
# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

## Facultad de Ingeniería en Electricidad y Computación

"ESTUDIO DEL ESTÁNDAR ISO 27001:2013 Y SU DISEÑO PARA LA APLICACIÓN A LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN DE LA ESPOL"

## INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

**Licenciado en Redes y Sistemas Operativos**

Jorge Enmanuel Rendón Zambrano

Pamela Solange Zambrano Martínez

Guayaquil - Ecuador

2015

# AGRADECIMIENTO

Nuestro más sincero agradecimiento al Ing. Rayner Durango, por ser el promotor de este tema, por su paciencia y motivación que han sido fundamentales para nuestra formación.

Él ha mostrado ser amigo, consejero académico, siempre con palabras oportunas.

A los profesores de la materia integradora por inculcarnos un sentido de seriedad y organización en el desarrollo de un proyecto.

# DEDICATORIA

El presente proyecto está dedicado a Dios, el promotor de mi vida y creador de mis padres y de las personas que amo.

A mis padres por su amor y sacrificio en todos estos años de estudio, gracias a ustedes he llegado hasta aquí.

# TRIBUNAL DE EVALUACIÓN

| | |
|---|---|
| _____ | _____ |
| **José Roberto Patiño Sánchez** | **María Angélica Santacruz Maridueña** |
| PROFESOR EVALUADOR | PROFESOR EVALUADOR |

# DECLARACIÓN EXPRESA

La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

_____

Jorge Emmanuel Rendón Zambrano

_____

Pamela Solange Zambrano Martínez

# RESUMEN

Nuestro estudio realza el manejo de la información, donde los usuarios y miembros del área de redes interactúan dentro de una organización educativa.

Analizamos el uso de la norma ISO 27001:2013 porque las instituciones deben mantener un alto grado de integridad, confidencialidad y seguridad de la información, y de los sistemas que manejan el desarrollo de sus tareas los cuales pueden provocar la interrupción del flujo normal de actividades o en el peor de los casos se pierda información vital. Además empleamos la metodología MAGERIT para desarrollar el análisis de riesgos del hardware y del software.

Nuestro trabajo se basa en la información de la FIEC, bajo la supervisión de la Ing. Margarita Filian, Jefa de Laboratorio de Computación y la Ing. Katherine Campos, Asistente Técnico de Redes, mostrando los resultados en un reporte, junto con las recomendaciones del caso, donde se indique que los cambios se deberían hacer para que la facultad llegue a tener los requisitos para prepararse a la obtención de la certificación.

# ÍNDICE GENERAL

# CAPÍTULO 1

## 1. ANTECEDENTES Y JUSTIFICACIÓN

Conforme mejora la tecnología, las distancias tienden a reducirse, y se vuelve más sencillo comunicarse, esto a su vez indica que mucha información pasa por estos canales, corriendo graves riesgos de que esta pueda filtrarse o perderse en su recorrido, esto requiere que exista algún sistema para evitar o reducir en gran medida las posibilidades de que algo malo suceda, para esto necesitaremos un Sistema de Gestión de Seguridad de la Información (SGSI), el cual nos ofrece un conjunto de normas y reglas que garantizan que la información sea tratada de la forma más profesional y segura posible.

Y es de aquí donde se desprende la ISO 27001, la cual se desarrolla en base a la norma Británica 7799-2, donde se crea la ISO 27001:2005 que fue la primera revisión, y actualmente con ciertos cambios se dio la ISO 27001:2013. El SGSI se debe certificar con los requerimientos de estudio, como un seguimiento de las personas, los procesos y sistemas TI que se lleven a cabo en la empresa. [1]

La ISO 27001:2013 la aplicaremos a una institución educativa, ya que dichos centros deben mantener un alto grado de integridad, confidencialidad y seguridad de la información; y los sistemas que manejan para el desarrollo de sus actividades. Por lo tanto es bastante recomendable que las instituciones educativas cuenten con una planificación de riesgos, preventiva y correctiva a la filtración o sustracción de datos confidenciales, amenazas de virus/malware/spyware, acceso no autorizado debido a la vulnerabilidad que tengan los sistemas. Los cuales puedan provocar la interrupción del flujo normal de actividades o en el peor de los casos se pierda información vital.

Es necesario el incentivo de implantar esta ISO en centros de estudios que tenga su misión, visión bien planteadas, para alcanzar las categorías exigidas por los departamentos gubernamentales y ser una referencia frente a las demás, y por supuesto el desarrollo en conjunto como organización brindando excelencia a nivel educativo, automatización en las gestiones de procesos, tecnología informática y trabajo de quienes conformen la institución educativa.

## 1.1. Descripción

Nuestro estudio abarcara únicamente las áreas de la red informática y como la información es tratada mientras esta pasa por este medio, a su vez, de cómo los usuarios y miembros del área de redes interactúan con esta.

Al final de nuestro estudio los resultados serán presentados en un reporte, junto con las recomendaciones del caso, donde se indique que cambios se deberían hacer para que la facultad logre llegar a tener los requisitos mínimos para poder obtener la certificación.

## 1.2. Justificación

Las instituciones educativas de Ecuador se encuentran en un proceso de control y reforma a la calidad integral, para garantizar una mejora macro en el nivel académico de los futuros profesionales; correspondientes a los diferentes campos de la ciencia. Con este cambio se desea garantizar la integridad y la calidad de educación en el país. Con las facilidades y alcances que nos presenta hoy en día la tecnología mundial, los centros educativos de mayor prestigio y categoría, adquieren mayor infraestructura tecnológica, herramientas, sistemas para automatizar sus procesos internos y enlaces con diferentes organismos privados y públicos, al contar con mayor infraestructura, avances globales y tecnologías, es posible el manejo de gran cantidad de información privada tanto del personal de la institución, empleados, profesores como de estudiantes.

En la actualidad, las empresas grandes, medianas y/o pequeñas; las instituciones educativas, financieras, sociales, solo consideren como activo maquinarias, equipos de oficina, dispositivos portables, servidores, entre otros. Uno de los activos más importantes es la información, que se maneja dentro del negocio, como tarifas de precios, propiedad intelectual, cartera de clientes, nombres de proyecto, etc.

Para cuidar de nuestra información no solo es necesario gastar millones de dólares en dispositivos de seguridad, o en configuraciones de políticas

avanzadas. La norma principal es la ISO 27001:2013, que nos brinda un conjunto de reglas a seguir, y un Sistema de Gestión de Seguridad de la Información que nos garantiza la protección, confidencialidad, integridad y disponibilidad de la información.

El Objetivo de este estudio es conocer sobre la última actualización de la ISO 27001:2013 y elaborar un diseño con esta norma en la Facultad de Ingeniería en Electricidad y Computación (FIEC), perteneciente a la Escuela Superior Politécnica del Litoral (ESPOL). La FIEC como facultad enfocada al estudio de carreras del área de computación, telecomunicaciones y afines, mantiene altos estándares por lo que actualmente cuenta con certificaciones Nacionales e Internacionales como la acreditación ABET y la Certificación de Calidad ISO 9001:2000.

Nuestro estudio se basa en realizar un análisis de la red de la FIEC y comprobar si cumple con los requisitos necesarios para obtener la certificación ISO 27001:2013, y en el caso de que no se cumpla, ofrecer posibles soluciones.

## 1.3. Objetivos

### Objetivo General

Analizar la norma ISO/IEC 27001:2013 y realizar un estudio de una parte de la red de la FIEC para comprobar su cumplimiento con los requisitos de este estándar, y presentar propuestas en el caso de encontrarse fallas en el tratamiento de la información en la misma.

### Objetivos Específicos

- ✓ Analizar la norma y como esta puede adaptarse para centro de estudios superiores, usando la FIEC como base.
- ✓ Levantar la información de la red de la facultad.
- ✓ Analizar la información obtenida.
- ✓ Definir un sistema de gestión de riesgos adecuado para nuestro estudio.

- ✓ Definir si la red cumple o no con los requerimientos del estándar ISO/IEC 27001:2013.
- ✓ Presentar propuestas a mejoras en caso de que no se cumpla el estándar.

## 1.4. Metodología

La metodología se llevará a cabo con el desarrollo de las siguientes fases:

- ✓ **Descripción de la fase 1**

  Lectura de la ISO 27001:2013, importancia, beneficios y aplicabilidad a instituciones educativas, así como la evolución y conceptos que esta maneja.

- ✓ **Descripción de la fase 2**

  Realizar un estudio del activo más importante de la facultad, realizando un listado de requisitos basado en la norma ISO 27001:2013, además de analizar los riesgos empleando la metodología MAGERIT.

- ✓ **Descripción de la fase 3**

  Proceso de auditoría a la Facultad para elaborar el diseño final, próximo a una implementación. Diagrama de Gantt.

- ✓ **Descripción de la fase 4**

  Presentación de resultados, encuesta a las diferentes entidades, análisis técnico-económico, recomendaciones y Observaciones.

## 1.5. Limitaciones

Entre las posibles limitaciones que encontramos tenemos:

- ✓ Información confidencial de la FIEC, que por su nivel de seriedad no se pueda acceder para este estudio.
- ✓ Ciertos procesos de los cuales la FIEC no tiene control y depende de otras áreas de la universidad.
- ✓ Limitaciones financieras para acceso a información del estándar en su última versión.

# CAPÍTULO 2

# 2. MARCO TEÓRICO Y ANTECEDENTES BIBLIOGRÁFICOS

## 2.1. Fundamentos de la seguridad de la información

La seguridad de la información aparece cuando las conversaciones telefónicas eran escuchadas ya que la señal se transmitía por cable de cobre. La tecnología fue avanzando con el pasar del tiempo y se fueron desarrollando nuevos sistemas. Aun no se conocía el término de seguridad, los datos vía telefónica se seguían perdiendo tanto así que los operadores móviles dirigían mal las llamadas y estas seguían siendo espiadas. [2]

A medida que se daba la necesidad de comunicarse entre los usuarios, apareció la iniciativa de enlazar los equipos con las redes telefónicas para que la información pueda ser compartida. Esta conexión fue de gran interés y ayuda durante los días que sonaba la compartición en red; aunque esta con respecto a seguridad era muy débil.

Fueron apareciendo los correos electrónicos, los cuales llevan datos valiosos del usuario como es la contraseña, o el número de la tarjeta de crédito y el comercio virtual. Elementos vitales para la persona que dispone de estos bienes electrónicos; lamentablemente detrás de toda esta situación estaban los intrusos, que interceptaban los sistemas y corrompían la información personal.

*"A Julio César (50 B.C.) se le atribuye la invención del código de cifrado para proteger la confidencialidad de la información, con el fin de evitar que los mensajes secretos puedan ser leídos por otras personas. César utilizó una técnica sencilla de sustituir cada letra del texto llano por un cambio de la letra, este método lo utilizaban para comunicaciones militares."* [2]

Podemos definir seguridad de la información, como los procesos y reglas que se crean y siguen en una compañía, empresa u organización cuya

función es realizar una copia de seguridad y proteger la información de posibles filtraciones, ataques, destrucción o indisponibilidad, que podrían afectar negativamente la actividad que realizamos.

Antiguamente la seguridad de la información era considerada una simple disciplina en las pequeñas empresas, en la actualidad se encuentra implementándose como norma institucional en corporaciones alrededor del mundo.

El cibercrimen está creciendo cada vez más rápido, tanto así que las leyes aún no pueden ponerse al día con él. La historia de los crímenes cibernéticos ocurre por el incremento de computadores con acceso a internet, la administración de recursos por medio de la red; y por la evolución de malware. [3]

### 2.1.1. Objetivos de la protección de la información

El objetivo principal es la protección de los activos que incluyen las personas, sistemas y hardware donde se hace uso de los datos críticos de una organización u empresa, protegiendo así la tecnología con la que cuenta la entidad, políticas y procesos.

En los últimos años, con la llegada de nuevas tecnologías y la facilidad de adquisición de la misma, pasamos cada vez más tiempo en línea, y por lo tanto, constantemente transfiriendo información, mucha de esta corriendo graves riesgos si no se toman las medidas adecuadas para protegerla.

### 2.1.2. Riesgos de un mal manejo de la información

Al decir sobre los posibles riesgos de un mal manejo de información, lo primero que se nos puede venir en mente es la filtración o destrucción de datos, aunque esto es cierto, debemos

también pensar en los efectos que esto puede provocar a futuro, tales como:

- ✓ Pérdida de confianza.
- ✓ Pérdidas financieras.
- ✓ Riesgos para los trabajadores y clientes de empresas.
- ✓ Pérdida y filtración de información de terceros.

Según el artículo “Empresas: ¿perder el negocio por el mal manejo de información?”, escrito el 22 de agosto del 2012 por el empresario chileno Álvaro Cahn, Gerente de Líneas Financieras de Chile; cada vez es más difícil mantener a salvo nuestra información con los avances tecnológicos y su progreso en pasos gigantes. En este se muestra el porcentaje de pérdida de información por parte de los empleados deshonestos de una empresa, y a su vez de cómo es utilizada con fines de dañar a la misma [4]. A continuación en la figura 2.1. se muestra la información obtenida:

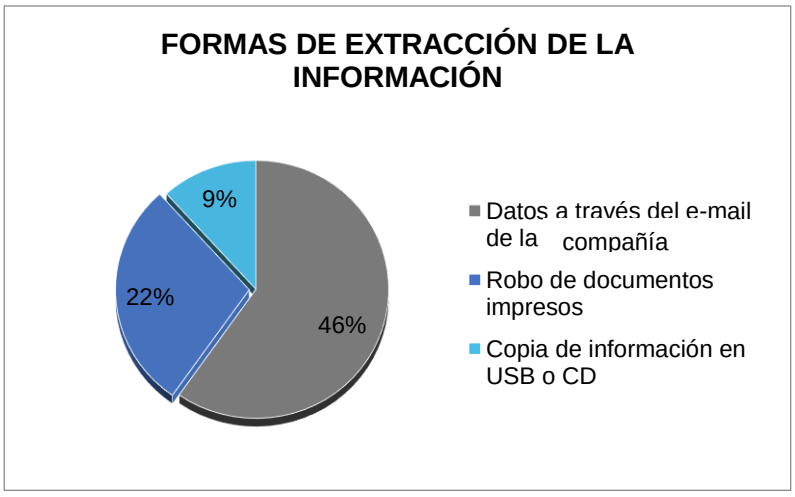



FIGURA 2.1-Formas en que la información es extraída

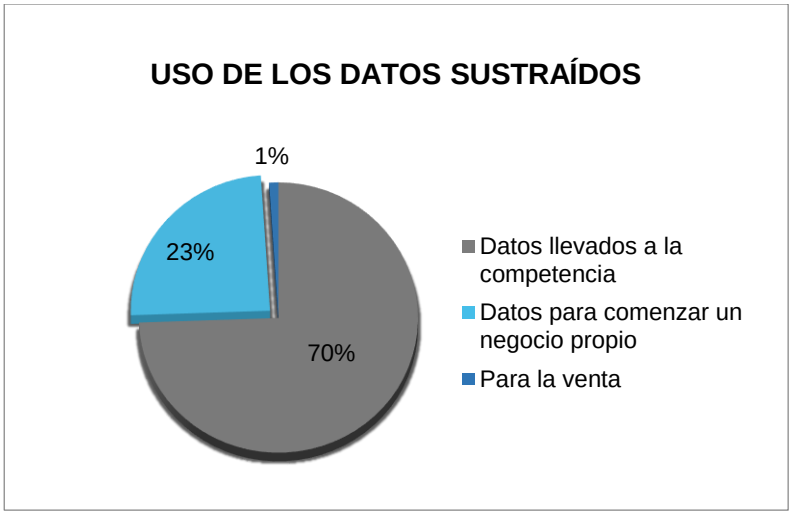



FIGURA 2.2-Uso de los datos sustraídos

Debemos recordar que no basta con endurecer los protocolos de seguridad, se debe aprender de los errores propios o debilidades, lo cual nos puede evitar inconvenientes a futuro; como lo sucedido en el 2014 a SONY, donde su sistema fue vulnerable por no superar los problemas que se le presentaron en el 2011. [5]

Otro acontecimiento fue el 03 de marzo del 2015, donde un ex director de la CIA, David Petraeus, se declara culpable de negligencia por filtración de documentos confidenciales, los cuales fueron entregados a su biógrafa con la que mantenía una relación extramatrimonial. [6]

## 2.2. Análisis de activos y Gestión de riesgos

El análisis de riesgos es uno de los requisitos de la norma ISO 27001:2013. Y es por medio de este método que se obtiene una visión general y prerrogativa de los riesgos a los que se enfrenta una entidad, sean estos fallos en la infraestructura, desastres naturales o riesgos del personal.

Existen muchos métodos o herramientas para ejecutar el análisis de riesgos, pero las metodologías más conocidas son: MAGERIT (Proceso sistemático para estimar la magnitud de los riesgos a la que está expuesta una organización), y ENS (utilización sistemática de la información disponible para identificar peligros y estimar riesgos). [7]

### 2.2.1. Magerit

MAGERIT es la metodología de análisis y gestión de riesgos de los sistemas de información. Este sistema se creó en España por el consejo Superior de Administración Electrónica, con el fin de ayudar a crear el Sistema de Gestión de Seguridad de la Información (SGSI).

Esta metodología recoge los siguientes informes y conclusiones, en síntesis:

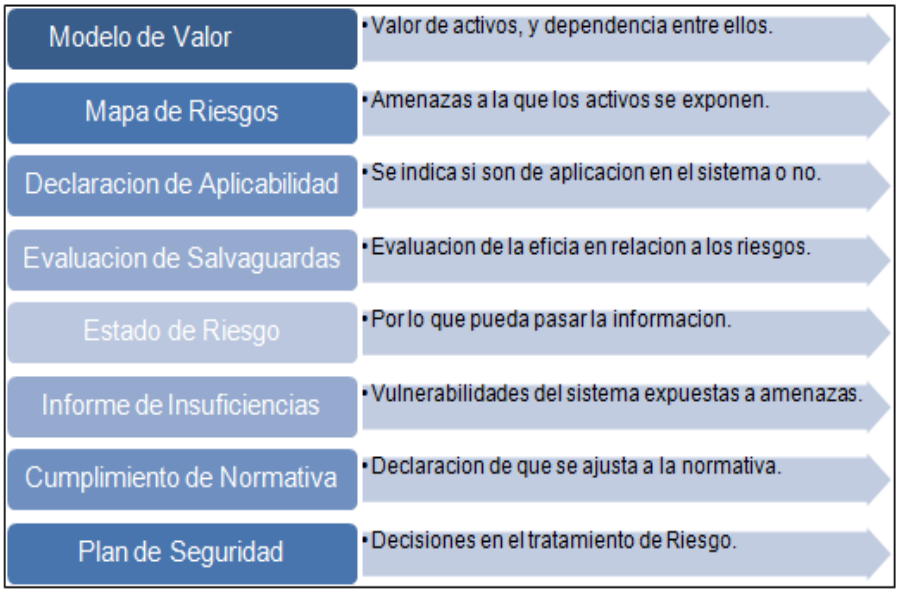



FIGURA 2.3-Informes y Conclusiones que persigue MAGERIT **[8]**

### 2.2.2. Objetivos

Tomados directamente del libro 1 de MAGERIT [9] los objetivos son:

- ✓ Directos*:*

  1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

  2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

  3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

- ✓ Indirectos:

  4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

### 2.2.3. Proceso de análisis y avalúo de activos

Para realizar el proceso de identificación de riesgos, será necesario identificar los activos, en nuestro caso, activos se refiere a los servicios, objetos, personas o lugares donde se interactúe con la información.

MAGERIT nos ofrece una clasificación predefinida, facilitándonos el proceso de selección de activos para nuestro estudio.

El avalúo de activos se refiere al proceso de generar un valor a cada activo encontrado según su necesidad para cumplir con los objetivos de Confidencialidad, Integridad y Disponibilidad.

### 2.2.4. Proceso de análisis y avalúo de riesgos

Para el proceso de avalúo de riesgo se tomarán en cuenta 2 aspectos:

- ✓ Ocurrencia.
- ✓ Degradación.

Analizaremos los activos con respecto a cada posible amenaza, analizando los valores de degradación en el caso de que estos se vean afectados, y la probabilidad de que suceda el inconveniente.

El impacto se determinara según los valores de degradación y probabilidad que se presente el problema, y usaremos la siguiente tabla para determinar el nivel del mismo:

TABLA 1 CUADRO DE EVALUACIÓN DE ACTIVOS

| | | ***Degradación*** | | | | |
|---|---|---|---|---|---|---|
| | *Impacto* | *1* | *2* | *3* | *4* | *5* |
| ***Ocurrencia*** | *1* | *1* | *2* | *3* | *4* | *5* |
| | *2* | *2* | *4* | *6* | *8* | *10* |
| | *3* | *3* | *6* | *9* | *12* | *15* |
| | *4* | *4* | *8* | *12* | *16* | *20* |
| | *5* | *5* | *10* | *15* | *20* | *25* |

Una vez determinado el impacto, podremos identificar los activos con un mayor riesgo, los cuales requerirán mayor atención.

## 2.3. ISO 27001:2013

ISO 27001:2013 es un estándar internacional que gestiona el tratamiento de la seguridad de la información de toda nuestra organización, siendo la 27001:2013 su última revisión. El nombre completo de este estándar es “Information Technology – Security Techniques; Information security management systems – Requirements”, traducido sería “Tecnologías de la información – Técnicas de seguridad; Sistemas de gestión de la seguridad

de información – Requerimientos", este nombre se refiere a las 2 secciones principales del estándar. [10]

Esta norma busca evaluar y tratar los riesgos a los cuales nuestros datos son expuestos en el día a día, con el fin de implementar medidas de seguridad. Por lo que el objetivo de esta norma es basada en la gestión de riesgos para luego tratarlos.

ISO/IEC 27001:2013 se divide en 11 secciones, además del Anexo A, las secciones 0 a 3 son introductorias y opcionales, 4 a 10 son obligatorias para su implementación, entre estas tenemos: [11]

- Sección 0: Introducción.
- Sección 1: Alcance.
- Sección 2: Referencias Normativas.
- Sección 3: Términos y definiciones.
- Sección 4: Contexto de la organización.
- Sección 5: Liderazgo.
- Sección 6: Planeación.
- Sección 7: Soporte.
- Sección 8: Operación.
- Sección 9: Evaluación de rendimiento.
- Seccion 10: Mejoras.
- Anexo A.

### 2.3.1. Origen y evolución

ISO/IEC 27001 en 1998 fue el nuevo estándar nacional certificable por la BSI (British Standards Institution) 7799-2. En 1999 se realizó la revisión conjunta de las partes 1 y 2 (BS 7799-2:1999). En el 2002 aparece la revisión de la ISO 9001, ISO 14001, OCDE (BS7799-2:2002). Recién en el 2005 aparece la ISO (Organización

Internacional de Normalización) Estándar Internacional (ISO/IEC 27001:2015). Con algunos cambios aparece en el 2013 la (ISO/IEC 27001:2013), siendo esta la actualización más reciente.

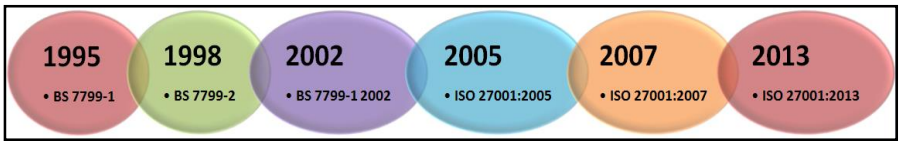



FIGURA 2.4 Evolución de la ISO 27001:2013 *[12]*

Entre los cambios que aparecen en la ISO/IEC 27001:2013 está el paso de 8 cláusulas a 10, donde también ciertos niveles de control con respecto al anexo aumenten o se fusionen; además ya no se basan en el ciclo PDCA “Plan-Do-Check-Act” (Planear-Hacer-Comprobar-Actuar).

### 2.3.2. Conceptos y aplicabilidad

El objetivo de ISO/IEC 27001:2013 es la protección de la confidencialidad, integridad y disponibilidad de la información. Este proceso se realiza identificando los posibles lugares donde se puedan existir riesgos de la información, y tratarlos de forma sistemática.

Salvaguardias suelen ser implementadas en forma de políticas, procedimientos e implementaciones técnicas, ya sean estas software o equipamiento, ISO 27001:2013 nos muestra como unir todos estos elementos en un solo Sistema de Gestión de la Seguridad de la Información. **[13]**

Entre los conceptos que se relacionan con el tema, está el ciclo Deming también conocido como ciclo de mejora continua PDCA con sus siglas en inglés y PHVA en español. En síntesis presentamos este gráfico explicativo:

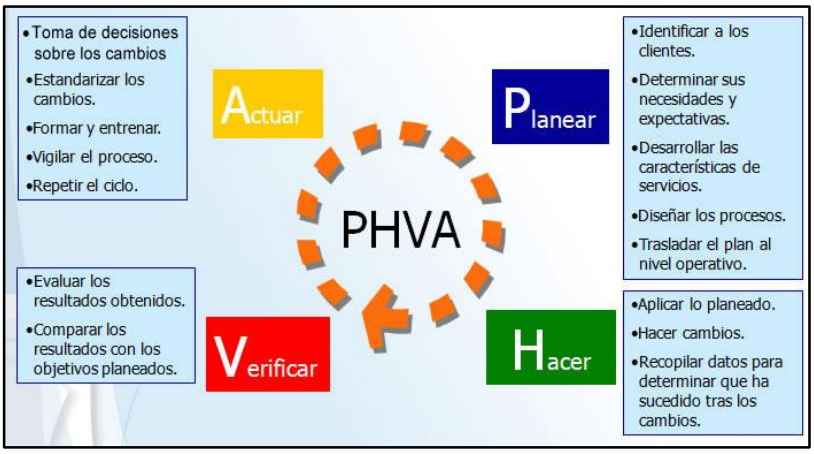



FIGURA 2.5 Ciclo PHVA

La ISO/IEC 27001 es una especificación para la creación de un SGSI. No obliga a tomar acciones específicas, pero incluye sugerencias para documentación, auditorías internas, mejoras continuas, acciones correctivas y preventivas. [14]

### 2.3.3. Sistema de Gestión de la Información

Un sistema de gestión de la seguridad de la información (SGSI) es un grupo de políticas y procesos para administrar la información importante de una organización. Para realizarlo se debe definir el ciclo C-I-D (Conficencialidad,Integridad y Disponibilidad) con este ciclo se busca cumplir los objetivos de la organización, mejorar el nivel de competitividad, la rentabilidad de los negocios y por supuesto estar al día a nivel legal y lograr una buena imagen en el ámbito empresarial.

Con este sistema se minimizan los riesgos encargándose de que exista continuidad y así evita posibles fallas de seguridad.

El SGSI se encarga de revisar el comportamiento de los empleados y procesos, así como de los datos y la tecnología usada. Un buen SGSI siempre debe incluir el Manual de

seguridad,Procedimientos,Instrucciones/Cheklist/Formularios, y Registros. [15]

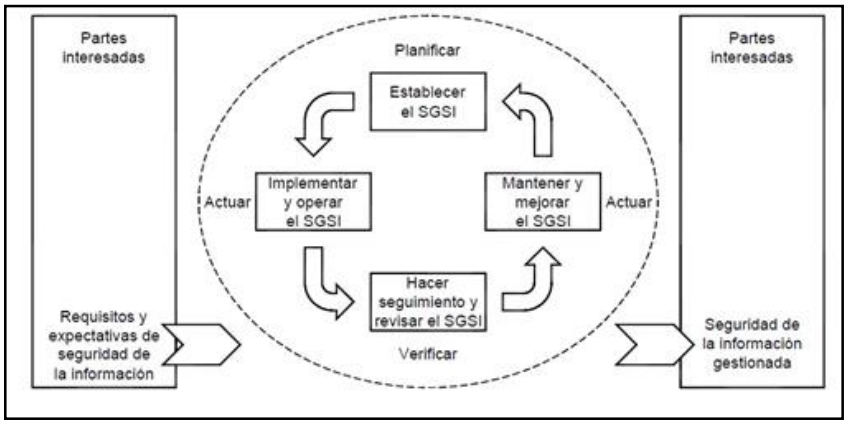



FIGURA 2.6 Proceso PDCA para implementar el SGSI

### 2.3.4. Certificación

Las organizaciones que requieran estar certificados con la ISO 27001:2013, necesitan demostrar que cumplen con cada uno de los requisitos y aprobar los 3 pasos que se ejecutan en una auditoría de certificación.

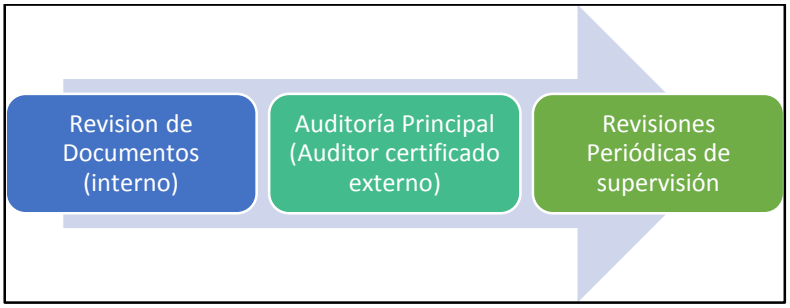



FIGURA 2.7 Pasos para obtener la certificación *[16]*

Si una persona requiere obtener la certificación, deberá asistir a cursos y aprobar el examen que lo certifique. En este estudio explicamos cuán importante es llevar en orden la información y procesos de las empresas o entidades, por lo que hemos demostrado que es de suma importancia certificarse, sea como empresa o como consultor.

### 2.3.5. Beneficios de implementar ISO 27001:2013

Existen varios beneficios en su implementación como:

- ✓ Mayor seguridad en el manejo de información.
- ✓ Capacidad de prevención a posibles fallas de seguridad y reacción ante ellas.
- ✓ Mayor nivel de competitividad al garantizar un manejo seguro de información.
- ✓ Reducción de costos al prevenir muchas brechas de seguridad.
- ✓ Mejor organización al tener todos los procesos documentados con sus respectivos responsables.
- ✓ Reducción de tiempo, tanto para el contratante como el contratado, ya que los procesos que la empresa maneja quedan definidos de manera organizada y categorizada. [17]

# CAPÍTULO 3

# 3. ANÁLISIS Y DISEÑO

En este capítulo presentaremos información de la Facultad de la ESPOL, para fines de guardar su confidencialidad e integridad de los datos y procesos que Fiec maneja, la información presentada ha sufrido modificaciones. Ciertas imágenes, son tomadas de la propia página de la FIEC, con el fin de llevar un estudio ordenado y metódico.

## 3.1. Descripción del escenario

Nuestro estudio se basa en la información que manejan los laboratorios de computación y el edificio de gobierno, (marcados en la Figura 3.1 de color azul). Dado que nuestro estudio habla sobre la norma ISO de seguridad de la información y según el levantamiento de información, es aquí donde se registran procesos administrativos, flujo de datos, manejo de equipos, y personal técnico de Fiec.

A continuación la Figura 3.1 nos muestra las áreas que la Fiec posee, tales como: aulas, oficinas de Cisco, laboratorios de redes, de telecomunicaciones , de circuitos impresos, de maquinaria eléctrica. Al otro lado, cuenta con el edificio de Gobierno con aulas y laboratorios.

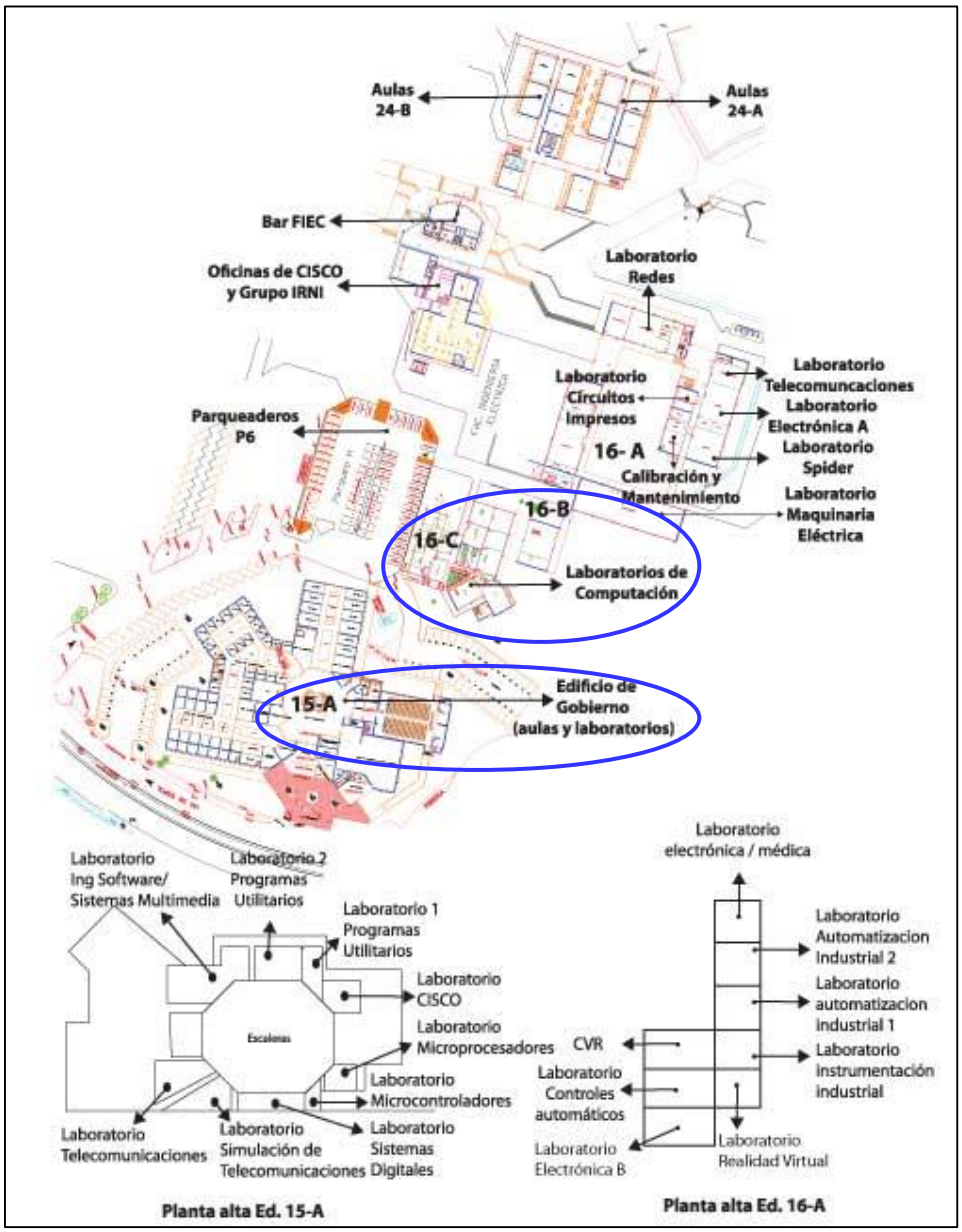



FIGURA 3.1 Tomada de la Facultad de Ingeniería en Electricidad y Computación *[18]*

### 3.1.1. Detalle de la red que posee FIEC

La red de la FIEC se encuentra detallada en el siguiente gráfico:

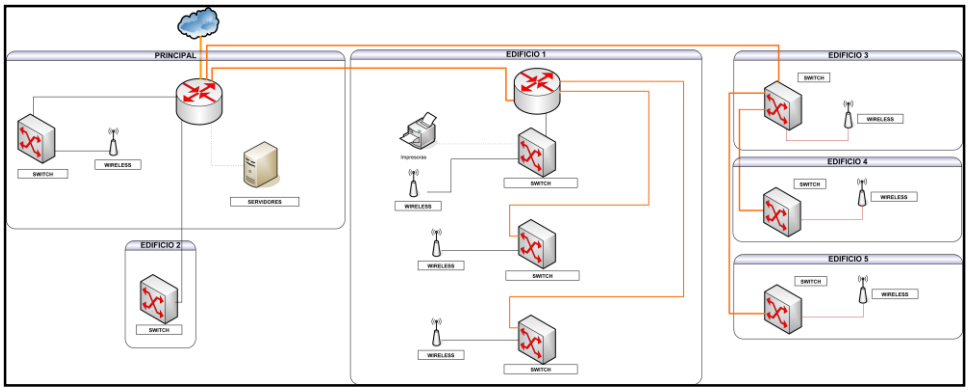



FIGURA 3.2 Red FIEC

### 3.1.2. Arquitectura de hardware y software

En el estudio realizado a la FIEC se hizo un análisis a los servidores en cuanto al software, enfocándonos sólo en los servicios que estos brindan, es decir el Sistema Operativo utilizado y el software requerido para que estos brinden los servicios a los usuarios.

Según los datos obtenidos pudimos separar al software en las siguientes categorías:

- Software de gestión de Correos.
- Software de Base de Datos.
- Software de Servicios Web.
- Antivirus.
- Software para Control de PCs.
- Servicio de DHCP.
- Software para streaming de video.
- Software para servidor RADIUS.

### 3.1.3. Mapa organizacional

Es de mucha importancia conocer el personal que se encuentra dentro de nuestra institución, y el cargo que éste desempeña. De esta forma tenemos una mejor visión del crecimiento de nuestra empresa en el logro de metas.

Además llevamos un control de quiénes son los responsables de manejar información confidencial, nos da una visión más clara de cuáles son las responsabilidades de cada trabajador y su jefe inmediato.

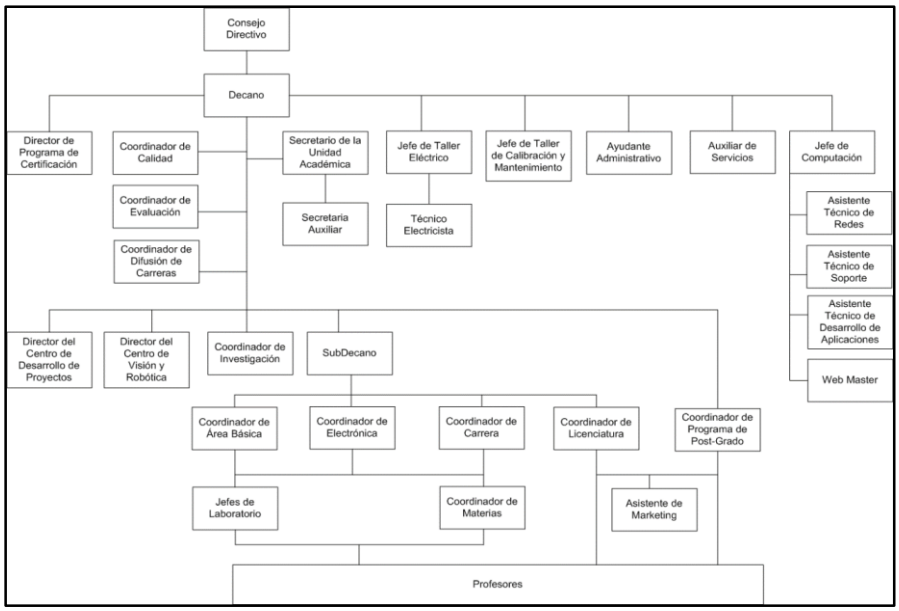



FIGURA 3.3 Tomada de la página de la FIEC- Mapa Organizacional de la Facultad. *[18]*

### 3.1.4. Documentos de trabajo

Para nuestro estudio utilizaremos una lista de control, para analizar si la red posee los requisitos necesarios para ISO 27001.

El objetivo principal de esta lista de control es facilitarnos el proceso de realizar una auditoría, ofreciéndonos una lista de preguntas.

Esta lista nos servirá para detectar más fácilmente en donde existen las falencias más graves y en donde poder enfocarnos más en solucionarlos.

## 3.2. Proceso de gestión de activos

### 3.2.1. Inventario de activos

TABLA 2 Arquitectura del Sistema

| **[ARCH] Arquitectura del sistema** |
|---|
| [sap] Servicios de la FIEC prestado a usuarios.<br>[ext] Servicios de correo FIEC. |

TABLA 3 Información General

| **[D] Datos/Información** |
|---|
| [files] Archivos de los equipos de la FIEC.<br>[backup] Respaldos de información de servidores o archivos importantes.<br>[conf] Datos de configuración de equipos y equipos de red.<br>[auth] Datos de autenticación para su uso en portal cautivo.<br>[log] Registro de actividades.<br>[source] Código fuente de proyectos.<br>[exe] Ejecutables obtenidos de proyectos.<br>[test] Datos de prueba obtenidos en proyectos. |

TABLA 4 Servicios Internos

| **[S] Servicios** |
| --- |
| [int] Servicios internos ofrecidos a estudiantes y trabajadores. |
| [email] Servicio de correo electrónico, se utiliza un tercero para su administración. |

TABLA 5 Software Estándar

| **[std] Software estándar** |
| --- |
| Software de gestión de Correos. |
| Software de Base de Datos. |
| Software de Servicios Web. |
| Antivirus. |
| Software para Control de PCs. |
| Servicio de DHCP. |
| Software para streaming de video. |
| Software para servidor RADIUS. |

TABLA 6 Hardware

| **[HW] Hardware** |
| --- |
| [host] Servidores de la FIEC. |
| [pc] Equipos de escritorio de oficinas y laboratorios. |
| [backup] Equipos usados para respaldos. |
| [peripheral] Impresoras y escáneres(todo en uno). |
| [bp] Router de salida de red FIEC a red general ESPOL. |
| [network] [switch] Conmutadores de la red. |
| [network] [router] Enrutadores de la red. |
| [network] [wap] Access Point para acceso a la red WiFi. |
| [ipphone] Telefonos IP de la facultad. |

TABLA 7 Redes de Comunicaciones

| **[COM] Redes de comunicaciones** |
| --- |
| [wifi] Red Inalámbrica general de la FIEC, Redes privadas para uso de oficinas o departamentos.<br>[lan] Red cableada de la FIEC. |

TABLA 8 Soportes de Información

| **[MEDIA] Soportes de información** |
| --- |
| [disk] Discos de los equipos y servidores.<br>[san] Almacenamiento de información en la red de la FIEC. |

TABLA.9 Equipamiento Auxiliar

| **[AUX] Equipamiento auxiliar** |
| --- |
| [power] Fuentes de alimentación eléctrica de laboratorios, oficinas y cuarto de servidor.<br>[ups] UPS del servidor.<br>[ac] Sistemas de aires acondicionados de laboratorios y servidor.<br>[cabling][wire] Cables de red donde se realizan las comunicaciones.<br>[furniture] Armarios donde se guarda información física. |

TABLA 10 Instalaciones

| **[L] Instalaciones** |
| --- |
| [site] Facultad de Ingeniería Eléctrica y Computación.<br>[building] Edificio donde se aloja el servidor.<br>[local] Cuarto donde se aloja el servidor. |

TABLA 11 Personal FIEC

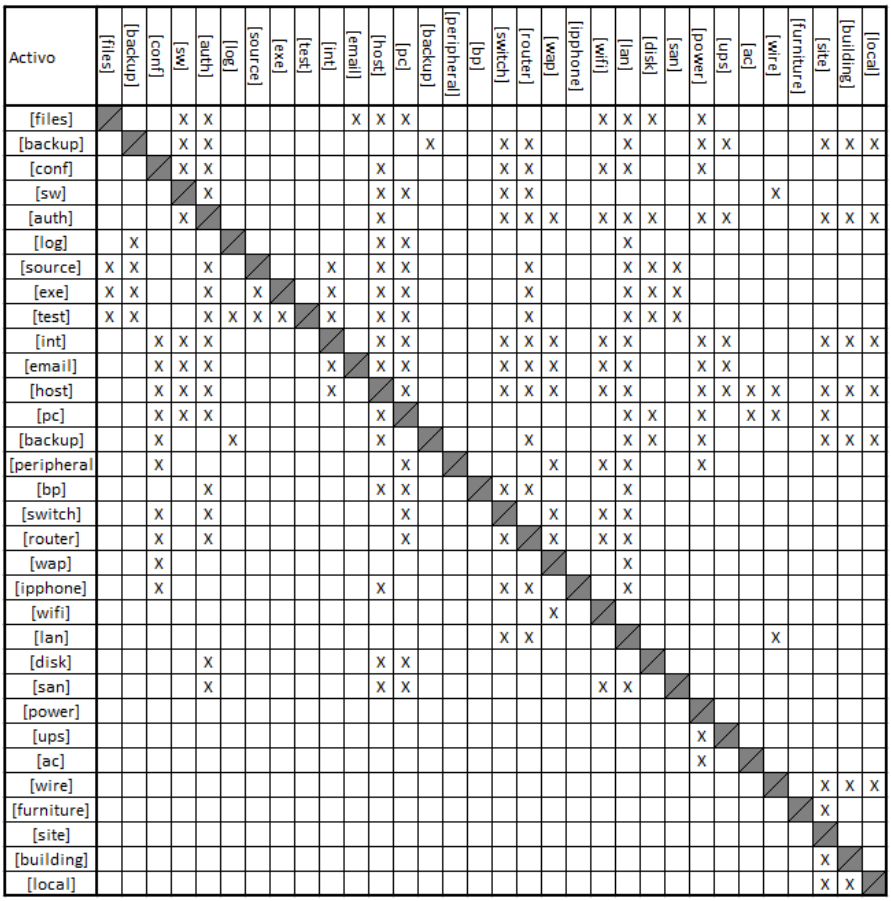
| **[P] Personal** |
| --- |
| [ui] Estudiantes, docentes y personal administrativo.<br>[adm] Administrador de sistemas.<br>[des] Desarrolladores/ Programadores en proyectos.<br>Nota: [adm] también se encarga de la administración de la base de datos y del área de seguridad, a pesar de su presencia no se incluyen los activos **[dba]Administrador de la base de datos** ni **[sec] Administradores de Seguridad** |

### 3.2.2. Dependencias de los activos

Se trata de los activos que se pueden ver afectados por algún fallo en la seguridad en un activo inferior a este, es ahí donde decimos que un activo puede depender de otro, cuando las necesidades del activo superior se reflejan con la necesidad de seguridad del inferior. Un ejemplo de activo primario o superior es la información que a la vez depende de otros activos como pueden ser los equipos, o las personas que trabajan con éste.

Para comprender de mejor forma la dependencia de activos, deberíamos atacar a un activo específico, buscando en primera instancia sus vulnerabilidades

En la Figura 3.4, se muestran los activos que existen dentro de la FIEC y sus respectivos activos secundarios o inferiores; llamados así porque estos son dependientes de los activos superiores.



| Activo | [files] | [backup] | [conf] | [sw] | [auth] | [log] | [source] | [exe] | [test] | [int] | [email] | [host] | [pc] | [backup] | [peripheral] | [bp] | [switch] | [router] | [wap] | [ipphone] | [wifi] | [lan] | [disk] | [san] | [power] | [ups] | [ac] | [wire] | [furniture] | [site] | [building] | [local] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [files] | | | | X | X | | | | | | X | X | X | | | | | | | | X | X | X | | X | | | | | | | |
| [backup] | | | | X | X | | | | | | | | | X | | | X | X | | | | X | | | X | X | | | | X | X | X |
| [conf] | | | | X | X | | | | | | | X | | | | | X | X | | | X | X | | | X | | | | | | | |
| [sw] | | | | | X | | | | | | | X | X | | | | X | X | | | | | | | | | | X | | | | |
| [auth] | | | | X | | | | | | | | X | | | | | X | X | X | | X | X | X | | X | X | | | | X | X | X |
| [log] | | X | | | | | | | | | | X | X | | | | | | | | | X | | | | | | | | | | |
| [source] | X | X | | | X | | | | | X | | X | X | | | | | X | | | | X | X | X | | | | | | | | |
| [exe] | X | X | | | X | | X | | | X | | X | X | | | | | X | | | | X | X | X | | | | | | | | |
| [test] | X | X | | | X | X | X | X | | X | | X | X | | | | | X | | | | X | X | X | | | | | | | | |
| [int] | | | X | X | X | | | | | | | X | X | | | | X | X | X | | X | X | | | X | X | | | | X | X | X |
| [email] | | | X | X | X | | | | | X | | X | X | | | | X | X | X | | X | X | | | X | X | | | | | | |
| [host] | | | X | X | X | | | | | X | | | X | | | | X | X | X | | X | X | | | X | X | X | X | | X | X | X |
| [pc] | | | X | X | X | | | | | | | X | | | | | | | | | | X | X | | X | | X | X | | X | | |
| [backup] | | | X | | | X | | | | | | X | | | | | | X | | | | X | X | | X | | | | | X | X | X |
| [peripheral | | | X | | | | | | | | | | X | | | | | | X | | X | X | | | X | | | | | | | |
| [bp] | | | | | X | | | | | | | X | X | | | | X | X | | | | X | | | | | | | | | | |
| [switch] | | | X | | X | | | | | | | | X | | | | | X | | X | X | X | | | | | | | | | | |
| [router] | | | X | | X | | | | | | | | X | | | | X | | X | | X | X | | | | | | | | | | |
| [wap] | | | X | | | | | | | | | | | | | | | | | | | X | | | | | | | | | | |
| [ipphone] | | | X | | | | | | | | | X | | | | | X | X | | | | X | | | | | | | | | | |
| [wifi] | | | | | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| [lan] | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | X | | | | |
| [disk] | | | | | X | | | | | | | X | X | | | | | | | | | | | | | | | | | | | |
| [san] | | | | | X | | | | | | | X | X | | | | | | | | X | X | | | | | | | | | | |
| [power] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| [ups] | | | | | | | | | | | | | | | | | | | | | | | | | X | | | | | | | |
| [ac] | | | | | | | | | | | | | | | | | | | | | | | | | X | | | | | | | |
| [wire] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X |
| [furniture] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | | |
| [site] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| [building] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | | |
| [local] | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | |

FIGURA 3.4 Dependencia de Activos

De una manera más simple, tomemos de ejemplo el activo [host], si queremos llegar a este, ya sea para acceso, o alteración de sus funciones, deberíamos pasar por uno o más de los siguientes activos: [conf], [sw], [auth], [int], [pc], [switch], [router], [wap], [wifi], [lan], [power], [ups], [ac], [wire], [site], [building], [local].

### 3.2.3. Valoración de activos

En nuestro estudio pondremos un valor a los activos según su necesidad para cumplimiento de funciones en cuanto a Confidencialidad, Integridad, Disponibilidad, con valores de 1 al 5, definidos por la siguiente tabla:

TABLA 12 Valoración de activos

| Valor | Descripción |
|---|---|
| 1 | Muy Bajo/No aplicable |
| 2 | Bajo |
| 3 | Normal |
| 4 | Alto |
| 5 | Muy Alto |

Clave: C=Confidencialidad, I=Integridad, D=Disponibilidad, T=Total

TABLA 13 Activos valorados según nuestro criterio

| Activo | C | I | D | T |
|---|---|---|---|---|
| [sap] Servicios de la FIEC prestado a usuarios. | 4 | 5 | 5 | 14 |
| [ext] Servicios de correo FIEC. | 5 | 5 | 5 | 15 |
| [files] Archivos de los equipos de la FIEC. | 3 | 4 | 4 | 11 |
| [backup] Respaldos de información de servidores o archivos importantes. | 3 | 5 | 5 | 13 |
| [conf] Datos de configuración de equipos y equipos de red. | 2 | 2 | 5 | 9 |
| [auth] Datos de autenticación para su uso en portal cautivo. | 3 | 3 | 5 | 11 |
| [log] Registro de actividades. | 2 | 5 | 1 | 8 |
| [source] Código fuente de proyectos. | 1 | 3 | 5 | 9 |
| [exe] Ejecutables obtenidos de proyectos. | 1 | 3 | 5 | 9 |
| [test] Datos de prueba obtenidos en proyectos. | 2 | 3 | 5 | 10 |
| [int] Servicios internos ofrecidos a estudiantes y trabajadores. | 4 | 4 | 5 | 13 |
| [email] Servicio de correo electrónico. | 5 | 4 | 5 | 14 |
| [host] Servidor de la FIEC. | 5 | 5 | 5 | 15 |
| [pc] Equipos de escritorio de oficinas y laboratorios. | 3 | 2 | 4 | 9 |
| [backup] Equipos usados para respaldos. | 3 | 4 | 5 | 12 |
| [peripheral] Impresoras y escáneres (all in one). | 1 | 1 | 4 | 6 |
| [bp] Router de salida de red FIEC a red general ESPOL. | 5 | 4 | 5 | 14 |
| [network] [switch] Conmutadores de la red. | 1 | 3 | 5 | 9 |

| | | | | |
|---|---|---|---|---|
| [network] [router] Enrutadores de la red. | 4 | 3 | 5 | 12 |
| [network] [wap] Access Point para acceso a la red WiFi. | 3 | 2 | 5 | 10 |
| [ipphone] Teléfonos IP de la facultad. | 3 | 4 | 5 | 12 |
| [wifi] Red Inalámbrica general de la FIEC, Redes privadas para uso de oficinas o departamentos. | 3 | 2 | 5 | 10 |
| [lan] Red cableada de la FIEC. | 4 | 4 | 5 | 13 |
| [disk] Discos de los equipos y servidores. | 3 | 5 | 5 | 13 |
| [san] Almacenamiento de información en la red de la FIEC. | 5 | 4 | 5 | 14 |
| [power] Fuentes de alimentación eléctrica de laboratorios, oficinas y cuarto de servidor. | 1 | 2 | 5 | 8 |
| [ups] UPS del servidor. | 1 | 2 | 5 | 8 |
| [ac] Sistemas de aires acondicionados de laboratorios y servidor. | 1 | 1 | 3 | 5 |
| [cabling][wire] Cables de red donde se realizan las comunicaciones. | 3 | 3 | 4 | 10 |
| [furniture] Armarios donde se guarda información física. | 4 | 4 | 4 | 12 |
| [site] Facultad de Ingeniería Eléctrica y Computación. | 4 | 4 | 5 | 13 |
| [building] Edificio donde se aloja el servidor. | 5 | 4 | 5 | 14 |
| [local] Cuarto donde se aloja el servidor. | 5 | 5 | 5 | 15 |
| [ui] Estudiantes, docentes, redes y personal administrativo. | 3 | 3 | 3 | 9 |
| [adm] Administrador de sistemas. | 5 | 5 | 5 | 15 |
| [dba] Administrador de la base de datos. | 5 | 5 | 5 | 15 |
| [sec] Administradores de seguridad. | 5 | 5 | 5 | 15 |
| [des] Desarrolladores/ Programadores en proyectos. | 3 | 3 | 5 | 11 |

## 3.3. Proceso de gestión de riesgos

### 3.3.1. Identificación de amenazas

Se definirán las posibles amenazas, con su posible probabilidad, la Tabla 14 nos muestra el modelo a seguir, para explicar cada una de estas.

TABLA 14 Descripción de Amenaza

| [CÓDIGO DE AMENAZA] Descripción de amenaza | |
|---|---|
| Lista de tipos de activos que pueden verse afectados. | Dimensiones de seguridad que se pueden ver afectadas por este tipo de amenazas, ordenadas por su relevancia, de mayor a menor. |
| Descripción detallada de la amenaza. | |

[N] Naturales – Se refieren a aquellas donde no existe interacción humana como causa directa o indirecta.

TABLA 15 Desastres Naturales

| [N.7] Desastres Naturales – Fenómeno Sísmico | |
|---|---|
| [HW] equipos informáticos (hardware).<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar.<br>[L] instalaciones. | [D] Disponibilidad. |
| ❖ Otros incidentes que se producen sin intervención humana: Rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.<br>❖ Un terremoto es algo imprevisto, uno realmente fuerte puede provocar problemas en las instalaciones. | |

[I] Origen Industrial – Pueden ocurrir de forma accidental, o deliberada, están derivados de la actividad humana de tipo industrial.

TABLA 16 Fuego

| [I.1] Fuego | |
|---|---|
| [HW] equipos informáticos (hardware).<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar.<br>[L] instalaciones. | [D] Disponibilidad. |
| ❖ Posibilidad de que el fuego acabe con los recursos del sistema, este se da de forma accidental, ya sea por un problema del entorno, o falla humana. | |

TABLA 17 Contaminación Mecánica

| [I.3] Contaminación mecánica | |
|---|---|
| [HW] equipos informáticos (hardware).<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar. | [D] Disponibilidad. |
| ❖ Ocurre por polvo o suciedad, en los equipos físicos, los cuales pueden afectar el desempeño de éstos. | |

TABLA 18 Contaminación Electromagnética

| [I.4] Contaminación electromagnética | |
|---|---|
| [HW] equipos informáticos (hardware).<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar. | [D] Disponibilidad. |

| |
|---|
| ❖ Interferencias de radio.<br>❖ Campos magnéticos.<br>❖ Luz ultravioleta.<br>*Éstas pueden afectar en comunicaciones inalámbricas. |

TABLA 19 Avería de Origen Físico o Lógico

| [I.5] Avería de origen físico o lógico | |
|---|---|
| [SW] aplicaciones (software).<br>[HW] equipos informáticos (hardware).<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar. | [D] Disponibilidad. |
| ❖ Fallo en los equipos y/o fallo en los programas. Puede ocurrir por un defecto de fábrica (origen) o durante el funcionamiento del sistema.<br>❖ El uso constante de los equipos de laboratorios reducen su tiempo de vida, los servicios brindados por éste se pueden ver afectados.<br>❖ El software desactualizado nos puede llevar a fallas de seguridad, éstas podrían generar limitaciones en los servicios brindados. | |

TABLA 20 Corte de Suministro eléctrico

| [I.6] Corte de suministro eléctrico | |
|---|---|
| [HW] equipos informáticos (hardware).<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar. | [D] Disponibilidad. |

| |
|---|
| ❖ Los equipos se pueden dañar cuando cesa la alimentación de potencia.<br>❖ Al no existir electricidad para suplir a los equipos, puede evitar el acceso a los servicios que estos ofrecen.<br>❖ La Fiec, no cuenta con un generador, sólo con un UPS; si hubiese un corte de energía la Fiec tendría un tiempo limitado para que la red y los servicios estén funcionando, despúes de ese tiempo la facultad se queda sin servicios y red. |

TABLA 21 Falla de servicios de comunicaciones

| [I.8] Falla de servicios de comunicaciones | |
|---|---|
| [COM] redes de comunicaciones. | [D] Disponibilidad. |
| ❖ Incapacidad de transmitir datos de un sitio a otro.<br>❖ Destrucción de los medios físicos de transporte.<br>❖ Detención de los centros de conmutación sea por fallos eléctricos o daño de los cables u conectores, sea por destrucción premeditada o degradación física de éstos.<br>❖ Detención de los centros de conmutación al tener un número de usuarios mayor al que puedan suplir.<br>❖ Las fallas de ciertos Access Points pueden dejar ciertos sectores de la FIEC sin comunicación inalámbrica. | |

TABLA 22 Degradación de los soportes de almacenamiento de información

| [I.10] Degradación de los soportes de almacenamiento de información | |
|---|---|
| [Media] soportes de información. | [D] Disponibilidad.<br>[I ] Integridad. |
| ❖ Se refiere a la degradación de los activos como consecuencia del paso del tiempo. Por ejemplo un disco duro de uno de los servidores de Fiec, que no tenga espacio disponible,y que haya superado el ciclo de | |

| |
|---|
| vida útil, es necesario que sea cambiado a tiempo antes de que se pueda perder esa información almacenada. |

[E] Errores y fallos no intencionados – Fallos y errores causados por las personas.

TABLA 23 Errores de los Usuarios

| [E.1] Errores de los usuarios | |
|---|---|
| [D] datos / información.<br>[S] servicios.<br>[SW] aplicaciones (software).<br>[Media] soportes de información. | [I] Integridad.<br>[C] Confidencialidad.<br>[D] Disponibilidad. |
| ❖ Equivocaciones de las personas cuando usan los servicios, datos, etc.<br>❖ Estudiantes dejan sesiones abiertas en los equipos de laboratorio.<br>❖ Personal deja equipos sin bloqueo.<br>❖ Información que pueda ser considerada confidencial puede ser dejada accidentalmente sobre un escritorio. | |

TABLA 24 Errores del administrador

| [E.2] Errores del administrador | |
|---|---|
| [D] datos / información.<br>[S] servicios.<br>[SW] aplicaciones (software).<br>[Media] soportes de información. | [I] Integridad.<br>[C] Confidencialidad.<br>[D] Disponibilidad. |
| ❖ Equivocaciones de personas con responsabilidades de instalación y operación.<br>❖ Administradores que por errores humanos puedan dar acceso a áreas restringidas, por ejemplo, no cerrar la puerta de acceso al cuarto de | |

| |
|---|
| servidores. |

TABLA 25 Errores de Monitorización

| [E.3] Errores de monitorización (log) | |
|---|---|
| [D.log] registros de actividad. | [I] Integridad.<br>[D] Disponibilidad. |
| ❖ Inadecuado registro de actividades, es decir que no se guarde el log del servidor, por corte de energía por ejemplo.<br>❖ Que alguien modifique y borre entradas de registros a los logs.<br>❖ Que exista algún fallo en el sistema. | |

TABLA 26 Errores de Configuración

| [E.4] Errores de configuración | |
|---|---|
| [D.conf] Datos de configuración. | [I] Integridad. |
| ❖ Introducción de datos de configuración erróneos por ejemplo: cambiar la configuración del reloj del sistema; esto nos puede traer grandes incovenientes ya que si sucede algo en cierta hora y necesitamos revisar los logs para deducir el daño, no lo podremos hacer porque no nos va a cuadrar la hora de los logs con la hora del sistema. | |

1. TABLA 27 Difusión de Software Dañino

| [E.8] Difusión de Software Dañino | |
|---|---|
| [S] servicios.<br>[SW] aplicaciones (software).<br>[COM] redes de comunicaciones. | [I] Integridad.<br>[C] Confidencialidad.<br>[D] Disponibilidad. |

| |
|---|
| ❖ Los laboratorios al ser de uso de los estudiantes, están propensos a infectarse de malware.<br>❖ A pesar de el uso de antivirus o programas que congelen la configuración y el estado de equipos en laboratorios, existen posibilidades de que puedan infectar otros medios externos antes de que el malware pueda ser eliminado. |

TABLA 28 Fugas de Información

| [E.19] Fugas de información | |
|---|---|
| [D] Datos / información.<br>[S] servicios.<br>[SW] aplicaciones (software).<br>[COM] redes de comunicaciones(tránsito).<br>[Media] soportes de información.<br>[L] instalaciones.<br>[P] personal (revelación). | [C] Confidencialidad. |
| ❖ Existe la posibilidad de que información confidencial sea filtrada de forma parcial o total, por medio de conversaciones, mal uso de documentos confidenciales, información digital presentada en computadores, entre otros. | |

TABLA 29 Vulnerabilidades del software

| [E.20] Vulnerabilidades de los programas (software) | |
|---|---|
| [SW] aplicaciones (software). | [I] Integridad.<br>[D] Disponibilidad.<br>[C] Confidencialidad. |

| |
|---|
| ❖ Fallas en el código, los cuales pueden afectar la integridad de la información o limiten los servicios. |

TABLA 30 Errores de mantenimiento/Actualización del software

| [E.21] Errores de mantenimiento / Actualización de programas (software) | |
|---|---|
| [SW] aplicaciones (software). | [I] Integridad.<br>[D] Disponibilidad. |
| ❖ La presencia de software desactualizado u obsoleto puede ser un riesgo grave para la red.<br>❖ Que no se tenga actualizado el navegador es un gran problema. | |

TABLA 31 Caída del sistema por agotamiento de recursos

| [E.24] Caída del sistema por agotamiento de recursos | |
|---|---|
| [S] servicios.<br>[HW] equipos informáticos (hardware).<br>[COM] redes de comunicaciones. | [D] Disponibilidad. |
| ❖ La carencia de recursos, como memoria, ancho de banda o procesamiento; provoca la caída del sistema.<br>❖ Cuando la carga de trabajo es desmesurada. | |

[A] Ataques intencionados - Fallos deliberados causados por las personas.

TABLA 32 Suplantación de identidad del usuario

| [A.5] Suplantación de identidad del usuario | |
|---|---|
| [D] datos / información.<br>[S] servicios.<br>[SW] aplicaciones (software).<br>[COM] redes de comunicaciones. | [C] Confidencialidad.<br>[A] Autenticidad.<br>[I] Integridad. |
| ❖ Cuando un atacante consigue hacerse pasar por un usuario autorizado, se beneficia de los privilegios de éste.<br>❖ Esta amenaza puede ser perpetrada por personal interno, personas ajenas a la organización o personal contratado temporalmente. | |

TABLA 33 Uso no previsto

| [A.7] Uso no previsto | |
|---|---|
| [S] servicios.<br>[SW] aplicaciones (software).<br>[HW] equipos informáticos (hardware).<br>[COM] redes de comunicaciones.<br>[Media] soportes de información.<br>[AUX] equipamiento auxiliar.<br>[L] instalaciones. | [D] Disponibilidad.<br>[C] Confidencialidad.<br>[I] Integridad. |
| ❖ Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal como: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. | |

TABLA 34 Difusión de software dañino

| [A.8] Difusión de software dañino | |
|---|---|
| [SW] aplicaciones (software). | [D] Disponibilidad.<br>[I] Integridad.<br>[C] Confidencialidad. |
| ❖ Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. | |

### 3.3.2. Valoración de amenazas

Se deben valorar las amenazas en 2 factores:

- ✓ Degradación: Que tanto se vería afectado el valor del activo.
- ✓ Probabilidad: Cuán probable o improbable es que se materialice la amenaza.

Para la degradación usaremos una tabla para medir el posible daño causado por algún incidente.

TABLA 35 Valoración de amenazas

| Nivel de degradación | Simbología a usar | Valor |
|---|---|---|
| Muy Alta | MA | 5 |
| Alta | A | 4 |
| Media | M | 3 |
| Baja | B | 2 |
| Muy Baja | MB | 1 |

Para el caso de la probabilidad, que es un poco más compleja su medición, usaremos una taza de probabilidad de ocurrencia durante un año, como parte de nuestro estudio.

TABLA 36 Probabilidad de que suceda

| Ocurrencia | Posibilidad de que suceda | |
|---|---|---|
| Muy Frecuente | En días | 5 |
| Frecuente | Meses | 4 |
| Normal | En un Año | 3 |
| Poco frecuente | En varios Años | 2 |
| Muy poco frecuente | Varias decadas | 1 |

### 3.3.3. Evaluación de riesgos y amenazas

Revisaremos los activos con respecto a cada posible amenaza, analizando los valores de degradación en el caso que éstos se vean afectados, y la probabilidad que suceda el inconveniente.

El impacto se determinará según los valores de degradación y probabilidad en que se presente el problema, y usaremos la siguiente tabla para determinar el nivel del mismo.

TABLA 37 Evaluación de riesgos y amenazas

| | | *Degradación* | | | | |
|---|---|---|---|---|---|---|
| | *Impacto* | *1* | *2* | *3* | *4* | 5 |
| *Ocurrencia* | *1* | *1* | *2* | *3* | *4* | 5 |
| | *2* | *2* | *4* | *6* | *8* | 10 |
| | *3* | *3* | *6* | *9* | *12* | 15 |
| | *4* | *4* | *8* | *12* | *16* | 20 |
| | *5* | *5* | *10* | *15* | *20* | 25 |

Una vez determinado el impacto, podremos identificar los activos con un mayor riesgo, los cuales requerirán mayor atención.

TABLA 38 Cuadro de activos VS impacto determinado

| Activo | Impacto Determinado |
|---|---|
| [files] Archivos de los equipos de la fiec. | 8.89 |
| [backup] Respaldos de información de servidores o archivos importantes. | 7.22 |
| [conf] Datos de configuración de equipos y equipos de red. | 7.42 |
| [auth] Datos de autenticación para su uso en portal cautivo. | 7.65 |
| [log] Registro de actividades. | 7.60 |
| [source] Código fuente de proyectos. | 6.32 |
| [exe] Ejecutables obtenidos de proyectos. | 6.69 |
| [test] Datos de prueba obtenidos en proyectos. | 6.25 |
| [int] Servicios internos ofrecidos a estudiantes y trabajadores. | 9.95 |
| [email] Servicio de correo electrónico. | 5.81 |
| [host] Servidor de la FIEC. | 7.15 |
| [pc] Equipos de escritorio de oficinas. | 8.35 |
| [pc] Equipos de escritorio de laboratorios. | 12.38 |
| [backup] Equipos usados para respaldos. | 6.05 |
| [peripheral] Impresoras y scanneres(all in one). | 8.44 |
| [bp] Router de salida de red FIEC a red general ESPOL. | 6.71 |
| [switch] Conmutadores de la red. | 7.94 |

| | |
|---|---|
| [router] Enrutadores de la red. | 6.24 |
| [wap] Access Point para acceso a la red WiFi. | 7.35 |
| [ipphone] Teléfonos IP de la facultad. | 7.12 |
| [wifi] Red Inalámbrica general de la FIEC, Redes privadas para uso de oficinas o departamentos. | 6.95 |
| [lan] Red cableada de la FIEC. | 6.06 |
| [disk] Discos de los equipos y servidores. | 7.65 |
| [san] Almacenamiento de información en la red de la FIEC. | 6.75 |
| [power] Fuentes de alimentación eléctrica de laboratorios, oficinas y cuarto de servidor. | 5.86 |
| [ups] UPS del servidor. | 4.23 |
| [ac] Sistemas de aires acondicionados de laboratorios y servidor. | 4.92 |
| [cabling][wire] Cables de red donde se realizan las comunicaciones. | 4.92 |
| [furniture] Armarios donde se guarda información física. | 4.22 |
| [site] Facultad de Ingeniería Electrica y Computación. | 4.63 |
| [building] Edificio donde se aloja el servidor. | 6.19 |
| [local] Cuarto donde se aloja el servidor. | 5.25 |

Para nuestro estudio no realizamos el proceso de análisis de riesgos para los siguientes activos:

- [SAP] – Existe un gran número de servicios ofrecidos por la facultad, los cuales se analizan con mayor detalle en otros activos.

- [EXT] – El único servicio externo es el de correo, el cual se analiza en otro servicio, la FIEC sólo se encarga de su disponibilidad.
- [UI],[ADM],[DES] – Realizar un análisis de personas es algo bastante complejo, y por las limitaciones de tiempo en nuestro estudio no se realiza.

Según los resultados obtenidos podremos definir una tabla de nivel de impacto, donde mostramos los activos que requerirán mayor atención.

TABLA 39 Nivel de impacto

| Valor | Nivel de Impacto | Detalles |
|---|---|---|
| Mayor a 0 y menor a 4 | Muy Bajo | El riesgo es mínimo |
| Mayor a 4 y menor a 8 | Bajo | El nivel de riesgo es bajo. |
| Mayor a 8 y menor a 14 | Medio | Existen fallas que requieren atención pronta. |
| Mayor a 14 y menor 19 | Alto | Existen fallas, requiere atención lo más pronto posible. |
| Entre 19 y 25 | Muy Alto | Fallas críticas, se requiere atención inmediata. |

Análisis de riesgos en el Software:

TABLA 40 Activo VS Impacto Determinado

| Activo | Impacto Determinado |
|---|---|
| Software de gestión de Correos | 6.63 |
| Software de Base de Datos | 6.84 |
| Software de Servicios Web | 6.84 |
| Antivirus | 5.84 |
| Software para Control de PCs | 6.42 |
| Servicio de DHCP | 6.89 |
| Software para streaming de video | 6.24 |
| Software para servidor RADIUS | 6.63 |

# CAPÍTULO 4

# 4. ANÁLISIS Y RESULTADOS

## 4.1. Medidas de protección

Para culminar nuestro estudio, presentaremos los activos analizados con un impacto mayor a 8 y sus respectivas recomendaciones.

- **[files] Archivos de los equipos de la fiec:**

  Pueden verse afectados de muchas formas, ya sea por errores del sistema, infección de malware, o por la persona mismo.

  Recomendaciones:

  Tener programas que protejan nuestro equipo, como un buen antivirus o simplemente configurar las políticas del firewall de Windows.

- **[int] Servicios internos ofrecidos a estudiantes y trabajadores:**

  Existen varios servicios en la FIEC, entre estos tenemos servicio de internet inalámbrico y uso de PCs en los laboratorios, estos se ven afectados en su disponibilidad por la utilización de recursos en actividades que no son de carácter académico, esto a su vez puede llevar a un agotamiento de los recursos.

  Recomendaciones:

  Inclusión de reglas en el uso de servicios, o realizar bloqueos de ciertos sitios en horas específicas, donde exista un gran uso de recursos para actividades académicas.

- **[pc] Equipos de escritorio de oficinas:**

  Un error detectado en el uso de computadores en las oficinas es el no cumplimiento de las políticas de seguridad, por lo que no existe un control en el software, programas que consumen demasiado recursos

de sistema y pueden provocar lentitud en los mismos.

Recomendaciones:

Capacitar al personal e influenciar en la adquisición de buenas costumbres, como por ejemplo la de “Pantalla limpia”, la cual consiste en bloquear equipos cuando no se lo tienen en uso, además, ofrecer una lista de software aprobado por la facultad para los posibles requerimientos que se tengan.

- **[pc] Equipos de escritorio de laboratorios:**

  Los equipos de los laboratorios son de uso de todos los estudiantes, por lo que son prospensos a posibles problemas. Estos equipos no cuentan con un software de congelamiento de la configuración. La infección de un equipo puede afectar a muchos usuarios. El uso continuo también reduce el tiempo de vida de los computadores. Por errores de usuarios existen casos donde sus sesiones, ya sean de cuentas de la universidad o redes sociales, quedan abiertas, dando apertura a la suplantación de identidad.

  Recomendaciones:

  Instalar software de congelación de configuración, no solucionaría problemas de infecciones de malware, pero los reduciría en gran medida. Para disminuir los problemas de sesiones abiertas, se puede capacitar a los usuarios a revisar los equipos antes de dejarlos y también configurar los navegadores para que eliminen todo tipo de información privada al cerrarse.

- **[peripheral] Impresoras y scanneres(all in one):**

  Los posibles problemas que puedan presentarse afectarían mayormente la disponibilidad, y el uso de las impresoras tiene mayor

demanda de uso en época de exámenes.

Recomendaciones:

Tener un control de uso cuando los requerimientos aumentan.

- **[std] Software estándar**

  Se realizó un estudio general del software de los servidores, los cuales proporcionan servicios a la facultad, y se determinó que ciertos programas se encuentran desactualizados, lo que podría provocar problemas de seguridad por la presencia de vulnerabilidades afectando la disponibilidad de los servicios que este ofrece.

  Recomendaciones:

  Analizar las posibles actualizaciones del software, de una forma que estos no afecten el desempeño del resto de programas presentes en el servidor.

## 4.2. Análisis técnico-económico

TABLA 41 Análisis Técnico Económico

| Empresas | Actividades | Honorarios | Monto | Plan de Facturación | |
|---|---|---|---|---|---|
| **DELOITTE** | Fase I: Planeación | Por diseño e Implementación del SGSI | U$S 205,500.00 | 1er.pago (10%) | ( Los honorarios mencionados no incluyen el IVA ni el impuesto a la renta, los cuales serán facturados a tasa vigente) |
| | Fase II: Diseño | | | 2do.pago (20%) | |
| | Fase III: Implementación | | | 3er. Pago (40%) | |
| **ELIXIRCORP.** | Planificación y Estudio | Consultoría especializada en seguridad de la | U$S 12,350.00 | Cuota Inicial (70%) | Gastos de viáticos corren por cuenta del |

| | | | | | |
|---|---|---|---|---|---|
| | Diagnóstico en Sitio | información + informe detallado y un plan de implementación recomendado | | Final (30%) | cliente |
| | Reportes e informes | | | | |
| **PROTIVITI** | Etapa I y II: Inicio y Planificación | Alcance e Implementación | U$S 139,500.00 | Inicio (25%) | (más IVA ) |
| | Etapa III: Ejecución | Acompañamiento del auditor | U$S 2,900.00 | Cuotas mensuales (60%) | (más IVA ) |
| | Etapa IV y V: Control y Cierre | | | Final (15%) | |
| **Consultora Warptech S.A.** | Planificación y Estudio | Consultoría especializada en seguridad de la información + informe detallado y un plan de implementación recomendado | U$S 8000 | Cuota Inicial (70%) | Gastos de viáticos corren por cuenta del cliente |
| | Diagnóstico en Sitio | | | Final (30%) | |
| | Reportes e informes | | | | |

# CONCLUSIONES Y RECOMENDACIONES

Luego de este estudio hemos llegado a las siguientes conclusiones y recomendaciones.

CONCLUSIONES:

1. ISO/IEC 27001:2013 es un estándar que se enfoca en la seguridad en el tratamiento de la información, además de ayudarnos a la creación de un SGSI.

2. La implementación de un SGSI permite una mejor administración de los recursos y servicios de la información, pues nos permitirá prevenir y reducir daños o fugas de información, así como recuperarse en poco tiempo luego de sufrir algún problema de cualquier tipo.

3. Determinamos que la sección de la FIEC en la cual realizamos nuestro estudio, no cumple con los requerimientos de la certificación ISO/IEC 27001:2013, al no existir políticas de seguridad documentadas, aun así, se considera que la red tiene un nivel alto de seguridad.

RECOMENDACIONES

1. Se debe crear un manual de políticas de seguridad, el cual debe ser de fácil acceso a todos los trabajadores de la facultad, este puede ser físico o digital.

2. La creación de una intranet podría ayudar a la difusión de la información no solo a nivel docente y estudiantil, sino también al personal técnico.

3. Se debe concientizar a todos los usuarios de los servicios, desde los estudiantes hasta los directivos acerca del tratamiento correcto de la información mediante políticas.

4. A pesar de que no exista un interés en adquirir la certificación ISO/IEC 27001:2013, es bastante recomendable que se trabaje en la implementación de un SGSI por motivos preventivos, ya que ha existido en los últimos meses bastante casos de fugas de información por parte de algunas organizaciones a nivel mundial.

5. Se debería aumentar el área de cobertura de la red inalámbrica segura, en ciertos sectores de la facultad donde no es posible conectarse a la misma, limitando al estudiante la disponibilidad de los servicios.

6. Según los resultados de este estudio, se debería en un plazo no mayor a 6 meses corregir las áreas determinadas de mayor afectación, y luego realizar otra auditoría.

# BIBLIOGRAFÍA

[1] U. H. &. U. Nayak, The InfoSec Handbook: An Introduction to Information Security, Rekha Umesh, 2014.

[2] D. Kosutic, 9 Steps to Cybersecurity, EPPS Services Ltd,Zagreb, 2012.

[3] Á. Cahn, «América Economía,» 22 08 2012. [En línea]. Available: http://www.americaeconomia.com/analisis-opinion/empresas-perder-el-negocio-por-el-mal-manejo-de-información.

[4] J. Gaudiosi, «Fortune,» 24 12 2014. [En línea]. Available: http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/.

[5] Univision, «Univision,» 03 03 2015. [En línea]. Available: http://notticias.univision.com/article/2261169/2015-03-03/estados-unidos/noticias/el-exdirector-de-la-cia-se-declara-culpable-por-mal-manejo-de-informacion. Consulta realizada en Junio del 2015.

[6] Huerta, Antonio, «Security ARTWORK,» 30 03 2012. [En línea]. Available: http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/.

[7] P. d. a. electrónica, «PAE,» [En línea]. Available: http://www.administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Medolog/pae_Magerit.html#.Vc2Rdyx_Oko.

[8] P. d. a. electrónica, «PAE,» [En línea]. Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[9] P. G. H, Getting an information security job, Canadá: John Wiley & Sons, Inc, 2015.

[10] SGSI, «SGSI,» 14 08 2013. [En línea]. Available: http://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/.

[11] 27001Academy, «27001Academy,» [En línea]. Available: http://advisera.com/27001academy/what-is-iso-27001/

[12] M. Rouse, «Search Security.in,» 2011. [En línea]. Available: http://searchsecurity.techtarget.in/definition/information-security-management-system-ISMS.

[13] "ISO/IEC 27001 - Information security management," [En linea]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

[14] M. Riveroll, «Emaze,» [En línea]. Available: https://www.emaze.com/@AOFTTLFO/Manual-del-SGSI.

[15] 27001Academy, «27001Academy,» [En línea]. Available: http://advisera.com/27001acade,u/es/que-es-iso-27001/.

[16] 27001Academy, «27001Academy,» [En línea]. Available: http://advisera.com/27001academy/what-is-iso-27001/ (Benefits of ISO 27001).

[17] FIEC, [En línea]. Available: https://www.fiec.espol.edu.ec/index.php/en/ubicacion-geografica/mapadelafacultad.

[18] 27001Academy, [En línea]. Available: http://advisera.com/27001academy/documentation/internal-audit-checklist-2/ .

[19] Ticcolombia, «Ticcolombia,» 05 09 2012. [En línea]. Available: http://ticcolombia.webnode.com.co/news/iso-9001/.

[20] «Implementacion SIG,» [En línea]. Available: http://implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-.

[21] ISO Org. (2013)ISOTools. [Online]. Available: https://www.isotools.org/pdfs/Monografico-ISO-27001-ISOTools.pdf

[22] PMG-SSI (2015, Abril) SSI. [Online]. Available: http://www.pmg-ssi.com/2015/04/iso-27001-implementacion-y-evaluacion/

[23] ISO 27001 (2013) [Online]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdf, Consulta realizada en julio del 2015.

# ANEXOS

## ANEXO 1: Glosario

ISMS.- es un conjunto de políticas que se ocupan de la seguridad de información o de TI riesgos relacionados.

Malware.- término informático que se utilice para referir a un intruso o software hostil.-

Cybercrimen.- se lo conoce como un delito informático, que se da por vías de red y tienen como objetivo dañar los ordenadores.

Magerit.- es una metodología que se utiliza para el análisis y Gestión de riesgos .

Integridad.- hace referencia a los datos correctos para que estos no sean modificados.

Confidencialidad.- es la protección de datos, informáticos, por lo que se garantiza el acceso a éstos tan solo por personal autorizado.

Disponibilidad.- es la condición o característica por la que la información debe estar disponible para personal autorizado(únicamente).

Seguridad de la Información.- es acerca de cómo mantener la confidencialidad, integridad y disponibilidad de la misma.// Mantener la información exenta de todo peligro o daño inaceptables.

ISO 9001.- es la base del sistema de Gestión de la Calidad , por lo que es una norma internacional que se centra en la administración de los elementos.

ISO 14001.- es el estándar internacional de Gestión Ambiental que se comenzó a publicar en 1996.

Activos.- según MAGERIT, los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por sus dirección.

Degradación.- pérdida de valor de un activo como consecuencia de la materialización de una amenaza.// Impacto que tiene la materialización de la amenaza en el activo.

Amenaza.- causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Análisis de Riesgos.- proceso sistemático para estimar la magnitud de los riesgos al que se expone la organización.

Ataque.- intento de destruir, exponer, alterar o inhabilitar un sistema o la información que éste maneja.

Riesgo.- estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios la organización.

Salvaguarda.- procedimiento o mecanismo tecnológico que reduce el riesgo.// Medida preventiva.

## ANEXO 2: Abreviaturas

ISO: Organización Internacional de Normalización.

IEC: Comisión Electrónica Internacional.

SGSI: Sistema de Gestión de Seguridad de la Información.

PDCA: Son sus siglas en inglés Plan-Do-Check-Act, llevado al español es Planificar-Hacer-Verificar-Actuar.

BSI: British Standards Institution (Entidad responsable de la publicación de importantes normas).

ISMS: Siglas en Inglés Information Security Management System.

## ANEXO 3: Tabla de Activos

| [D] Datos/Información |
| --- |
| [files] Archivos de los equipos de la FIEC<br>- Documentos de trabajo<br>- Correos electrónicos<br>- Exámenes<br>- Tareas digitales<br>- Material de estudio digital |
| [backup] Respaldos de información de servidores o archivos importantes<br>- Archivos de respaldo de los servidores<br>- Documentos importantes con cierto nivel de antigüedad |
| [conf] Datos de configuración de equipos y equipos de red<br>- Configuración de los servidores<br>- Configuración de los conmutadores<br>- Configuración de los enrutadores<br>- Configuración de los equipos de laboratorios<br>- Configuración de los equipos de docentes y trabajadores |
| [auth] Datos de autenticación para su uso en portal cautivo.<br>- Datos de autenticación de cuentas de usuario de FIEC |
| [log] Registro de actividades<br>- Registro de uso de equipos<br>- Registro de acceso a servidores<br>- Registro de uso de servicios<br>- Registro de actualización de software<br>- Registro de cambios en hardware<br>- Registro de problemas que se presenten en la red |
| [source] Código fuente de proyectos<br>- Código fuente de proyectos realizados dentro de la FIEC |

| |
|---|
| [exe] Ejecutables obtenidos de proyectos<br>- Ejecutables que se generen en los proyectos de la FIEC al culminar los proyectos |
| [test] Datos de prueba obtenidos en proyectos<br>- Información obtenida durante el proceso de creación de software en los diferentes proyectos de la facultad |

## ANEXO 4: Tabla de valoración de amenazas e impacto

Clave: Dim = Dimensión del problema, Deg = Degradación, Prob = Probabilidad, [C] =Confidencialidad, [I]=Integridad, [D]=Disponibilidad

| Activo | Amenaza | DIM | DEG | PROB | IMP |
|---|---|---|---|---|---|
| [files] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 2 | 10 |
| | [I.3] Contaminación mecánica | [D] | 2 | 2 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 3 | 15 |
| | [I.6] Corte de suministro eléctrico | [D] | 4 | 3 | 12 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 3 | 3 | 9 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 3 | 15 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 2 | 8 |
| | [E.4] Errores de configuración | [I] | 3 | 1 | 3 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 3 | 15 |
| | [E.19] Fugas de información | [C] | 5 | 2 | 10 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 2 | 8 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 4 | 2 | 8 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 2 | 8 |
| | [A.7] Uso no previsto | [I],[C],[D] | 2 | 1 | 2 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 8.89 |
| [backup] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 2 | 10 |
| | [I.3] Contaminación mecánica | [D] | 1 | 2 | 2 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 1 | 3 | 3 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 1 | 1 | 1 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 3 | 15 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 1 | 5 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 2 | 8 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 2 | 10 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 2 | 1 | 2 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 3 | 15 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 1 | 3 |
| | | | | | 7.22 |
| [conf] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 2 | 1 | 2 |
| | [I.1] Fuego | [D] | 2 | 1 | 2 |
| | [I.3] Contaminación mecánica | [D] | 1 | 2 | 2 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 4 | 3 | 12 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 4 | 3 | 12 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 3 | 2 | 6 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 2 | 2 | 4 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 3 | 15 |
| | [E.3] Errores de monitorización (log) | [I] | 3 | 2 | 6 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 4 | 2 | 8 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 4 | 2 | 8 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 3 | 2 | 6 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 7.42 |
| [auth] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 2 | 8 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 4 | 2 | 8 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 3 | 2 | 6 |
| | [E.2] Errores del administrador | [I],[C],[D] | 4 | 2 | 8 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 4 | 1 | 4 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 2 | 8 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 7.65 |
| [log] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 3 | 15 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 3 | 2 | 6 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 3 | 1 | 3 |
| | [E.2] Errores del administrador | [I],[C],[D] | 4 | 2 | 8 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 2 | 8 |
| | [E.19] Fugas de información | [C] | 3 | 2 | 6 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 2 | 8 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 3 | 2 | 6 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 1 | 4 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 2 | 10 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 1 | 3 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 4 | 1 | 4 |
| | | | | | 7.60 |
| [source] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 2 | 8 |
| | [I.3] Contaminación mecánica | [D] | 3 | 2 | 6 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 3 | 2 | 6 |
| | [I.6] Corte de suministro eléctrico | [D] | 2 | 2 | 4 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 2 | 2 | 4 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 4 | 2 | 8 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 3 | 15 |
| | [E.2] Errores del administrador | [I],[C],[D] | 3 | 1 | 3 |
| | [E.4] Errores de configuración | [I] | 2 | 2 | 4 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 2 | 8 |

| | | | | | |
|---|---|---|---|---|---|
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 2 | 8 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 4 | 2 | 8 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 2 | 8 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 4 | 1 | 4 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 1 | 4 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.32 |
| [exe] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 2 | 8 |
| | [I.3] Contaminación mecánica | [D] | 3 | 2 | 6 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 4 | 2 | 8 |
| | [I.6] Corte de suministro eléctrico | [D] | 4 | 2 | 8 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 2 | 2 | 4 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 2 | 10 |
| | [E.2] Errores del administrador | [I],[C],[D] | 3 | 2 | 6 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 2 | 8 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 2 | 8 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 1 | 4 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.69 |
| [test] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 4 | 2 | 8 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 1 | 5 |
| | [I.8] Falla de servicios de | [D] | 2 | 2 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | comunicaciones | | | | |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 2 | 8 |
| | [E.2] Errores del administrador | [I],[C],[D] | 3 | 2 | 6 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 4 | 2 | 8 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 3 | 1 | 3 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 3 | 2 | 6 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 1 | 4 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.25 |
| [int] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 2 | 10 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 3 | 12 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 3 | 15 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 3 | 15 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 3 | 2 | 6 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 3 | 12 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 2 | 8 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 1 | 5 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 3 | 15 |

| | | | | | |
|---|---|---|---|---|---|
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 3 | 15 |
| | [A.7] Uso no previsto | [I],[C],[D] | 5 | 4 | 20 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 9.95 |
| [email] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 3 | 1 | 3 |
| | [I.1] Fuego | [D] | 3 | 2 | 6 |
| | [I.3] Contaminación mecánica | [D] | 3 | 1 | 3 |
| | [I.4] Contaminación electromagnética | [D] | 2 | 1 | 2 |
| | [I.5] Avería de origen físico o lógico | [D] | 2 | 2 | 4 |
| | [I.6] Corte de suministro eléctrico | [D] | 3 | 2 | 6 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 3 | 2 | 6 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 2 | 10 |
| | [E.2] Errores del administrador | [I],[C],[D] | 3 | 2 | 6 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 2 | 8 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 3 | 1 | 3 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 3 | 1 | 3 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 1 | 4 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 3 | 3 | 9 |
| | [A.5] Suplantación de identidad del usuario(Docente, administrativo) | [C],[A],[I] | 5 | 2 | 10 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 3 | 9 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 5.81 |
| [host] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 2 | 10 |
| | [I.3] Contaminación mecánica | [D] | 4 | 1 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 1 | 2 | 2 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 1 | 4 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 7.15 |
| [pc] Interno | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 4 | 2 | 8 |
| | [I.6] Corte de suministro eléctrico | [D] | 4 | 2 | 8 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 4 | 2 | 8 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 3 | 15 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 3 | 2 | 6 |
| | [E.4] Errores de configuración | [I] | 5 | 3 | 15 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 3 | 15 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 2 | 8 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 3 | 9 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 8.35 |
| [pc] Labs | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 5 | 3 | 15 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 2 | 10 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 4 | 20 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 3 | 15 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 3 | 15 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 4 | 20 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 3 | 15 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 4 | 20 |
| | [E.19] Fugas de información | [C] | 5 | 3 | 15 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 3 | 15 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 5 | 3 | 15 |
| | [A.5] Suplantación de identidad del usuario(Docente, administrativo) | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 4 | 12 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 2 | 10 |
| | | | | | 12.38 |
| [backup] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |

| | | | | | |
|---|---|---|---|---|---|
| | [I.4] Contaminación electromagnética | [D] | 5 | 2 | 10 |
| | [I.5] Avería de origen físico o lógico | [D] | 4 | 2 | 8 |
| | [I.6] Corte de suministro eléctrico | [D] | 4 | 2 | 8 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 3 | 2 | 6 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 3 | 1 | 3 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 1 | 4 |
| | [E.19] Fugas de información | [C] | 3 | 1 | 3 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 3 | 1 | 3 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 3 | 1 | 3 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 4 | 1 | 4 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 3 | 1 | 3 |
| | [A.5] Suplantación de identidad del usuario(Docente, administrativo) | [C],[A],[I] | 3 | 1 | 3 |
| | [A.7] Uso no previsto | [I],[C],[D] | 5 | 1 | 5 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.05 |
| [peripheral] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 2 | 10 |
| | [I.3] Contaminación mecánica | [D] | 5 | 3 | 15 |
| | [I.4] Contaminación electromagnética | [D] | 2 | 2 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 3 | 15 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 3 | 15 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 2 | 8 |
| | [E.2] Errores del administrador | [I],[C],[D] | 4 | 1 | 4 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 1 | 4 |
| | [E.4] Errores de configuración | [I] | 5 | 3 | 15 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 3 | 1 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 3 | 15 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 2 | 6 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 8.44 |
| [bp] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 2 | 8 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 1 | 5 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 1 | 5 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 5 | 1 | 5 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.71 |
| [switch] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 2 | 10 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 2 | 8 |
| | [E.19] Fugas de información | [C] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 4 | 2 | 8 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 2 | 10 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 1 | 4 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 7.94 |
| [router] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 5 | 2 | 10 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 1 | 5 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 1 | 5 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 1 | 4 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.24 |
| [wap] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 2 | 8 |
| | [I.4] Contaminación | [D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | electromagnética | | | | |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 1 | 5 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 4 | 2 | 8 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 3 | 2 | 6 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 1 | 5 |
| | [E.4] Errores de configuración | [I] | 5 | 2 | 10 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 1 | 4 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 1 | 5 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 3 | 15 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 4 | 3 | 12 |
| | [A.5] Suplantación de identidad del usuario(Docente, administrativo) | [C],[A],[I] | 5 | 2 | 10 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 3 | 12 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 7.35 |
| [ipphone] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 3 | 2 | 6 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 2 | 8 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 1 | 4 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 2 | 10 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 2 | 8 |
| | [E.21] Errores de mantenimiento / Actualización | [I],[D] | 4 | 2 | 8 |

| | | | | | |
|---|---|---|---|---|---|
| | de programas | | | | |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 3 | 9 |
| | | | | | 7.12 |
| [wifi] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 3 | 2 | 6 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 3 | 15 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 1 | 5 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 1 | 5 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 2 | 8 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 2 | 10 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 1 | 5 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 3 | 3 | 9 |
| | [A.5] Suplantación de identidad del usuario(Docente, administrativo) | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 2 | 8 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.95 |
| [lan] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 3 | 1 | 3 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 1 | 5 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 1 | 5 |
| | [I.6] Corte de suministro eléctrico | [D] | 2 | 2 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 3 | 12 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 1 | 4 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 4 | 1 | 4 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 4 | 1 | 4 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 2 | 10 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 3 | 9 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.06 |
| [disk] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 5 | 3 | 15 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 2 | 10 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 4 | 2 | 8 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 4 | 2 | 8 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 2 | 8 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 1 | 4 |
| | [E.4] Errores de configuración | [I] | 4 | 1 | 4 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 1 | 5 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 4 | 1 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 2 | 8 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 7.65 |
| [san] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 1 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 1 | 5 |
| | [I.5] Avería de origen físico o lógico | [D] | 4 | 1 | 4 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 4 | 3 | 12 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 2 | 10 |
| | [E.3] Errores de monitorización (log) | [I] | 4 | 1 | 4 |
| | [E.4] Errores de configuración | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.20] Vulnerabilidades de los programas | [I],[C],[D] | 5 | 2 | 10 |
| | [E.21] Errores de mantenimiento / Actualización de programas | [I],[D] | 5 | 2 | 10 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 1 | 5 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 2 | 10 |
| | [A.7] Uso no previsto | [I],[C],[D] | 3 | 1 | 3 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.75 |
| [power] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 4 | 1 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 3 | 15 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 3 | 2 | 6 |
| | [E.2] Errores del administrador | [I],[C],[D] | 4 | 1 | 4 |
| | [E.3] Errores de monitorización | [I] | 4 | 1 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| | (log) | | | | |
| | [E.4] Errores de configuración | [I] | 4 | 2 | 8 |
| | [E.19] Fugas de información | [C] | 4 | 1 | 4 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 1 | 5 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 3 | 1 | 3 |
| | [A.7] Uso no previsto | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 5.86 |
| [ups] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 4 | 1 | 4 |
| | [I.3] Contaminación mecánica | [D] | 4 | 1 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 1 | 2 | 2 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 1 | 1 | 1 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 1 | 5 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 3 | 1 | 3 |
| | [E.19] Fugas de información | [C] | 4 | 1 | 4 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 4 | 1 | 4 |
| | [A.7] Uso no previsto | [I],[C],[D] | 4 | 1 | 4 |
| | | | | | 4.23 |
| [ac] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 3 | 3 | 9 |
| | [I.4] Contaminación electromagnética | [D] | 2 | 1 | 2 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 2 | 2 | 4 |
| | [E.2] Errores del administrador | [I],[C],[D] | 4 | 2 | 8 |
| | [E.4] Errores de configuración | [I] | 3 | 2 | 6 |
| | [A.7] Uso no previsto | [I],[C],[D] | 2 | 2 | 4 |
| | | | | | 6.30 |
| [wire] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 2 | 1 | 2 |
| | [I.4] Contaminación electromagnética | [D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 2 | 10 |
| | [I.6] Corte de suministro eléctrico | [D] | 3 | 1 | 3 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 2 | 2 | 4 |
| | [I.10] Degradación de los soportes de almacenamiento de información | [D] | 1 | 2 | 2 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 2 | 3 | 6 |
| | [E.2] Errores del administrador | [I],[C],[D] | 4 | 2 | 8 |
| | [E.19] Fugas de información | [C] | 3 | 1 | 3 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 2 | 1 | 2 |
| | | | | | 4.92 |
| [furniture] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 4 | 1 | 4 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 1 | 2 | 2 |
| | [I.4] Contaminación electromagnética | [D] | 1 | 1 | 1 |
| | [E.1] Errores de los usuarios | [I],[C],[D] | 5 | 2 | 10 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 4 | 1 | 4 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 3 | 1 | 3 |
| | [A.7] Uso no previsto | [I],[C],[D] | 1 | 4 | 4 |
| | | | | | 4.22 |
| [site] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 2 | 2 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 1 | 1 | 1 |
| | [I.6] Corte de suministro eléctrico | [D] | 3 | 1 | 3 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 4 | 1 | 4 |
| | | | | | 4.63 |
| [building] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 2 | 4 | 8 |
| | [I.4] Contaminación electromagnética | [D] | 2 | 1 | 2 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 2 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| | [E.1] Errores de los usuarios | [I],[C],[D] | 3 | 3 | 9 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 1 | 5 |
| | [E.8] Difusión de Software Dañino | [I],[C],[D] | 4 | 1 | 4 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [E.24] Caída del sistema por agotamiento de recursos | [D] | 5 | 1 | 5 |
| | [A.5] Suplantación de identidad del usuario(Estudiantes) | [C],[A],[I] | 3 | 2 | 6 |
| | [A.5] Suplantación de identidad del usuario(Docente, administrativo) | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 2 | 5 | 10 |
| | [A.8] Difusión de software dañino | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 6.19 |
| [local] | [N.7] Desastres Naturales – Fenómeno Sísmico | [D] | 5 | 1 | 5 |
| | [I.1] Fuego | [D] | 5 | 1 | 5 |
| | [I.3] Contaminación mecánica | [D] | 4 | 1 | 4 |
| | [I.4] Contaminación electromagnética | [D] | 4 | 1 | 4 |
| | [I.5] Avería de origen físico o lógico | [D] | 5 | 1 | 5 |
| | [I.6] Corte de suministro eléctrico | [D] | 5 | 2 | 10 |
| | [I.8] Falla de servicios de comunicaciones | [D] | 5 | 1 | 5 |
| | [E.2] Errores del administrador | [I],[C],[D] | 5 | 1 | 5 |
| | [E.3] Errores de monitorización (log) | [I] | 5 | 1 | 5 |
| | [E.19] Fugas de información | [C] | 5 | 1 | 5 |
| | [A.5] Suplantación de identidad del usuario | [C],[A],[I] | 5 | 1 | 5 |
| | [A.7] Uso no previsto | [I],[C],[D] | 5 | 1 | 5 |
| | | | | | 5.25 |

# ANEXO 5: Herramienta de trabajo (CheckList)

| **Referencias** | | | | **Resultados** |
|---|---|---|---|---|
| **Checklist** | | Sección | | |
| | ***A.5*** | ***Políticas de la seguridad de información*** | | |
| | A.5.1 | Dirección de gestión para seguridad de la información | | |
| | A.5.1.1 | Políticas para la Seguridad de la Información | 1.¿Existen políticas?<br>2.¿Estas políticas son conocidas? | |
| | A.5.1.2 | Revisión de políticas para seguridad de la información | 1.¿Las políticas son revisadas constantemente?<br>2.¿Las políticas son expuestas a revisión según las circunstancias? | |
| | ***A.6*** | ***Organización de la seguridad de la Información*** | | |
| | A.6.1 | Organización interna | | |
| | A.6.1.1 | Roles y responsabilidades en la seguridad de la información | ¿Las responsabilidades de protección cada activo y procesos específicos de seguridad están claramente identificados, definidos y comunicados a las partes pertinentes? | |
| | A.6.1.2 | Segregación de las tareas | ¿Cada área y función están debidamente separadas para reducir el riesgo de modificaciones no autorizadas o uso indebido de información o servicios? | |
| | A.6.1.3 | Contacto con las autoridades | 1.¿Existe un procedimiento documentado por el cual se indique cuándo y por quién se realizará la comunicación con las respectivas autoridades?<br><br>2. Existe un proceso que nos indique cuando este contacto es requerido? | |
| | A.6.1.4 | Contacto con grupos de interés especial | ¿Existe individuos dentro de la facultad con membrecías activas a grupos de interés especial relevantes? | |

| | | | | |
|---|---|---|---|---|
| | A.6.1.5 | Seguridad de Información en administración de proyectos | ¿Todos los proyectos pasan por alguna evaluación de seguridad de Información? | |
| | A.6.2 | Dispositivos Móviles y Tele trabajadores | | |
| | A.6.2.1 | Políticas para dispositivos móviles | 1.¿Existe políticas para uso de dispositivos móviles?<br><br>2.¿Esta política documenta aborda los riesgos que trae el uso de dispositivos móviles? | |
| | A.7 | Seguridad en Recursos Humanos | | |
| | A.7.1 | Previo a su empleo | | |
| | A.7.1.1 | Screening | ¿Se realiza una verificación de los antecedentes de los candidatos? | |
| | A.7.1.2 | Términos y Condiciones del empleo | 1 ¿Se requiere la firma de un acuerdo de confidencialidad en cuanto a información interna de la facultad? | |
| | A.7.2 | Durante el Empleo | | |
| | A.7.2.1 | Responsabilidades de administración | 1.¿Están todos los administradores comprometidos en mantener la seguridad dentro de la facultad? | |
| | A.7.2.2 | Concientización, educación y entrenamiento sobre Seguridad de la Información | Todos los empleados tienen capacitación constante referente a la seguridad de la información en su respectivo rol en la facultad? | |
| | A.7.2.3 | Procesos Disciplinarios | 1.¿Existe procesos disciplinarios para quien provoque una fuga de información?<br>2. ¿Estos procesos se hacen conocer a los trabajadores? | |
| | A.7.3 | Terminación y cambio de empleo | | |

| | | | | |
|---|---|---|---|---|
| | A.7.3.1 | Terminación o cambio de las responsabilidades del empleado | 1.¿Existe procesos documentados para la terminación o cambio de las responsabilidades del empleado?<br>2.¿La facultad tiene como hacer cumplir estos procesos? | |
| | A.8 | Gestión de Bienes | | |
| | A.8.1 | Responsabilidad para los bienes | | |
| | A.8.1.1 | Inventario de Bienes | 1. ¿Existe un inventario de todos los bienes asociados con la información e instalaciones de procesamiento de información?<br>2. ¿Este inventario es actualizado constantemente? | |
| | A.8.1.2 | Propiedad de los bienes | Todos los bienes deben poseer un propietario definido, quien será responsable de este. | |
| | A.8.1.3 | Uso aceptable de los bienes | 1. ¿Existe una política sobre el uso aceptable de los tipos de bienes de información?<br>2. ¿Se comunica de esta política a los usuarios? | |
| | A.8.1.4 | Retorno de los bienes | ¿Existe una política que garantice el retorno de los bienes cuando se da por culminado el empleo, contrato o acuerdo? | |
| | A.8.2 | Clasificación de la Información | | |
| | A.8.2.1 | Clasificación de la Información | 1. ¿Existe una política que gobierne la clasificación de la información?<br>2. ¿Existe un proceso en el cual toda la información pueda ser clasificada de forma apropiada? | |
| | A.8.2.2 | Etiquetado de la información | ¿Existe un procedimiento en el cual se garantice que cada bien sea marcado de forma correcta según su clasificación de Información? | |

| | | | | |
|---|---|---|---|---|
| | A.8.2.3 | Manipulación de los bienes | 1. ¿Existe un proceso para el manejo de cada clase de información?<br>2. ¿Los usuarios de estos bienes de información saben acerca de estos procesos? | |
| | A.8.3 | Manejo de Medios | | |
| | A.8.3.1 | Manejo de medios extraíbles | 1. ¿Existen políticas referentes a medios extraíbles?<br>2.¿Existen procesos sobre el manejo de medios extraíbles?<br>3. ¿Esto es informado a usuarios de medios extraíbles? | |
| | A.8.3.2 | Desecho de medios | ¿Existe un procedimiento formal en cuanto a desechos de medios? | |
| | A.8.3.3 | Transferencia de medios físicos | 1. ¿Existen políticas documentadas de como los medios físicos deban ser transportados?<br>2. ¿Los medios transportados poseen métodos para evitar el acceso no autorizado, uso indebido o corrupción de su información? | |
| | A.9 | Control de Acceso | | |
| | A.9.1 | Requerimientos del negocio para control de acceso | | |
| | A.9.1.1 | Políticas de control de Acceso | 1. ¿Existen políticas de control de acceso?<br>2. Estas políticas se basan en los requerimientos de la facultad?<br>3. Estas políticas son comunicadas? | |
| | A.9.1.2 | Acceso a la red y servicios de la red | ¿Existen controles para que los usuarios solo puedan acceder a los recursos de red que están autorizados y que son requeridos para sus tareas? | |
| | A.9.2 | Administración de acceso de usuarios | | |

| | | | | |
|---|---|---|---|---|
| | A.9.2.1 | Registro y de-registro de Usuarios | ¿Existe un proceso formal de registro de usuarios? | |
| | A.9.2.2 | Provisión de acceso a usuarios | ¿Existe un proceso formal de provisión de acceso a usuarios para asignar permisos de acceso para todo tipo de usuario y servicio? | |
| | A.9.2.3 | Administración de permisos de acceso privilegiados | ¿Las cuentas de acceso privilegiados son administradas y controladas de manera separada? | |
| | A.9.2.4 | Administración de información de autenticación secreta de usuarios | ¿Existe un proceso formal para controlar la información de autenticación secreta a usuarios? | |
| | A.9.2.5 | Revisión de permisos de acceso de usuarios | 1. Existe un proceso para que los dueños de los bienes puedan revisar los permisos de acceso a sus bienes?<br>2. Este proceso de revisión es verificado? | |
| | A.9.2.6 | Retiro o ajustes de permisos de acceso | ¿Existe un proceso para asegurar el retiro de los permisos de acceso en la terminación de empleo, o los ajustes necesarios en el caso de un cambio de rol? | |
| | A.9.3 | Responsabilidades de usuarios | | |
| | A.9.3.1 | Uso de información de autenticación secreta | 1. ¿Existe políticas que cubran las prácticas sobre cómo la información de autenticación secreta deba manejarse?<br>2. ¿Se comunican a todos los usuarios? | |
| | A.9.4 | Control de Acceso de sistema y aplicaciones | | |

| | | | | |
|---|---|---|---|---|
| | A.9.4.1 | Restricciones de acceso a la información | Es el acceso de la información y restricciones de las funciones de aplicación de sistema en línea con las políticas de control de acceso? | |
| | A.9.4.2 | Proceso de inicio de sesión seguro | Donde las políticas de control de acceso lo requieren, el acceso es controlado por un proceso de inicio de sesión seguro? | |
| | A.9.4.3 | Sistema de administración de contraseña | Es requisito tener contraseñas complejas? | |
| | A.9.4.4 | Uso de programas utilitarios privilegiados | Se monitorea y restringe el uso de programas utilitarios privilegiados? | |
| | A.9.4.5 | Control de acceso a código fuente de programas | El acceso al código fuente de los programas se mantiene protegido? | |
| | A.10 | Criptografía | | |
| | A.10.1 | Controles Criptográficos | | |
| | A.10.1.1 | Políticas de uso de controles criptográficos | ¿Existe una política en el uso de controles criptográficos? | |
| | A.10.1.2 | Administración de llaves | ¿Existe una política que gobierna el tiempo de vida de llaves de cifrado? | |
| | A.11 | Seguridad Física y Ambiental | | |
| | A.11.1 | Áreas seguras | | |

| | | | | |
|---|---|---|---|---|
| | A.11.1.1 | Perímetros de seguridad física | 1.¿Existe un perímetro de seguridad designado?<br>2. ¿Áreas con información critica o sensitiva están segregadas y controladas? | |
| | A.11.1.2 | Controles de entrada física | Las áreas seguras poseen un sistema adecuado de control de ingreso para que solo personal autorizado tenga acceso? | |
| | A.11.1.3 | Seguridad de oficinas, habitaciones e instalaciones | 1. ¿Las oficinas fueron diseñadas pensando primero en seguridad?<br>2. ¿Existen procesos para mantener seguridad?(bloqueo de equipos, escritorios limpios). | |
| | A.11.1.4 | Protegiendo de amenazas externas y ambientales | ¿Se han diseñado medidas de protección física para la prevención de desastres naturales, ataques maliciosos, o accidentes? | |
| | A.11.1.5 | Trabajando en áreas seguras | 1. ¿Existen áreas seguras?<br>2. ¿Existen políticas para estas áreas? | |
| | A.11.1.6 | Áreas de entrega y descarga | 1. ¿Existen áreas separadas para entrega y descargas?<br>2. ¿Se controla el acceso a estas áreas?<br>3. ¿El acceso de estas áreas está aislada de instalaciones de procesamiento de información? | |
| | A.11.2 | Equipos | | |
| | A.11.2.1 | Protección y localización de equipos | 1. ¿Se identifican los posibles riesgos ambientales cuando se escoge la localización de equipos?<br>2. ¿Se considera el riesgo de acceso no autorizado cuando se escoge la localización de equipos? | |

| | | | | |
|---|---|---|---|---|
| | A.11.2.2 | Utilidades de soporte | 1. Existe un UPS o generador en caso de corte de energía?<br>2. ¿Se los han probado en un tiempo apropiado? | |
| | A.11.2.3 | Seguridad de cableado | 1. ¿Se han valorado los riesgos en la localización de los cables eléctricos y de telecomunicaciones?<br>2. ¿Se han localizado para protegerlos de interferencia, intercepción o daño? | |
| | A.11.2.4 | Mantenimiento de equipos | ¿Hay una programación rigurosa para el mantenimiento de equipos? | |
| | A.11.2.5 | Retiro de bienes | 1. ¿Existe un proceso definido para el retiro de los bienes?<br>2. ¿Se refuerzan estos procesos? | |
| | A.11.2.6 | Seguridad de equipos y bienes fuera de las instalaciones | 1. ¿Existe una política para mantener la seguridad de los equipos fuera de las instalaciones?<br>2. ¿Estas políticas se hacen conocer? | |
| | A.11.2.7 | Eliminación segura o reutilización de equipos | 1. ¿Existe una política de cómo se pueden reutilizar los bienes de información pueden ser reutilizados?<br>2. ¿Cuando la información de un medio es eliminada, se verifica esto antes de su reutilización? | |
| | A.11.2.8 | Equipos de usuario desatendidos | 1. ¿La facultad posee políticas de cómo mantener la seguridad de equipos desatendidos?<br>2. ¿Existen controles para asegurar un equipo que ha sido involuntariamente desatendido? | |
| | A.11.2.9 | Políticas de escritorio limpio y pantalla limpia | 1. ¿Existe una política de Escritorio Limpio/Pantalla Limpia?<br>2. ¿Se refuerza esta política? | |

| | | | | |
|---|---|---|---|---|
| | A.12 | Seguridad de Operaciones | | |
| | A.12.1 | Procedimientos y responsabilidades operacionales | | |
| | A.12.1.1 | Procedimientos operativos documentados | 1. ¿Los procedimientos operativos están bien documentados?<br>2. ¿Los procedimientos están disponibles para los usuarios que lo necesiten? | |
| | A.12.1.2 | Administración de cambios | ¿Se mantiene un ambiente controlado cuando existe algún tipo de cambio durante algún proceso? | |
| | A.12.1.3 | Administración de capacidad | ¿Existe un control en cuanto a la utilización de recursos? | |
| | A.12.1.4 | Separación de ambientes de desarrollo, pruebas y operacionales | ¿La facultad refuerza la segregación de los ambientes de desarrollo, pruebas y operaciones? | |
| | A.12.2 | Protección contra Malware | | |
| | A.12.2.1 | Control contra Malware | 1. ¿Existen procesos para detección de Malware?<br>2. ¿Existen procesos de prevención contra Malware?<br>3. ¿La facultad posee la capacidad de recuperarse de una infección de Malware? | |
| | A.12.3 | Respaldos | | |
| | A.12.3.1 | Respaldo de Información | 1. ¿Existe una política para respaldos?<br>2. ¿Los respaldos según lo indica esta política?<br>3. ¿Los respaldos son revisados? | |
| | A.12.4 | Registros y monitoreo | | |
| | A.12.4.1 | Registro de Eventos | ¿Se mantienen y revisan regularmente los registros de eventos? | |

| | | | | |
|---|---|---|---|---|
| | A.12.4.2 | Protección de la información de los registros | ¿Las instalaciones de registro están protegidas contra manipulación y acceso no autorizado? | |
| | A.12.4.3 | Registro de administradores y operadores | ¿Los registros de SysAdmin/ Sysop son mantenidos, protegidos y revisados regularmente? | |
| | A.12.4.4 | Sincronización de relojes | ¿Los relojes de los equipos de la facultad están sincronizados? | |
| | A.12.5 | Control de Software operacional | | |
| | A.12.5.1 | Instalación de Software en sistemas operacionales | ¿Existe un sistema para controlar la instalación de software en los sistemas operacionales? | |
| | A.12.6 | Administración de vulnerabilidades técnicas | | |
| | A.12.6.1 | Administración de vulnerabilidades técnicas | 1. ¿La facultad posee información actualizada sobre vulnerabilidades técnicas?<br>2. ¿Existe algún tipo de proceso de evaluación y reacción de los riesgos ante una nueva vulnerabilidad que se encuentre? | |
| | A.12.6.2 | Restricción en instalación de software | ¿Existen procesos para restringir la instalación de software por parte de los usuarios? | |
| | A.12.7 | Consideraciones para auditar los Sistemas de información | | |
| | A.12.7.1 | Controles para auditar los Sistemas de Información | ¿Los Sistemas de Información están sujetos a auditorias? | |
| | A.13 | Seguridad de comunicaciones | | |

| | | | | |
|---|---|---|---|---|
| | A.13.1 | Administración de la seguridad de la red | | |
| | A.13.1.1 | Controles de la red | ¿Existe una administración de la red? | |
| | A.13.1.2 | Seguridad de los servicios de la red | ¿La facultad implementa un enfoque de gestión de riesgos que identifique todos los servicios de la red? | |
| | A.13.1.3 | Segregación en las redes | ¿La topología de la red mantiene una segregación de las diferentes redes según su tipo y requerimientos? | |
| | A.13.2 | Transferencia de Información | | |
| | A.13.2.1 | Políticas y procedimientos para la transferencia de información | 1. ¿Las políticas internas gobiernan la forma en cómo la información es transferida?<br>2. Estos procedimientos están disponibles para el personal?<br>3. Existen controles técnicos para prevenir la transferencia no autorizada de información? | |
| | A.13.2.2 | Acuerdos sobre transferencia de información | Los contratos con agentes externos, y acuerdos dentro de la facultad detallan los requerimientos para una transferencia segura de la información? | |
| | A.13.2.3 | Mensajería electrónica | Las políticas de seguridad cubren la transferencia de información mediante mensajería electrónica? | |
| | A.13.2.4 | Acuerdos de confidencialidad y no divulgación | 1. Los trabajadores firman acuerdos de confidencialidad y no divulgación?<br>2. Estos acuerdos están sujetos a revisiones?<br>3. Se mantienen registros de los acuerdos? | |
| | A.14 | Adquisición, desarrollo y mantenimiento de sistemas | | |

| | | | | |
|---|---|---|---|---|
| | A.14.1 | Requerimientos de seguridad de los sistemas de información | | |
| | A.14.1.1 | Análisis y especificaciones de los requerimientos de los sistemas de información | 1. Los requerimientos de seguridad son especificados cuando un nuevos sistema es introducido?<br>2. Cuando sistemas son actualizados o mejorados, se especifican los requerimientos de seguridad? | |
| | A.14.1.2 | Seguridad de servicios de aplicaciones en redes publicas | Las aplicaciones que envían información por medio de redes públicas protegen la información de actividad fraudulenta, divulgación no autorizada o modificaciones no autorizadas? | |
| | A.14.1.3 | Protección de las transacción de los servicios de aplicación | Existen controles para prevenir transmisiones incompletas, alteración del mensaje, divulgación, o duplicación del mensaje? | |
| | A.14.2 | Seguridad en desarrollo y procesos de soporte | | |
| | A.14.2.1 | Políticas de seguridad en desarrollo | 1. Se desarrolla software dentro de la facultad?<br>2. De ser el caso, existen políticas que ordenen la implementación y valoración de controles de seguridad? | |
| | A.14.2.2 | Procedimientos para el control de cambios en el sistema | Existe un procedimiento formal para el control de cambios? | |
| | A.14.2.3 | Revisión técnica de las aplicaciones después de un cambio en las plataformas operativas | Existe un proceso para asegurar una revisión técnica se realice cuando la plataforma operativa sea cambiada? | |
| | A.14.2.4 | Restricciones sobre cambios a los paquetes de software | Existe una política sobre cómo y cuando los paquetes de software pueden ser cambiados? | |

| | | | | |
|---|---|---|---|---|
| | A.14.2.5 | Principios de ingeniera de sistemas seguros | La facultad posee principios documentados sobre como los sistemas pueden ser diseñados para asegurar seguridad? | |
| | A.14.2.6 | Ambiente de desarrollo seguro | 1. Se ha definido un ambiente de desarrollo seguro?<br>2. Todos los proyectos usan un ambiente de desarrollo seguro durante el proceso de desarrollo del sistema? | |
| | A.14.2.7 | Desarrollo tercerizado | 1. Se supervisa el desarrollo tercerizado de software?<br>2. El código externo es sujeto a una revisión de seguridad antes de ser implementado? | |
| | A.14.2.8 | Pruebas de sistema de seguridad | Donde se realiza el proceso de desarrollo, se realizan pruebas de seguridad como parte del proceso de desarrollo? | |
| | A.14.2.9 | Pruebas de aceptación de sistema | Existe un proceso establecido para aceptar nuevos sistemas/aplicaciones, o actualizaciones para uso de la producción? | |
| | A.14.3 | Datos de prueba | | |
| | A.14.3.1 | Protección de datos de prueba | 1. Existe un proceso para selección de estos datos?<br>2. Los datos de prueba están adecuadamente protegidos? | |
| | A.15 | Relación con proveedores | | |
| | NO APLICA EN ESTE CASO | | | |
| | A.16 | Gestión de incidentes de la seguridad de Información | | |
| | A.16.1 | Gestión de incidentes de la seguridad de información y mejoras | | |

| | | | | |
|---|---|---|---|---|
| | A.16.1.1 | Responsabilidades y procedimientos | Las responsabilidades de los administradores están claramente identificadas y documentadas en los procesos de gestión de incidentes? | |
| | A.16.1.2 | Reportar eventos de seguridad de información | 1. Existe un proceso para el reporte oportuno de eventos de seguridad de información?<br>2. Existe un proceso para revisar y actuar en base a los eventos de seguridad de información reportados? | |
| | A.16.1.3 | Reportar debilidades de la seguridad de información | 1. Existe un proceso para reportar debilidades de seguridad de información?<br>2. Este proceso es comunicado?<br>3. Existe un proceso para revisar y tratar estos reportes de manera oportuna? | |
| | A.16.1.4 | Evaluación de y decisiones sobre eventos de seguridad de información | Existe un proceso para asegurar que los eventos de la seguridad de información son evaluados y clasificados? | |
| | A.16.1.5 | Respuestas a incidentes de seguridad de información | Existe un proceso que refleje la clasificación y severidad de incidentes de la seguridad de información? | |
| | A.16.1.6 | Aprendizaje sobre incidentes de seguridad de información | Existe un proceso por el cual la facultad pueda aprender sobre incidentes pasados de la seguridad de la información para reducir el impacto o probabilidad de que vuelva a suceder en el futuro? | |
| | A.16.1.7 | Recolección de evidencia | 1. Existe una política de disposición forense?<br>2. En el caso de un evento de la seguridad de información, la información relevante es adquirida de forma que pueda ser usada como evidencia? | |
| | A.17 | Aspectos de la seguridad de la información de la gestión de continuidad del negocio | | |
| | A.17.1 | Continuidad de la seguridad de la información | | |

| | | | | |
|---|---|---|---|---|
| | A.17.1.1 | Planeación de continuidad de seguridad de la información | La seguridad de la información se incluye en los planes de continuidad de la facultad? | |
| | A.17.1.2 | Implementación de continuidad de seguridad de información | Existen procesos documentados, implementados y mantenidos sobre cómo mantener la continuidad de un servicio en situaciones adversas? | |
| | A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Los planes de continuidad son constantemente revisados y evaluados? | |
| | A.17.2 | Redundancias | | |
| | A.17.2.1 | Disponibilidad de las instalaciones de seguridad de la información | Las instalaciones de procesamiento de información poseen la suficiente redundancia para cumplir con los requisitos de disponibilidad de la facultad? | |
| | A.18 | Conformidad | | |
| | A.18.1 | Conformidad con los requerimientos legales y contractuales | | |
| | A.18.1.1 | Identificación de la legislación aplicable y requerimientos contractuales | La facultad ha identificado y documentado todos los requerimientos legislativos, regulatorios o contractuales relacionados a la seguridad? | |
| | A.18.1.2 | Derechos de propiedad Intelectual | 1. La facultad posee un registro de todos los derechos de propiedad intelectual y uso de software propietario? 2. La facultad monitorea el uso de software sin licencia? | |
| | A.18.1.3 | Protección de registros | Los registros son protegidos de perdida, destrucción, falsificación, o acceso no autorizado? | |

| | | | | |
|---|---|---|---|---|
| | A.18.1.4 | Privacidad y protección de información de identificación personal | 1. La información personal es identificada y clasificada de forma apropiada?<br>2. La información personal es protegida de acuerdo a las legislaciones relevantes? | |
| | A.18.1.5 | Regulación de controles criptográficos | Los controles criptográficos están protegidos de acuerdo a los acuerdos, legislaciones y regulaciones relevantes? | |
| | A.18.2 | Revisión de la seguridad de la información | | |
| | A.18.2.1 | Revisión independiente de la seguridad de la información | 1. Es el enfoque de la facultad de someter la administración de la seguridad de la información a revisiones independientes?<br>2. Es la implementación de controles de seguridad sujeto a revisiones independientes regulares? | |
| | A.18.2.2 | Conformidad con políticas y estándares de seguridad | 1. La facultad instruye a los administradores de realizar regularmente revisiones de conformidad con las políticas y procedimientos dentro de su área de responsabilidad?<br>2. Los registros de estas revisiones son mantenidos? | |
| | A.18.2.3 | Revisión de conformidad técnica | La facultad realiza regularmente revisiones de conformidad técnica de sus sistemas de información? | |

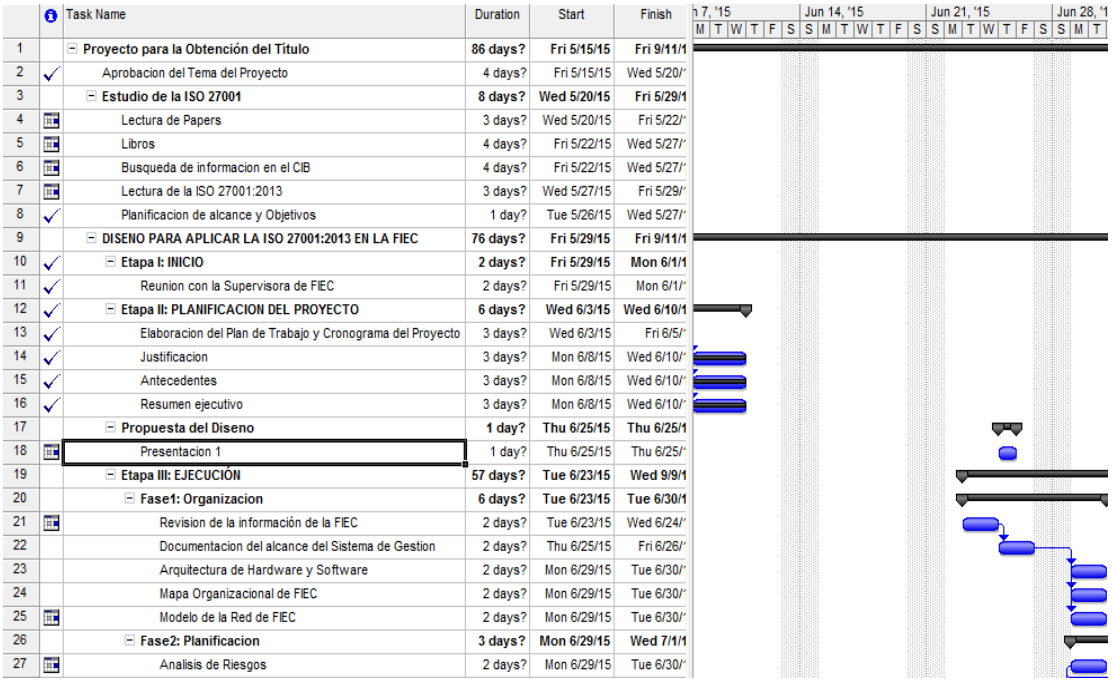
## ANEXO 6: Diagrama de Gantt

| Secuencia de la Elaboracion del Proyecto de Tesis | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | *Mayo* | | | *Junio* | | | | *Julio* | | | | | *Agosto* | | | | *Septiembre* | | | | | | |
| Tareas | Responsables | Actividades | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | | | | | |
| A | Jorge R.-Pamela Z. | Búsqueda de Información, revistas, papers, ISO 27001:2013 | x | x | | | | | | | | | | | | | | | | | | | | | |
| B | Ing.Rayner D.-Jorge R.-Pamela | Titulo del Proyecto y Expectativas | | | x | | | | | | | | | | | | | | | | | | | | |
| C | Pamela Z. - Jorge R. | Elaboración de Objetivos, Justificación, Metodología, Antecedentes | | | | x | x | | | | | | | | | | | | | | | | | | |
| D | Pamela Z. - Jorge R. | Desarrollo del Resumen Ejecutivo, Alcances y Restricciones | | | | | | x | | | | | | | | | | | | | | | | | |
| E | Pamela Z. - Jorge R. | Cronograma de Tareas Proyect, Diagrama de Gantt General | | | | | | x | | | | | | | | | | | | | | | | | |
| F | Jorge R. -Pamela Z. | Desarrollo del Capitulo 2 y Formato tipo Tesis de lo elaborado (Act) | | | | | | x | x | | | | | | | | | | | | | | | | |
| G | Ing.Jose P. -Jorge R. - Pamela | Presentación Formal de la Propuesta | | | | | | | x | | | | | | | | | | | | | | | | |
| H | Pamela Z. | Termino del Cap.2 / Inicio del Cap.3 | | | | | | | x | x | | | | | | | | | | | | | | | |
| I | Ing. Margarita F. -Jorge R. | Desarrollo del Diseno correspondiente al cap.3 | | | | | | | | x | x | | | | | | | | | | | | | | |
| J | Ing.Jose P. -Jorge R. - Pamela | Presentacion Media del Proyecto ( Parcial ) | | | | | | | | | x | | | | | | | | | | | | | | |
| K | Jorge R. -Pamela Z. | Correcciones/ Capitulo 3- Detalles y estudio | | | | | | | | | x | x | x | | | | | | | | | | | | |
| I | Jorge R. | Término del Cap.3 / Inicio del Cap.4 | | | | | | | | | | | | x | | | | | | | | | | | |
| M | Jorge R. -Pamela Z. | Desarrollo cap.4 / Recomendaciones | | | | | | | | | | | | | x | x | x | | | | | | | | |
| N | Jorge R. -Pamela Z. | Formato Formal y Formato Tipo Tesis | | | | | | | | | | | | | | | | x | | | | | | | |
| O | Ing.Jose P. -Jorge R. - Pamela | Presentacion presta a Correcciones | | | | | | | | | | | | | | | | x | x | | | | | | |
| P | Ing.Jose P. -Jorge R. - Pamela | Presentacion Final | | | | | | | | | | | | | | | | | | x | | | | | |

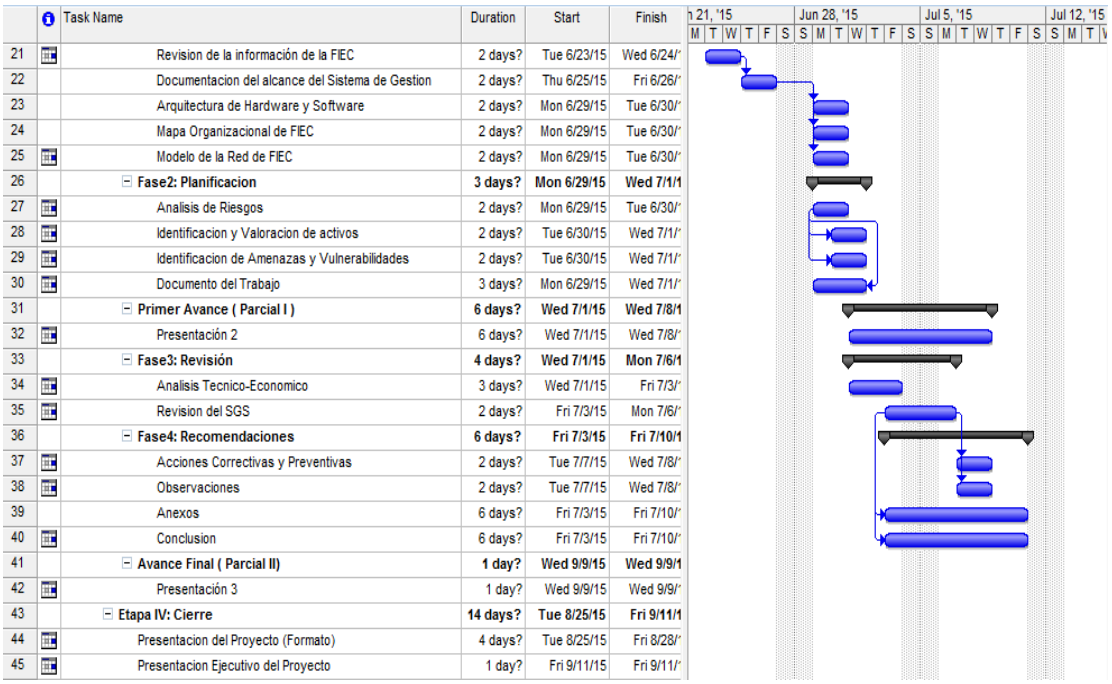
| | |
|---|---|
| Alumnos responsables del Proyecto | |
| Primera pesentacion del proyecto | |
| Intervención de los Ingenieros | |

*Todas las tareas son Independientes, ninguna depende de otra para ser terminada.

# ANEXO 7: Cronograma de Trabajo



| | Task Name | Duration | Start | Finish |
|---|---|---|---|---|
| 1 | **Proyecto para la Obtención del Título** | **86 days?** | **Fri 5/15/15** | **Fri 9/11/1** |
| 2 | Aprobacion del Tema del Proyecto | 4 days? | Fri 5/15/15 | Wed 5/20/ |
| 3 | **Estudio de la ISO 27001** | **8 days?** | **Wed 5/20/15** | **Fri 5/29/1** |
| 4 | Lectura de Papers | 3 days? | Wed 5/20/15 | Fri 5/22/ |
| 5 | Libros | 4 days? | Fri 5/22/15 | Wed 5/27/ |
| 6 | Busqueda de informacion en el CIB | 4 days? | Fri 5/22/15 | Wed 5/27/ |
| 7 | Lectura de la ISO 27001:2013 | 3 days? | Wed 5/27/15 | Fri 5/29/ |
| 8 | Planificacion de alcance y Objetivos | 1 day? | Tue 5/26/15 | Wed 5/27/ |
| 9 | **DISENO PARA APLICAR LA ISO 27001:2013 EN LA FIEC** | **76 days?** | **Fri 5/29/15** | **Fri 9/11/1** |
| 10 | **Etapa I: INICIO** | **2 days?** | **Fri 5/29/15** | **Mon 6/1/1** |
| 11 | Reunion con la Supervisora de FIEC | 2 days? | Fri 5/29/15 | Mon 6/1/ |
| 12 | **Etapa II: PLANIFICACION DEL PROYECTO** | **6 days?** | **Wed 6/3/15** | **Wed 6/10/1** |
| 13 | Elaboracion del Plan de Trabajo y Cronograma del Proyecto | 3 days? | Wed 6/3/15 | Fri 6/5/ |
| 14 | Justificacion | 3 days? | Mon 6/8/15 | Wed 6/10/ |
| 15 | Antecedentes | 3 days? | Mon 6/8/15 | Wed 6/10/ |
| 16 | Resumen ejecutivo | 3 days? | Mon 6/8/15 | Wed 6/10/ |
| 17 | **Propuesta del Diseno** | **1 day?** | **Thu 6/25/15** | **Thu 6/25/1** |
| 18 | Presentacion 1 | 1 day? | Thu 6/25/15 | Thu 6/25/ |
| 19 | **Etapa III: EJECUCIÓN** | **57 days?** | **Tue 6/23/15** | **Wed 9/9/1** |
| 20 | **Fase1: Organizacion** | **6 days?** | **Tue 6/23/15** | **Tue 6/30/1** |
| 21 | Revision de la información de la FIEC | 2 days? | Tue 6/23/15 | Wed 6/24/ |
| 22 | Documentacion del alcance del Sistema de Gestion | 2 days? | Thu 6/25/15 | Fri 6/26/ |
| 23 | Arquitectura de Hardware y Software | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 24 | Mapa Organizacional de FIEC | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 25 | Modelo de la Red de FIEC | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 26 | **Fase2: Planificacion** | **3 days?** | **Mon 6/29/15** | **Wed 7/1/1** |
| 27 | Analisis de Riesgos | 2 days? | Mon 6/29/15 | Tue 6/30/ |



| | Task Name | Duration | Start | Finish |
|---|---|---|---|---|
| 21 | Revision de la información de la FIEC | 2 days? | Tue 6/23/15 | Wed 6/24/ |
| 22 | Documentacion del alcance del Sistema de Gestion | 2 days? | Thu 6/25/15 | Fri 6/26/ |
| 23 | Arquitectura de Hardware y Software | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 24 | Mapa Organizacional de FIEC | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 25 | Modelo de la Red de FIEC | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 26 | **Fase2: Planificacion** | **3 days?** | **Mon 6/29/15** | **Wed 7/1/1** |
| 27 | Analisis de Riesgos | 2 days? | Mon 6/29/15 | Tue 6/30/ |
| 28 | Identificacion y Valoracion de activos | 2 days? | Tue 6/30/15 | Wed 7/1/ |
| 29 | Identificacion de Amenazas y Vulnerabilidades | 2 days? | Tue 6/30/15 | Wed 7/1/ |
| 30 | Documento del Trabajo | 3 days? | Mon 6/29/15 | Wed 7/1/ |
| 31 | **Primer Avance ( Parcial I )** | **6 days?** | **Wed 7/1/15** | **Wed 7/8/1** |
| 32 | Presentación 2 | 6 days? | Wed 7/1/15 | Wed 7/8/ |
| 33 | **Fase3: Revisión** | **4 days?** | **Wed 7/1/15** | **Mon 7/6/1** |
| 34 | Analisis Tecnico-Economico | 3 days? | Wed 7/1/15 | Fri 7/3/ |
| 35 | Revision del SGS | 2 days? | Fri 7/3/15 | Mon 7/6/ |
| 36 | **Fase4: Recomendaciones** | **6 days?** | **Fri 7/3/15** | **Fri 7/10/1** |
| 37 | Acciones Correctivas y Preventivas | 2 days? | Tue 7/7/15 | Wed 7/8/ |
| 38 | Observaciones | 2 days? | Tue 7/7/15 | Wed 7/8/ |
| 39 | Anexos | 6 days? | Fri 7/3/15 | Fri 7/10/ |
| 40 | Conclusion | 6 days? | Fri 7/3/15 | Fri 7/10/ |
| 41 | **Avance Final ( Parcial II)** | **1 day?** | **Wed 9/9/15** | **Wed 9/9/1** |
| 42 | Presentación 3 | 1 day? | Wed 9/9/15 | Wed 9/9/ |
| 43 | **Etapa IV: Cierre** | **14 days?** | **Tue 8/25/15** | **Fri 9/11/1** |
| 44 | Presentacion del Proyecto (Formato) | 4 days? | Tue 8/25/15 | Fri 8/28/ |
| 45 | Presentacion Ejecutivo del Proyecto | 1 day? | Fri 9/11/15 | Fri 9/11/ |