ESCUELA SUPERIOR POLITECNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

IV PROMOCION

"ESTANDAR ISO/IEC 27002 PARA CENTRO DE CÓMPUTO DE LA FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACIÓN (FIEC- ESPOL)"

TESIS DE GRADO

Previa a la Obtención del Título de:

DIPLOMA SUPERIOR EN AUDITORIA INFORMATICA

Presentada por:

Célida Fabiola Romero Vera

José Ricardo Castillo Ley

Año 2011

AGRADECIMIENTO

Al Ing. Juan Moreno, por la apertura y apoyo para la realización del presente proyecto.

A la Ing. Karol Hidalgo, directora de tesis por su confianza, ayuda invaluable y por su tiempo brindado.

RESUMEN

La presente tesis muestra una revisión en los dominios de seguridad física y ambiental; y de la gestión de la continuidad del negocio, tal como se establece en el estándar ISO/IEC 27002; aplicado al Centro de Cómputo de la Facultad de Ingeniería en Electricidad y Computación.

La tesis está constituida por cuatro capítulos: En el capítulo 1 se establece los antecedentes sobre la importancia de la Seguridad de la información; además se indican las justificaciones para el desarrollo de esta tesis, así como hacia donde se encuentra orientado.

En el capítulo 2 se describen los fundamentos teóricos de un sistema de gestión de la seguridad de la información, así como la familia de Normas ISO 27000, involucrando la ISO/IEC 27002, como estándar a ser revisado.

En el capítulo 3 se detalla la situación actual que envuelven las actividades desarrolladas dentro del Centro de Cómputo de la FIEC.

En el capítulo 4 se muestran la ejecución del plan de trabajo realizada al área.

Por último se presentan las conclusiones y recomendaciones basadas en la revisión realizada en el presente documento.

ÍNDICE GENERAL

RESUMEN ..... **III**
ÍNDICE GENERAL ..... **V**
ÍNDICE DE GRÁFICOS ..... **VII**
ÍNDICE DE TABLAS ..... **VII**
INTRODUCCIÓN ..... **IX**

CAPÍTULO 1 ..... **1**
ANTECEDENTES Y JUSTIFICACIÓN **1**
1.1 Seguridad de la información 1
1.2 Justificación 4
1.3 Alcance 5
1.4 Objetivo General 5
CAPÍTULO 2 ..... **6**
FUNDAMENTOS TEÓRICOS **6**
2.1 Sistema de Gestión de Seguridad de la Información (SGSI) 6
2.1.1¿Para qué sirve un SGSI? 7
2.1.2 ¿Qué incluye un SGSI? 8
2.1.3 ¿Cómo se implementa un SGSI? 10
2.2 International Standards Organization (ISO 27000) 16
2.2.1 Beneficios de implementar la Serie 27000 18
2.3 ISO 27001 19
2.3.1 Control de la documentación 23
2.4 International Standards Organization (ISO 27002) 24
2.4.1 Reseña Histórica 24
2.4.2 Objeto de la Norma 25
2.4.3 Estructura de esta Norma 25
2.4.4 Dominios de la norma ISO 27002 26
2.4.5 Categorías principales de Seguridad 30
2.4.6 Objetivos y Controles de la norma ISO 27002 31
2.5 Diferencias entre las normas ISO 27001 e ISO 27002 33
CAPITULO 3 ..... **34**
SITUACIÓN ACTUAL DEL CENTRO DE CÓMPUTO DE LA FIEC **34**
3.1 Misión del LAB-FIEC 34
3.2 Visión del LAB-FIEC 35
3.3 Estrategia Staff Lab-Fiec 35
3.4 Funciones Staff Lab-Fiec 36
3.5 Objetivos y Controles asociados a la Seguridad Física y ambiental 39
3.6 Objetivos y Controles asociados a la Gestión de la Continuidad del Negocio 45

CAPÍTULO 4..... 51
EJECUCION DE PLAN DE TRABAJO REALIZADO AL CENTRO DE CÓMPUTO DE LA FIEC..... 51
4.1 Metodología de trabajo..... 51
4.2 Programa de auditoría..... 52
4.3 Desarrollo del programa de auditoría..... 53
4.4 Revisión in situ al centro de cómputo..... 53
4.4.1 Seguridad Física y Ambiental..... 53
4.4.2 Gestión de la Continuidad del Negocio..... 59
4.5 Evaluación de Riesgos..... 65
4.6 Formulación del Informe final de auditoría..... 67
CONCLUSIONES..... 68
RECOMENDACIONES..... 70
ANEXOS
BIBLIOGRAFIA

ÍNDICE DE GRÁFICOS

Gráfico 1.1 Proceso para la obtención de información 3
Gráfico 2.1 Procedimientos sobre el SGSI 8
Gráfico 2.2 Niveles de un SGSI 8
Gráfico 2.3 Ciclo de un SGSI 10

ÍNDICE DE TABLAS

Tabla 2.2.1 Normas que componen la Serie 27000 18
Tabla 2.4.4.1 Dominios de la Norma ISO 27002 29
Tabla 2.4.6.1 ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133) / 32
Tabla 2.5.1 Diferencias entre normas ISO 33
Tabla 3.3.1 Funciones del personal del Lab-FIEC 38
Tabla 4.1.1 Metodología de Trabajo 52
Tabla 4.5.1 Calificación de acuerdo al Nivel de Vulnerabilidad e Impacto… 66

INTRODUCCIÓN

En la actualidad, el activo más importante de una organización es la Información; razón por la cual existe normas o estándares internacionales definidos por la Organización Internacional para la Estandarización (ISO por sus siglas en inglés); las cuales brindan una guía describiendo objetivos de control y controles recomendables en cuanto a seguridad de la información se refiere.

La Norma ISO/IEC 27002, al ser una guía de buenas prácticas para la seguridad de la información, no es certificable. Está norma contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

El trabajo surge ante la situación de aportar a la Facultad de Ingeniería en Electricidad y Computación, en conceptos de Seguridad de la información; conociendo previamente como son llevadas las actividades dentro del centro de cómputo; es por esto que una revisión cobra importancia; pues podría indicarnos las formas en que deben ser contemplados para que guarden

criterio con la norma ISO 27002, en los dominios de seguridad física y ambiental y de la gestión de la continuidad del negocio; mejorando la calidad de prestación en sus servicios.

CAPÍTULO 1

ANTECEDENTES Y JUSTIFICACIÓN

1.1 Seguridad de la información

En la actualidad, cualquier ejecutivo de empresas sabe que la información que permanece almacenada en sus archivos de computación electrónica, la cual fluye dentro de la empresa o ingresa o sale de ella, es más valiosa que el equipo que la sustenta.

También sabe que cualquier contingencia que pueda dañar esa información (o sin dañarla, ser de conocimiento de terceros indebidamente) puede provocar un serio impacto en la organización.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es por tanto, un objetivo de primer nivel.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (o de fuentes externas) o de la fecha de elaboración, ver gráfico 1.1

Gráfico 1.1 Proceso para la obtención de información

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de toda organización, en donde sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades que son algunos de los aspectos fundamentales en los que un SGSI (Sistema de Gestión de la Seguridad de la Información) es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

1.2 Justificación

La justificación del presente trabajo es plantear a la Facultad de Ingeniería en Electricidad y Computación (FIEC), la importancia de tomar decisiones basadas en mejores prácticas de un estándar internacional para la seguridad de la información en su centro de cómputo; es esencial, que la facultad identifique sus requisitos de seguridad en base a una evaluación de riesgos que presente las amenazas de sus activos, evaluando su vulnerabilidad y la probabilidad de ocurrencia e impacto en sus objetivos.

1.3 Alcance

Nuestro proyecto, consiste en alinear la seguridad de la información con la visión del centro de cómputo de la FIEC basados en la metodología que la ISO establece en su norma 27002 para los siguientes dominios:

1. Seguridad física y ambiental
2. Gestión de la continuidad del Negocio.

El trabajo a desarrollar, no busca preparar a la FIEC para una eventual certificación en materia de Seguridad de la Información, es plantear bases en la consecución de mejores prácticas y los beneficios que esta ofrece.

1.4 Objetivo General

Evaluar que las actividades realizadas en el centro de cómputo de la FIEC, guarden criterios con la norma ISO 27002 (Seguridad de la información) para los dominios señalados en el alcance.

CAPÍTULO 2

FUNDAMENTOS TEÓRICOS

2.1 Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

2.1.1 ¿Para qué sirve un SGSI?

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que han decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente, ver gráfico 2.1

Gráfico 2.1 Procedimientos sobre el SGSI

2.1.2 ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, ver gráfico 2.2

Gráfico 2.2 Niveles de un SGSI

Manual de seguridad: por analogía con el manual de seguridad, aunque el término se usa también en otros ámbitos, sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

2.1.3 ¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA (Plan, Do, Check, Act) tradicional en los sistemas de gestión de la calidad, ver gráfico 2.3

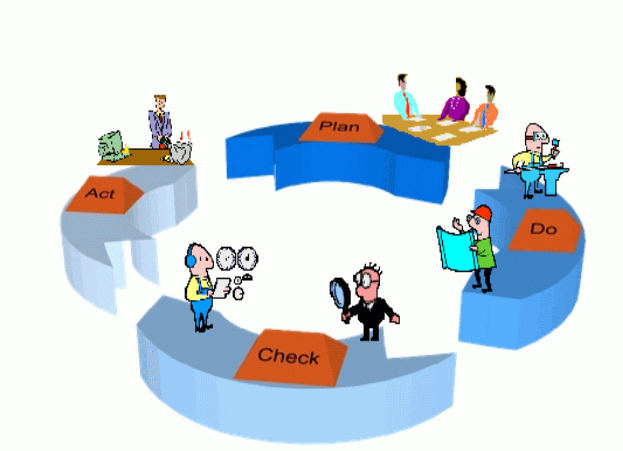


Gráfico 2.3 Ciclo de un SGSI

	Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
Plan: Establecer el SGSI	Definir una política de seguridad que: ➢ incluya el marco general y los objetivos de seguridad de la información de la organización; ➢ considere requerimientos legales o contractuales relativos a la seguridad de la información;

- esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
- establezca los criterios con los que se va a evaluar el riesgo;
- esté aprobada por la dirección.

Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas **metodologías** estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia)**.**

Identificar los Riesgos:

- identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
- identificar las amenazas en relación a los activos;
- identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
- identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

Analizar y evaluar los riesgos:

- evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un

activo de información;

- evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
- estimar los niveles de riesgo;
- determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:

- aplicar controles adecuados;
- aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
- evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
- transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.

Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.

Definir una declaración de aplicabilidad que incluya:

- los objetivos de control y controles seleccionados y los motivos para su elección;

	➢ los objetivos de control y controles que actualmente ya están implantados; ➢ los objetivos de control y controles (Tabla 2.4.3.1) excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.
Do: **Implementar y utilizar el SGSI**	➢ Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información. ➢ Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades. ➢ Implementar los controles anteriormente seleccionados que lleven a los objetivos de control. ➢ Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles. ➢ Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal. ➢ Gestionar las operaciones del SGSI. ➢ Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información. ➢ Implantar procedimientos y controles que

	permitan una rápida detección y respuesta a los incidentes de seguridad.
Check: **Monitorizar y revisar el SGSI**	Ejecutar procedimientos de monitorización y revisión para: ➢ detectar a tiempo los errores en los resultados generados por el procesamiento de la información; ➢ identificar brechas e incidentes de seguridad; ➢ ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto; ➢ detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; ➢ determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas. Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas. Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad. Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la

	organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-. Realizar periódicamente auditorías internas del SGSI en intervalos planificados. Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes. Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión. Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.
Act: **Mantener y mejorar el SGSI**	➢ Implantar en el SGSI las mejoras identificadas. ➢ Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones. ➢ Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder. ➢ Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases.

Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

2.2 International Standards Organization (ISO 27000)

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña, ver tabla 2.2.1

Todo este proceso es el que constituye un Sistema de gestión de seguridad de la Información (SGSI), que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

ISO/IEC 27000	**Introducción y Vocabulario (Publicado 30.04.09)**
ISO/IEC 27001	Sistema de Administración de Seguridad de la Información (P. 15.10.05)
ISO/IEC 27002	Código de buenas prácticas para la administración de la seguridad de la información (P. 15.06.05)
ISO/IEC 27003	Guía de implementación del sistema de administración de la seguridad de la información (P. 01.02.10)
ISO/IEC 27004	Métricas para la gestión de la seguridad de la información (P. 07.12.09)
ISO/IEC 27005	Administración de riesgos de la seguridad de la información (P. 04.06.08)
ISO/IEC 27006	Requisitos de los organismos que realizan auditoría y certificación del SGSI (P. 13.02.07)
ISO/IEC 27007	Directrices al auditar el SGSI (Probable publicación 2012)
ISO/IEC 27008	Orientación para Auditores sobre los controles SGSI (Probable publicación 2013)
ISO/IEC 27010	Directrices de seguridad de información en comunicaciones intersectoriales (Probable publicación 2012)
ISO/IEC 27011	Guías de SGSI para las organizaciones de telecomunicaciones basadas en la ISO 27002 (P. 15.12.08)
ISO/IEC 27013	Orientación sobre la aplicación integral de las ISO 20000 e ISO 27001 (Probable publicación 2012)
ISO/IEC 27014	Marco de trabajo para el gobierno de la seguridad de la información (Probable publicación 2012)
ISO/IEC 27031	Preparación para la continuidad del negocio (Probable publicación 2012)
ISO/IEC 27032	Guías para la cyberseguridad (Probable publicación 2013)
ISO/IEC 27033	Seguridad de red (Probable publicación 2013)
ISO/IEC 27034-1	Guías para la seguridad de aplicaciones-Parte 1 Introducción y conceptos (Probable publicación 2012)

ISO/IEC 27035	Gestión de incidentes en la seguridad de la información. (Probable publicación 2012)
ISO/IEC 27037	Guías para la identificación, colección, adquisición y preservación de la evidencia digital (Probable publicación 2013)

Tabla 2.2.1 Normas que componen la Serie 27000

2.2.1 Beneficios de implementar la Serie 27000

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

2.3 ISO 27001

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• **Integridad:** esto significa que solo puede ser modificada por personas autorizadas y dentro de un programa de actualización previamente aprobado. La integridad puede ser alterada en forma intencional, o bien en forma accidental por falla del hardware, del software o por la acción de un virus informático.

• **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.

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

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

2.3.1 Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.

• Garantizar que la distribución de documentos está controlada.

• Prevenir la utilización de documentos obsoletos.

• Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

2.4 International Standards Organization (ISO 27002)

2.4.1 Reseña Histórica

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005.

Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en **AENOR**). Otros países donde también está publicada en español son, por ejemplo, **Colombia** (NTC-ISO-IEC 27002), **Venezuela** (Fondonorma ISO/IEC 27002), **Argentina** (IRAM-ISO-IEC 27002), **Chile** (NCh-ISO27002) o **Perú** (como ISO 17799).

Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación en 2012.

2.4.2 Objeto de la Norma

Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos. Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones[1]

2.4.3 Estructura de esta Norma

Esta norma contiene once secciones sobre controles de seguridad que en conjunto tienen un total de 39 categorías principales de seguridad y una sección de introducción a la evaluación y el tratamiento del riesgo.

[1] Norma Técnica Colombiana NTC-ISO/IEC 27002

2.4.4 Dominios de la norma ISO 27002

La Norma ISO 27002, contiene 11 dominios, el orden de los dominios no implica su importancia. Dependiendo de las circunstancias, todos los dominios podrían ser importantes, por lo tanto cada organización que aplique esta norma debe identificar los dominios aplicables, su importancia y su aplicación a procesos individuales del negocio. (Ver Tabla 2.4.4.1)

1. **Política de seguridad:** Se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.

2. **Organización de la seguridad de la información:** Sugiere diseñar una estructura de administración dentro la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

3. **Gestión de Activos:** Necesita un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

4. **Seguridad ligada a los recursos humanos:** Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe tener que implementar un plan para reportar los incidentes.

5. **Seguridad física y del entorno:** Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

6. **Gestión de comunicaciones y operaciones:** Los objetivos de esta sección son:
    - Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
    - Minimizar el riesgo de falla de los sistemas.
    - Proteger la integridad del software y la información.
    - Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
    - Garantizar la protección de la información en las redes y de la infraestructura de soporte.

- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

7. **Control de acceso:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

8. **Adquisición, Desarrollo y mantenimiento de los sistemas de información:** Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

9. **Gestión de incidentes:** Asegurar que los eventos y las debilidades de la seguridad de información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente. Adicionalmente, asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

10. **Gestión de continuidad del negocio:** Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

11. **Conformidad:** Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con requisitos jurídicos, también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

<table>
<tr><td colspan="4">Política de Seguridad</td></tr>
<tr><td colspan="4">Organización de la Seguridad de la Información</td></tr>
<tr><td colspan="4">Gestión de Activos</td></tr>
<tr><td>Seguridad ligada a los Recurso Humano</td><td>Seguridad física y del entorno</td><td>Gestión de Comunicaciones y Operaciones</td><td rowspan="2">Adquisición, Desarrollo y mantenimiento de los sistemas de información</td></tr>
<tr><td colspan="3">Control de Acceso</td></tr>
<tr><td colspan="4">Gestión de incidentes</td></tr>
<tr><td colspan="4">Gestión de la continuidad del Negocio</td></tr>
<tr><td colspan="4">Conformidad</td></tr>
</table>

Tabla 2.4.4.1 Dominios de la Norma ISO 27002

2.4.5 Categorías principales de Seguridad

Cada dominio contiene una cantidad de categorías principales de seguridad, las mismas que incluyen:

a) Un objetivo de control que establece lo que se debe lograr,

b) Uno o más controles que se pueden aplicar para lograr el objetivo de control.

Las descripciones de los controles tienen la siguiente estructura:

Control

Define la declaración específica del control para cumplir *el* objetivo de control.

Guía de implementación

Suministra información más detallada para apoyar la implementación del control y satisfacer el objetivo de control. Algunas partes de esta guía pueden no ser adecuadas en todos los casos y por ello pueden ser más apropiadas otras formas de implementación del control.

Información adicional

Suministra información que puede ser necesario considerar, por ejemplo las consideraciones legales y las referencias a otras normas.

2.4.6 Objetivos y Controles de la norma ISO 27002

Tabla 2.4.6.1 ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133) /

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información.

5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.

6.1.1 Compromiso de la Dirección con la seguridad de la información.

6.1.2 Coordinación de la seguridad de la información.

6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información.

6.1.5 Acuerdos de confidencialidad.

6.1.6 Contacto con las autoridades.

6.1.7 Contacto con grupos de especial interés.

6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

6.2.2 Tratamiento de la seguridad en la relación con los clientes.

6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.

7.1.2 Propiedad de los activos.

7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.

7.2.1 Directrices de clasificación.

7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.

8.1.1 Funciones y responsabilidades.

8.1.2 Investigación de antecedentes.

8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.

8.2.1 Responsabilidades de la Dirección.

8.2.2 Concienciación, formación y capacitación en seguridad de la información.

8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.1 Responsabilidad del cese o cambio.

8.3.2 Devolución de activos.

8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.

9.1.2 Controles físicos de entrada.

9.1.3 Seguridad de oficinas, despachos e instalaciones.

9.1.4 Protección contra las amenazas externas y de origen ambiental.

9.1.5 Trabajo en áreas seguras.

9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.

9.2.1 Emplazamiento y protección de equipos.

9.2.2 Instalaciones de suministro.

9.2.3 Seguridad del cableado.

9.2.4 Mantenimiento de los equipos.

9.2.5 Seguridad de los equipos fuera de las instalaciones.

9.2.6 Reutilización o retirada segura de equipos.

9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.

10.1.1 Documentación de los procedimientos de operación.

10.1.2 Gestión de cambios.

10.1.3 Segregación de tareas.

10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.

10.2.1 Provisión de servicios.

10.2.2 Supervisión y revisión de los servicios prestados por terceros.

10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.

10.3.1 Gestión de capacidades.

10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.

10.4.1 Controles contra el código malicioso.

10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.

10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.

10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.

10.7.1 Gestión de soportes extraíbles.

10.7.2 Retirada de soportes.

10.7.3 Procedimientos de manipulación de la información.

10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.

10.8.2 Acuerdos de intercambio.

10.8.3 Soportes físicos en tránsito.

10.8.4 Mensajería electrónica.

10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.

10.9.1 Comercio electrónico.

10.9.2 Transacciones en línea.

10.9.3 Información públicamente disponible.

10.10 Supervisión.

10.10.1 Registros de auditoría.

10.10.2 Supervisión del uso del sistema.

10.10.3 Protección de la información de los registros.

10.10.4 Registros de administración y operación.

10.10.5 Registro de fallos.

10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.

11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.

11.2.1 Registro de usuario.

11.2.2 Gestión de privilegios.

11.2.3 Gestión de contraseñas de usuario.

11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.

11.3.1 Uso de contraseñas.

11.3.2 Equipo de usuario desatendido.

11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.

11.4.1 Política de uso de los servicios en red.

11.4.2 Autenticación de usuario para conexiones externas.

11.4.3 Identificación de los equipos en las redes.

11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.

11.5 Control de acceso al sistema operativo.

11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.

11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.

11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.

12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.

12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.

12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la cont. del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sistemas de información.

2.5 Diferencias entre las normas ISO 27001 e ISO 27002

Por lo antes mencionado, la ISO 27002 permite implementar la ISO 27001; sin embargo, existen diferencias que mostramos a continuación:

ISO 27001	ISO 27002
Es una norma de gestión: define como ejecutar un sistema.	Mucho más detallada y más precisa.
Es Certificable.	No es certificable.
Exige la realización de una evaluación de riesgos sobre cada control para identificar si es necesario disminuir los riesgos.	Los controles tienen igual denominación que los indicados en el Anexo A de la ISO 27001

Tabla 2.5.1 Diferencias entre normas ISO

CAPITULO 3

SITUACIÓN ACTUAL DEL CENTRO DE CÓMPUTO DE LA FIEC

El centro de cómputo de la Facultad de Ingeniería en electricidad y computación, actualmente gestiona recursos vitales para el funcionamiento de sus laboratorios de computación, creados con la finalidad de brindar servicio a los estudiantes de la Facultad en el desarrollo de sus actividades académicas por medio del préstamo de computadores, dictado de cursos, seminarios, entre otros servicios que paulatinamente se han ido incorporando; creando un marco que regulariza y facilita la normal ejecución de sus actividades, permitiendo la mejora constante de la calidad en sus servicios.

3.1 Misión del LAB-FIEC

Servir de apoyo tecnológico para profesores y estudiantes, a fin de que los recursos informáticos con los que cuenta la Facultad sean aprovechados al máximo, para potenciar el desarrollo académico-científico de la FIEC.

3.2 Visión del LAB-FIEC

Forjar líderes emprendedores para que aportando con sus capacidades, podamos llegar a funcionar como una entidad autónoma, capaz de generar recursos económicos-científicos, para colaborar con el desarrollo de la ESPOL y de la sociedad en general.

3.3 Estrategia Staff Lab-Fiec

El Laboratorio de Computación de la FIEC tiene los siguientes puntos como lineamientos básicos para establecer su conducta organizacional y estrategia administrativa:

• Establecer virtudes internas del personal, tales como:

- ❖ Excelencia
- ❖ Puntualidad
- ❖ Responsabilidad y asertividad
- ❖ Dinamismo
- ❖ Efectividad y Eficiencia
- ❖ Orden

• Incentivar que quienes conforman el Laboratorio estén continuamente actualizando sus conocimientos.

• Incentivar que los integrantes del Laboratorio asuman su trabajo no sólo como una obligación, sino como una forma de alto aprendizaje. De esta manera, podrán aplicar los conocimientos adquiridos en su futuro profesional.

• Mantener un régimen de calidad, alineado con los objetivos establecidos en la Política de Calidad de la ESPOL.

3.4 Funciones Staff Lab-Fiec

Las funciones del personal del Laboratorio de Computación, relacionadas con la seguridad de la información, son detalladas en la tabla 3.3.1

Responsables	Funciones
Jefe del Laboratorio de Computación	❖ Administrar el Laboratorio de Computación y los recursos de red (diseño) de la FIEC. ❖ Servir de apoyo en la parte administrativa, según disposiciones del Coordinador del Área o del Decano de la Facultad. ❖ Dar Soporte de Última Línea a los Profesores y Otros Laboratorios de la FIEC. ❖ Planificar Mantenimientos de Hardware y Software de las PCs del Laboratorio de Computación así como de otros Laboratorios de la FIEC. ❖ Coordinar el manejo de inventario de Hardware y Software de las PCs de la FIEC. ❖ Verificar el uso de software licenciado. ❖ Asesorar en la compra de equipos, actualización o averías que no pueden ser cubiertas por garantía. ❖ Mantener comunicación con proveedores en cuanto existan inconvenientes con las Pc's y demás dispositivos en período de garantía técnica. ❖ Servir de ayuda en las distintas áreas que abarcan los Recursos Informáticos de la Facultad. ❖ Responsable del cumplimiento de normas internas tanto administrativas, operativas como de seguridad del área que abarca el

	laboratorio de computación
Asistente Técnico de Redes (1 Persona)	❖ Cuidar el buen funcionamiento de los servidores del laboratorio y el normal desempeño de la red. ❖ Realizar respaldos periódicos de la información de los servidores. ❖ Crear y mantener las cuentas de correo del personal y estudiantes. ❖ Compilar y mantener copia de los paquetes de software que son usados por los servidores. ❖ Mantener actualizado los diagramas de la red. ❖ Mantener funcionando los servicios de: autenticación, Mail, impresión, mensajería instantánea, actualización de antivirus y Base de Datos. ❖ Recomendar la adquisición de nuevos equipos de red, computadores y paquetes de software. ❖ Evaluar los paquetes de software a ser instalados en los servidores. ❖ Participar en el diseño e instalación de nuevas redes que se coloquen en los laboratorios. ❖ Dar soporte en cuanto a problemas con Impresión en la Secretaría y administración de la facultad y a los docentes.
Asistente de Soporte Técnico (3 Personas)	❖ Dar soporte al personal administrativo de la FIEC: Decano, SubDecano, secretarías, coordinadores de carrera y profesores de la facultad. ❖ Coordinar con el respectivo Jefe, el mantenimiento correctivo y preventivo de las computadoras (una vez al semestre) que están al servicio de los estudiantes y dar soporte de última línea (en el caso de que algún ayudante no pueda resolver un problema) ❖ Evaluar los paquetes de software a ser instalados en las estaciones del laboratorio. ❖ Atender vía CRM los tickets de asistencia técnica de los laboratorios y personal que tiene a su cargo. ❖ Coordinar la instalación de software en los laboratorios de computación. ❖ Compilar y mantener copia de los paquetes de software (disquetes, Cdroms y manuales) que son usados dentro del laboratorio. ❖ Recomendar la adquisición de nuevos equipos y/o paquetes de software para el laboratorio.
Web-Máster (1 Persona)	❖ Revisar diariamente el buen funcionamiento del Web-site de la FIEC, así como evaluar periódicamente el desempeño del mismo. ❖ Realizar periódicamente respaldos de la información del Web-Site.

	❖ Recomendar la incorporación de nuevos contenidos, tecnologías y servicios dentro del Web-Site de la FIEC. ❖ Compilar y mantener copia de los paquetes de software (disquetes, CD-ROM y manuales) que son usados dentro del Web site de la FIEC. ❖ Colaborar en la creación de contenido impreso o digital para su uso con fines de promoción, información y distribución por parte de la FIEC. ❖ Actualizar periódicamente en el Web las actividades llevadas a cabo dentro de la FIEC, seminarios, exposiciones, presentaciones, visitas, etc. ❖ Realizar mejoras, adaptaciones y renovaciones periódicas del Web-site de la FIEC. ❖ Dar soporte al sistema de comunicación Cursos Web (METIS) ❖ Crear, mantener y administrar las bases de datos del sistema Lotus Notes.
Asistente de desarrollo (1 Persona)	❖ Instalación, configuración y soporte en sitio de las copias de software que son vendidas por la FIEC. ❖ Proveer de cursos de capacitación a los responsables de los sistemas en otras unidades ❖ Desarrollo de herramientas de software que faciliten las tareas del laboratorio y de la FIEC. ❖ La actualización de los programas a nuevas versiones o diferentes de sistemas operativos. ❖ Buscar nuevas herramientas que puedan ser utilizadas para mejorar la calidad del trabajo en los laboratorios. ❖ Mantener y dar soporte a los siguientes sistemas: SMALC para control de laboratorios, CRM de Asistencia Técnica en Línea y Sistema de Reserva de Salas.

Tabla 3.3.1 Funciones del personal del Lab-FIEC

Por la importancia de los procesos que se realizan en la FIEC y dado al entorno del objeto de estudio, los dominios de la norma ISO 27002, a aplicar son:

- ❖ Seguridad Física y ambiental
- ❖ Gestión de la continuidad del Negocio.

3.5 Objetivos y Controles asociados a la Seguridad Física y ambiental.

La estructura de este dominio se basa en dos ítems cuyos objetivos son:

- ➢ **Áreas Seguras:** evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

Asociados con:	Controles	Guía de Implementación
Perímetro de la Seguridad Física	Se deben utilizar perímetros de seguridad para proteger las áreas que contienen información y servicios de procesamiento de información.	El área debe ser robusta físicamente: las paredes externas del sitio deben ser de construcción sólida, las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas; Establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación; Las puertas de incendio en el perímetro de seguridad deberían tener alarmas y ser sometidas a pruebas junto con las paredes para establecer grados requeridos de resistencia; Sistemas para detectar intrusos que sean sometidos a pruebas regularmente para verificar todas las puertas y ventanas accesibles; Los servicios de procesamiento de información deben estar físicamente separados de los dirigidos por terceras partes;
Controles físicos de entrada	Acceso solo a personal autorizado.	Todo acceso debe estar previamente autorizado y registrado; El acceso a áreas de información sensibles, debe realizarse con tarjetas de autenticación

		más número de identificación personal (PIN) para validar el acceso; Se debe exigir a todos los empleados, contratistas y usuarios de tercera partes la utilización de alguna forma de identificación visible y se debería notificar al personal de seguridad si se encuentra visitantes sin acompañante o sin identificación; Los accesos del personal de soporte de terceras partes debe ser autorizado y monitoreado.
Seguridad de Oficinas, despachos y recursos	Diseñar y aplicar la seguridad física para oficina, recintos e instalaciones.	Tener presente los reglamentos y las normas pertinentes a la seguridad y la salud; Las instalaciones claves se deberían ubicar de modo que se evite el acceso al público; Cuando sea viable, las edificaciones deberían ser discretas y no tener indicaciones sobre su propósito, sin señales obvias, fuera o dentro de ellas, que identifiquen la presencia de actividades de procesamiento de información; Los directorios y los listados telefónicos internos que indican las ubicaciones de los servicios de procesamiento de información sensible no deberían ser de fácil acceso al público.
Protección contra amenazas externas y del entorno	Se deberían diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.	Tener en cuenta todas las amenazas para la seguridad que presentan las instalaciones circundantes; Los materiales combustibles o peligrosos se deberían almacenar a una distancia prudente del área de seguridad. Los suministros a granel tales como los materiales de oficina, no se deberían almacenar en un área segura; Los equipos de repuesto y los medios de soporte de seguridad se deberían ubicar a una distancia prudente para evitar daño debido a algún desastre que afecte a las instalaciones principales; Se debería suministrar equipo apropiado contra incendios y ubicarlo adecuadamente.
Trabajo en áreas seguras	Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.	El personal sólo debería conocer la existencia de un área segura o las actividades dentro de ella en función de la necesidad con base conocida; Se debería evitar el trabajo no supervisado

		en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas; Las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente; No se debería permitir equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.
Áreas aisladas de carga y descarga	Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deberían controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.	El área de despacho y carga se debería designar de forma tal que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación; Las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén abiertas; El material que llega se debería inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso; Así como su registro de acuerdo a procedimientos establecidos; Los envíos entrantes y salientes deberían estar organizados físicamente, cuando sea posible.

- **Seguridad de los equipos:** evitar pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.

Asociados con:	Controles	Guía de Implementación
Instalación y protección de equipos	Los equipos deberían estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.	Los equipos se deberían ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo; Los servicios de procesamiento de información que manejan datos sensibles, deberían estar ubicados de forma tal que se reduzca el riesgo de visualización de la información por personas no autorizadas durante su uso, y los sitios de almacenamiento se deberían asegurar para evitar el acceso no autorizado;

		Los elementos que requieran protección especial deberían estar aislados para reducir el nivel general de protección requerida de los demás elementos; Se recomienda adoptar controles para minimizar el riesgo de amenazas físicas potenciales, por ejemplo robo, incendio, explosión, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencia con el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo; Se deberían establecer directrices para comer, beber y fumar en las cercanías de los servicios de procesamiento de información; Es conveniente monitorear las condiciones ambientales, como temperatura y humedad, para determinar las condiciones que podrían afectar adversamente el funcionamiento de los servicios de procesamiento de información; Se debería aplicar protección contra rayos a todas las edificaciones y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación; Es recomendable considerar la utilización de métodos especiales de protección para equipos en ambientes industriales, tales como membranas para los teclados; Los equipos de procesamiento de información sensible deberían estar protegidos para minimizar el riesgo de fuga de información debido a filtración.
Suministro eléctrico	Los equipos deberían estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	Todos los servicios de suministro, tales como electricidad, agua, alcantarillado, calefacción/ ventilación y aire acondicionado deberían ser adecuados para los sistemas a los que dan apoyo; Los servicios de suministro se deberían inspeccionar regularmente y someter a las pruebas apropiadas para garantizar su funcionamiento adecuado y reducir cualquier riesgo debido a su mal funcionamiento o falla; Se recomienda el suministro de energía sin interrupción (UPS) para dar soporte al cierre ordenado o al funcionamiento continuo de equipos que soportan operaciones críticas para el negocio;

		Se recomienda pensar en una planta de energía alterna, si se requiere la continuidad del procesamiento en caso de fallas energéticas prolongadas. Debería estar disponible un suministro adecuado de combustible para garantizar que el generador pueda funcionar por un periodo prolongado. Los interruptores de emergencia para apagar la energía deberían estar cerca de las salidas de emergencia en los recintos de los equipos para facilitar el corte rápido de energía en caso de emergencia. Se recomienda tener iluminación de emergencia en caso de falla del suministro principal. El equipo de telecomunicaciones se debería conectar al proveedor del servicio mediante al menos dos rutas diferentes para evitar que la falla en una ruta de conexión elimine los servicios de voz. Estos servicios deberían ser adecuados para satisfacer los requisitos legales locales para comunicaciones de emergencia.
Seguridad del cableado	El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deberían estar protegidos contra interceptaciones o daños.	Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada. El cableado de la red debería estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos o evitando rutas a través de áreas públicas. Los cables de energía deberían estar separados de los cables de comunicaciones para evitar interferencia. Se deberían utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones accidentales de cables erróneos a la red. Es recomendable emplear un plano del cableado para reducir la posibilidad de error. Para sistemas críticos o sensibles considerar los siguientes controles: Instalación de conductos blindados y recintos o cajas bloqueadas en los puntos de inspección y terminación. Uso de medios alternos de enrutamiento y / o transmisión que suministren seguridad adecuada. Uso de cableado de fibra óptica.

		Uso de cubiertas (blindaje) electromagnéticas para proteger los cables. Inicio de reconocimientos técnicos e inspecciones físicas en busca de dispositivos no autorizados conectados al cableado. Acceso controlado a los módulos de cableado (Patch panel) y a cuartos de cableado.
Mantenimiento de equipos	Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	El mantenimiento de los equipos debería estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor. Sólo personal de mantenimiento autorizado debería realizar las reparaciones y el servicio de los equipos. Se recomienda conservar registros de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo. Es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, teniendo en cuenta si el mantenimiento lo realiza el personal dentro o fuera de la organización. Se deberían cumplir todos los requisitos impuestos por las pólizas de seguros.
Seguridad de equipos fuera de los locales de la organización	Se debería suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización	Independientemente del propietario, la dirección debería autorizar el uso del equipo de procesamiento de información fuera de las instalaciones de la organización. El equipo y los medios llevados fuera de las instalaciones no se deberían dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes. Se deberían observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra la exposición a campos electromagnéticos fuertes. Se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgos y controles adecuados que se aplican de forma idónea, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina. Se debería establecer el cubrimiento

		adecuado del seguro para proteger el equipo fuera de las instalaciones. El almacenamiento de información y el equipo de procesamiento incluyen todas las formas de computadores personales, organizadores, teléfonos móviles, tarjetas electrónicas, papel u otras formas que se conservan para el trabajo en el domicilio o que se transportan lejos del sitio normal de trabajo.
Seguridad en la reutilización o eliminación de equipos	Se deberían verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.	Los dispositivos que contienen información sensible se deberían destruir físicamente o su información se debería destruir, borrar o sobrescribir usando *técnicas* que permitan que la información original no se pueda *recuperar,* en lugar de utilizar las funciones de borrado o formateado estándar. Los dispositivos deteriorados que contengan datos sensibles pueden requerir una evaluación de riesgos para determinar si los elementos se deberían destruir físicamente en lugar de enviarlos a reparación o desecharlos.
Traslado de Activos	Ningún equipo, información ni software se deberían retirar sin autorización previa.	Ni los equipos, ni la información, *tampoco* el software se deberían retirar sin autorización previa. Los empleados, contratistas y usuarios de *terceras* partes que tengan autoridad para permitir retirar activos deberían estar claramente identificados. Se recomienda *establecer* límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de devolución. Cuando sea necesario y adecuado, se debería registrar que el equipo ha sido retirado y se debe registrar cuando fue devuelto

3.6 Objetivos y Controles asociados a la Gestión de la Continuidad del Negocio.

La estructura de este dominio se basa en un ítem cuyo objetivo es:

- **Aspectos de la seguridad de la información en la gestión de la continuidad del Negocio:** Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurando una recuperación oportuna, todo dentro del proceso de evaluación de riesgos.

Asociados con:	Controles	Guía de Implementación
Proceso de la gestión de la continuidad del negocio	Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.	Comprensión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio. Identificación de todos los activos involucrados en los procesos críticos del negocio. Comprensión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información (es importante encontrar soluciones para manejar los incidentes que producen impactos menores, así como los incidentes graves que puedan amenazar la viabilidad de la organización), y establecer los objetivos del negocio para los servicios de procesamiento de información. Consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos. Identificación y consideración de la implementación de controles preventivos y mitigantes adicionales. Identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información. Garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización. Formulación y documentación de los planes de continuidad del negocio que abordan los

		requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio. Prueba y actualización regular de los planes y procesos establecidos. Garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización.
Continuidad del negocio y análisis de impactos	Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.	Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización. Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación. Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.
Redacción e implantación de planes de continuidad	Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el	Identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio. Identificar la pérdida aceptable de información y servicios. Implementar los procedimientos que permitan recuperar y restaurar las operaciones del negocio y la disponibilidad de la información

	negocio.	en las escalas de tiempo requeridas; es necesario atender la evaluación de las dependencias internas y externas del negocio y de los contratos establecidos. Procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración. Formación apropiada del personal en los procedimientos y procesos acordados, incluyendo el manejo de las crisis. Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organización y, por lo tanto, pueden contener información sensible que es necesario proteger adecuadamente. Las copias de los planes de la continuidad del negocio se deberían almacenar en un lugar lejano, a suficiente distancia para escapar a cualquier daño por algún desastre en la sede principal. Si se utilizan lugares alternos temporales, el nivel de los controles de seguridad implementados en estos lugares debería ser equivalente al de la sede principal. Es conveniente observar que los planes y las actividades de la gestión de crisis pueden ser diferentes de la gestión de la continuidad del negocio; es decir, se puede presentar una crisis que se pueda adaptar con procedimientos de gestión normales
Marco de planificación para la continuidad del negocio	Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.	Cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan. Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente. Cada plan debería tener un dueño específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los dueños de los recursos o procesos apropiados del negocio involucrados. Las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.

		Los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio. Los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos. Los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración. Los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad. Una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan. Actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces. Las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes. Los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.
Prueba, mantenimiento y reevaluación de planes de continuidad	Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.	La programación de las pruebas para los planes de continuidad del negocio debería indicar cómo y cuándo se va a probar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia. La prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplos de interrupciones) Las pruebas de recuperación técnica (garantizando que los sistemas de información se pueden restaurar eficazmente) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal)

	Las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído) Los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones). Se debería asignar responsabilidad para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se reflejan en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo. Los ejemplos de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, la mejora de los sistemas y cambios en: El personal. Las direcciones o los números telefónicos. La estrategia del negocio. Los lugares, dispositivos y recursos. La legislación. Los contratistas, proveedores y clientes principales. Los procesos existentes, nuevos o retirados. Los riesgos (operativos y financieros).

CAPÍTULO 4

EJECUCION DE PLAN DE TRABAJO REALIZADO AL CENTRO DE CÓMPUTO DE LA FIEC

4.1 Metodología de trabajo

El plan de trabajo del proyecto estuvo compuesto de etapas y actividades delineadas, que fueron realizadas de acuerdo a los esquemas de seguridad que la ISO expidió en su norma ISO/IEC 27002; adicionalmente, apoyadas en procedimientos de auditoría considerados de acuerdo a las circunstancias, ver tabla 4.1.1

Etapas	Actividades
Estudio de la Norma ISO/IEC 27001 – 27002.	Elaboración de la Propuesta del Proyecto (Selección de dominios).
Recopilación de políticas y normas del ente a auditar.	Solicitudes de manuales y documentación de la organización.
Enfoque de auditoría basado en los controles de la norma ISO 27002.	Elaboración del Programa de Auditoría basado en los dominios: Seguridad física y ambiental y de gestión de la continuidad del negocio.

Revisión in situ al centro de cómputo.	Entrevistas a responsables de área. Elaboración del check list, papeles de trabajo y pruebas a los controles. Recolección de evidencias.
Evaluación de Riesgos.	Elaborar la matriz de riesgos por los dominios revisados cuantificados en vulnerabilidad e impacto.
Comunicación de Hallazgos.	Informe borrador para coordinación con el Jefe de área.
Formulación del informe final de auditoría.	Entrega al Jefe del área responsable.

Tabla 4.1.1: Metodología de Trabajo

.

4.2 Programa de auditoría

Se procedió con la elaboración del programa de auditoría basado en los dominios de Seguridad Física y ambiental, y de la Gestión de la continuidad del negocio; permitiéndonos tener una guía o herramienta para determinar en forma lógica, ordenada y sistemática el grado de cumplimiento y adherencia a controles y políticas emanadas por la administración; así como la verificación del cumplimiento de leyes, regulaciones, resoluciones, reglamentos, etc. implantados por los organismos que rigen la actividad.

Nos permitió además medir el grado de eficiencia con que están manejando y controlando los procesos involucrados en los dominios en revisión.

Los programas de trabajo de auditoría, ver anexo 1; incluyen: el dominio a ser evaluado, los objetivos, fuente de referencia, aplicabilidad, fecha de revisión, las actividades que se van a auditar; tomando en consideración el alcance de trabajo de auditoría planeado.

4.3 Desarrollo del programa de auditoría

Una vez finalizada la planificación, y previa a la ejecución de la auditoria, quedó definido el tema y área a auditar, el objetivo de la auditoría, su alcance, las habilidades técnicas y recursos necesarios y la identificación de las fuentes de información para ejecución de pruebas y revisiones.

4.4 Revisión in situ al centro de cómputo

La revisión realizada en el mes de julio del año 2011 al centro de cómputo de la FIEC, nos permite detallar los hallazgos siguientes:

4.4.1 Seguridad Física y Ambiental

1. Dentro del área de procesamiento de información, se encuentra embodegado afiches y carteles que no tiene relación con el área.

Riesgo Asociado: Propagación de incendio dentro del centro de cómputo. Al almacenar material ajeno dentro del área de procesamiento de datos se es partícipe en el daño provocado por un siniestro de incendio, afectando directamente a las instalaciones y equipos del centro de cómputo.

Recomendación: En el área de centro de cómputo no debe existir material ajeno al procesamiento de información, por ello los suministros tales como materiales de oficina, no deben ser almacenados en el área, ya que son altamente combustibles y podían originar un incendio y/o propagar rápidamente el mismo.

2. El área de procesamiento de información no dispone de protección adecuada ante un daño de incendio. Tiene un solo extintor para un área aproximada de 250 mts cuadrados.

Riesgo Asociado: Pérdida de activos de información. El número de extintores actual en caso de materializarse un siniestro de incendio no cubre el área; cuyos activos ascienden a 140,000 dólares aproximadamente.

Recomendación: El área debe estar provista de equipos suficientes y apropiados para la extinción de incendios, los que deben estar ubicados estratégicamente, para su uso, minimizando así las posibles pérdidas económicas en caso de concretarse un incendio. Adicionalmente el personal del centro de cómputo debe ser capacitado en forma permanente en el uso de extintores, ya sea por parte del proveedor o cuerpo de bomberos, de manera que asegure una adecuada respuesta ante incidentes de esta índole.

3. No existe supervisión para los trabajos realizados en el área de procesamiento de información por parte de terceras personas.

Riesgo Asociado: Daños a los equipos pertenecientes al área. El permitir el ingreso de terceras personas para realizar trabajos no supervisados dentro del área de procesamiento de información, sin tener las debidas seguridades, podría ocasionar la ejecución de actividades maliciosas y/o intencionales, que deriven en pérdidas de información e inclusive robo de equipos.

Recomendación: Las disposiciones para el trabajo en áreas seguras según las mejores prácticas, recomiendan manejar una Supervisión y registro de todo trabajo efectuado en el área de procesamiento de

información; a fin de evitar la pérdida de equipos que pertenecen a la empresa, así como evitar que errores mal intencionados provoquen la desconexión de equipos y por consiguiente la pérdida de servicios.

4. Las cintas de respaldo están siendo almacenadas en un área independiente al centro de cómputo; pero, estas son resguardadas en un escaparate que no es de entera exclusividad para las mismas. Adicionalmente, no presta las debidas seguridades por falta de cerradura.

   Riesgo Asociado: Mal uso o pérdida de cintas de respaldo, impidiendo la recuperación de información oportuna, de ocurrir un siniestro.

   Recomendación: Asignar dentro del área independiente al centro de cómputo, una gaveta exclusiva para el almacenamiento y custodio de las cintas de respaldo, que cuente con seguridades apropiadas, con el fin de evitar el daño malicioso a las mismas, así como también minimizar la pérdida de cintas con el propósito de causar daño a la operativa de los servicios que brinda el centro de cómputo.

5. Los interruptores de energía de emergencia que permiten cortar el fluido eléctrico, en casos de un siniestro de incendio, no están ubicados cerca de la salida del centro de cómputo.

   Riesgo Asociado: El personal tiene imposibilitado ante un desastre que afecte al área, tal como un incendio al interior del centro de cómputo o durante una evacuación de emergencia, la desactivación inmediata de los breakers o interruptores principales del área.

   Recomendación: Analizar la reubicación de los interruptores de energía eléctrica del área del centro de cómputo, y etiquetarlos claramente; de forma que faciliten la desconexión rápida y oportuna del suministro de energía, en caso de emergencia.

6. El área del centro de cómputo no cuenta con iluminación de emergencia.

   Riesgo Asociado: La falta de iluminación de emergencia en el área de procesamiento de información puede incidir a la desconexión no intencionada de equipos por parte del personal, causando daños de operatividad del centro de cómputo conllevando inclusive a pérdida de información.

Recomendación: Implementar iluminación de emergencia dentro del centro de cómputo, para minimizar la pérdida de información, por desconexiones accidentales de los equipos que se encuentran al interior del área.

7. Si bien, por el momento no han tenido la necesidad de proceder a la destrucción de equipos de procesamiento de información sensible, tales como: cintas de respaldo y discos duros (internos, externos), no tienen documentado un procedimiento para su ejecución.

Riesgo Asociado: No tener cuidado y proceder a la destrucción de equipos con información sensible.

Recomendación: Elaborar y documentar un procedimiento a usar en casos de reutilización o eliminación de equipos usados para el procesamiento de información, cerciorándose que dichos componentes no contengan información sensible del área.

Riesgo Asociado: Proceder a la destrucción de equipos sin documentación de respaldo de los mismos.

Recomendación: Registrar en un documento la eliminación de los elementos sensibles de los equipos con el objeto de mantener una prueba de auditoría. Este documento deberá contener básicamente: Nombre del equipo, modelo, serie, motivo de destrucción, Fecha, hora y firma del responsable.

4.4.2 Gestión de la Continuidad del Negocio

1. Actualmente la gestión de la continuidad del negocio no se encuentra incorporada dentro de los procesos y estructura de la FIEC.

   Riesgo Asociado: La FIEC no cuenta con políticas de control que incluyan aspectos de seguridad de la información en sus procesos.

   Recomendación: Incorporar dentro de la estructura de la FIEC un plan que conlleve a la continuidad de procesamiento de información, establecido para administrar la disponibilidad de los procesos críticos e información, ante un desastre que ocasione interrupción en el centro de cómputo.

2. La FIEC tiene identificado sus procesos pero estos no han sido documentados en función a un análisis de riesgos que presenten su probabilidad e impacto dentro la organización.

   Riesgo Asociado: Desconocer las amenazas (internas o externas) que interrumpirían el desenvolvimiento normal del centro de cómputo, incidiendo en pérdida de información.

   Recomendación: Previo análisis, elaborar un documento que detalle los procesos críticos del centro de cómputo y su impacto dentro de la organización.

3. Los equipos que se encuentran ubicados en el centro de cómputo no tiene cobertura de póliza de seguros que forme parte de un proceso de continuidad del negocio.

   Riesgo Asociado: Pérdida total de equipos frente a un siniestro de carácter interno o externo.

   Recomendación: Contratar póliza de seguro contra todo riesgo, o al menos contra incendio para los equipos que están ubicados en el centro de cómputo.

4. No existen manuales, ni instructivos de un plan de continuidad del negocio que haga frente a los riesgos que interrumpirían con la seguridad de la información.

   Riesgo Asociado: Pérdida de información, al no tener procedimientos que permitan restaurar en corto tiempo el funcionamiento del centro de cómputo.

   Recomendación: Elaborar un manual o instructivo que incluya políticas de seguridad para la información critica que se procesa en el centro de cómputo.

5. La FIEC no tiene identificado (para la continuidad del negocio) los eventos (o secuencia de eventos) que podrían causar interrupciones en sus procesos. Por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas.

   Riesgo Asociado: Pérdida de información por desconocimiento a los eventos que causan interrupciones a los procesos.

   Recomendación: Documentar todos los escenarios posibles que causarían interrupciones en los procesos del centro de cómputo.

6. La Norma ISO, establece la participación en las evaluaciones de riesgo para la continuidad del negocio a dueños de los recursos y procesos.

   Riesgo Asociado: Plan de Continuidad del Negocio mal definido.

   Recomendación: Involucrar al personal del centro de cómputo en el análisis de las amenazas al procesamiento de información.

7. Una vez elaborada la estrategia de la continuidad del negocio, debe estar aprobada por la dirección (decanato) adjuntando el plan de implementación.

   Riesgo Asociado: Falta de recursos en la elaboración del Plan de Continuidad.

   Recomendación: Exponer las estrategias desarrolladas para la aprobación por el decanato a fin de asegurar los recursos estimados.

8. La Norma ISO, establece la asignación de responsabilidades y procedimientos de continuidad del negocio al personal a cargo del centro de cómputo.

Riesgo Asociado: Plan de Continuidad del Negocio mal Desarrollado.

Recomendación: Definir funciones y responsabilidades al personal ante una eventualidad que active el plan de continuidad del negocio.

9. La FIEC no tiene documentada la aceptación de pérdida de información y de servicios por interrupción a sus procesos.

Riesgo Asociado: No tener cuantificadas las pérdidas esperadas en función a la interrupción de los procesos en escalas de tiempo.

Recomendación: Documentar los tiempos máximos de interrupción que se aceptan perder en los servicios brindados por el centro de cómputo.

10. No se han efectuado pruebas (simulacros) ante desastres que no permitirían continuar con el procesamiento de información en el centro de cómputo.

Riesgo Asociado: Desconocimiento de las actividades a desarrollar para afrontar la contingencia.

Recomendación: Realizar y documentar los escenarios identificados que podrían interrumpir el procesamiento de información en el centro de cómputo con sus resultados.

11. La FIEC no tiene un plan de continuidad del negocio estructurado.

    Riesgo Asociado: Estar imposibilitados en contrarrestar pérdidas por interrupciones en las actividades del centro de cómputo.

    Recomendación: La Norma ISO establece para la estructuración del Plan lo siguiente: identificar condiciones para su activación, indicar procedimientos de emergencia y de respaldos, programación de mantenimientos del plan de pruebas, formación al personal en los procesos de continuidad del negocio, definir responsabilidades a las personas en la ejecución del plan y definición de recursos necesarios por parte de la dirección.

12. La FIEC no ha realizado una programación de pruebas para los planes de continuidad del negocio que indiquen cómo y cuándo se

va a probar cada elemento del plan; no han realizado pruebas de recuperación en un sitio alterno; no han realizado pruebas de los recursos y servicios del proveedor, no existen registros de los resultados de las pruebas que mejoren las acciones del plan de continuidad; además de no tener asignado responsables para las revisiones regulares de cada etapa del plan de continuidad del negocio.

Riesgo Asociado: Si el plan de continuidad del negocio no es probado y revaluado no se lo puede considerar efectivo para ser puesto en práctica en la organización.

Recomendación: Para llevar a cabo las pruebas y evaluación de planes de continuidad, se requiere primeramente: Gestión de recursos, Análisis de Impactos, Redacción e implantación, Marco de planificación, además de las pruebas necesarias que validen la efectividad del Plan de continuidad del negocio, definiendo primeramente un sitio alterno al centro de cómputo.

4.5 Evaluación de Riesgos

Se realizó una evaluación de riesgo, determinando las vulnerabilidades que afectan a los dominios de seguridad física y ambiental y de la gestión de la

continuidad del negocio; y calificando en base a su nivel de vulnerabilidad e impacto dentro de la organización.

La escala para la calificación, establecida por el equipo de trabajo se muestra en la tabla 4.5.1

Calificación	Nivel de Ocurrencia
Muy Alto	5
Alto	4
Media	3
Bajo	2
Muy Bajo	1

Tabla 4.5.1 Calificación de acuerdo al Nivel de Vulnerabilidad e Impacto

La estimación de los niveles de vulnerabilidad e impacto sobre las vulnerabilidades planteadas en cada uno de los dominios, se basó en la revisión in situ, realizada al centro de cómputo; en donde la calificación nos otorgó un nivel de criticidad definido como bajo, medio o alto; con lo que procedimos a sugerir controles que garanticen la mitigación del riesgo asociado. Ver anexo 2.

4.6 Formulación del Informe final de auditoría

Como parte final del presente trabajo realizado, se emite un informe de auditoría dirigido al Ing. Juan Moreno, responsable del centro de cómputo de la Facultad de Ingeniería en Electricidad y Computación ; el cual acoge los resultados de la revisión efectuada al área, incluyendo las conclusiones y recomendaciones pertinentes.

CONCLUSIONES

Una vez finalizado el presente proyecto de tesis, y realizada la revisión de los dominios de seguridad física y ambiental, y de la gestión de la continuidad del negocio; dominios del estándar ISO/IEC 27002, aplicados al Centro de cómputo de FIEC- ESPOL; se establecen las siguientes conclusiones:

- ✓ El área del Centro de cómputo es vulnerable a incidentes que podrían impactar negativamente en pérdida, daño, o puesta en peligro de los activos, y la interrupción de actividades.

- ✓ Tienen un déficit de extintores de incendio y de luminarias de emergencia, así como difícil acceso a los interruptores de energía eléctrica; características que no permiten mitigar actualmente y/o prepararse para eventos no contemplados.

- ✓ El centro de cómputo no cuenta con un proceso formal para la gestión de la continuidad del negocio, ante riesgos que pueden ocasionarle

interrupciones a sus procesos, no está definido un plan de continuidad del negocio.

- ✓ A pesar de tener identificado sus procesos, éstos no han sido documentados, en función a un análisis de riesgos que presenten su probabilidad e impacto dentro de la organización, tal como lo exige la norma ISO 27002.

RECOMENDACIONES

La Norma ISO 27002 está compuesta de 11 dominios, y constituye un proceso que conlleva al cumplimiento de requisitos en el mediano y largo plazo frente a una certificación; por lo que recomendamos a la FIEC lo siguiente:

- ✓ Con respecto a la Seguridad Física y Ambiental; realizar como punto de partida un análisis de riesgos a los procesos que se llevan a cabo dentro del centro de cómputo, a fin de identificar las vulnerabilidades que afecten a la seguridad de la información, y a la interrupción de sus servicios.

- ✓ En otro punto, vemos necesaria la contratación de una póliza de seguros contra incendios, a fin de trasladar el riesgo de pérdida total de equipos frente a un siniestro de carácter interno o externo en el centro de cómputo; previamente deberá existir una implementación de un número adecuado y ubicación estratégica de extintores que cubra el área en revisión.

- ✓ Con respecto a la Gestión de la Continuidad del Negocio; realizar como punto de partida, la identificación de sus procesos críticos o considerados de importancia estratégica, definición de tiempos máximos de interrupción, documentación de las amenazas y soluciones posibles como respuesta a incidentes simples hasta interrupciones totales, dentro del centro de cómputo; incidentes que puedan impactar en el personal, las operaciones y la capacidad de entregar servicios, conllevando a la pérdida de información.

BIBLIOGRAFIA

1. Norma ISO/IEC 27002, **"Código de buenas prácticas para la administración de la seguridad de la información",** Junio 2005.

2. ISACA, **"Manual de Preparación al Examen CISA"**, Edición 2008.

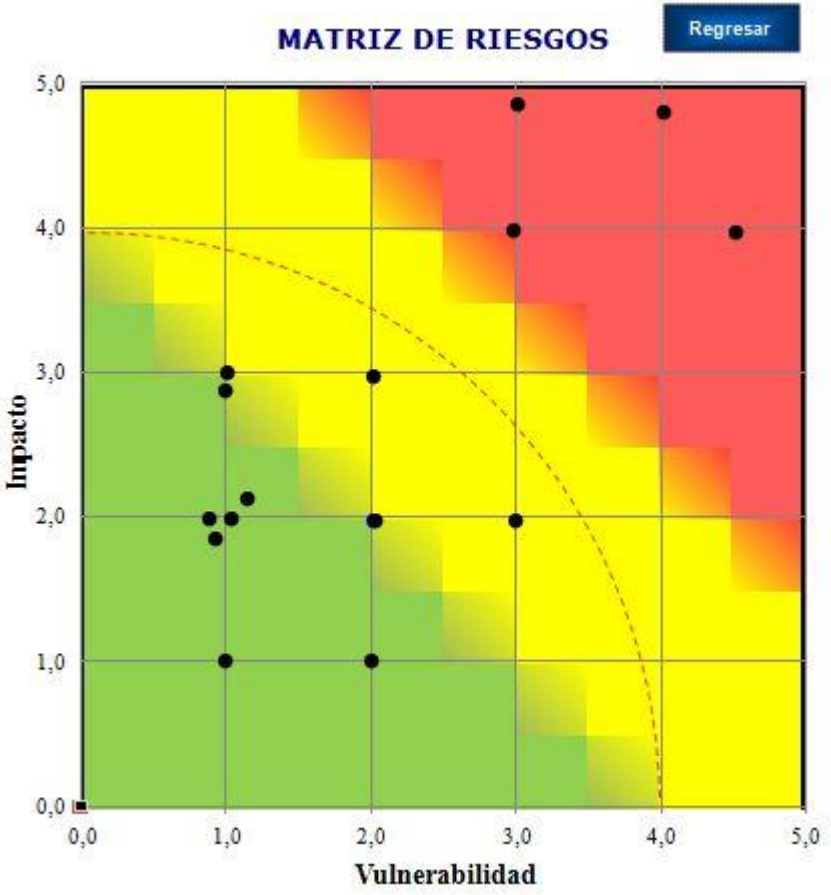
3. Apuntes, **"Módulo 5: Seguridad de la Información y Seguridad Informática – DAI IV Promoción",** Junio 2010.

4. Página Web: Sistema de Gestión de la Seguridad de la Información, Fecha de último acceso: Abril 2011. Disponible en http://www.iso27000.es

5. Página Web: Seguridad de la Información, Fecha de último acceso: Abril 2011. Disponible en http://www.segu-info.com.ar

ANEXO 2

Mapeo de Riesgos
Seguridad Física y del Entorno

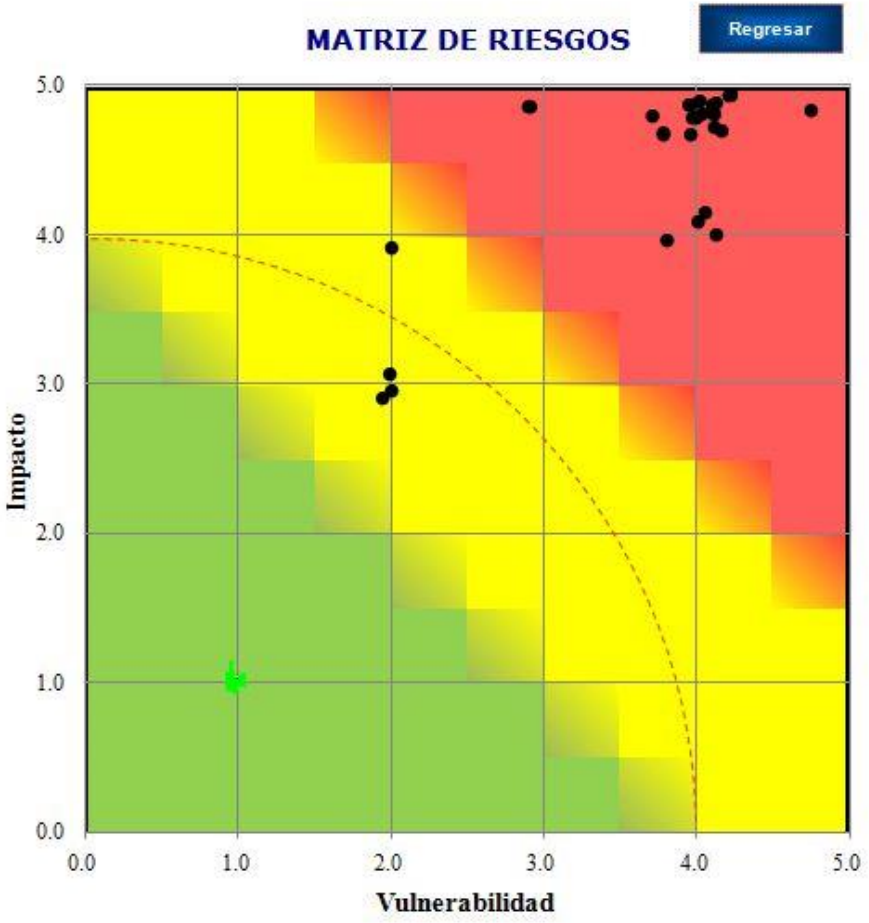


Riesgos Altos

- Propagación de Incendio.
- Pérdida de Activos de Información.
- Mal Uso o pérdida de Cintas de Respaldo.
- Imposibilidad de desactivar por parte del personal el fluido eléctrico ante una emergencia.

ANEXO 2

Mapeo de Riesgos
Gestión de la Continuidad del Negocio



Riesgo Alto

- Plan de Continuidad del Negocio No Definido.