equipos informáticos	1.- Determinar manual de directrices para la ubicación y protección de los proyectores en las aulas.	1.- Establecer manual de directrices para la ubicación y protección adecuada del activo dentro del aula de acuerdo a las especificaciones del espacio. 2.- Realizar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Elaborar y comunicar informes periódicos.	1. Personal Administrativo/Decana RESPONSABLE 2. Personal Administrativo/Área Técnica 3. Docentes - Usuario interno y externo	Periódico: Revisar y actualizar cada año	1.- Manual de directrices para la ubicación y protección adecuada del activo. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Informes
4.1.1.2	Establecer protección del equipo y periféricos ante posibles interrupciones de fallas de energía de los equipos	1.- Desarrollar protecciones generales para los equipos de posibles fallas de energía.	1.- Establecer procedimientos de protección general para los equipos y periféricos informáticos ante las posibles fallas de energía en el suministro eléctrico. 2.- Crear un cronograma para inspecciones periódicas del sistema eléctrico. 3.- Utilizar plantilla de mantenimiento del sistema eléctrico. 4.- Elaborar modelo de registro de las fallas internas encontradas en mantenimiento. 5.- Generar y comunicar informes de las inspecciones realizadas.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Procedimientos de protección general para los equipos y periféricos. 2.- Cronograma para inspecciones del sistema eléctrico. 3.- Plantilla de mantenimiento. 4.- Modelo de registro de fallas internas. 5.- Informes

4.1.1.3	Establecer procedimientos de mantenimiento de equipo y periféricos para asegurar su continua disponibilidad e integridad	1.- Determinar procedimientos de mantenimiento preventivo y correctivo de equipos y periféricos. 2.- Determinar controles apropiados para guiar el programa de mantenimiento de los equipos y periféricos. 3.- Determinar modelo de solicitud para el retiro de equipos y periféricos.	1.- Establecer procedimientos de mantenimiento de equipos y periféricos. 2.- Elaborar controles apropiados cuando se programa el equipo para mantenimiento 3.- Generar un cronograma de mantenimiento periódico. 4.- Utilizar plantilla de mantenimiento HW. 5.- Implantar una plantilla modelo de solicitud para el retiro formal del equipo y periférico. 6.- Diseñar un modelo de registro de las fallas internas encontradas en el soporte. 7.- Elaborar y comunicar informes del mantenimiento realizado.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada período	1.- Procedimientos de mantenimiento de equipos y periféricos. 2.- Controles para mantenimiento 3.- Cronograma de mantenimiento periódico. 4.- Plantilla de mantenimiento de hardware. 5.- Modelo de solicitud para el retiro formal del equipo y periférico. 6.- Modelo de registro de las fallas internas. 7.- Informes
4.1.1.4	Establecer manual para el uso adecuado de los activos informáticos	1.- Determinar manual de guía de uso de activos. 2.- Desarrollar plan de educación y capacitación.	1.- Establecer manual de uso de activos. 2.- Instaurar manual de funciones y responsabilidades para usuarios internos y externos. 3.- Fijar un plan de sensibilización y capacitación. 4.- Disponer un cronograma de capacitación periódico. 5.- Elaborar certificado de participación a los asistentes y firmas de actas. 6.- Realizar informes de las capacitaciones.	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes 5.- Usuario interno y externo	Periódico: Revisar y actualizar cada período	1.- Manual de uso de activos. 2.- Manual de funciones y responsabilidades para usuarios internos y externos. 3.- Plan de sensibilización y capacitación. 4.- Cronograma de capacitación periódico. 5.- Certificado de participación a los asistentes y firmas de actas. 6.- Informes
4.2.1.1	Establecer controles para la seguridad de la redes	1.- Determinar manual de seguridad con los controles estándares para la red	1.- Establecer manual de seguridad con los controles estándares para la red. 2.- Instaurar manual de funciones y responsabilidades para el personal administrativo/área técnica. 3.- Realizar informes	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica	Periódico: Revisar y actualizar cada año	1.- Manual de seguridad con los controles estándares para la red. 2.- Manual de funciones y responsabilidades para el personal administrativo/área técnica. 3.- Informes
4.2.1.2	Establecer políticas sobre el uso de las redes y los servicios de la red	1. - Determinar manual normativas internas para el uso de los servicios de la red inalámbrica. 2.- Desarrollar plan de educación y capacitación	1.- Establecer manual normativas internas para el uso de los servicios de la red inalámbrica de acuerdo a la política de uso de internet elaborado por UCCI. 2.- Elaborar plan de sensibilización y capacitación. 3.- Establecer un cronograma de capacitación periódico. 4.- Realizar informe de actividades	1.- Personal Administrativo/Decana RESPONSABLE 2.- Personal Administrativo/Área Técnica 3.- Miembros del SGSI 4.- Docentes - Usuarios	Periódico: Revisar y actualizar cada período	1.- Manual de normativas internas para el uso de los servicios de la red inalámbrica 2.- Plan de sensibilización y capacitación. 3.- Cronograma de capacitación periódico. 4.- Informe

En la tabla 13 se muestra los resultados medidas de control de los activos informáticos definido por aulas, de acuerdo a las normas aplicables de las normas ISO y amenazas detectadas. Fuente: Las autoras de la investigación

PROPUESTA PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN

3.2. Plan de Sensibilización, Comunicación y Capacitación

3.2.1. Introducción

Una vez analizados los resultados de la tarea investigativa, a continuación, se presenta la propuesta de seguridad informática denominada "PLAN DE SENSIBILIZACIÓN, COMUNICACIÓN Y CAPACITACIÓN PARA MINIMIZAR LOS RIESGOS INFORMÁTICOS EN LA FACULTAD DE CIENCIAS INFORMÁTICAS", que permitirá conocer el estado del hardware, software y otros activos frente a los riesgos informáticos, además permitirá determinar en qué líneas se debe actuar para fortalecer los niveles de seguridad.

El éxito y el impacto de un proyecto de investigación está en la cooperación institucional y de manera especial en la colaboración del personal en las actividades de sensibilización, comunicación, difusión y capacitación. Conjuntamente se debe garantizar una planificación estratégica, una gestión eficaz de las actividades y herramientas que se utilicen. Es por eso que ponemos a consideración esta propuesta a la Facultad de Ciencias Informáticas para su estudio, aprobación e implementación.

La propuesta permitirá optimizar el uso de los recursos informáticos, para lo cual se debe proveer capacitación a los usuarios, orientando así las actuaciones que contribuirán al logro del propósito mencionado. El resultado de esto permitirá a la FACCI ser cada vez más eficiente y efectiva en beneficio propio y de sus usuarios.

3.2.2. Justificación

El plan busca ser una guía de referencia para la implementación de un "Sistema de Gestión de la Seguridad de la Información" bajo la norma ISO 27001 en la Facultad de Ciencias Informáticas de la ULEAM, mediante la orientación y capacitación de los servicios y activos informáticos. La norma se implementó sólo como referencia y no como herramienta; los lineamientos y medidas están basados en las políticas de seguridad definida anteriormente.

El buen uso de los recursos dentro de una institución de tecnología habla de la calidad de enseñanza que se brinda en esta unidad académica, de ahí surge la necesidad de encontrar la información necesaria para elaborar la propuesta del plan de sensibilización, comunicación y capacitación, basada en los requerimientos reales del personal usuario que labora y estudia en esta entidad, cubriendo así en gran parte las vulnerabilidades existentes, incrementando el nivel de enseñanza de seguridad informática con temas relativos a la funciones y responsabilidades.

3.2.3. Objetivo

3.2.3.1.Objetivo General

Diseñar un plan de sensibilización, comunicación y capacitación interna de los lineamientos del proceso de la gestión de seguridad informática para el buen uso de activos informáticos en la Facultad de Ciencias Informáticas de la ULEAM.

*3.2.3.2. **Objetivos Específicos***

- Verificar los resultados obtenidos de los análisis de riesgos informáticos presentados en la Facultad.
- Definir los temas a implementar en las respectivas sensibilizaciones y capacitaciones.
- Proporcionar una base documental referencial para la ejecución del plan.
- Mejorar los niveles de educación en seguridad informática del personal usuario.

3.2.4. Metas

Se establecen metas correspondientes a los objetivos para determinar el alcance del plan de sensibilización, comunicación y capacitación.

Tabla 14. *Tabla de alcance de objetivos*

OBJETIVO	META	INDICADOR	MÉTODO DE VERIFICACIÓN
Verificar los resultados obtenidos del análisis de riesgo informático presentado en la Facultad	Verificar la validez de los resultados obtenidos por el grupo de trabajo.	La existencia de un solo filtro de verificación realiza el 70% de la confiabilidad de los resultados	Mediante el resultado de la Tarea "Evaluación y Tratamiento del Riesgo Informático en la FACCI" fase uno del proyecto SGSI.

Definir los temas a implementar en las respectivas sensibilizaciones y capacitaciones	Las vulnerabilidades consideradas de alto riesgo deben ser catalogadas parte de la sensibilización o la capacitación respectivamente.	Menos del 20% del personal usuario de la FACCI tiene conocimiento de las vulnerabilidades existentes.	Encuesta Interna.
Proporcionar una base documental referencial para la ejecución del plan.	Dar a conocer al 100% la documentación interna de la FACCI existente para establecer el buen uso de los activos informáticos	El 70% de la documentación carece de una estructura correcta para su manipulación. Existe menos del 15% de la documentación requerida.	La nueva estructura y elaboración de la documentación oficial debe ser solicitada al proyecto SGSI.
Mejorar los niveles de educación en seguridad informática del personal usuario.	Extender en un 20% los conocimientos sobre el buen uso de los activos y la seguridad informática del personal usuario en la FACCI	Cubrir con el 80% del personal usuario existente en la FACCI. Obtener el número total de participantes dentro del programa de socialización y capacitación.	Informes estadísticos basados en encuestas previas y posteriores de las actividades planteadas.

En la tabla 14, se muestra cómo se desarrolla el alcance de los objetivos de acuerdo con la meta, indicador y método de verificación. Fuente: Las autoras de la investigación.

3.2.5. Destinatarios

Con el fin de manifestar de manera específica a los diversos grupos de personal usuario, en conjunto con las diversas acciones y materiales destinados para la difusión y capacitación se agrupan en tres ejes de actuación:

Ilustración 7. Destinatarios

Ilustración 7.- Muestra el nivel jerárquico de la estructura de los participantes dentro del proyecto.
Fuente: Las autoras de la investigación.

1. **Personal administrativo. -** Se le asigna la difusión y capacitación esencial para su área de trabajo, así como la manipulación y responsabilidades de

grupos de activos, informes y documentación diseñadas por el proyecto de SGSI. EL personal administrativo está distribuido por diversas áreas de trabajo que son:

1.1. Área Técnica.
1.2. Área Comisión de Investigación.
1.3. Área de Coordinación Académica.
1.4. Área de Comisión Interna de Evaluación.
1.5. Área de Coordinación de Carrera.
1.6. Área de Vinculación con la Sociedad.
1.7. Área de Secretaría.
1.8. Área de Decanato.
1.9. Área de Asociación Estudiantil.
1.10. Área de Profesores

2. **Personal Docente. -** Se le asigna la difusión y capacitación esencial para su área de trabajo, así como las asignaciones de responsabilidad, informes y documentación diseñadas en el proyecto de SGSI.

3. **Estudiantes. -** Se le asigna la difusión y capacitación esencial para cuidar sus áreas de estudio, así como las medidas del buen uso de activos informáticos diseñado en el proyecto de SGSI.

Las actividades de comunicación y capacitación tienen como objetivo transmitir una serie de mensajes e informaciones a unos grupos de destinatarios claramente identificados.

3.2.6. Estrategias y actividades

Estos ejes de actuación que forman los pilares de la estrategia de sensibilización y capacitación prevén la adecuación coherente de las actividades y herramientas necesaria para los diferentes objetivos.

Tabla 15. *Estrategias y actividades para cumplir objetivos*

DESTINATARIOS / OBJETIVOS	PERSONAL ADMINISTRATIVO	DOCENTES	ESTUDIANTES
Verificar los resultados obtenidos del análisis de riesgo informático presentado en la Facultad	*Encuestas*	*Encuestas*	*Encuestas*
	Informes de vulnerabilidades	*Informes de vulnerabilidades*	*Informes de vulnerabilidades*
Definir los temas a implementar en las respectivas sensibilizaciones y capacitaciones	*Sensibilización (reuniones, videos, volantes)*	*Sensibilización (reuniones, videos, volantes)*	*Sensibilización (reuniones, videos, volantes)*
	Capacitación (talleres, folleos, videos, eventos)	*Capacitación (talleres, folleos, videos, eventos)*	
Proporcionar una base documental referencial para la ejecución del plan.	*Documento de lineamientos de buen uso de activos informáticos.*	*Documento de lineamientos de buen uso de activos informáticos.*	*Documento de lineamientos de buen uso de activos informáticos.*
	Documentos oficiales de responsabilidades, informes del uso de activos dentro de la FACCI	*Documentos oficiales de responsabilidades, informes del uso de activos dentro de la FACCI*	
	Documentos oficiales para configurar, administrar y realizar pruebas sobre el uso de activos y los permisos de acceso dentro de la FACCI		
Mejorar los niveles de educación en seguridad informática del personal usuario	*Encuestas previas a las actividades*	*Encuestas previas a las actividades Encuestas*	*Encuestas previas a las actividades*
	Encuestas posteriores a las actividades	*Encuestas posteriores a las actividades*	*Encuestas posteriores a las actividades*

En la tabla 15 se muestra las herramientas y actividades necesarias para cumplir los objetivos de acuerdo con el personal usuario. Fuente: Las autoras de la investigación

La estrategia del programa de sensibilización y capacitación está dividida por actividades dirigidas a los destinatarios dependiendo de los objetivos que se plantean en esta propuesta.

3.2.6.1. Comunicación Interna

Es muy común encontrar que en las empresas el personal confunde seguridad informática con seguridad de la información, así como otros están convencidos que la información es solo la documentación digital, desconociendo que la impresa también lo es. La mayoría de las vulnerabilidades provienen desde el interior de las propias empresas (empleados descontentos, fraude interno, accesos no autorizados, poca motivación, carencia de entrenamiento organizacional y desconocimientos de las políticas de seguridad).

Por este motivo es muy importante esclarecer las vulnerabilidades y atacar desde raíz, brindando un tratamiento efectivo cultivando al personal y estudiantes en la ciencia de seguridad informática, determinando y clasificado los temas vulnerables son de parte de la sensibilización, además cuáles temas vulnerables están definitivos para la capacitación.

Información y Sensibilización

Los temas a sensibilizar son:

1. Gestión de Activos
   1.1. Lineamientos de buen uso de activos informáticos
   1.2. Reporte de debilidades o vulnerabilidades de seguridad
2. Control de Acceso
   2.1. Políticas de control de acceso
   2.2. Control de accesos remotos
   2.3. Restricciones de accesos
   2.4. Gestión de acceso a usuarios
      2.4.1. Políticas de responsabilidad de acceso a usuarios
   2.5. Control de acceso a sistemas y aplicaciones
      2.5.1. Restricciones de acceso a información
3. Seguridad Física y Ambiental
   3.1. Áreas Seguras
   3.2. Equipos
      3.2.1. Mantenimiento de equipos
4. Adquisición, desarrollo y mantenimiento de sistemas
   4.1. Políticas para establecer los requerimientos del uso de software patentado.
   4.2. Requisitos de seguridad de los sistemas de información
   4.3. Gestión de la prestación de los sistemas a terceros
5. Gestión de incidentes de seguridad de la información
   5.1. Políticas de filtración o fuga de información

6. Procesos disciplinarios

Talleres de Comunicación y Capacitación

Los temas a capacitar son:

1. Organización de Seguridad de la Información
   1.1. Roles y responsabilidades
2. Gestión de Activos
   2.1. Lineamientos de buen uso de los activos informáticos
   2.2. Responsabilidad por los activos informáticos
   2.3. Inventario de activos
   2.4. Manejo de los soportes de almacenamiento
      2.4.1. Gestión de medios extraíbles
      2.4.2. Eliminación de soporte
   2.5. Reporte de debilidades o vulnerabilidades de seguridad
3. Control de Acceso
   3.1. Políticas de control de acceso
   3.2. Controles de accesos remotos
   3.3. Restricciones de acceso
   3.4. Gestión de acceso a usuarios
      3.4.1. Políticas de responsabilidad de acceso a usuarios
   3.5. Control de acceso a sistemas y aplicaciones
      3.5.1. Restricciones de acceso a información
4. Seguridad Física y Ambiental
   4.1. Áreas Seguras
      4.1.1. Perímetros de seguridad física
      4.1.2. Controles físicos de entrada
      4.1.3. Condiciones de áreas de trabajo
      4.1.4. Límites de seguridad de oficinas, habitaciones y medios
      4.1.5. Protecciones sobre amenazas ambientales
   4.2. Equipos

4.2.1. Mantenimiento de equipos

4.2.1.1. Informes de Mantenimiento

4.2.2. Seguridad del cableado

4.2.3. Ubicación y protección de los equipos

5. Seguridad de las operaciones

5.1. Protección contra código malicioso

5.1.1. Controles contra código malicioso

5.2. Copias de Respaldo

5.2.1. Políticas para realizar las copias de seguridad

5.2.2. Registro y seguimiento de eventos de los sistemas y aplicativos

5.2.3. Control de software operacional

5.2.3.1. Control de software en sistemas operativos

5.2.4. Gestión de vulnerabilidades

5.2.4.1. Restricciones sobre la instalación de software

6. Adquisición, desarrollo y mantenimiento de sistemas

6.1. Políticas para establecer los requerimientos del uso de software patentado

6.2. Requisitos de seguridad de los sistemas de información

6.3. Gestión de la prestación de los sistemas a terceros

7. Gestión de incidentes de seguridad de la información

7.1. Políticas de filtración o fuga de información

8. Procesos disciplinarios

3.2.6.2.Responsable de comunicación

El proyecto Plan de sensibilización, comunicación y capacitación nombra Responsable de Comunicación al líder de proyecto "Sistema de Gestión de la Seguridad de la Información bajo la Norma ISO/IEC 27001", Ing. Denise Vera. Mg.

Como responsable de comunicación debe velar por el buen desarrollo del presente plan, controlar que todas las actividades que están incluidas en esta propuesta se lleven a cabo de forma exitosa y que las actividades de comunicación y capacitación sean

coherentes entre sí. Además de ayudar a coordinar las diferentes actividades necesarias para la ejecución de éste.

3.2.7. Herramientas

Las herramientas y elementos necesarios para desarrollar este plan de difusión y capacitación son:

Ilustración 8. Herramientas del Plan

Ilustración 8.- Representa cuáles son las herramientas necesarias para desarrollar las actividades del plan.
Fuente: Las autoras de la investigación

- **Medios de comunicación:** Son medios esenciales y centrales donde se ofrece información centralizada y directa, las podremos utilizar como herramienta de difusión a los eventos, talleres y demás actos que se realizaran para cumplir con las actividades.

Usando medios de información comunes (correo electrónico, redes sociales, memorándum, etc.). Se podrán desarrollar notas de prensa, artículos que se difundirán y deben estar adaptadas al lenguaje de los medios de comunicación, utilizando titulares, subtítulos, organizando la información según su importancia, utilizando herramientas visuales. (Videos, Imágenes, Gif, Otros)

- **Reuniones:** Elemento importante para entablar sensibilizaciones de alto nivel que corresponden a las autoridades de la FACCI donde se tomarán decisiones drásticas para eliminar una valiosa cantidad de vulnerabilidades existentes.

- **Actos y Eventos:** El proceso de la sensibilización, comunicación y capacitación, implica realizar una serie de actividades que representan un buen porcentaje de las tareas que deben ser organizadas por el responsable del proyecto de SGSI, una vez detectadas las necesidades del plan se desarrollan cursos, programas, eventos, actos, etc., se debe proceder a impartirlos de manera adecuada y para el personal indicado.

  Se debe tener en cuentas las características de las actividades, sea de sensibilización, comunicación o capacitación, verificando el uso técnicas didácticas adecuadas, utilizadas por el instructor o facilitador al pretender transmitir sus conocimientos con el propósito de que la información sea entendida y/o asimilada por los presentes.

- **Talleres:** Propuesta de medios adquiridos con personal capacitado y expertos en temas de seguridad informática, donde se brindará capacitación y material didáctico fundamental para el aprendizaje del personal usuario de la FACCI y así poder medir el estado de nivel de educación que se ha implementado mediante pruebas y encuestas.

- **Documentos Oficiales:** Medios físicos o digitales que deben ser sociabilizados con el Honorable Consejo de Facultad, brindando capacitación al personal usuario para su correcta manipulación en su vida laboral, la cual permite que el protocolo de seguridad a implementarse por el proyecto de seguridad

informática obtenga resultados positivos en la FACCI. Los documentos oficiales necesarios para el plan de capacitación son:

Tabla 16. *Documento Medidas de Seguridad de SGSI*

MEDIDAS DE SEGURIDAD DE SGSI	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos de Medidas de Seguridad de Información implementado en la FACCI.
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Políticas de Seguridad en las Contraseñas - Políticas de Criptografía - Directrices Sobre el Intercambio de Información por Correo Electrónico y Cualquier Medio de Información. - Clasificación de la Información - Política de Backup de la Información - Guía de Procesos Generales en Copias de Seguridad - Formatos para la Entrega de las Copias de Backup realizadas - Procesos Generales para el Proceso de Respaldo de la Información - Procesos Alternativos para Realizar Copias o Respaldo de la Información - Políticas Generales y Especificas que involucren procesos y manipulación de activos o sistemas.

En la tabla 16 se muestra las especificaciones del documento de Medidas de Seguridad SGSI
Fuente: Las autoras de la investigación

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 17. *Documento Plan de Mantenimiento*

PLAN DE MANTENIMIENTO	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos de Mantenimiento de Activos implementado en la FACCI.
Observación:	La documentación está existente y fue elaborada por el Ing. Víctor Domínguez que fue autor de una de las tareas del Proyecto de Seguridad SGSI.

En la tabla 17 se muestra las especificaciones del documento Plan de Mantenimiento.
Fuente: Las autoras de la investigación.

Tabla 18. *Documento Plan de Continuidad*

PLAN DE CONTINUIDAD	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos de Contingencia y Continuidad del Proyecto de SGSI implementado en la FACCI.

Observación:	La documentación está existente y fue elaborada por el Ing. Víctor Domínguez que fue autor de una de las tareas del Proyecto de Seguridad SGSI.

En la tabla 18 se muestra las especificaciones del documento Plan de Continuidad.
Fuente: Las autoras de la investigación

Tabla 19. *Documento Plan de Contingencia*

PLAN DE CONTINGENCIA	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos de Contingencia y Continuidad del Proyecto de SGSI implementado en la FACCI.
Observación:	La documentación está existente y fue elaborada por el Ing. Víctor Domínguez que fue autor de una de las tareas del Proyecto de Seguridad SGSI.

En la tabla 19 se muestra las especificaciones del documento Plan de Continuidad.
Fuente: Las autoras de la investigación

Tabla 20. *Documento Lineamientos del Buen Uso de Activos*

LINEAMIENTOS DEL BUEN USO DE ACTIVOS INFORMÁTICOS	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos del Plan de Sensibilización, comunicación y Capacitación del Proyecto SGSI implementado en la FACCI.
Observación:	La documentación está existente y fue elaborada por la Srta. Joselyne Rodríguez y la Srta. Diana Sánchez que fueron autoras de una de las tareas del Proyecto de Seguridad SGSI.

En la tabla 20 se muestra las especificaciones del documento Lineamientos del buen uso de activos informáticos.
Fuente: Las autoras de la investigación

Tabla 21. *Documento Procedimientos de Control*

PROCEDIMIENTOS DE CONTROL DE ACCESO	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos Control de Acceso
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Políticas de Gestión de Privilegios - Privilegios por Áreas de Trabajo

En la tabla 21 se muestra las especificaciones del documento Procedimientos de Control de Acceso.
Fuente: Las autoras de la investigación

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 22. *Documento Requisitos para el desarrollo de aplicaciones y sistemas*

REQUISITOS PARA EL DESARROLLO DE APLICACIONES Y SISTEMAS	
Descripción:	Documentos de Desarrollo de Software
Pertenece a:	Documentos Control de Acceso
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Requerimientos para el Desarrollo de Aplicaciones o Sistemas para la Aprobación de las Materias del Pensum Académico. - Requerimientos para la Contratación de Aplicaciones o Sistemas para la Implementación en la Unidad Académica.

En la tabla 22 se muestra las especificaciones del documento Requisitos para el desarrollo de aplicaciones y sistemas.
Fuente: Las autoras de la investigación

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 23. *Documento Pruebas e Informes de Seguridad*

PRUEBAS E INFORMES DE SEGURIDAD	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos Pruebas de Seguridad implementado en la FACCI.
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Cronograma de Pruebas de seguridad - Diseño de las Pruebas de Seguridad - Tipo de Pruebas para Implementar (Lógicas, Físicas, etc.) - Informe de las Pruebas

En la tabla 23 se muestra las especificaciones del documento Pruebas e Informes de Seguridad.
Fuente: Las autoras de la investigación.

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 24. *Documento Inventario de Activos*

INVENTARIO DE ACTIVOS	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos Medidas de Seguridad Física implementado en la FACCI.
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Política de Responsabilidad de Activos - Política de Control de Activos - Ficha Solicitud de Activo - Ficha Eliminación de Activo - Formato de Inventario para Hardware Y Software - Solicitud Retiro de Equipo - Solicitud Entrega de Equipo - Estado de Activos (De Baja, En Movimiento, En Implementación)

En la tabla 24 se muestra las especificaciones del documento Inventario de Activos.
Fuente: Las autoras de la investigación

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 25. *Documento Seguridad Física*

SEGURIDAD FÍSICA	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos Medidas de Seguridad Física implementado en la FACCI.
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Política de Seguridad Física en Activos - Política de Seguridad Física en Áreas de Trabajo - Asignar un Responsable por Área de Trabajo - Modelo de Procedimiento - Perímetros de Seguridad Física en el Área de Trabajo - Perímetros de Seguridad Física en los Activos Informáticos - Perímetro de Control de Acceso - Controles de Seguridad Física en la entrada de las Áreas de Trabajo - Registro de personas autorizadas y las no autorizadas que ingresan a manipular activos e información en las áreas de trabajo

En la tabla 25 se muestra las especificaciones del documento Seguridad Física.
Fuente: Las autoras de la investigación

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 26. *Documento Procedimientos Generales para el Manejo, Almacenamiento y Comunicación de Información*

PROCEDIMIENTOS GENERALES PARA EL MANEJO, ALMACENAMIENTO Y COMUNICACIÓN DE INFORMACIÓN	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos Medidas de Seguridad Física implementado en la FACCI.
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Políticas de almacenamiento de Información - Controles de manejo de información - Controles de eliminación de información - Estrategias de comunicación Interna y Externa

En la tabla 26 se muestra las especificaciones del documento Procedimientos Generales para el Manejo, Almacenamiento y Comunicación de Información.
Fuente: Las autoras de la investigación.

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 27. *Documento Registro de Actividades*

REGISTRO DE ACTIVIDADES	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos Medidas de Seguridad Física implementado en la FACCI.
Observación:	El líder del proyecto de SGSI junto a los integrantes de las diversas tareas deberán desarrollar esta documentación en la que deben definir: - Formato del Informe Diario de Actividades de los Usuarios - Formato del Informe Mensual de Actividades de los Usuarios - Formato de Vulnerabilidades y Debilidades encontradas - Reporte de Vulnerabilidades y Debilidades encontradas

En la tabla 27 se muestra las especificaciones del documento Registro de Actividades.
Fuente: Las autoras de la investigación.

El contenido de este documento deberá ser revisado por el área de tecnología y será aprobado por el Honorable Consejo de Facultad y la Autoridad competente.

Tabla 28. *Documento Informe de Auditoría*

INFORME DE AUDITORÍA	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Documentos de Auditoria Interna implementado en la FACCI
Observación:	La documentación esta existente y fue elaborada por el Srta. Kimberly Delgado que fue autora de una de las tareas del Proyecto de Seguridad SGSI.

En la tabla 28 se muestra las especificaciones del documento Informe de Auditoría.
Fuente: Las autoras de la investigación.

Tabla 29. *Documento Procesos Disciplinarios*

PROCESOS DISCIPLINARIOS	
Descripción:	Comprende a los documentos oficiales del Proyecto
Pertenece a:	Todos los Documentos implementado en la FACCI.
Observación:	Los procesos disciplinarios deben estar existente en todos documentos y a su vez recolectados en uno solo como reglamento oficial de la FACCI para ejecutarlo mediante el Honorable Consejo de Facultad y la Autoridad Competente.

En la tabla 29 se muestra las especificaciones del documento Informe de Auditoría.
Fuente: Las autoras de la investigación.

- **Encuestas:** Material de referencia descriptiva por el cual se recopilarán datos mediante un cuestionario elaborado dependiendo de la actividad a desarrollarse, la cual brindará información esencial que se analizará y se tomará como muestra de resultados.

- **Material Promocional:** Se compone de folletos de difusión y otro material como papelería, banners a usar durante eventos y actos oficiales. Su realización será coordinada por el líder que recibirá las opiniones de las autoridades competentes de la FACCI.

- **Redes Sociales:** Elemento esencial cumpliendo la función de comunicarnos con el nivel más bajo de los participantes de este proyecto, realizando invitaciones a los actos, eventos y talleres a realizarse. La responsabilidad

del uso y difusión en las redes sociales será del líder del proyecto que se encargará de su gestión y actualización constante.

- **Materiales de Referencia:** Asigna, las publicaciones que tendrán una divulgación direccionada y de edición mayor, y otro tipo de materiales de referencia accesibles (formato electrónico o PDF), podrán servir como base documental o material de trabajo considerando también las publicaciones y el material de referencia.

3.2.8. Presupuesto

En el proyecto está previsto el siguiente presupuesto para actividades de sensibilización y capacitación, presentado a continuación. Efectuado en dólares:

Tabla 30. *Presupuesto para las actividades del Plan*

ACTIVIDAD	DESCRIPCIÓN	COSTO POR ACTIVIDAD	TOTAL
Materiales impresos para la divulgación, socialización y formación.	Material desarrollado bajo estándares locales, materiales como folletos, afiches, volantes, trípticos, etc.	$150	$1,050
Campaña del Buen Uso de Activos Informáticos	Afiches, folletos, botones, lapiceros, tazas, otros. (Audiovisuales y material para las redes sociales y medios de comunicación)	$200	$1,400
Divulgación de Talleres, Actos y Eventos de capacitación.	Afiches y banners (audiovisuales y materiales para las redes sociales y medios de comunicación)	$100	$700
Contratación del Personal capacitado como ponentes principales en Talleres, Actos y Eventos de capacitación.	Contrato por evento del personal capacitado en temas especializados de seguridad informática, con materiales didácticos específicos.	$250	$1,750
Actividades extralaborales	Refrigerios, material impreso (identificadores, etc.), carpetas, etc.	$180	$1,260
TOTAL		$880	$6,160

En la tabla 30 se muestra el presupuesto para las actividades de sensibilización y capacitación planteada para la Facultad. las actividades deben ser implementada en los temas de las sensibilizaciones y de las capacitaciones siendo 7 temas centrales, se multiplicará por este número para obtener el total por actividad.
Fuente: Las autoras de la investigación

3.2.9. Cronograma

Este cronograma de Sensibilización y Comunicación se implementará en todo el personal usuario de la FACCI.

Tabla 31. *Cronograma de Sensibilización*

Fecha de Difusión - Sensibilización	ABRIL SEMESTRE 1 (ABRIL-SEPTIEMBRE)																								
Temas	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
Campaña de Sensibilización en la FACCI																									
Resultado del Análisis de Riesgo en la FACCI																									
1. Gestión de Activos																									
1.1. Lineamientos de Buen Uso de Activos Informáticos																									
1.2. Reporte de debilidades o vulnerabilidades de seguridad																									
2. Control de Acceso																									
2.1. Política de control de acceso																									
2.2. Control de accesos remotos																									
2.3. Restricción de accesos																									
2.4. Gestión de acceso a usuarios																									
2.4.1. Política de responsabilidad de acceso a usuarios																									
2.5. Control de acceso a sistemas y aplicaciones																									
2.5.1. Restricción de acceso a información																									
3. Seguridad Física y Ambiental																									
3.1. Áreas Seguras																									
3.2. Equipos																									
3.2.1. Mantenimiento de equipos																									
4. Adquisición, desarrollo y mantenimiento de sistemas																									
4.1. Política para establecer los requerimientos del uso de software patentado.																									
4.2. Requisitos de seguridad de los sistemas de información																									
4.3. Gestión de la prestación de los sistemas a terceros																									
5. Gestión de incidentes de seguridad de la información																									
5.1. Políticas de filtración o fuga de información																									
6. Procesos disciplinarios																									

En la tabla 31 se aprecia el cronograma estipulado para la sensibilización, a modo de inducción, de los resultados obtenidos de las investigaciones previas y los temas en aspectos de seguridad informática, definido para el mes de abril. Fuente: Las autoras de la investigación

Talleres y Eventos de Capacitación, estos talleres pueden ser actos o eventos para el personal específico que maneja los controles de seguridad o responsabilidad adquirida.

Tabla 32. *Cronograma de Talleres de Capacitación*

Fecha de Talleres de capacitación	ABRIL SEMESTRE 1 (ABRIL-SEPTIEMBRE)		MAYO SEMESTRE 1(ABRIL-SEPTIEMBRE)																							
Temas	29	30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Campaña de Capacitación en la FACCI																										
1. Organización de Seguridad de la Información																										
1.1. Roles y Responsabilidades																										
2. Gestión de Activos																										
2.1. Lineamientos de Buen Uso de Activos Informáticos																										
2.2. Responsabilidad por los activos informáticos																										
2.3. Inventario de Activos																										
2.4. Manejo de los soportes de almacenamiento																										
2.4.1. Gestión de medios extraíbles																										
2.4.2. Eliminación de soporte																										
2.5. Reporte de debilidades o vulnerabilidades de seguridad																										
3. Control de Acceso																										
3.1. Política de control de acceso																										
3.2. Control de accesos remotos																										
3.3. Restricción de accesos																										
3.4. Gestión de acceso a usuarios																										
3.4.1. Política de responsabilidad de acceso a usuarios																										
3.5. Control de acceso a sistemas y aplicaciones																										
3.5.1. Restricción de acceso a información																										
4. Seguridad Física y Ambiental																										
4.1. Áreas Seguras																										
4.1.1. Perímetros de seguridad física																										
4.1.2. Controles físicos de entrada																										
4.1.3. Condiciones de áreas de trabajo																										
4.1.4. Límites de seguridad de oficinas, habitaciones y medios																										
4.1.5. Protección sobre amenazas ambientales																										
4.2. Equipos																										
4.2.1. Mantenimiento de equipos																										
4.2.1.1. Informes de Mantenimiento																										

4.2.2. Seguridad del cableado																									
4.2.3. Ubicación y protección de los equipos																									
5. Seguridad de las operaciones																									
5.1. Protección contra código malicioso																									
5.1.1. Controles contra código malicioso																									
5.2. Copias de respaldo																									
5.2.1. Políticas para realizar las copias de seguridad																									
5.2.2. Registro y seguimiento de eventos de los sistemas y aplicativos																									
5.2.3. Control de Software operacional																									
5.2.3.1. Control de software en sistemas operativos																									
5.2.4. Gestión de vulnerabilidades																									
5.2.4.1. Restricciones sobre la instalación de software																									
6. Adquisición, desarrollo y mantenimiento de sistemas																									
6.1. Política para establecer los requerimientos del uso de software patentado.																									
6.2. Requisitos de seguridad de los sistemas de información																									
6.3. Gestión de la prestación de los sistemas a terceros																									
7. Gestión de incidentes de seguridad de la información																									
7.1. Políticas de filtración o fuga de información																									
8. Procesos disciplinarios																									

En la tabla 32 se aprecia el cronograma estipulado para el proceso de capacitación que involucra la realización de talleres de los temas sensibilizados anteriormente, definido en los últimos días de abril y el mes de mayo. Fuente: Las autoras de la investigación.

3.2.10. Seguimiento y evaluación de resultados

Para garantizar la realización de las medidas preventivas en materia de seguridad informática y el buen uso de activos informáticos es necesario tener una excelente difusión, y capacitación se debe facilitar una gestión eficaz y transparente del proyecto en general, para obtener los resultados esperados de las actividades, definidas al inicio del proyecto. Por este motivo las personas autorizadas a realizar el seguimiento y la evaluación de resultado es el representante de la Comisión de Investigación y el Decano(a) de la FACCI.

Tabla 33. *Tabla para el seguimiento y evaluación de resultados del Plan*

TIPO DE INDICADOR	INDICADOR	ESTADO ESPERADO
Realización del Evento	Reuniones de Sensibilización.	100%
	Entrega de lineamientos del Buen Uso de Activos Informáticos a los asistentes.	100%
	Entrega de documentación oficial al personal competente.	100%
	Campaña de Sensibilización.	90%
	Campaña de Capacitación.	90%
	Contratación o Gestión de Ponentes expertos en seguridad informática.	100%
	Material de medios de comunicación	80%
	Áreas de capacitación y realización de talleres con buen estado (a/c, proyector, pizarra, PC's, etc.)	100%
	Cobertura de prensa universitaria	100%
Medir resultados de Eventos	Desarrollo de encuesta de niveles de educación informática (previa las capacitaciones y posterior a las capacitaciones)	80%
	Presencia de Asistentes en los seminarios. Medir el comportamiento y nivel de compromiso de los asistentes.	100%

En la tabla 33 se muestra el tipo de indicador, la descripción de dicho indicador y el estado esperado es definido en porcentaje.
Fuente: Las autoras de la investigación.

La realización de una evaluación intermedia y la evaluación de las actividades hace posible la detección de problemas internos y su corrección a tiempo, de modo que se consiga una gestión y coordinación más eficaz y eficiente.

3.2.11. Aspectos legales

Los procesos de capacitación para el sector público están orientados a obtener, desarrollar y potencializar al talento humano en las instituciones del Estado, de conformidad con este principio, el ordenamiento jurídico interno compuesto por la Constitución de la República, las leyes y demás normativa vigente reconocen y garantizan a la capacitación como un derecho

Al respecto, según lo prescrito en el artículo 234 de la Constitución de la República del Ecuador, "El Estado garantizará la formación y capacitación continua de las servidoras y servidores públicos a través de las escuelas, institutos, academias y programas de formación o capacitación del sector público; y la coordinación con instituciones nacionales e internacionales que operen bajo acuerdos con el Estado" (Ministerio del Trabajo)

Por tanto, siendo la capacitación un derecho irrenunciable de los servidores y trabajadores públicos, demanda responsabilidad y compromiso para aportar en la construcción de un Estado que responda de manera incluyente, eficiente, y práctica a las necesidades de la ciudadanía y al fortalecimiento del Plan Nacional de Desarrollo.

Al respecto, según lo prescrito en el artículo Art. 83 del Reglamento de Régimen Académico, "La educación continua hace referencia a procesos de capacitación, actualización y certificación de competencias laborales específicas, desarrolladas en el marco de la democratización del conocimiento, que no conducen a una titulación de educación superior" (Consejo de Educación Superior, 2018).

Por lo tanto, siendo la capacitación una competencia de labores específicas es necesaria para la continuidad de las labores, determinando así la eficiencia de los servicios prestados a nuestra comunidad estudiantil.

Al respecto, según lo prescrito en el Art. 14 del Reglamento Igualdad de Todos los Actores de la ULEAM aprobado por el Órgano Colegiado Académico Superior., "Derechos del personal administrativo y trabajadores. - Son sus derechos: literal a:) "Acceder, permanecer y ascender en la trayectoria profesional, capacitación, cargos

directivos y de representación sin discriminación de género, credo, orientación sexual, pertenencia étnica, cultura, preferencia política, edad, condición socioeconómica o discapacidad conforme a sus necesidades y características específicas." (ULEAM, 2018)

Por lo tanto, garantizará la formación y capacitación continua sin discriminación alguna, mediante la implementación y desarrollo de programas de capacitación.

La estructura del Plan de Sensibilización, Comunicación y Capacitación está desarrollada bajo la autoría de las investigadoras Srta. Joselyne Rodríguez y Srta. Diana Sánchez, por medio de una exhaustiva investigación de documentación Nacional e Internacional basada en Planes de Capacitación y Sensibilización.

Creando así un híbrido que une la necesidad primordial en cualquier medio, la comunicación efectiva.

3.2.12. Glosario

Sensibilización. – Hacer sensible algo o a alguien. (RAE, 23° Edición , 2014)

Debilidades. – Establecer un análisis sincero de lo negativo y lo positivo y, posteriormente, aplicar una estrategia adecuada. (Editorial Definición MX, 2014)

Vulnerabilidades. – Referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. (ALEGSA ©, 2016)

Concienciación. – Acción y efecto de concienciar o concienciarse. (RAE, 23° Edición , 2014)

SGSI. – Sistema de Gestión de Seguridad Informática.

FACCI. – Facultad de Ciencias Informáticas.

Análisis de Riesgo. – Pruebas que permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. (Amaya, 2012)

Personal usuario. – Usuarios pertenecientes a todo el personal administrativo y estudiantes que administran, consumen y manipulan los sistemas y activos informáticos dentro de la FACCI. (Las autoras)

Gestión. – Acción y efecto de gestionar y administrar. (RAE, 23° Edición , 2014)

Lineamientos. – Es el programa o plan de acción que rige a cualquier institución. De acuerdo con esta aceptación, se trata de un conjunto de medidas, normas y objetivos que deben respetarse dentro de una organización. (Porto, 2008)

Control. – Actividad o acción realizada manualmente y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos. (Carlos, Susana, & Arturo, s.f.)

Restricción. – Ceñir, circunscribir, reducir a menores límites. (RAE, 23° Edición , 2014)

Adquisición. – Persona cuyos servicios o ayuda se consideran valiosos. (RAE, 23° Edición , 2014)

Políticas. – Son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. (EmprendePyme, s.f.)

Requisitos. – Circunstancia o condición necesaria para algo. (RAE, 23° Edición , 2014)

Roles. – Función que alguien o algo desempeña. (RAE, 23° Edición , 2014)

Soportes. – Es un servicio que ofrecen especialistas en apoyo técnico y de este modo proporcionan asistencia técnica y asesoramiento de aparatos tecnológicos. (CISTE, s.f.)

Perímetros. – Contorno de una superficie. Medida del contorno de una figura. (RAE, 23° Edición , 2014)

Condiciones. – Hacer depender algo de una condición. (RAE, 23° Edición , 2014)

Incidentes. – Se define como un evento adverso o una violación a la Política de Seguridad de la Información de la Universidad; que compromete o puede comprometer la seguridad de la información. (Universidad Nacional de Luján, 2010)

Filtración. – Divulgar indebidamente información secreta o confidencial. (RAE, 23° Edición , 2014)

Adjudicando. - Asignar o atribuir algo a una persona o a una cosa. (RAE, 23° Edición , 2014)

Destinatarios. – Dicho de una persona o de una cosa: A la que se destina o dirige algo. (RAE, 23° Edición , 2014)

Adecuación. – Acción y efecto de adecuar. (RAE, 23° Edición , 2014)

Banner. – Es una palabra del inglés que se usa para designar un anuncio publicitario de internet. (Significados, 2015)

CAPÍTULO VI: CONCLUSIONES, LIMITACIONES Y RECOMENDACIONES

6.1. Conclusiones

Este trabajo de investigación permitió analizar y generar una propuesta que se estructuró en un plan de Sensibilización, Comunicación y Capacitación, el que permitirá minimizar los riesgos informáticos latentes en la FACCI; mediante el manejo de diferentes documentos oficiales necesarios y la elaboración de informes, los cuales permiten desarrollar de forma más especializada los trabajos concernientes a la gestión de la seguridad informática.

De acuerdo a los objetivos se concluye que:

- El análisis de los riesgos informáticos mostró la necesidad de crear un plan de sensibilización comunicación y capacitación, ya que la comunidad FACCI por desconocimiento, no se han podido detectar técnicamente las vulnerabilidades que existen actualmente, consiguiendo provocar en cualquier momento incidentes que comprometan el funcionamiento normal de las operaciones. Nuestra propuesta y diseño está enfocada a detectar técnicamente las vulnerabilidades de mayor riesgo e irlas corrigiendo y resolviendo los problemas presentes.

- De los procesos que tiene el SGSI, se identificó que el informe de declaración de aplicabilidad es fundamental en la alineación con la norma ISO 27001 mediante el cual se indica las políticas de esta norma aplicables a la Facultad de acuerdo con su realidad. Sin embargo, en el transcurso del proceso de verificación de las vulnerabilidades se hizo preciso encontrar sustento con la norma ISO 17799, misma que, complementa a la anterior mencionada, está direccionada a minimizar las vulnerabilidades no contempladas en la norma 27001, dando como resultado un mayor alcance en la protección de los activos siendo un proceso exitoso.

- Del análisis de riesgo desarrollado, la actualización y desarrollo de la gestión documental del proyecto de investigación, se pudo evidenciar la baja capacitación que tiene el personal para el manejo de procesos críticos, sobre todo los estudiantes que son los usuarios finales.

- La propuesta de un plan de sensibilización, capacitación y comunicación que fomente los lineamientos del buen uso de activos informáticos, involucrando a toda la

comunidad de la FACCI, permitirá mejorar los ámbitos relacionados con el tratamiento de riesgos, ayudará a generar una cultura de seguridad que permita disminuir la inseguridad informática, como los errores de los usuarios que resultan siendo los más comunes y provocan amenazas con alto impacto y frecuencia dentro de la unidad académica.

De forma general se concluye:

- La elaboración de este plan de sensibilización, comunicación y capacitación apoyará la mitigación de riesgos informáticos siendo una importante labor, pero será solo el punto de partida, queda mucho por realizar. Habiendo logrado los objetivos planteados, se ha avanzado un buen tramo en el fortalecimiento del SGSI institucional. Así mismo conocimos y aprendimos mucho de nuestra facultad con el diagnóstico de seguridad informática.

- Este fue un esfuerzo que vale la pena, ya que mejorará la seguridad informática y la comunicación interna de la Facultad; por lo que será necesario definir acciones claras para así optimizar los recursos que en toda organización son limitados. Así pues, con la difusión de este plan, cumplimos con el desarrollo de un plan sencillo, coherente, fundamentado en teorías y diagnóstico, para una institución pública, con recursos limitados y grandes necesidades respecto a la seguridad informática

6.2. Limitaciones

Al concluir la investigación es necesario señalar la presencia de ciertas limitantes que afectaron el desarrollo de nuestra investigación.

Estructuración del tema:

El tema base de la tarea investigativa fue asignada por el docente líder del proyecto, mismo que en primera instancia no tenía la claridad necesaria ya que se prestaba para diversas interpretaciones. Después en reunión de expertos y los miembros del proyecto se pudo dar claridad y precisión a la temática. Esto causó retraso en el inicio de nuestra tarea investigativa.

Falta de insumos:

La información de las otras tareas de investigación previas a la nuestra, eran insumos claves para el logro de nuestros objetivos, sin embargo, tuvimos retraso porque las tareas investigativas previas no habían culminado.

Ambiente comunicacional del equipo de investigación:

En el desarrollo de la investigación es inevitable encontrarse con dudas y desacuerdo entre los estudiantes que desarrollan el trabajo de campo y los estudiantes que desarrollan el trabajo cualitativo del proyecto de investigación, la vinculación de estos factores se vio afectada por diversos medios que involucran directamente a los responsables del proyecto (Docentes Investigadores) lo que ocasiona una asincronía en las decisiones tomadas por ellos, limitando al desarrollo de las tareas asignadas que están en ejecución. La situación de inestabilidad comunicacional influyó considerablemente en la dispersión del equipo de investigación.

Resultados de las tareas de investigación:

La información que se ha utilizado como resultado de las anteriores tareas de investigación han sido elaboradas en base a la observación y criterio de los autores, lo cual provocó que se realizara una verificación de los resultados. Este hecho genera muchas limitaciones, no solo por el tiempo invertido en ratificar los datos, sino por el hecho de no contar con resultados avalados por expertos en la materia, que cuentan con una visión mucho más global y exacta de la seguridad informática. De esta forma estamos seguras de que el número de errores en el desarrollo de la investigación disminuiría drásticamente.

6.3. Recomendaciones

Culminada la tarea investigativa asignada, nos permitimos realizar las siguientes recomendaciones:

- Revisar las nuevas versiones de los estándares metodológicos de las ISO en lo referente a seguridad informática.

- Conformar un grupo o comité oficial de seguridad informática con profesionales del área asignándoles sus respectivas funciones y responsabilidades.
- Se recomienda asesorarse con personal experto en seguridad informática para el mejoramiento del plan propuesto.
- Para una efectiva y eficiente gestión del proceso de seguridad informática se recomienda realizar capacitaciones de forma continua.
- Revisar de forma periódica el proceso de "Evaluación y Tratamiento del análisis de riesgos informáticos de la FACCI", el mismo que debe convertirse en una práctica permanente.
- Realizar auditorías anuales internas, como parte esencial dentro de la estructuración del plan, ya que mejoraría la identificación de las debilidades en la Facultad.
- Medir los resultados del plan para realizar un análisis de los avances en la seguridad informática de la Facultad e identificar las fallas que necesitan atención para su pronta solución.

REFERENCIAS BIBLIOGRÁFICAS

REFERENCIAS BIBLIOGRÁFICAS[1]

- ALEGSA ©. (2016). Alegsa.com.ar. Obtenido de ALEGSA: https://t2m.io/Qx2j80xe
- Amaya, C. G. (16 de 08 de 2012). We Live Security . Obtenido de We Live Security : https://t2m.io/oqjDvq09
- Carlos, V. L., Susana, R. P., & Arturo, G. S. (s.f.). Edumed.net Enciclopedia Virtual. Obtenido de MEJORES PRÁCTICAS PARA EL ESTABLECIMIENTO Y ASEGURAMIENTO DE LA CALIDAD DE SOFTWARE: https://t2m.io/yV1KBXcZ
- CISTE. (s.f.). CISTE. Obtenido de Soporte Informático: https://t2m.io/WbX5kacz
- Consejo de Educación Superior. (Enero de 2018). Consejo de Educación Superior. Obtenido de REGLAMENTO DE REGIMEN ACADEMICO CONSEJO: https://t2m.io/5C5BxkFG
- Editorial Definición MX. (22 de 12 de 2014). Definición MX. Obtenido de https://t2m.io/N2bjRrGX
- EmprendePyme. (s.f.). EmprendePyme.net. Obtenido de Politicas de Seguridad : https://t2m.io/1dNFD1Tb
- ISO/IEC 13335-1. (2004). ISO/IEC 13335-1.
- Jimenez, D. (27 de Septiembre de 2014). Pymes y calidad 20. Obtenido de Pymes y calidad 20: https://t2m.io/mW2a6rN7
- Meiras, R. (22 de 06 de 2017). El Insignia. Obtenido de PROCESO DE INDUCCIÓN Y SOCIALIZACIÓN DENTRO DE LAS ORGANIZACIONES: https://t2m.io/K7cQS7bc
- Ministerio del Trabajo. (s.f.). Norma Técnica del Subsistema de Capacitación. Registro Oficial Nro. 865.
- Misión Sucre. (s.f.). PcSucre. Obtenido de Misión Sucre : https://t2m.io/9NG81SRs
- PÉREZ, A. L. (12 de 07 de 2018). EQ2B. Obtenido de EQ2B Consulting: https://t2m.io/wsSXR8Nh
- Porto, J. P. (2008). Definición.es. Obtenido de https://t2m.io/Zdocfguh
- RAE, 23° Edición . (2014). Real Academia Española . Obtenido de DEL : https://t2m.io/w1JNZ5RQ
- Real Academia Española . (2001). Real Academia Española . Obtenido de DEL: https://t2m.io/zyxwjz7H
- Sema Group. (2006). MAP-Magerit Versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Secretaría del Consejo Superior de Administración Electrónica. . Ministerio de Administraciones Públicas. Madrid. España. : Sema Group.
- Significados. (10 de 11 de 2015). Significados. Obtenido de Banner: https://t2m.io/PUVKpW9X
- SO/IEC 13335-1. (2004). Information technology. Técnicas de seguridad, gestión de la información y las comunicaciones tecnología seguridad--parte 1: conceptos y modelos de gestión de seguridad de tecnología información y comunicaciones.
- Solarte, F., Enriquez, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista tecnológica ESPOL, 498.
- Soldano, A. (11 de 2008). Rimd. Obtenido de CONAE: https://t2m.io/9msD3nmp

[1] Las URL de las referencias bibliográficas han sido abreviadas.

- Tocabens, M. B. (12 de 12 de 2010). SciELO. Obtenido de Revista Cubana de Higiene y Epidemiología: https://t2m.io/WY3TFVwP
- ULEAM. (12 de 2018). Universidad Laica Eloy Alfaro de Manabí. Obtenido de ULEAM: https://t2m.io/B9YzNxP0
- Universidad Nacional de Luján. (s.f.). Universidad Nacional de Luján. Obtenido de REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: https://t2m.io/gR6LkMqq
- VladimirMC. (15 de 07 de 2013). Slideshare. Obtenido de Riesgos Informáticos: https://t2m.io/YsyL4oxQ
- Galeon. (2010). audisistemas. Obtenido de audisistemas: https://t2m.io/XM5fe9Q7
- Burke, T. (2005). Constructing Red Hat enterprise Linux 4. Linux J., 2005(134), 4.
- Colinas, J. (2004). Plan De Seguridad para una Pequeña Empresa, 94. Retrieved from https://t2m.io/BW0EFpP1
- Del Cid, A., Méndez, R., & Sandoval, F. (2011). Investigación. Fundamentos y Metodología. (V. Melvin Núñez, A. Calderón Salas, & E. Trejo Hernández, Eds.) (Segunda Ed). México: Prentice Hall: Pearson Educación de México, S.A. de C.V. Retrieved from https://t2m.io/dN2Up6Jh
- Domanda, F., Inserimento, D. I., Di, I., & Del, D. (2012). Modulo 1. Slide Claudio Civitillo. https://t2m.io/vpv4tnVD
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). Metodología de la Investigación. (M. Rocha Martínez, J. Mares Chacón, Z. García García, & M. Á. Toledo Castellanos, Eds.) (Sexta edic). México: McGraw-Hill / Interamericana Editores, S.A. de C.V. Retrieved from https://t2m.io/p9i43UH2
- ISOTools. (2017). 4 opciones de mitigación en el tratamiento de riesgos según ISO 27001 - Software ISO. ISOTools Excellence Perú. (2013). ISO 27001: ¿Cuál es la utilidad de un SGSI?
- Learning Communities. (n.d.). 1. Sensibilización – Comunidades de Aprendizaje.
- Marín, G. B. M. (2006). Directrices del Plan Director de Seguridad: ISO 17799. Tecnimap Sevilla, 9.
- Monje Álvarez, C. A. (2011). Metodología de la investigación cuantitativa y cualitativa. Guía didáctica. In Universidad Surcolombiana (pp. 1–217). https://t2m.io/XThPGkfD
- Moreno Flórez, P. A. (n.d.). El profesorado de educación física y las competencias básicas en TIC en el desarrollo de su actividad profesional caso: profesores de la III etapa de educación básica de los municipios Torbes e Independencia del Estado Táchira-Venezuela.
- Ongallo, C. (2007). Guía para gestionar el Conocimiento, la información y las relaciones humanas en empresas y organizaciones. MANUAL DE COMUNICACIÓN, 32(10), 1–56. https://t2m.io/iXCbOPiq
- Recursos Humanos. (n.d.). Tipos de capacitación de personal | LosRecursosHumanos.com.
- Tecno XXI. (2017). Concientización en seguridad informática y medidas preventivas - Tecno XXI.
- Tecnológico de Monterrei. (2017). ¿Cuáles son las mejores técnicas de capacitación? - Blog Posgrados Tec.
- Thorp, C. (2004). Implantando ISO17799.

ANEXOS

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Facultad de Ciencias Informáticas

Manta, 24 de septiembre de 2018

Licenciada
Dolores Muñoz Verduga, Mg., Decana
Facultad de Ciencias Informáticas
Ciudad. -

Señora Decana:

Yo, **Rodríguez Zambrano Joselyne Elizabeth** con número de identificación **131214296-9**, y mi compañera **Sánchez Montes Diana Fernanda**, con número de identificación **131698344-2**, estudiantes de la carrera de Ingeniería en Sistemas, solicitamos se nos facilite una copia de las siguientes tareas de investigación: **"Evaluación y Tratamiento del análisis de riesgo de la Facultad de Ciencias Informáticas"** e **"Instauración de un Plan de Contingencia y Continuidad de los servicios informáticos que brinda la Facultad de Ciencias Informáticas"** del proyecto, **Sistema de Gestión de la Seguridad de la Información bajo Normas ISO/IEC 27001,** que fueron sustentados en días anteriores.

Este pedido lo realizamos ya que dichos trabajos sirven como insumo para elaborar nuestra tarea de investigación.

Agradeceremos a usted, por la atención favorable que dé a la presente.

Atentamente,

Rodríguez Zambrano Joselyne Elizabeth
Cédula/Pasaporte:131214296-9
Correo electrónico:
elizzarz.1296@gmail.com
Celular No.:0995923599

Sánchez Montes Diana Fernanda
Cédula/Pasaporte:131698344-2
Correo electrónico:
diana.sanchezfm@hotmail.com
Celular No.:0990761958

UNIVERSIDAD LAICA ELOY ALFARO DE MANABI
FACULTAD DE CIENCIAS INFORMATICAS
Recepcion de Documentos

FECHA:	24 / 9 / 2018
HORA:	10:50
RECIBIDO POR	
N° GUIA	1208

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Facultad de Ciencias Informáticas

Manta, 26 de octubre 2018

Ingeniera
Denisse Vera Navarrete, Mg., Docente
Facultad de Ciencias Informáticas
Ciudad. -

Ingeniera:

Yo, **Rodríguez Zambrano Joselyne Elizabeth** con número de identificación **131214296-9**, y mi compañera **Sánchez Montes Diana Fernanda**, con número de identificación **131698344-2**, estudiantes de la carrera de Ingeniería en Sistemas, solicitamos a usted, en calidad de líder del proyecto de investigación: "**Sistema de Gestión de Seguridad de la Información bajo Normas ISO/IEC 27001**", toda la información generada por la tarea de investigación "**Elaboración de Declaración de Aplicabilidad**" realizada por la señorita Kerly Delgado, adicional esperamos que la información respectiva se entregue mediante oficio como medio de comunicación formal.

Este pedido lo realizamos ya que dicho trabajo sirve como insumo para elaborar nuestra tarea de investigación.

Agradeceremos a usted, por la atención favorable que dé a la presente.

Atentamente,

Rodríguez Zambrano Joselyne Elizabeth
Cédula/Pasaporte:131214296-9
Correo electrónico:
elizzarz.1296@gmail.com
Celular No.:0995923599

Sánchez Montes Diana Fernanda
Cédula/Pasaporte:131698344-2
Correo electrónico:
diana.sanchezfm@hotmail.com
Celular No.:0990761958

26/OCT/2018

Facultad de Ciencias Informáticas

Manta, 6 de noviembre de 2018

Ingeniera
Denisse Vera Navarrete, Mg., Docente
Facultad de Ciencias Informáticas
Ciudad. -

Ingeniera:

De conformidad a la solicitud de información con oficio del 26 de octubre del presente año, del proyecto "**Sistema de Gestión de Seguridad de la Información bajo Normas ISO/IEC 27001**", en la fecha 5 de noviembre se realizó el levantamiento y análisis de información de la Declaración de Aplicabilidad, entregada en días anteriores para su respectiva validación.

De acuerdo a lo presentado se ha encontrado los siguientes hallazgos: se exponen controles de la ISO/IEC 27001 que no están siendo considerados como aplicables dentro del proceso y en base a la parte conceptual, al entorno, al contexto y al alcance del informe de Declaración de Aplicabilidad, deberían formar parte de éste.

A manera más detallada se muestra en anexo lo antes mencionado. Sugerimos sistematizar la información verificando su coherencia y correlación, en caso de ser necesario una reunión para discutir lo antes expuesto.

Agradeceremos a usted, por la atención favorable que dé a la presente.

Atentamente,

Rodríguez Zambrano Joselyne Elizabeth
Cédula/Pasaporte:131214296-9
Correo electrónico:
elizzarz.1296@gmail.com
Celular No.:0995923599

Anexo

Sánchez Montes Diana Fernanda
Cédula/Pasaporte:131698344-2
Correo electrónico:
diana.sanchezfm@hotmail.com
Celular No.:0990761958

6/11/2018

Políticas ISO 27001:2005		Aplica	Razón	Justificación de aplicabilidad
Sección	**Descripción del control**			
A.7.1.3	Uso aceptable de los activos	NO	Los departamentos encargados de 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 en la Universidad son la UCCI y mantenimiento técnico. No la FACCI.	Nuestro tema trata sobre la capacitación en el uso adecuado de los recursos informáticos, además que, internamente se debe manejar controles dirigidos hacia los estudiantes, docentes y personal administrativo enfocados en el uso éstos dentro de la Facultad.
A.8.1.1	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.	Aunque dicho proceso sea llevado a cabo por el departamento de Recursos Humanos, la decana, como máxima autoridad, debe especificar textualmente las funciones y responsabilidades que tendrá a su cargo el nuevo empleado.
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 las autoridades de la Facultad, específicamente el departamento de Recursos Humanos de la Universidad. No la FACCI.	
A.8.2.1	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.	Como en la Facultad se está implementando un SGSI, en el cual se tenga documentos donde se especifique cada rol y responsabilidad para uno de los actores dentro de este proceso.
A.8.3.1	Responsabilidades de terminación	NO	Se debe definir y asignar claramente las responsabilidades para realizar la terminación del empleo	Aunque dicho proceso sea llevado a cabo por el departamento de Recursos Humanos, la decana, como máxima autoridad, debe especificar textualmente lo que implica la terminación del contrato de un empleado.
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.	Una vez que los recursos informáticos son entregados a la Unidad Académica pasan ser responsabilidad de ésta, la cual debe velar por su correcta utilización y protección.
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.	Aunque sea responsabilidad de la Universidad, internamente se debe asegurar que los servicios públicos brindados a la comunidad FACCI estén acorde a las necesidades de ésta.

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.	Aunque sea responsabilidad de la Universidad, internamente se debe implementar medidas en las que se manejen la seguridad del cableado no únicamente por los activos informáticos que hagan uso de éste si no por las personas que lo manejan
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.	En caso de que exista la necesidad de que los equipos permanezcan fuera de las instalaciones o de su lugar habitual, se debe mantener la seguridad de éstos estableciendo responsabilidades al personal encargado.
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.	
A.10.1.1	Procedimientos de operación documentados	NO	Todos los procedimientos operativos de cualquier SI son realizados, supervisados y controlados por la UCCI y no por la Facultad.	Aunque este proceso sea manejado por la UCCI, llevar una adecuada documentación de los procedimientos de operación realizados asegura el correcto desempeño de las responsabilidades asignadas.
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.	Aunque este proceso sea manejado por la UCCI, llevar una adecuada documentación de la gestión de cambio realizado asegura el correcto desempeño de las responsabilidades asignadas.
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.	Para un mejor desarrollo de actividades de cualquier proceso, internamente en la Unidad Académica se debe establecer la división de asignaciones para cada uno de los involucrados.
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.	Aunque este proceso sea manejado por la UCCI, llevar una adecuada documentación de la gestión de cambio realizado asegura el correcto desempeño de las responsabilidades asignadas.
A.10.2.1	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.	Aunque este proceso sea manejado por UCCI, no está de más establecer controles que brinden seguridad en los servicios que se presta internamente en la Unidad Académica.
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	Aunque este proceso sea manejado por UCCI, no está de más establecer controles que brinden seguridad en los servicios que se presta

			las autoridades de la Universidad no por la Facultad.	internamente en la Unidad Académica.
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.	
A.10.3.1	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	La Facultad es quien realiza el pedido de equipamiento de acuerdo a las necesidades de ésta, podrían plantearse recomendaciones oportunas para el POA
A.10.4.2	Controles contra códigos móviles	NO	Quien controla de manera adecuada los códigos maliciosos, asegurándose que los códigos móviles autorizados operen de acuerdo a las políticas de seguridad definidas es la UCCI no la Facultad	Consciente de la seguridad informática dentro de la Unidad Académica, internamente se debe plantear políticas contra los códigos maliciosos, concretamente los códigos móviles dándole dirección hacia laptops.
A.10.6.1	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.	Aunque este proceso sea realizado por la UCCI, no está de más que se implementen controles que correspondan a aspectos que brinden seguridad al acceder a los servicios de la red interna.
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.	
A.10.7.1	Gestión de los medios removibles	NO	Quien debe tener control y planes de sensibilización con respecto a los medios removibles es la UCCI no la Facultad	Consideramos que este proceso debe ser manejado internamente como Unidad Académica responsable con la seguridad en la gestión de los medios removibles estableciendo controles y medidas para asegurar su adecuado utilización
A.10.7.2	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	Consideramos que este proceso debe ser manejado internamente como Unidad Académica responsable con la seguridad en la eliminación de los medios estableciendo controles y medidas.
A.10.7.3	Procedimientos de manejo de la información	NO	Quien debe establecer los procedimientos para el manejo y almacenamiento de la información protegiéndola de divulgación no autorizada o mal uso de la misma es la UCCI no la Facultad	Internamente se maneja información reservada o sensible, en la que se debe establecer los controles respectivos en cuanto al acceso a ella, preservando su seguridad
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	
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	Aunque este proceso sea realizado por la UCCI, no está de más que se implementen controles que correspondan al

			o corrupción durante el transporte de la información, no la Facultad	acceso no autorizado y en la gestión de contraseñas para los sistemas institucionales.
A.10.8.4	Mensajería electrónica	NO	Las áreas o departamentos hacen uso de la mensajería y aplicaciones de transacciones (online) como una herramienta de trabajo, por ello quien protege esto es la UCCI no la Facultad.	Se deben establecer controles sobre el uso del correo institucional para el correcto funcionamiento de la herramienta como medio de comunicación y forjar una cultura de correo seguro.
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	Se podría plantear medidas y controles, como planes a futuro (en caso de que se llegase a implementar en la Facultad), que aseguren la protección de la información asociada con la interconexión de los sistemas de información comercial, comercio electrónico y transacciones en línea.
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.	
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.	
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.	
A.10.10.2	Monitoreo del uso del sistema	NO		
A.10.10.3	Protección de la información del registro	NO	Los sistemas son monitoreados de manera regular por la UCCI no por la Facultad	Aunque este proceso sea manejado por la UCCI, llevar una adecuada protección de la información del registro de los sistemas asegura el correcto desempeño de las responsabilidades asignadas.
A.10.10.4	Registros del administrador y del operador	NO	Los logs y registros son configurados y protegidos para validaciones, monitoreo y manejo de incidentes de seguridad por la UCCI no por la Facultad	Aunque este proceso sea manejado por la UCCI, llevar una adecuada protección de los registros del administrador y del operador asegura el correcto desempeño de las responsabilidades asignadas.
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).	La sincronización de relojes trata los problemas surgidos por la necesidad de comunicar distintos computadores que trabajan en una tarea conjunta por lo que es requerido que sean considerados en la aplicación de las Normas.
A.11.2.1	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.	Aunque el proceso de asignación de permisos los otorga la UCCI, no está de más sociabilizar los controles establecidos por ésta, las

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.	políticas en la gestión de contraseñas para los diferentes sistemas institucionales, sus derechos de accesos y privilegios en cada uno de dichos sistemas para evitar inconvenientes a futuro.
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.	
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.	
A.11.3.1	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.	Establecer políticas para la gestión de contraseñas que fortalezcan las ya establecidas por la UCCI que contribuyan a mejorar la seguridad sería lo adecuado.
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.	Se debería requerir al personal administrativo y docentes aseguren dar la protección apropiada al equipo que tienen a su cargo, en este caso al equipo desatendido.
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.	Es una medida que debería ser considerada por acciones a futuro que pudiesen ser llevadas a cabo por terceras personas y que equivaldría una vulnerabilidad para la Unidad Académica.
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.	Internamente se debería considerar la posibilidad la identificación automática del equipo (laptops) de estudiantes, principalmente, como un medio para autenticar las conexiones desde equipos y ubicaciones.
A.11.4.4	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	Internamente se debería considerar la implementación de controles sobre el acceso físico y lógico a los puertos de diagnóstico y configuración.
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.	Se debería, internamente, plantear una separación, de los servicios de información, usuarios y sistemas de información, de la red interna de la Facultad para aprovechar de forma óptima los recursos.
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	Se debería, internamente, restringir la capacidad de conexión de los usuarios en las redes compartidas.

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 infrinjan la política de control de acceso de las aplicaciones comerciales en caso de que existan, no la Facultad.	Implementar este tipo de controles aseguran que las conexiones de cómputo y los flujos de información no infrinjan las políticas de control de acceso en las aplicaciones comerciales que pudiesen implementarse a futuro.
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.	Aunque este proceso sea manejado por la UCCI, llevar un adecuado control del acceso de los servicios operativos asegura el correcto desempeño de las responsabilidades asignadas.
A.11.5.2	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.	Aunque el proceso de asignación de permisos los otorga la UCCI, no está de más sociabilizar los controles establecidos por ésta, las políticas en la gestión de contraseñas para los diferentes sistemas institucionales, sus derechos de accesos y privilegios en cada uno de dichos sistemas para evitar inconvenientes a futuro.
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	
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	
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	
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.	
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 establecidas y puestas en prácticas por la UCCI no por la Facultad.	Se debe implementar controles de restricción de acceso a la información manejada por los sistemas institucionales de acuerdo a lo estipulado por la UCCI.
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	Los sistemas sensibles manejados internamente en la Unidad Académica deben tener un ambiente de cómputo dedicado.
A.12.2.1	Validación de los datos de entrada	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.	Esta norma podría ser aplicada en la gestión de la calidad de software de los Proyectos Integradores.
A.12.2.2	Control de procesamiento interno	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.	Se debe incorporar chequeos de validación para detectar cualquier corrupción de la información, identificar los requerimientos para asegurar la autenticidad y protección de la integridad del mensaje, así como los datos de salida generados en los softwares generados por los Proyectos Integradores.
A.12.2.3	Integridad del mensaje	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.	
A.12.2.4	Validación de los datos de salida	NO	La Facultad no trabaja desarrollando aplicaciones para terceros.	

A.12.3.1	Política sobre el uso de controles criptográficos	NO	La Facultad no crea controles criptográficos para proteger la información en el SGSI. Usa otros métodos	Se debe implementar una política interna sobre el uso de controles criptográficos sobre la información confidencial generados dentro de la Unidad Académica. (Decana - Honorable Consejo de Facultad)
A.12.3.2	Gestión de llaves	NO	La Facultad no crea controles criptográficos para proteger la información en el SGSI. Usa otros métodos	
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.	Contar con procedimientos para controlar la instalación de software en los sistemas operacionales, la protección de los datos de prueba y la restricción del acceso al código fuente, aseguran un adecuado desempeño de las actividades dentro de la Unidad Académica.
A.12.4.2	Protección de los datos de prueba del sistema	NO		
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.	
A.12.5.2	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.	Aunque este proceso sea manejado por la UCCI, llevar un adecuado registro de la revisión técnicas de las aplicaciones y cambios en los paquetes de software, asegura el correcto desempeño de las responsabilidades asignadas.
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.	
A.13.2.1	Responsabilidades y procedimientos	NO	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. Dicho proceso es hecho por la UCCI no por la Facultad.	Establecer responsabilidades y procedimientos aseguran una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
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	Debe existir mecanismos para permitir la cuantificación y monitoreo de tipos, volúmenes y costos de los incidentes en la seguridad de la información.
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.	Se debe recolectar, mantener y presentar evidencia, como Unidad Académica, para cumplir as reglas de evidencia establecidas en la jurisdicción.
A.14.1.1	Inclusión de la seguridad de la inf. 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.	Desarrollar y mantener un proceso para la continuidad de la institución para tratar los requerimientos de seguridad de la información, así como, la identificación eventos que causan interrupciones en los procesos manejados internamente, deben ser considerados.
A.14.1.2	Continuidad comercial y evaluación de riesgos	NO		

A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen la seguridad de la información.	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.	Se debe impulsar el desarrollo del Plan de Continuidad realizado en una de las tareas de investigación del proyecto.
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.	Se debe mantener un mismo marco referencial de planes de continuidad que pudiesen desarrollarse a futuro, para asegurar que sean consistentes y se traten los requerimientos de la seguridad de la información. De igual forma revisar y actualizar regularmente dichos planes para cerciorar su efectividad.
A.14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	NO		
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.	Aunque este proceso sea manejado por la UCCI, llevar una adecuada protección de los registros de la institución, asegura el correcto desempeño de las responsabilidades asignadas.
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.	Utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes aseguran la seguridad de la información interna.
A.15.2.2	Verificación del cumplimiento técnico	NO	Los planes de auditoria, que validen y se ajusten los objetivos del SGSI, son realizados por la UCCI o en su defecto personal asignado por la UCCI.	Se debe aplicar las plantillas de Mantenimiento Correctivo y Preventivo, así como las de Auditorías Internas.
A.15.3.1	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.	Se deben planear cuidadosamente los requerimientos y actividades de las auditorías futuras internas, que involucran chequeos de los sistemas operacionales y minimizar el riesgo de interrupciones en los procesos. Así como asegurar la protección de las herramientas utilizadas en la auditoría para evitar cualquier mal uso.
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.	

Facultad de Ciencias Informáticas

Manta, 8 de noviembre de 2018

Ingeniera
Denisse Vera Navarrete, Mg., Docente
Facultad de Ciencias Informáticas
Ciudad. -

Ingeniera:

De acuerdo a la reunión suscitada el día 7 de noviembre del presente año precedida por su persona, conjuntamente con nosotras, para llevar a cabo el respectivo análisis y validación de información del informe de Declaración de Aplicabilidad entregado en días anteriores.

Se ha podido establecer la sistematización y corrección de los puntos planteados en el oficio con fecha de 6 de noviembre en base a la fundamentación conceptual, al entorno y al contexto de ambas partes, esclareciendo inquietudes presentadas. De igual manera se adjunta el archivo donde se especifican las correcciones realizadas a dicho documento.

Extendemos nuestro agradecimiento por su colaboración y pronta respuesta a la solicitud. A su vez, esperamos la entrega de la versión actualizada del documento en cuestión, con las correspondientes correcciones.

Atentamente,

Rodríguez Zambrano Joselyne Elizabeth
Cédula/Pasaporte:131214296-9
Correo electrónico:
elizzarz.1296@gmail.com
Celular No.:0995923599

Sánchez Montes Diana Fernanda
Cédula/Pasaporte:131698344-2
Correo electrónico:
diana.sanchezfm@hotmail.com
Celular No.:0990761958

8/11/2018

Facultad de Ciencias Informáticas

Manta, 5 de diciembre 2018

Ingeniero
Briones Veliz Ítalo Becquer
Unidad Central de Coordinación Informática (UCCI) ULEAM
Ciudad. -

Distinguido Ingeniero:

Reciba un cordial saludo, a nombre de la Facultad de Ciencias Informáticas (FACCI), a la vez que le deseamos éxitos en sus nobles funciones.

Yo, **Rodríguez Zambrano Joselyne Elizabeth** con número de identificación **131214296-9**, y mi compañera **Sánchez Montes Diana Fernanda**, con número de identificación **131698344-2**, estudiantes de la carrera de Ingeniería en Sistemas, formamos parte de uno de los proyectos de investigación que se está implementado en la FACCI, denominado, "**Sistema de Gestión de Seguridad de la Información bajo Normas ISO/IEC 27001**", el cual está integrado por diversas tareas investigativas y entre ellas la nuestra, **"Plan de Sensibilización, Comunicación y Capacitación para minimizar los riesgos informáticos en la Facultad de Ciencias Informáticas",** para continuar con el desarrollo de ésta solicitamos a usted, se nos pudiese facilitar información sobre:

Políticas internas de uso, control y seguridad de:

- Tratamiento de Datos e información. (Backups, documentos físicos y digitales)
- Protocolos de seguridad para el uso del servicio de correo electrónico.
- Procedimientos del manejo de la seguridad para el software utilizado. (sistemas operativos, ofimática, antivirus)
- Procedimientos de seguridad física para el hardware. (Computadores, servidores, impresora, dispositivos de respaldo)
- Controles para las comunicaciones (equipamiento, configuraciones de red)
- Seguridad del edificio e infraestructura física.

Agradeceremos a usted, por la atención favorable que dé a la presente.
Atentamente,

Recibido
05-12-2018.
8:156.

Rodríguez Zambrano Joselyne Elizabeth
Cédula/Pasaporte:131214296-9
Correo electrónico:
elizzarz.1296@gmail.com
Celular No.:0995923599

Sánchez Montes Diana Fernanda
Cédula/Pasaporte:131698344-2
Correo electrónico:
diana.sanchezfm@hotmail.com
Celular No.:0990761958

Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

Facultad de Ciencias Informáticas

Manta, 09 de enero de 2019

Ingeniera
Denisse Vera Navarrete, Mg., Docente
Facultad de Ciencias Informáticas
Ciudad. -

Ingeniera:

Yo, **Rodríguez Zambrano Joselyne Elizabeth** con número de identificación **131214296-9**, y mi compañera **Sánchez Montes Diana Fernanda**, con número de identificación **131698344-2**, estudiantes de la carrera de Ingeniería en Sistemas, solicitamos se nos facilite los materiales de oficina necesarios para desarrollar nuestra tarea de investigación: **"Plan de Sensibilización, Comunicación y Capacitación para minimizar los riesgos informáticos en la Facultad de Ciencias Informáticas"** del proyecto, **Sistema de Gestión de la Seguridad de la Información bajo Normas ISO/IEC 27001,** solicitamos a siguiente lista de materiales necesarios:

- Resmas de hojas
- Esferos
- Marcadores
- Folder

Este pedido lo realizamos ya que dichos materiales de trabajo sirven para el desarrollo de evidencia para elaborar nuestra tarea de investigación.

Agradeceremos a usted, por la atención favorable que dé a la presente.

Atentamente,

09/01/2019

Rodríguez Zambrano Joselyne Elizabeth
Cédula/Pasaporte:131214296-9
Correo electrónico:
elizzarz.1296@gmail.com
Celular No.:0995923599

Sánchez Montes Diana Fernanda
Cédula/Pasaporte:131698344-2
Correo electrónico:
diana.sanchezfm@hotmail.com
Celular No.:0990761958

PROPUESTA DE LINEAMIENTOS PARA EL BUEN USO DE LOS ACTIVOS INFORMÁTICOS DE LA FACULTAD DE CIENCIAS INFORMÁTICAS

Control de Versiones

Revisión	Fecha	Motivo del cambio
1.0	29/01/2019	Borrador

Realizado y revisado	Aprobado
Joselyne Elizabeth Rodríguez Zambrano Diana Fernanda Sánchez Montes Fecha 29/01/2019	 Fecha --/--/--

Tabla de contenido

1. Objeto 3
2. Justificación 3
3. Alcance 4
4. Actores y responsabilidades 4
5. Propuesta de Lineamientos de uso 5
5.1. Confidencialidad 7
5.2. Uso de computadores de escritorio, portátiles y otros dispositivos 9
5.3. Uso y protección de la información 12
5.3.1. Protección de la información en forma electrónica 12
5.3.2. Protección de la información a través del uso de equipos multifuncionales (impresora, escáner) 14
5.3.3. Escritorio Limpio y Bloqueo de sesión 14
5.4. Control de acceso a los activos informáticos 16
5.4.1. Gestión de cuentas de usuarios y contraseñas 16
5.4.2. Verificación y mantenimiento de los privilegios de acceso 18
5.4.3. Prevención de acceso a usuarios no autorizados 19
5.5. Control de acceso a la red 20
5.6. Uso del sistema operativo y software instalado en los computadores de escritorio, portátiles y demás recursos informáticos 21
5.7. Uso de periféricos en los computadores de escritorio, portátiles y demás recursos informáticos (impresora, monitor, mouse, teclado, medios de almacenamiento removibles) 22
5.7.1. Protección frente a software malicioso 23
5.8. Uso del correo electrónico 24
5.9. Acceso a internet 28
5.10. Propiedad intelectual de la información 29
5.11. Respuesta a incidentes relacionados con Seguridad Informática y uso inadecuado de los activos informáticos 30
5.12. Copias de Respaldo 31
5.13. Distribución, almacenamiento y eliminación de información electrónica 32
6. Monitorización 34
7. Consecuencias del incumplimiento de los lineamientos 34
7.1. Colaboración del personal 34
7.2. Acciones correctivas 35
7.3. Medidas sancionadoras 35

1. Objeto

El objetivo de la presente normativas es establecer una guía para el buen uso de los activos informáticos dirigido al personal administrativo, docentes de la Facultad y a los estudiantes que hacen uso de los servicios e instalaciones.

2. Justificación

La Facultad de Ciencias Informáticas pone a disposición de los usuarios un conjunto de recursos basados en tecnologías de la información y las comunicaciones (TIC's) con el objeto de servir y apoyar a las actividades (académicas, institucionales y administrativas) desarrolladas en los procesos internos, de acuerdo con las competencias que las leyes y Estatutos le atribuyen.

Siendo los activos informáticos, recursos necesarios y vitales para la unidad académica, es indispensable tomar las acciones adecuadas para asegurar que la información y recursos se encuentren debidamente protegidos de toda posibilidad de riesgos y amenazas. Por lo que, los usuarios deben actuar de una manera responsable, ética, cuando utilicen dichos activos.

Cabe mencionar que un uso adecuado de los recursos implica respetar los derechos de otros usuarios, la integridad de las instalaciones, los acuerdos y contratos con terceros cuando sea aplicable.

El propósito fundamental de la propuesta descrita a continuación, es asegurar una gestión eficiente y efectiva en el uso de los activos informáticos, así como salvaguardar la información, resultado de la producción y gestiones de la Facultad (academia y administración).

3. Alcance

- **Agentes**

  La presente propuesta de lineamientos o reglas se aplica a la comunidad FACCI: personal administrativo, personal docente, estudiantes, personal temporal de la Facultad, usuarios externos que requieran hacer uso de los recursos e instalaciones.

- **Recursos**

  Tecnologías de información y de telecomunicaciones, los recursos informáticos de hardware, software y de telecomunicaciones, que apoyan directamente la gestión de los usuarios para el cumplimiento de sus labores, entre los que se puede mencionar:

  - Computadoras de escritorio, portátiles, impresoras;
  - Aplicaciones de ofimática, sistemas operativos, antivirus, software de programación;
  - Uso de internet, del correo electrónico, sistemas institucionales (Aula Virtual, Sistema de Gestión Académica)
  - Así mismo, comprende la infraestructura de redes: servidores, equipos de telecomunicación que soportan los servicios informáticos.

  Los lineamientos establecidos en este documento están orientados a proporcionar las directrices de utilización de los activos informáticos descritos anteriormente, y para apoyar de manera adecuada las buenas prácticas de seguridad de la información que busca, la protección de la información que en ellos reside y se transmite a través de éstos.

4. Actores y responsabilidades

Las responsabilidades definidas por las actividades descritas en la presente, son las siguientes:

- **Usuarios (Estudiantes, Personal docente y administrativo, personas externas):** cumplir con las directrices establecidas en la propuesta de lineamientos para el buen uso de los activos informáticos, actuando de manera responsable y ética.

- **Personal Administrativo/área técnica – Miembros del proyecto SGSI**:

    - Verificar el cumplimiento de las reglas por parte de los usuarios, coordinando actuaciones de auditoría, en un período idóneo para ello, conjuntamente con los miembros del proyecto SGSI.

    - Mantener actualizado los lineamientos conforme a nuevos requerimientos, necesidades y ámbitos.

5. Propuesta de Lineamientos de uso

A continuación, se definen una serie de lineamientos que regulan el buen uso, disponibilidad y nivel de servicio de los activos informáticos. Cabe mencionar que, aquellos usuarios que de forma reiterada o deliberada o por negligencia las ignoren o infrinjan, se pueden ver sujetas a sanciones según sean determinadas por la Facultad.

Consideraciones generales:

a) Los activos informáticos disponibles en la FACCI deben ser utilizados con fines estrictamente profesionales y académicos, no se autoriza su uso para intereses personales.

b) Se recomienda no almacenar información de alta relevancia en las computadoras de los laboratorios para los estudiantes, al ser utilizados por otras personas no pueden efectuar reclamos a la Facultad, ni por la información albergada, ni responsabilidades por el acceso de dicha información.

c) De igual forma, para los administrativos y docentes se recomienda no almacenar información personal en los puestos de trabajo (PC) por los motivos antes expuestos.

d) La información contenida en el computador de escritorio, portátil o demás recursos informáticos que se asigna al personal para su trabajo, los servicios asociados, tanto

internos como externo, los mensajes de correo electrónico, los documentos, entre otros, no podrán reproducirse o utilizarse para fines ajenos a las funciones de la Facultad y en concordancia al cargo desempeñado.

e) Toda información, dato, obra literaria, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de uno de los computadores de escritorio, portátiles y demás recursos informáticos propiedad de la FACCI, será propiedad de la unidad académica, aunque la información, dato, obra literaria, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho, haya surgido mediante el esfuerzo personal del usuario.

f) Hasta donde las leyes lo permitan, la FACCI se reserva el derecho de revelar información o material obtenido por cualquier medio, relacionado con el control efectuado sobre el uso de los activos informáticos, así como cualquier información o material creado, almacenado o transmitido usando esos activos.

g) Cabe destacar que los usuarios, indistintamente, deben respetar la integridad de los recursos sobre los que se soportan, los derechos de otros usuarios, las leyes y regulaciones vigentes.

h) Los lineamientos estipulados son aplicables, de manera general, a todos los empleados, estudiantes y personas externas (contratistas, estudiantes practicantes y personas que solicitan las instalaciones de la Facultad)

i) Respecto a la privacidad y derechos de terceros: no está permitido acceder al correo electrónico, copiar direcciones, datos, programas u otros ficheros sin permiso del titular de la Facultad.

j) Se recomienda a los usuarios que traten los servicios y/o recursos tecnológicos e información disponible en la Facultad como un activo valioso.

k) Para cualquier duda técnica del estado o funcionamiento de los activos informáticos: hardware, software, comunicaciones, etc. Se debe contactar con el personal administrativo/área técnica.

l) Algunos lineamientos o reglas tienen variaciones en base a la pertenencia de los usuarios, debido a los roles desempeñados dentro de los procesos de la Unidad Académica.

5.1. Confidencialidad

Todos los usuarios de los activos informáticos de la Facultad, empleados, estudiantes y personas suministradas por terceras partes, deben firmar un acuerdo de confidencialidad y de cumplimiento de los lineamientos o reglas para el buen uso.

Dichos acuerdos deben ser anexados, por parte del personal de secretaría, a los contratos de trabajo para los empleados y contratistas e historial académico para los estudiantes. Para los estudiantes practicantes y personas que solicitan instalaciones, de igual forma, se anexará dicho acuerdo a la documentación respectiva relacionada su desempeño dentro de la unidad académica.

Lineamientos dirigidos a todos los usuarios

- El usuario reconoce que la reproducción, copia, modificación, comunicación pública, distribución o cualquier ore medio de difusión de datos o información de la Universidad sin autorización de la misma, constituye un delito contra la propiedad intelectual.

- El usuario se compromete expresamente a no realizar ninguna de las siguientes acciones:

  - Intentar distorsionar la información.

- Intentar descifrar las contraseñas o cualquier otro elemento de seguridad que intervenga en los procesos de la Universidad o intentar descifrar mensajes o ficheros de datos sin autorización.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas, documentos electrónicos o recursos tecnológicos de la Universidad, o de terceros.

Lineamientos dirigidos a los empleados

El empleado se compromete a:

- Guardar reserva sobre la información a la que tiene acceso por razón de su actividad profesional,
- No divulgar dicha información, así como no publicarla de ningún modo, bien directamente o a través de terceras personas, para ponerla a disposición de terceros sin el previo consentimiento de la Universidad.

Ningún empleado podrá acceder a una información clasificada, si no reúne las siguientes condiciones:

- Tener necesidad de su conocimiento en virtud de su cargo o de sus actividades.
- Haber sido informado, previamente al acceso, sobre la responsabilidad que adquiere al acceder a la información sensible de acuerdo con la legislación vigente.
- Tener la autorización de la autoridad competente de la FACCI, quien deberá verificar si el empleado dispone de la habilitación requerida.

De igual manera, el empleado se compromete, tras la terminación de la relación laboral, guardar la máxima reserva y a no divulgar ni utilizar directamente ni a través de terceras personas, los datos y demás información a la que tenga acceso durante su relación con la Universidad.

5.2. Uso de computadores de escritorio, portátiles y otros dispositivos

Los recursos informáticos son provistos por la Facultad, con el objetivo de desarrollar actividades relacionadas con la academia y administración asignado, por lo que, dichos recursos deben ser utilizados de forma adecuada y eficiente.

Lineamientos dirigidos a todos los usuarios

- Los computadores de escritorio, portátiles y demás recursos informáticos de la FACCI, deben ser operados y utilizados solamente por el personal que se encuentre autorizado para ello y/o responsable de los mismos, así como, no deben ser utilizados para actividades personales o ajenas a la Facultad.

- Todos los computadores de escritorio, portátiles y demás recursos informáticos (oficinas, laboratorios, aulas y medios visuales) deben ser apagados al finalizar la jornada laboral.

- Los computadores de escritorio, portátiles y demás recursos informáticos asignados a los usuarios o que hagan uso de ellos, deben someterse a las instrucciones, lineamientos, políticas, medidas y disposiciones que imparta el área técnica y miembros del proyecto del SGSI, y que sean autorizados por los niveles correspondientes.

- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los computadores de escritorio, portátiles y demás recursos informáticos propiedad de la FACCI, sólo puede ser realizado por el personal del área técnica autorizado. Por ningún motivo los usuarios podrán abrir o desarmar los equipos de cómputo.

- En caso de pérdida, robo o extravío de computadores de escritorio, portátiles y/o demás recursos informáticos, se deberá informar directamente al área técnica.

- Los equipos para soporte en presentaciones y actividades que requieran movilidad, deberán permanecer en las áreas, para que puedan ser utilizados por los distintos usuarios. La responsabilidad del buen uso del recurso recae en los usuarios que hagan uso de dichos recursos.
- Se deberá ser comunicado al personal del área técnica, cualquier deficiencia o mal funcionamiento que se observe en los recursos informáticos.
- Los usuarios deberán cuidar y respetar los recursos informáticos, comprometiéndose a realizar las siguientes actividades:
    - No usar los equipos como portapapeles o repisas.
    - No dañar, destruir, ni inutilizar los recursos informáticos de la Facultad.
    - No mover los recursos informáticos dentro o fuera de la Facultad sin la debida autorización de la autoridad competente o de acuerdo a su rol.
    - Apagado normal de los equipos informáticos.
    - No ingerir alimentos y bebidas cerca de los equipos informáticos.

Lineamientos dirigidos a los empleados

- Todos y cada uno de los computadores de escritorio, portátiles y demás recursos informáticos asignados a una persona, son responsabilidad de la misma por el buen uso de éstos. En caso de que el recurso informático vaya a ser utilizado por una persona diferente a la que se le asignó, debe ser comunicado al jefe del área técnica mediante un oficio especificando los motivos y este último debe asegurar el cumplimiento del buen uso de dicho recurso.
- La protección física de los computadores de escritorio, portátiles y demás recursos informáticos, corresponde a las personas asignadas, y es su deber notificar al personal administrativo/área técnica sobre cualquier eventualidad (falla o problema de

hardware o software) que ocurra sobre dichos recursos. La notificación se debe realizar a través de un oficio detallado.

- Cuando un usuario termine su vinculación laboral con la Facultad, por alguna circunstancia indiferente deje de utilizar el recurso asignado deberá entregar dicho recurso formalmente al área técnica.

Lineamientos dirigidos al área técnica

- El ingreso o salida de computadores de escritorio, portátiles y demás recursos informáticos de las instalaciones de la Facultad, deben seguir el procedimiento establecido por el área técnica.

- Se debe mantener un inventario actualizado del hardware y software que sea propiedad de la Facultad.

- La entrega y recepción de computadores de escritorio, portátiles y demás recursos informáticos, debe ser efectuada mediante una revisión previa por parte del personal administrativo/área técnica, la cual es la responsable de su administración, por lo tanto, la asignación de estos recursos informáticos debe quedar formalmente documentada.

- Está prohibido realizar movimientos y asignaciones de los recursos informáticos a cualquier usuario que no sea del área técnica, pues ésta área es la única autorizada para ejecutar tales gestiones.

- Se debe procurar que los recursos informáticos se encuentren continuamente actualizados con el fin de incrementar la calidad y efectividad en las actividades realizadas, al igual que garantizar la protección ante amenazas.

5.3. Uso y protección de la información

La Facultad de Ciencias Informáticas debe facilitar los mecanismos para que la información que se maneja a través de los recursos informáticos sea veraz, íntegra, oportuna y fluya de manera adecuada dentro de la unidad académica y hacia los estudiantes, empleados y personas externa, garantizando la protección de la misma de divulgación o modificación no autorizada.

Se debe recordar que la información de la Facultad deberá mantenerse disponible a las personas autorizadas para ello, en el momento en que se necesite, así mismo, se debe preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad y Disponibilidad de la información de la Unidad Académica.

5.3.1. Protección de la información en forma electrónica

Lineamientos dirigidos a todos los usuarios

- Los usuarios son responsables por el buen uso de la información de la Facultad, sea que la obtengan de documentos, medios magnéticos o electrónicos.

- No se permite difundir interna ni externamente información confidencial de la Facultad, ni transferir electrónicamente programas de software de ésta a terceras partes sin autorización ni licenciamiento apropiado. Estas infracciones pueden dar lugar a sanciones de tipo administrativo y hasta penal en caso de violaciones a las leyes de derechos de autor y protección de la propiedad intelectual.

Lineamientos dirigidos a los empleados

- Los empleados deben garantizar la oportunidad, veracidad, exactitud, confiabilidad y disponibilidad de la información electrónica que generan.

- Los empleados deben, al momento de abandonar su puesto de trabajo, bloquear el acceso al computador de escritorio o portátil.

- Los empleados son responsables de aplicar los controles de la información según el nivel de la clasificación.

- El protector de pantalla de los computadores de escritorio y portátiles debe ser activado después de un periodo de inactividad. La reactivación del protector de pantalla debe exigir las credenciales de acceso.

- Los empleados deben utilizar los mecanismos y procedimientos disponibles para proteger sus ficheros. Si los datos u otros componentes fuesen dañados por un problema de acceso indebido, se debe notificar al jefe del área técnica.

Lineamientos dirigidos al área técnica

- Es responsabilidad del personal administrativo/área técnica garantizar la confidencialidad e integridad de la información crítica para la unidad académica almacenada en los servidores, algunos computadores de escritorio y portátiles, de propiedad de la FACCI.

- El área deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean adecuadas en cuanto a costo/beneficio.

- Los niveles de protección y clasificación establecidos para la información de la Facultad deberán ser mantenidos en todo momento (acceso, respaldo, transporte, recuperación, otros), por lo que, se deben mantener los controles y medidas establecidas para ello.

5.3.2. Protección de la información a través del uso de equipos multifuncionales (impresora, escáner)

Los usuarios deben tener en cuenta las siguientes consideraciones cuando impriman documentos a través de los equipos multifuncionales e impresoras que se encuentren dentro de las instalaciones de la FACCI, o que son propiedad de ésta:

Lineamientos dirigidos a todos los usuarios

- Se debe imprimir sólo lo que es estrictamente necesario.
- Verificar el equipo multifuncional o impresora y las áreas adyacentes para asegurarse de que no queden copias adicionales. Si encuentra copias adicionales se procede a destruir.
- Asegurarse que se tiene el documento original antes de retirarse del equipo multifuncional o de la impresora, en caso de realizar copias de documentos.
- Si el equipo multifuncional o la impresora, no está funcionado, borrar el archivo de la cola de impresión.
- Recoger inmediatamente todas las impresiones y/o copias que contengan información confidencial para evitar su revelación.

5.3.3. Escritorio Limpio y Bloqueo de sesión

Para la Facultad es crucial proteger la información sensible, evitando que sea conocida.

Lineamientos dirigidos a todos los usuarios

- Los usuarios de la información son responsables, mientras tengan la información bajo su control, de mantener los niveles de protección y clasificación establecidos

para la misma, en todo momento, haciendo uso adecuado de los recursos a su disposición.

- Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento.

Lineamientos dirigidos a los empleados

- Es responsabilidad del empleado identificar riesgos asociados a disponer de la información en su puesto de trabajo e iniciar las acciones para mitigarlas.

- Los sistemas institucionales y elementos de procesamiento deberán ser adecuadamente protegidos, teniendo presente que se debe al menos guardar documentos sensibles o elementos de almacenamiento de información (CDs, dispositivos USB, discos externos, portátiles, etc) en los cajones bajo llave, en todo momento que no se esté utilizando.

- Es responsabilidad de cada empleado la protección de la información a su cargo, por lo que debe mantener presente no publicar o dejar a la vista, documentos o datos sensibles, por ejemplo: nombres de usuario y contraseñas, contratos, propiedad intelectual, cualquier cosa que no desea publicar.

- Los empleados deberán tomarse el tiempo necesario antes de abandonar la oficina o cubículo para recoger y asegurar el material sensible, y, cerrar bajo llave gabinetes, cajones, puertas de las oficinas.

- Cada empleado de la Facultad para mantener su estación de trabajo bajo control, deberá bloquear la sesión al alejarse de su computador o portátil, aunque sea por poco tiempo, minimizando el tiempo que la estación quedaría sin control.

5.4. Control de acceso a los activos informáticos

Se debe prevenir, restringir y monitorear el acceso no autorizado a los activos informáticos de la FACCI, utilizando los mecanismos de contención, detección, protección, recuperación y/o reacción que sean necesarios.

5.4.1. Gestión de cuentas de usuarios y contraseñas

Lineamientos dirigidos a todos los usuarios

- La asignación de nombres de usuarios y contraseñas (credenciales de acceso) para los sistemas institucionales (aula virtual, Sistema de Gestión académica) de la universidad lo realiza la UCCI, una vez que es estudiante sea haya matriculado en la institución, el cual no debe ser compartido con ninguna otra persona. La solicitud de creación de cuentas de usuario lo realiza personal de secretaría de la Facultades.

- El préstamo de credenciales para el ingreso a los sistemas institucionales está prohibido.

- La cuenta de usuario podrá tener privilegios y restricciones de seguridad por la UCCI, en virtud de las actividades desempeñadas.

- Queda estrictamente prohibido el uso de contraseñas de acceso distinto al propio, con el fin de evadir normas de control de recursos.

- Cada usuario autorizado es responsable por las acciones realizadas dentro de los diferentes sistemas institucionales, por cualquier otra persona a quien haya divulgado sus credenciales. Se debe recordar que, la contraseña de acceso a dichos sistemas es individual e intransferible.

- Los usuarios deben cambiar las contraseñas de manera regular, para evitar que ésta sea conocida y utilizada por otras personas.

- Se recomienda prestar la debida atención a los boletines de recomendaciones para la gestión de contraseñas impulsada por UCCI presentada en el Aula Virtual.

Lineamientos dirigidos a los estudiantes

- Para realizar el restablecimiento de contraseña del aula virtual deben acercarse al área de secretaría para llevar a cabo ese proceso.

Lineamientos dirigidos al área técnica

- La pantalla de inicio de sesión en los computadores de escritorio y portátiles propiedad de la FACCI, debe advertir a los usuarios que están entrando a un recurso informático propiedad de la unidad y que el acceso es permitido solamente a personas debidamente autorizadas.

- Impulsar la comunicación de la **Política de Contraseña**[2] establecida por la UCCI conjuntamente con los miembros del proyecto de SGSI, para el debido cumplimiento de dichas políticas y, a su vez, enriquecer el documento de lineamientos.

Lineamientos dirigidos a los empleados

- Se recomienda a los empleados cumplir con las normas y procedimientos establecidos en la política de **Política de Contraseña** definida por la UCCI, alojada en la página principal de la Universidad.

- Para el restablecimiento de contraseña de los sistemas institucionales deben realizar la solicitud respectiva a UCCI para llevar a cabo ese proceso a través de los medios formales exponiendo su caso respectivamente.

[2] URL de acceso a la Política de Contraseña: http://www.uleam.edu.ec/wp-content/uploads/2016/10/Politica-de-Contraseñas.pdf

5.4.2. Verificación y mantenimiento de los privilegios de acceso

Lineamientos dirigidos a los empleados

- La creación y/o modificación de perfiles de usuario y/o accesos a los sistemas de información debe ser solicitada, aprobada y documentada por el área técnica de la Facultad.

Lineamientos dirigidos al área técnica

- El acceso de un usuario debe ser restringido solamente a la información específica para las funciones del cargo que desempeña.
- Sólo debe existir una cuenta de usuario con privilegios de administrador local en los computadores de escritorio y portátiles propiedad de la FACC, la cual debe ser diferente a la(s) cuentas(s) de usuario(s) asignada(s) al(los) usuarios(s) del recurso informático.
- La contraseña de la cuenta con privilegios de administrador local en los computadores de escritorio no debe ser divulgada a ningún usuario y solo debe ser conocida por el personal autorizado del área técnica. Dicha contraseña debe ser cambiada regularmente.
- Para los computadores de escritorio se deben establecer bloqueos o terminación de sesiones automáticas, en caso de que queden desentendidos, con el propósito de no permitir que personas sin autorización tengan acceso al recurso.

Lineamientos dirigidos al área de Secretaría

- El área de secretaría debe solicitar la eliminación de las cuentas de usuarios y de privilegios de acceso a los sistemas institucionales, a la UCCI, de manera oportuna, cuando los empleados se retiran de la unidad académica, o cambian de cargo.

- El área de secretaría debe revisar las solicitudes de accesos de las instalaciones de la Facultad (laboratorios y aulas) con el fin de verificar que las solicitudes sean pertinentes de acuerdo a la descripción de las actividades de la(s) persona(s) que solicita el acceso.

Lineamientos dirigidos al área administrativa

- El área administrativa debe solicitar, a la eliminación de privilegios de acceso a los servicios informáticos de manera oportuna, cuando se finaliza un contrato con un tercero o cuando el tercero realice cambios a nivel del personal que utiliza para cumplir con el objeto del contrato.

5.4.3. Prevención de acceso a usuarios no autorizados

Lineamientos dirigidos a todos los usuarios

- Las contraseñas no deben ser divulgados a ningún otro usuario, en caso de haya sido divulgada por un algún motivo, ésta debe ser cambiada durante el próximo ingreso.

- No utilizar ningún tipo de programa para interferir con la sesión del usuario.

- Se prohíbe realizar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la unidad académica a través de medio físico o electrónico alguno. Se podrán realizar intentos de intrusión, sólo con la autorización de la UCCI y supervisión directa del jefe del área técnica, con el fin de encontrar fallas de seguridad.

Lineamientos dirigidos a los empleados

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel o almacenarlas en medio digitales no encriptados.

Lineamientos dirigidos al área técnica

- La revocación de los privilegios de acceso a una persona, cualquier sea el motivo, es realizado por la UCCI, así como la deshabilitación de la cuenta de un usuario si ha existido un máximo de intentos consecutivos de conexión sin éxito.

5.5. Control de acceso a la red

Lineamientos dirigidos a todos los usuarios

- El usuario se compromete a aceptar las condiciones estipuladas en los lineamientos y políticas de la Facultad en las que se señala el uso del servicio de red para fines académicos, de investigación y administrativos, lo que excluye cualquier uso comercial de la red, así como prácticas desleales o cualquier otra actividad que voluntariamente afecte a otros usuarios de la red, tan en las prestaciones de ésta como en la privacidad de su información.

- No obstaculizar el acceso a otros usuarios a los servicios de red mediante el consumo masivo de los recursos dado por el uso de programas ajenos a los intereses de la Facultad, así como realizar acciones u omisiones que dañen, interrumpan o generen errores en los servicios o cualquier otra actividad que alter su normal funcionamiento.

Lineamientos dirigidos al área técnica

- Se deben adoptar medidas para garantizar la disponibilidad de los servicios de red de la FACCI y la conexión de los computadores de escritorio, portátiles y demás recursos informáticos a ella.

- Deben establecerse controles especiales para salvaguardar la confidencialidad de los datos que viajan por la red de la FACCI.

- La conectividad que no sea requerida debe ser inhabilitada.
- El área técnica efectuará un registro y monitoreo automatizado cuando sea técnicamente factible del tráfico de comunicaciones generado en los equipos institucionales con fines estadísticos, para la detección de fallas y garantía de calidad de servicio, siempre que se cuente con la autorización de la autoridad competente de la FACCI y UCCI.

5.6. Uso del sistema operativo y software instalado en los computadores de escritorio, portátiles y demás recursos informáticos

La Facultad, debe velar por el software instalado en los computadores de escritorio, portátiles y demás recursos informáticos suministrados a los empleados y estudiantes, cumpla con los requerimientos legales y de licenciamiento necesarios.

Lineamientos dirigidos a todos los usuarios

- La modificación de los parámetros de configuración establecidos en los computadores de escritorio, portátiles y demás recursos informáticos, sólo serán realizados por el personal administrativo/área técnica.
- La FACCI debe tener establecido un listado de programas y aplicaciones permitidos en los computadores de escritorio, portátiles y demás recursos informáticos, que apoyan el desarrollo de las actividades laborales y académicas. Por lo anterior, los usuarios no deben instalar programas o aplicaciones adicionales sin previa autorización y asistencia del personal autorizado del área técnica.

Lineamientos dirigidos al área técnica

- El área técnica debe mantener actualizado el sistema operativo y el software instalado en los computadores de escritorio, portátiles y demás recursos informáticos propiedad de la FACCI, de acuerdo a lo estipulado en el Plan de Actualizaciones de

software (planteado como propuesta para su realización), con el fin de prevenir problemas de seguridad informática relacionados con los mismos y que pongan en riesgo la disponibilidad y continuidad de los recursos informáticos.

5.7. Uso de periféricos en los computadores de escritorio, portátiles y demás recursos informáticos (impresora, monitor, mouse, teclado, medios de almacenamiento removibles)

El uso de periféricos y medios de almacenamiento en los computadores de escritorio, portátiles y demás recursos informáticos de la FACCI, debe ser restringido acorde con las actividades internas desempeñadas por los empleados y estudiantes.

Lineamientos dirigidos a todos los usuarios

- Ningún usuario de la Facultad podrá instalar o conectar al computador de escritorio, portátil y demás recursos informáticos, asignados o en calidad de préstamo, elementos adicionales a los proporcionados con estos. Se incluyen, pero no se limitan a: cámaras web o digitales, grabadoras de sonido, impresoras, escáner, reproductores multimedia, puntos de acceso inalámbricos, dispositivos móviles, etc. En caso de requerir el uso de cualquier elemento adicional, se deberá solicitar autorización al área técnica.

Lineamientos dirigidos al área técnica

- Se deben adoptar medidas para garantizar que no se conecten a los computadores de escritorio, portátiles y demás recursos informáticos de la FACCI, medios de almacenamiento no autorizados, que incluyen, pero no se limitan a: memorias USB, CD’s, discos externos, que no sean propiedad de la Facultad.

5.7.1. Protección frente a software malicioso

La FACCI debe proteger sus recursos informáticos contra el acceso, modificación o daño permanente ocasionados por la contaminación y el contagio de software malicioso. Por tal razón, debe tomar las medidas necesarias para evitar que este tipo de contagio, en cualquiera de sus formas, se presente en los computadores de escritorio, portátiles, servidores y en general, cualquier dispositivo que se conecte a la red de la Facultad.

Lineamientos dirigidos a todos los usuarios

- Todos los computadores de escritorio y portátiles que se conecten a la red de la Facultad, deben tener instalado un software antivirus que mitigue el riesgo de contaminación y contagio de software malicioso, actualizado y debidamente configurado.

- El usuario no debe cambiar la configuración del software antivirus definida por el personal del área técnica y únicamente podrá realizar tareas de escaneo de archivos y directorios.

- Los usuarios únicamente deben descargar archivos adjuntos que provengan de fuentes conocidas para evitar contaminación por virus informáticos y/o instalación de software malicioso en los computadores de escritorio o portátiles.

- Todos los medios de almacenamiento externos, como CD, dispositivos USB, memorias flash, deberán ser escaneados por el software antivirus antes de intercambiar información con el computador de escritorio o portátil.

- Los usuarios de la FACCI no deben intentar erradicar los virus detectados en los computadores de escritorio o portátiles. Para esto se debe informar al personal administrativo/área técnica en donde se les prestará soporte especializado.

- Los usuarios no deben intencionalmente escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto-replicarse, deteriorar o que obstaculice el desempeño de cualquier servicio y/o recurso informático.

Lineamientos dirigidos al área técnica

- Es responsabilidad del área técnica mantener licenciado y actualizado el software antivirus en todos los computadores de escritorio, portátiles y demás recursos informáticos en donde aplique, que se conecten a la red de la Facultad.

5.8. Uso del correo electrónico

El correo electrónico es una herramienta que facilita la comunicación entre los usuarios. Por lo que se debe garantizar que sea utilizado de manera adecuada y racional para las funciones propias de las actividades académicas y laborales, respetando los principios de confidencialidad, privacidad y autenticidad.

La Facultad no realizará monitoreo o inspecciones de los contenidos del buzón de correo electrónico sin el consentimiento del usuario, salvo en los casos en que éste viole los lineamientos y políticas establecidos para el uso del servicio.

Lineamientos dirigidos a todos los usuarios

- La cuenta de correo asignada es de carácter individual e intransferible, por lo tanto, ninguna persona bajo ninguna circunstancia, debe usar una cuenta de correo que no se le haya asignado explícitamente.
- Todos los usuarios tienen derecho a la privacidad de correo electrónico, el mismo que deberá ser usado de acuerdo a su cuenta de usuario.

- Cuando se realicen envíos de documentos adjuntos, estos deben haberse elaborado usando aplicaciones estándar autorizadas de ofimática (Word, Excel, Power Point, Libre office). Sólo se deben enviar archivos elaborados con otros programas en casos específicos y cuando esté seguro que la persona a la que se lo envía tiene dichos programas. Procurar siempre enviar los documentos del menor tamaño posible, no superando los 8 MB. Se recomienda hacer uso de los programas que comprimen el tamaño de los archivos.

- El correo electrónico debe usarse únicamente para aspectos relacionados con la academia y laborales relacionados a la unidad académica.

- El servicio de correo no tendrá restricciones de horario para los usuarios y estará disponible 24 horas diarias, 7 días a la semana.

- Se prohíbe el envío de mensajes de correo electrónico ofensivos, subversivos, amenazantes, fraudulentos e intimidantes, o pensamientos políticos, religiosos que puedan afectar la integridad o dignidad de otras personas.

- Todo mensaje de correo electrónico debe enviarse con el campo “Asunto” diligenciado con información que permita identificar fácilmente el tema que trata el mensaje.

- Se prohíben las cadenas de mensajes electrónicos de cualquier tipo y la propaganda de tipo comercial, político religioso, al igual que cualquier contenido ofensivo o inapropiado.

- Se prohíbe enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a un tercero, identificarse como una persona ficticia o no identificarse.

- Antes de enviar un mensaje de correo electrónico, verifique que los destinatarios son los correctos y que el contenido del mensaje es de interés para ellos.

- Cuando necesite responder un mensaje de correo electrónico que contiene archivos anexos, elimine éstos antes de hacerlo.
- Si el mensaje requiere de acción por parte de alguien en específico, diríjalo a esa persona, en el campo “CC” (con copia a).
- Solamente el personal autorizado del área de Secretaría podrá enviar comunicados, mensajes que sean de interés para todos los usuarios.
- Evite suscribirse a cualquier lista de correos que genere mensajes cuyo contenido no se relaciones con las actividades, académicas y laborales, dentro de la Facultad.
- El usuario tiene la obligación de realizar la clasificación y depuración de la información recibida a través del correo electrónico periódicamente.
- El correo electrónico, no deberá almacenar archivos, software y demás fuentes que violen la ley de derechos de autor.
- El usuario se compromete expresamente a no realizar ninguna de las siguientes acciones:
    - Enviar mensajes internos de correo electrónico conteniendo datos o información ajena a los intereses de la Facultad.
    - Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico de otros usuarios.
    - Envío de correos anónimos.
    - No mandar, ni contestar cadenas de correo.

Lineamientos dirigidos a los empleados

- Se recomienda a los empleados cumplir con las normas y procedimientos establecidos en la política de **Política de uso de Correo Electrónico**[3] definida por la UCCI, alojada en la página principal de la Universidad.

Lineamientos dirigidos al área técnica

- Impulsar la comunicación de la **Política de uso de Correo Electrónico e**stablecida por la UCCI conjuntamente con los miembros del proyecto de SGSI, para el debido cumplimiento de dichas políticas y, a su vez, enriquecer el documento de lineamientos.

- El área técnica deberá implementar mecanismos de verificación del cumplimiento de este lineamiento, conjuntamente con los miembros del proyecto de SGSI.

Lineamientos dirigidos al área administrativa

- Cuando un empleado se retira de la Facultad, se debe comunicar a UCCI y solicitar la eliminación de la cuenta., debidamente documentado.

- Cuando haya ingresado un nuevo empleado a la unidad académica, se debe comunicar la estructura formal para el envío de correos electrónicos.

Lineamientos dirigidos al área de secretaría

- Cuando sea necesario enviar mensajes de correo electrónico a un grupo amplio de destinatarios, adiciones el siguiente texto al final del mensaje: “FAVOR NO RESPONDER A ESTE CORREO”, si el mensaje debe ser respondido. En caso en que el mensaje deba ser respondido adicione: “EN CASO DE RESPONDER ESTE

[3] URL de acceso a la Política de uso de Correo Electrónico: http://www.uleam.edu.ec/wp-content/uploads/2016/10/Politica-de-Correo-Electronico-V02.pdf

MENSAJE, POR FAVOR HÁGALO SOLO AL REMITENTE Y NO A TODOS LOS DESTINATARIOS".

5.9. Acceso a internet

Los usuarios de la FACCI que hagan uso del servicio de internet debe ser utilizado como una herramienta de consulta, para propósitos de las actividades, académicas y laborales, de la unidad académica, acatando y respetando los lineamientos y políticas vigentes alrededor de su uso.

Lineamientos dirigidos a todos los usuarios

- Cumplir con las disposiciones estipuladas en el **Política de uso del Servicio de Internet** [4] definida por la UCCI, alojada en la página principal de la Universidad.
- La descarga de archivos y ejecución de programas desde internet debe estar restringida a las actividades necesarias para el desempeño de éstas, sean académicas o laborales.
- Se prohíbe el intercambio y descarga de archivo haciendo uso de protocolos P2P (Peer to peer), Torrents, etc.

Lineamientos dirigidos al área técnica

- Impulsar la comunicación de la **Política de uso del Servicio de Internet** establecida por la UCCI conjuntamente con los miembros del proyecto de SGSI, para el debido cumplimiento de dichas políticas y, a su vez, enriquecer el documento de lineamientos.

[4] URL de acceso a la Política de uso del Servicio de Internet: http://www.uleam.edu.ec/wp-content/uploads/2016/10/Politica-de-Uso-de-Internet.pdf

- De acuerdo con las necesidades específicas y relacionadas con las actividades de la Facultad, se debe solicitar, a UCCI, el acceso a los servicios y sitios restringidos fundamentando con la debida justificación.

5.10. Propiedad intelectual de la información

Los usuarios de la FACCI tienen la obligación de respetar la legislación de la propiedad intelectual y los derechos de autor concernientes a los productos software instalados en los computadores de escritorio, portátiles y demás recursos informáticos.

Lineamientos dirigidos a todos los usuarios

- La FACCI mantiene una gestión de la marca de software, Microsoft, para obtención de software (paquetes estudiantiles) con licenciamiento, que son utilizados internamente, por lo que, está prohibido copiar cualquiera de los aplicativos instalados.

- La información proveniente de internet y otros recursos electrónicos no puede ser usada sin la autorización de los propietarios (derechos de autor).

Lineamientos dirigidos al área técnica

- El personal del área técnica es responsable de verificar que sólo se instalen productos con licencia y software autorizado en los computadores de escritorio, portátiles y demás recursos informáticos propiedad de la FACCI. De igual manera, es su deber implementar controles para evitar exceder el número máximo permitido de usuarios en los modelos de licenciamientos existentes.

5.11. Respuesta a incidentes relacionados con Seguridad Informática y uso inadecuado de los activos informáticos

Es un deber de la unidad académica promover entre la comunidad FACCI de los servicios informáticos el reporte de los incidentes relacionados con la seguridad informática y el uso inadecuado de los activos informáticos. De igual forma, se debe investigar y solucionar de manera transparente y efectiva dichos incidentes, tomando las medidas o acciones necesarias para prevenir su ocurrencia.

Lineamientos dirigidos a todos los usuarios

- Es responsabilidad de todos los usuarios de la FACCI, reportar cualquier tipo de incidente relacionado con la seguridad informática y/o uso inadecuado tan pronto como sea posible. El reporte se debe ser comunicado al personal del área técnica.

Lineamientos dirigidos al área técnica

- El uso de los computadores de escritorio, portátiles y demás recursos informáticos debe ser monitoreado regularmente.
- Los incidentes de seguridad informática y uso inadecuado que estén relacionados con requerimientos legales regulaciones deberán ser reportados a la autoridad competente de la Facultad.
- Todos los incidentes de seguridad informática y uso inadecuado deben ser evaluados acorde a su circunstancia particular e impacto. Cuando sea necesario se deben enviar lo informes correspondientes a el área administrativa para aplicar sanciones disciplinarias acorde con la falta cometida.
- Los incidentes relacionados con seguridad informática y uso inadecuado, deben ser apropiadamente investigados por el personal calificado.

- Deben ser creadas bases de conocimientos de incidentes con sus respectivas soluciones para ayudar a reducir el tiempo de respuesta.

Lineamientos dirigidos al área administrativa

- Se deben identificar las causas y planear como prevenir su ocurrencia, por lo que, la evidencia debe ser apropiadamente recolectada.

5.12. Copias de Respaldo

Todos los empleados, administrativos y docentes, de la FACCI, son responsables por la confiabilidad y oportunidad de la información que emiten o procesan y, es su deber identificar las fuentes de información que requieran protección electrónica e informar de éste requerimiento al área técnica de tal forma que ésta pueda aplicar los mecanismos que sean necesarios.

Lineamientos dirigidos a los empleados

- Es responsabilidad de los empleados de la FACCI, identificar qué información crítica del computador de escritorio, portátil o demás recursos informáticos asignados, debe ser respaldada y comunicarlo al área técnica, para llevar a cabo la actividad.

- Los empleados son responsables de eliminar toda la información no actualizada, inutilizada o no relacionada con la unidad académica del computador de escritorio, portátil o demás recursos informáticos.

- Los empleados respaldarán y protegerán, con medidas que eviten accesos de personas no autorizadas, aquellos activos digitales de información que estén almacenados en elementos informáticos de uso personal, que se les haya asignados.

Lineamientos dirigidos al área técnica

- El área técnica debe indicar a los empleados las condiciones de almacenamiento de todos los medios en ambientes seguros y protegidos.
- El área técnica deberá asegurar el respaldo de la información considerada sensitiva alta de la Facultad, al igual de la contenida en los servidores de ésta, mediante la puesta en marcha de los procedimientos de rutina para el respaldo.
- El área técnica deberá asegurar la custodia de los medios magnéticos, a través de la utilización de la infraestructura propia adecuada para tal propósito.
- El área técnica deberá asegurar la disponibilidad de la información respaldada utilizando mecanismos de comprobación del estado de las copias, tales como secuencias de recuperación de pruebas.
- El área técnica deberá llevar un registro, a modo de bitácora, de los respaldos realizados para realizar el seguimiento respectivo.

5.13. Distribución, almacenamiento y eliminación de información electrónica

La FACCI debe establecer las directrices y proveer los mecanismos para la adecuada distribución, almacenamiento y eliminación de la información que se encuentre en medios de almacenamiento digitales, cumpliendo con las políticas y lineamientos vigentes para la Unidad Académica.

Lineamientos dirigidos a todos los usuarios

- Se deben definir procedimientos para el transporte de medios de almacenamiento que contemplen la utilización de medios de transporte o servicios de mensajería confiables y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensitiva alta contra divulgación o modificaciones.

Lineamientos dirigidos a los empleados

- Cumplir con las disposiciones estipuladas en el **Política de Seguridad de la Información**[5] definida por la UCCI, alojada en la página principal de la Universidad.

- Bajo ninguna circunstancia se debe almacenar información sensible de la FACCI en las unidades locales de los computadores de escritorio, portátiles, o en dispositivos de almacenamiento móviles. La información que se considere sensible para el desarrollo de las actividades de la Facultad, debe ser almacenada en los repositorios centrales de almacenamiento de información digital institucional proporcionado por UCCI para lo cual debe solicitar la creación de un espacio en éste.

- En los repositorios de almacenamiento no se podrá almacenar información diferente con las actividades de la Facultad. Se prohíbe almacenar fotos, música, vídeos, programas maliciosos, contenido para adultos, juegos o todo tipo de archivo que no tenga relación con las actividades propias de cada función o cargo.

Lineamientos dirigidos al área técnica

- El área técnica debe definir procedimientos para la destrucción y/o eliminación segura de los medios de almacenamiento de la información acorde con las políticas vigentes para la Facultad.

- Impulsar la comunicación de la **Política de Seguridad de la Información e**stablecida por la UCCI conjuntamente con los miembros del proyecto de SGSI, para el debido cumplimiento de dichas políticas y, a su vez, enriquecer el documento de lineamientos.

[5] URL de acceso a la Política de Seguridad de la Información: http://www.uleam.edu.ec/wp-content/uploads/2016/10/Politica-de-seguridad-de-la-informacion.pdf

- La eliminación de la información digital debe ser efectuada por el personal del área técnica, estableciendo los correspondientes acuerdos de confidencialidad y se deben dejar registro de la información eliminada.
- La información de la FACCI contenida en medios de almacenamiento electrónico debe ser destruida de tal forma que quede ilegible.

6. Monitorización

Los usuarios conectados a la infraestructura tecnológica de la FACCI son conscientes de que los activos informáticos son propiedad exclusiva de la Facultad. Por ello, estas personas entienden que no tienen el derecho de propiedad y la respectiva confidencialidad en su uso.

Así mismo, la FACCI se guarda el derecho de monitorizar toda actividad relacionada con sus activos informáticos, para asegurar el correcto funcionamiento y uso, por parte de los usuarios, respetando en todo momento la ley vigente.

En caso de que, en los activos informáticos, se detecte un uso inadecuado, por parte de algún usuario, se comunicará de ésta, formándole, en caso de que sea necesario, para el uso adecuado de dichos activos. Si se detectase un uso malintencionado, la autoridad competente de la FACCI puede ejercer las acciones disciplinarias que estime oportunas.

Para finalizar, la FACCI podrá realizar controles, mediante el personal encargado y especializado, para observar el cumplimiento de los lineamientos, procedimientos, políticas o normas establecidas.

7. Consecuencias del incumplimiento de los lineamientos

7.1. Colaboración del personal

Los usuarios, cuando se les solicite, deben colaborar con el personal administrativo/área técnica y miembros designados del proyecto de SGSI, en la medida de sus posibilidades, en

cualquier investigación que se haga sobre incidentes de seguridad o uso inadecuado de los recursos aportando la información que se les requiera.

7.2. Acciones correctivas

En caso de que el personal administrativo/área técnica detectara la existencia de un uso inadecuado de los activos informáticos y éste proceda de las actividades o equipo de un usuario determinado, pueden tomar cualquiera de las siguientes medidas para proteger a otros activos y personas:

- Notificar la incidencia a miembros designados del proyecto de SGSI.
- Suspender o restringir el acceso o uso de los servicios de los activos mientras dure la investigación, requerida ante la autoridad competente.
- Inspeccionar, con la debida justificación (funcional y legal), ficheros o dispositivos de almacenamiento del usuario implicado.
- Informar a la autoridad competente de la Facultad con el respectivo informe de los resultados de la investigación y evidencias del agravio cometido.

7.3. Medidas sancionadoras

En caso que fuese necesario y una vez informado por el personal administrativo/área técnica y/o miembros designados del proyecto SGSI, corresponderá a la autoridad competente de la FACCI, la adopción de sanciones oportunas hacia los usuarios infractores de estos lineamientos, según lo establecido en la ley vigente.