

UNIVERSIDAD LAICA “ELOY ALFARO DE MANABÍ”



Uleam
UNIVERSIDAD LAICA
ELOY ALFARO DE MANABÍ

FACULTAD DE CIENCIAS INFORMÁTICAS



TEMA:

**“SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO
MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE
APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS”**

**TRABAJO DE TITULACIÓN: MODALIDAD PROYECTO INTEGRADOR,
PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO/A EN SISTEMAS**

AUTORES:

Acosta Alvarado Nexar Jesús
Carrillo Morán Fátima Guadalupe

DIRECTOR:

Ing. Moreira Centeno Robert Wilfrido

CODIRECTORA:

Ing. Vera Navarrete Denise Soraya

MANTA -ECUADOR

2018

	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO.	REVISIÓN: 1 Página ii de 200

CERTIFICACIÓN

En calidad de docente tutor y docente Cotutora de la Facultad de Ciencias Informáticas de la Universidad Laica "Eloy Alfaro" de Manabí, certificamos:

Haber dirigido y revisado el trabajo de titulación, cumpliendo el total de 60 horas, bajo la modalidad de Proyecto Integrador, cuyo tema del proyecto es "SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS", el mismo que ha sido desarrollado de acuerdo a los lineamientos internos de la modalidad en mención y en apego al cumplimiento de los requisitos exigidos por el Reglamento de Régimen Académico, por tal motivo CERTIFICO, que el mencionado proyecto reúne los méritos académicos, científicos y formales, suficientes para ser sometido a la evaluación del tribunal de titulación que designe la autoridad competente.

La autoría del tema desarrollado, corresponde a los señores: ACOSTA ALVARADO NEXAR JESÚS y CARRILLO MORÁN FÁTIMA GUADALUPE estudiantes de la carrera de Ingeniería en Sistemas, período académico 2016-2017(2), quien se encuentra apto para la sustentación de su trabajo de titulación.

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

Lugar, 28 de Febrero de 2018.

Lo certificamos,


Ing. ROBERT MOREIRA CENTENO


Ing. DENISE VERA NAVARRETE

Docentes de la Facultad de Ciencias Informáticas
 Universidad Laica Eloy Alfaro de Manabí



UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
Creada el 13 de noviembre de 1993 mediante Decreto Ley No. 20, publicado en el Registro Oficial No. 513
FACULTAD DE CIENCIAS INFORMÁTICAS
Creada, Resolución N. Consejo Universitario del 13 de julio del 2004



**TRABAJO DE TITULACIÓN MODALIDAD PROYECTO INTEGRADOR,
PREVIO A LA OBTENCIÓN DEL TÍTULO DE: INGENIERO E INGENIERA
EN SISTEMAS**

**"SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS
APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC
27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS
INFORMÁTICAS"**

**Tribunal examinador que declara APROBADO el Grado de INGENIERO
E INGENIERA EN SISTEMAS, del señor: NEXAR JESÚS ACOSTA
ALVARADO y señora: FÁTIMA GUADALUPE CARRILLO MORÁN**

Ing. Winther Molina Loo, Mg.

Lic. Vilka Choez Ramírez, Mg

Lic. Klever Delgado Reyes

Manta, 01 de marzo del 2018

DECLARACIÓN EXPRESA DE AUTORÍA

Nosotros, **ALVARADO ACOSTA NEXAR JESÚS** con Cédula de Identidad N° 131228697-2 y **CARRILLO MORÁN FÁTIMA GUADALUPE** con Cédula de Identidad N° 130947803-8, declaramos ser los responsable del contenido del presente proyecto integrador, cuyo tema es: “SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS.”, y derechos patrimoniales a la Universidad Laica “Eloy Alfaro de Manabí” en virtud de lo dispuesto en el Art. 15 de la Ley de Propiedad Intelectual.

A sí mismo, autorizamos a la ULEAM para que realice la digitalización y publicación de este Proyecto integrador en el repositorio digital de conformidad a lo dispuesto en el Art. 144 de la ley Orgánica de educación Superior.

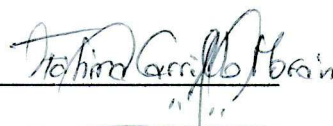
Además, la ejecución se respetaron las disposiciones legales que protegen los derechos de autores vigentes. Finalmente, la responsabilidad del contenido de este Proyecto Integrador corresponde exclusivamente a nuestra autoría.

Lo certificamos:



Acosta Alvarado Nexar Jesús

C.I. 131228697-2



Carrillo Morán Fátima Guadalupe

CI: 130947803-8

DEDICATORIA

El presente trabajo se lo dedico a Dios por la bendición de la vida y darme la fortaleza para no rendirme, a mi madre por ayudarme en este camino, a mi esposo e hijos por su apoyo y comprensión.

Fátima Guadalupe Carrillo Morán

AGRADECIMIENTO

Quiero agradecer a mi esposo Jimmy Romero por su infinita paciencia y apoyo incondicional, a mis hijos Teddy e Ithan porque son mi motivo de inspiración para siempre avanzar y mejorar.

También agradezco a mi madre, Magna Morán, y demás familiares, amigos, compañeros que me han apoyado, de una u otra forma durante todo el camino que me ha llevado hasta ahora.

A mis tutores, en especial a la Ing. Denise Vera ya que la propuesta de este proyecto surgió de ella.

Fátima Guadalupe Carrillo Morán

DEDICATORIA

Este presente proyecto se lo dedico a mis padres por el sacrificio, paciencia y esfuerzo que me brindaron día a día, por darme la oportunidad del estudio, de prepararme, de ser mejor tanto en lo personal como profesional y poder tener una vida digna.

A mis hermanos por la paciencia y la ayuda económica siempre desinteresadamente para verme realizado como profesional a mis amigos y en especial a esas personas que no creyeron en mí, el cual era para mí la mayor fuente de motivación para superarme.

También a mis compañeros de clases que pasamos por tantas penurias, que sin esperar nada a cambio compartieron sus conocimientos, alegrías, y tristezas.

Nexar Jesús Acosta Alvarado

AGRADECIMIENTO

Este presente trabajo quiero agradecer antes que nada a Dios porque nada fuera posible por él, a mis Padres, hermanos por el apoyo incondicional y económicamente, la motivación que me brindaban día a día por ser alguien mejor en la sociedad y ser orgullo de ellos y de toda la familia.

También agradezco amigos y compañeros que me han apoyado, de una u otra forma durante todo el camino que me ha llevado hasta ahora.

A la Facultad de Ciencias Informáticas, por la formación y crecimiento académica y personal, que me brindaron los profesores.

A mis tutores, en especial a la Ing. Denise Vera ya que la idea de este proyecto fue de ella.

Nexar Jesús Acosta Alvarado

ÍNDICE

RESUMEN	1
INTRODUCCIÓN.....	3
PLANTEAMIENTO DEL PROBLEMA	4
DIAGRAMA CAUSA-EFECTO DEL PROBLEMA	6
Objetivos.....	7
Objetivo general	7
Objetivos específicos de investigación y de resolución del problema	7
CAPITULO I.....	9
1 MARCO TEORICO DE LA INVESTIGACIÓN	9
1.1 Antecedentes de investigaciones relacionadas al tema presentado	10
1.2 Definiciones conceptuales	11
1.2.1 Seguridad Informática	11
1.2.2 Seguridad de la Información	13
1.2.2.1 Confidencialidad	13
1.2.2.2 Integridad	13
1.2.2.3 Disponibilidad	14
1.2.2.4 Autenticación	14
1.2.3 Activos	15
1.2.4 Vulnerabilidades.....	16
1.2.5 Amenazas	16
1.2.6 Riesgos	17
1.2.7 Análisis de Riesgos	18
1.2.8 Gestión de Riesgos	18
1.2.9 Ataque Informático.....	20
1.2.10 Impacto.....	21
1.2.11 Desastres.....	21
1.2.12 Políticas de Seguridad	22
1.2.13 ISO/IEC 17799.....	22
1.2.14 ISO/IEC 27001	23
1.2.15 Controles Informáticos	23
1.2.16 Herramientas de análisis de riesgos.....	23
1.2.16.1 EAR/PILAR Entorno de análisis de riesgos.....	24
1.2.16.2 HERRAMIENTA DE EVALUACIÓN DE SEGURIDAD DE MICROSOFT (MSAT)	27
1.2.16.3 RISICARE	28
1.2.17 Metodologías de análisis de riesgos	29
1.2.17.1 MAGERIT	30
1.2.17.1.1 Evolución de Magerit	31
1.2.17.1.2 Objetivos	31
1.2.17.1.3 Pasos de la metodología MAGERIT	33
CAPITULO II.....	41

2	MARCO INVESTIGATIVO	41
2.1	Introducción	42
2.2	Tipo(s) de Investigación	42
2.2.1	Por el nivel de conocimientos que se adquieren:	42
2.2.1.1	Investigación Descriptiva	42
2.2.2	Por las características de los medios utilizados para obtener los datos:	43
2.2.2.1	Investigación Exploratoria	43
2.2.3	Según el propósito o finalidad que se persigue:	43
2.2.3.1	Investigación Documental	43
2.3	Método de Investigación	43
2.3.1	Observación	43
2.3.2	Hipotético-Deductivo	44
2.4	Herramienta(s) de recolección de datos	44
2.4.1	Encuesta	44
2.4.2	Entrevista	44
2.4.3	Observación	44
2.5	Fuentes de Información de datos	44
2.5.1	Fuentes Primarias	45
2.5.2	Fuentes Secundarias	45
2.6	Instrumental Operacional	46
2.6.1	Estructura y características de lo(s) instrumento(s) de recolección de datos	46
2.6.1.1	Encuesta	46
2.6.1.2	Entrevista	46
2.6.1.3	Observación	46
2.7	Estrategia Operacional para la recolección y tabulación de datos	47
2.7.1	Plan de recolección	47
2.7.2	Tabulación y Análisis e interpretación de los datos	47
2.8	PLAN DE MUESTREO	48
2.8.1	Segmentación	48
2.8.2	Técnica de muestreo	48
2.8.3	Tamaño de la muestra	49
2.9	PRESENTACIÓN Y ANALISIS DE LOS RESULTADOS	50
2.9.1	Presentación y Descripción de los Resultados Obtenidos	50
2.9.2	Análisis de los Resultados	91
2.9.2.1	Análisis de Resultados de Encuesta a toda la comunidad de la FACCI (Docentes, estudiantes y personal administrativo y de servicio)	91
2.9.2.2	Análisis de Resultados de Entrevista	92
	CAPITULO III	94
3	MARCO PROPOSITIVO	94
3.1	Introducción	95
3.2	Descripción de la propuesta	95
3.3	Determinación de Recursos	96

3.3.1	Humanos.....	96
3.3.2	Tecnológicos	96
3.3.2.1	Hardware.....	96
3.3.2.2	Software	97
3.3.2.3	Materiales y otros.....	97
3.3.3	Económicos (presupuesto).....	98
3.3.3.1	Presupuesto de Recursos Humanos.....	98
3.3.3.2	Presupuesto de recursos tecnológicos	99
3.3.3.3	Presupuesto de otros recursos materiales	100
3.3.3.4	Presupuesto Total.....	100
3.4	Etapas de acción para el desarrollo de la propuesta	101
3.4.1	FASE I: ANÁLISIS DE LA INSTITUCIÓN	101
3.4.1.1	Antecedentes de la FACCI (Reseña Histórica)	101
3.4.1.2	Misión	102
3.4.1.3	Visión.....	102
3.4.1.4	Organigrama estructural de la FACCI	103
3.4.1.5	Personal involucrado en el proyecto	103
3.4.2	FASE II: ACTIVIDADES PRELIMINARES.....	104
3.4.2.1	Estudio de Oportunidad	104
3.4.2.2	Determinación del alcance del proyecto	104
3.4.2.3	Identificación de los activos	105
3.4.3	FASE III: PLANIFICACIÓN.....	106
3.4.3.1	Descripción de la metodología de trabajo	106
3.4.3.2	Bosquejo de la Metodología de Trabajo SCRUM.....	107
3.4.3.2.1	Personas o roles del Proyecto.	107
	El equipo de trabajo aplicando SCRUM se definió de la siguiente forma:.....	107
3.4.3.2.2	Descripción de los objetivos del producto (Product Backlog).....	108
3.4.3.2.3	Planeación de Sprint	108
3.4.4	FASE V: DISEÑO E IMPLEMENTACIÓN	109
3.4.4.1	Descripción de Sprints	109
3.4.4.1.1	Descripción Sprint 1	109
3.4.4.1.2	Descripción Sprint 2	109
3.4.4.1.3	Descripción Sprint 3	109
3.4.4.1.4	Descripción Sprint 4	109
3.4.4.1.5	Descripción Sprint 5	110
3.4.4.1.6	Descripción Sprint 6	110
3.4.4.1.7	Descripción Sprint 7	110
3.4.4.1.8	Descripción Sprint 8	111
3.4.4.1.9	Descripción Sprint 9	111
3.4.4.2	Detalle de cada Sprint	111
3.4.4.2.1	Requisitos y Análisis (Sprint 1)	112
3.4.4.2.1.1	Requisitos Funcionales	113

3.4.4.2.1.2	Requisitos no Funcionales	113
3.4.4.2.2	Diseño y Desarrollo de Base de Datos (Sprint 2)	113
3.4.4.2.3	Configuración de Plataformas de desarrollo (Sprint 3).....	116
3.4.4.2.4	Inicio Sesión –Home (Sprint 4)	118
3.4.4.2.5	Módulo de Ingreso (Sprint 5).....	120
3.4.4.2.6	Módulo de Cruces (Sprint 6)	124
3.4.4.2.7	Módulo de Análisis y Aplicación (Sprint 7)	126
3.4.4.2.8	Testeo (Sprint 8)	129
3.4.4.2.9	Implementación (Sprint 9).....	130
CAPITULO IV		132
4	EVALUACIÓN DE RESULTADOS	132
4.1	Introducción.....	133
4.2	Seguimiento y Monitoreo de Resultados	133
	Conclusiones.....	133
	Recomendaciones	134
	Bibliografía.....	135
ANEXOS		138
ANEXO A		139
ANEXO B		147
ANEXO C		149
ANEXO D		150
ANEXO E		151
ANEXO F		152
ANEXO G		157
ANEXO H		159
ANEXO I		160
MANUAL DE USUARIO		161
Glosario		182

ÍNDICE TABLAS

<i>Tabla 1: Listado de Activos Magerit v3</i>	35
<i>Tabla 2: Clasificación de Amenazas</i>	36
<i>Tabla 3: Tipos de Salvaguardas</i>	37
<i>Tabla 4: Comparación de Metodologías</i>	39
<i>Tabla 5: Significado de Variables de Fórmula de Tamaño de Muestra</i>	49
<i>Tabla 6: Resultado de Muestreo</i>	50
<i>Tabla 7: Frecuencia de pregunta #1</i>	51
<i>Tabla 8: Frecuencia de Pregunta #2</i>	52
<i>Tabla 9: Frecuencia de pregunta #3</i>	53
<i>Tabla 10: Frecuencia de Pregunta #4</i>	54
<i>Tabla 11: Frecuencia de Pregunta #5</i>	56
<i>Tabla 12: Frecuencia de Pregunta #6</i>	57
<i>Tabla 13: Frecuencia de Pregunta #7</i>	58
<i>Tabla 14: Frecuencia de Pregunta #8</i>	59
<i>Tabla 15: Frecuencia de Pregunta #9</i>	60
<i>Tabla 16: Frecuencia de Pregunta #10</i>	61
<i>Tabla 17: Frecuencia de Pregunta #11</i>	63
<i>Tabla 18: Frecuencia de Pregunta #12</i>	64
<i>Tabla 19: Frecuencia de Pregunta #13</i>	65
<i>Tabla 20: Frecuencia de Pregunta #14</i>	66
<i>Tabla 21: Frecuencia de Pregunta #15</i>	67
<i>Tabla 22: Frecuencia de Pregunta #16</i>	69
<i>Tabla 23: Frecuencia de Pregunta #17</i>	70
<i>Tabla 24: Frecuencia de Pregunta #18</i>	71
<i>Tabla 25: Frecuencia de Pregunta #19</i>	72
<i>Tabla 26: Frecuencia de Pregunta #20</i>	73
<i>Tabla 27: Frecuencia de Pregunta #21</i>	75
<i>Tabla 28: Frecuencia de Pregunta #22</i>	76
<i>Tabla 29: Frecuencia de Pregunta #23</i>	77
<i>Tabla 30: Frecuencia de Pregunta #24</i>	78
<i>Tabla 31: Frecuencia de Pregunta #25</i>	79
<i>Tabla 32: Frecuencia de Pregunta #26</i>	80
<i>Tabla 33: Frecuencia de Pregunta #27</i>	81
<i>Tabla 34: Frecuencia de Pregunta #28</i>	82
<i>Tabla 35: Frecuencia de Pregunta #29</i>	83
<i>Tabla 36: Frecuencia de Pregunta #30</i>	85
<i>Tabla 37: Frecuencia de Pregunta #31</i>	86
<i>Tabla 38: Frecuencia de Pregunta #32</i>	87
<i>Tabla 39: Frecuencia de Pregunta #33</i>	88
<i>Tabla 40: Frecuencia de Pregunta #34</i>	89
<i>Tabla 41: Frecuencia de Pregunta #35</i>	90
<i>Tabla 42: Recursos Humanos</i>	96
<i>Tabla 43: Recursos Tecnológicos - Hardware</i>	96
<i>Tabla 44: Recursos Tecnológicos - Software</i>	97
<i>Tabla 45: Recursos Materiales y otros</i>	97
<i>Tabla 46: Presupuesto Recursos Humanos</i>	98
<i>Tabla 47: Presupuesto Recursos Tecnológicos</i>	99
<i>Tabla 48: Presupuesto Recursos Tecnológicos</i>	100
<i>Tabla 49: Presupuesto Total</i>	100
<i>Tabla 50: Identificación de Activos Informáticos de la FACCI</i>	105
<i>Tabla 51: Personas o roles del Proyecto</i>	107
<i>Tabla 52: Product Backlog</i>	108

ÍNDICE DE ILUSTRACIONES

<i>Ilustración 1: Diagrama Causa-Efecto</i>	6
<i>Ilustración 2: Objetivos de Magerit</i>	31
<i>Ilustración 3: Elementos del análisis de riesgos potenciales</i>	34
<i>Ilustración 4: Organigrama funcional de la FACCI</i>	103
<i>Ilustración 5: Título de encuesta</i>	139
<i>Ilustración 6: Preguntas 1 y 2 de encuesta</i>	139
<i>Ilustración 7: Preguntas 3, 4 y 5 de encuesta</i>	140
<i>Ilustración 8: Preguntas 6 y 7 de encuesta</i>	140
<i>Ilustración 9: Preguntas 8, 9 y 10 de encuesta</i>	141
<i>Ilustración 10: Preguntas 11 y 13 de encuesta</i>	141
<i>Ilustración 11: Preguntas 13, 14 y 15 de encuesta</i>	142
<i>Ilustración 12: Preguntas 16 y 17 de encuesta</i>	142
<i>Ilustración 13: Preguntas 18,19 y 20 de encuesta</i>	143
<i>Ilustración 14: Preguntas 21,22 y 23 de encuesta</i>	143
<i>Ilustración 15: Preguntas 24 y 25 de encuesta</i>	144
<i>Ilustración 16: Preguntas 26, 27 y 28</i>	144
<i>Ilustración 17: Preguntas 29 y 30 de encuesta</i>	145
<i>Ilustración 18: Preguntas 31, 32 y 33 de encuesta</i>	145
<i>Ilustración 19: Preguntas 34 de encuesta</i>	146
<i>Ilustración 20: Pregunta 35 de encuesta</i>	146
<i>Ilustración 21: Documento 1 de entrevista con Jefe de Informática de la FACCI</i>	147
<i>Ilustración 22: Documento 2 de entrevista con Jefe de Informática de la FACCI</i>	148
<i>Ilustración 23: Fotografía realizando entrevista a Jefe de Laboratorios</i>	149
<i>Ilustración 24: Oficio de solicitud de Activos</i>	150
<i>Ilustración 25: Resumen de participantes de la encuesta</i>	151
<i>Ilustración 26: Hoja 1 Activos de la FACCI</i>	152
<i>Ilustración 27: Hoja 2 Activos de la FACCI</i>	153
<i>Ilustración 28: Hoja 3 Activos de la FACCI</i>	154
<i>Ilustración 29: Hoja 4 Activos de la FACCI</i>	155
<i>Ilustración 30: Hoja 5 Activos de la FACCI</i>	156

ÍNDICE DE GRAFICOS

<i>Gráfico 1: Frecuencia de la Pregunta #1</i>	50
<i>Gráfico 2: Frecuencia de la Pregunta #2</i>	52
<i>Gráfico 3: Frecuencia de la Pregunta #3</i>	53
<i>Gráfico 4: Frecuencia de la Pregunta #4</i>	54
<i>Gráfico 5: Frecuencia de la Pregunta #5</i>	55
<i>Gráfico 6: Frecuencia de la Pregunta #6</i>	57
<i>Gráfico 7: Frecuencia de la Pregunta #7</i>	58
<i>Gráfico 8: Frecuencia de la Pregunta #8</i>	59
<i>Gráfico 9: Frecuencia de la Pregunta #9</i>	60
<i>Gráfico 10: Frecuencia de la Pregunta #10</i>	61
<i>Gráfico 11: Frecuencia de la Pregunta #11</i>	62
<i>Gráfico 12: Frecuencia de la Pregunta #12</i>	63
<i>Gráfico 13: Frecuencia de la Pregunta #13</i>	65
<i>Gráfico 14: Frecuencia de la Pregunta #14</i>	66
<i>Gráfico 15: Frecuencia de la Pregunta #15</i>	67
<i>Gráfico 16: Frecuencia de la Pregunta #16</i>	68
<i>Gráfico 17: Frecuencia de la Pregunta #17</i>	70
<i>Gráfico 18: Frecuencia de la Pregunta #18</i>	71
<i>Gráfico 19: Frecuencia de la Pregunta #19</i>	72
<i>Gráfico 20: Frecuencia de la Pregunta #20</i>	73
<i>Gráfico 21: Frecuencia de la Pregunta #21</i>	74
<i>Gráfico 22: Frecuencia de la Pregunta #22</i>	75
<i>Gráfico 23: Frecuencia de la Pregunta #23</i>	76
<i>Gráfico 24: Frecuencia de la Pregunta #24</i>	78

Gráfico 25: Frecuencia de la Pregunta #25.....	79
Gráfico 26: Frecuencia de la Pregunta #26.....	80
Gráfico 27: Frecuencia de la Pregunta #27.....	81
Gráfico 28: Frecuencia de la Pregunta #28.....	82
Gráfico 29: Frecuencia de la Pregunta #29.....	83
Gráfico 30: Frecuencia de la Pregunta #30.....	84
Gráfico 31: Frecuencia de la Pregunta #31.....	85
Gráfico 32: Frecuencia de la Pregunta #32.....	86
Gráfico 33: Frecuencia de la Pregunta #33.....	87
Gráfico 34: Frecuencia de la Pregunta #34.....	89
Gráfico 35: Frecuencia de la Pregunta #35.....	90
Gráfico 36: Planeación de Sprint.....	108
Gráfico 37: Sprint 1.....	109
Gráfico 38: Sprint 2.....	109
Gráfico 39: Sprint 3.....	109
Gráfico 40: Sprint 4.....	110
Gráfico 41: Sprint 5.....	110
Gráfico 42: Sprint 6.....	110
Gráfico 43: Sprint 7.....	111
Gráfico 44: Sprint 8.....	111
Gráfico 45: Sprint 9.....	111
Gráfico 46: Historia Sprint 1.....	112
Gráfico 47: Seguimiento Sprint 1.....	113
Gráfico 48: Historia Sprint 2.....	114
Gráfico 49: Seguimiento Sprint 2.....	114
Gráfico 50: Modelo Entidad / Relación.....	115
Gráfico 51: Script de creación de BD y tablas.....	115
Gráfico 52: Historia Sprint 2.....	116
Gráfico 53: Seguimiento Sprint 2.....	116
Gráfico 54: Seguimiento Sprint 3.....	117
Gráfico 56: Ejecutable Netbeans 8.0.....	117
Gráfico 55: Netbeans 8.0.....	117
Gráfico 57: Librerías en Netbeans 8.0.....	118
Gráfico 58: Métodos de Conexión de Netbeans con MySQL.....	118
Gráfico 59: Historia Sprint 4.....	118
Gráfico 60: Seguimiento Sprint 4.....	119
Gráfico 61: Interfaz Login.....	119
Gráfico 62: Interfaz Información y Contacto.....	120
Gráfico 63: Historia Sprint 5.....	121
Gráfico 64: Seguimiento Sprint 5.....	121
Gráfico 65: Ingreso usuario Administrador.....	121
Gráfico 66: Ingreso Activos usuario Administrador.....	122
Gráfico 67: Ingreso Activos usuario Auxiliar.....	122
Gráfico 68: Ingreso Amenazas Usuario Administrador.....	123
Gráfico 69: Ingreso Amenazas Usuario Auxiliar.....	123
Gráfico 70: Historia Sprint 6.....	124
Gráfico 71: Seguimiento Sprint 6.....	125
Gráfico 72: Cruce Activo-Amenaza Usuario Administrador.....	125
Gráfico 73: Cruce Activos-Amenazas de Usuario Auxiliar.....	126
Gráfico 74: Historia Sprint 7.....	126
Gráfico 75: Seguimiento Sprint 7.....	127
Gráfico 76: Interfaz de Análisis de Usuario Administrador.....	127
Gráfico 77: Interfaz Análisis Usuario Auxiliar.....	128
Gráfico 78: Interfaz de Aplicación Usuario Administrador.....	128
Gráfico 79: Interfaz de Aplicación Usuario Auxiliar.....	129
Gráfico 80: Historia Sprint 8.....	129
Gráfico 81: Seguimiento Sprint 8.....	130
Gráfico 82: Historia Sprint 9.....	131
Gráfico 83: Seguimiento Sprint 9.....	131

RESUMEN

Este proyecto consiste en la realización de un análisis de riesgo de seguridad de la información de los activos de una Organización, para poder definir los controles necesarios que se necesitan para cumplir todos los requerimientos de protección de sus activos.

En el desarrollo de este proyecto se ha definido una metodología de trabajo acorde a las necesidades, cultura, y estructura específicas de la Institución y de uso habitual en el mercado de la seguridad de la información.

Una vez definida la metodología se ha diseñado y desarrollado un software como herramienta informática de soporte, que permite aplicar la metodología de forma eficaz y eficiente, mostrando controles de las ISO/IEC 17799 e ISO/IEC 27001 recomendados para su aplicabilidad.

Finalmente como caso de aplicación se ha realizado pruebas con los activos de laboratorios de la Facultad de Ciencias Informáticas

ABSTRACT

This project consists of carrying out an analysis of the security risk of the information of the assets of an Organization, in order to be able to define the necessary controls that are needed to fulfill all the protection requirements of its assets.

In the development of this project, a working methodology has been defined according to the specific needs, culture, and structure of the Institution and of habitual use in the information security market.

Once the methodology has been defined, software has been designed and developed as a support tool for the application of the methodology in an effective and efficient manner, showing controls of the ISO / IEC 17799 and ISO / IEC 27001 recommended for its applicability.

Finally, as an application case, tests were carried out with the assets of laboratories of the Faculty of Computer Science

INTRODUCCIÓN

En la actualidad el capital más importante de las organizaciones es su información, por tanto es un reto informático mantener este bien con características de confidencialidad, disponibilidad, e integridad. Los riesgos de los sistemas de información pueden provocar grandes pérdidas en los negocios si no son controlados a tiempo y mediante una forma adecuada. Por ello existen hoy en día metodologías de gestión de riesgos tecnológicos para proteger la información y conocer las fortalezas y debilidades que pueda tener un servicio.

La Facultad de Ciencias Informáticas está sufriendo en la actualidad robos y daños de activos, por ello este trabajo de titulación realizara una investigación de metodologías de análisis de riesgos donde seleccionaremos la automatización de MAGERIT, donde se indicaran los controles de las ISO/IEC 17799 e ISO/IEC 27001 a aplicar para mitigar las vulnerabilidades y amenazas de los sistemas de información y la infraestructura de la FACCI.

En el primer capítulo de este trabajo se va a contemplar de forma teórica los temas investigados, tanto la comparación de metodologías, como la elección de MAGERIT para la implementación, así como algunos software que existen en la actualidad, su funcionalidad, y adquisición.

En el segundo capítulo es el marco investigativo (diseño metodológico), donde se van a indicar las herramientas, técnicas y métodos utilizados para la recolección de datos que sirven para el desarrollo de este Proyecto Integrador.

En el tercer capítulo se realiza la descripción de la propuesta de este trabajo de titulación, detallando su alcance, los recursos como es el humano, tecnológico, así como la factibilidad, los riesgos y la selección de las herramientas de desarrollo.

En el capítulo final se tiene previsto la implementación para realización de análisis de riesgos de los activos facilitados por la Facultad de Ciencias Informáticas.

UBICACIÓN Y CONTEXTUALIZACIÓN DE LA INVESTIGACIÓN

PLANTEAMIENTO DEL PROBLEMA

El reciente intento de robo o detención de información, en grandes empresas de Europa que pedían a cambio de la liberación dinero en bitcoin, lo realizaron través de un virus malicioso rasomwere, esto se produjo por desconocimiento y falta de sensibilización de los usuarios y de los responsables de Informática al no detectar correos malicioso o páginas web maliciosas. El análisis de riesgos permite estar preparados en cualquier tipo de emergencia como esta y más que todo conocer los tipos de amenazas y deficiencias o huecos existentes en los sistemas de información, ya sea físico y lógico de la organización.

Se suma el aumento y la necesidad de aplicar las nuevas tecnologías en las empresas, lo que conlleva a que estas se vean obligadas a depender cada vez más de la información, de su procesamiento y sobre todo de TI. Los riesgos de los sistemas de información pueden provocar grandes pérdidas en los negocios si no son controlados a tiempo y mediante una forma adecuada. Por ello existen hoy en día metodologías de gestión de riesgos tecnológicos para proteger la información y conocer las fortalezas y debilidades que pueda tener un servicio.

Debido a la falta de control de riesgos existen vulnerabilidades de los sistemas de Información y en muchas de las organizaciones se presentan problemas, como la fuga de información, hackeo, daño de infraestructura por desastres naturales entre otros, esto se debe a que no realizan análisis de riesgos para obtener posibles amenazas y luego mitigarlas y así

aplicar el plan de contingencia y estar preparado en caso de que exista algún problema como el que se ha mencionado.

Específicamente este proyecto se va a enfocar en la Facultad de Ciencias Informáticas de la ULEAM, ya que se ha identificado deficiencia en el establecimiento y ejecución metodológica de normas que minimicen los riesgos a la información, la infraestructura informática y al mismo personal.

DIAGRAMA CAUSA-EFECTO DEL PROBLEMA

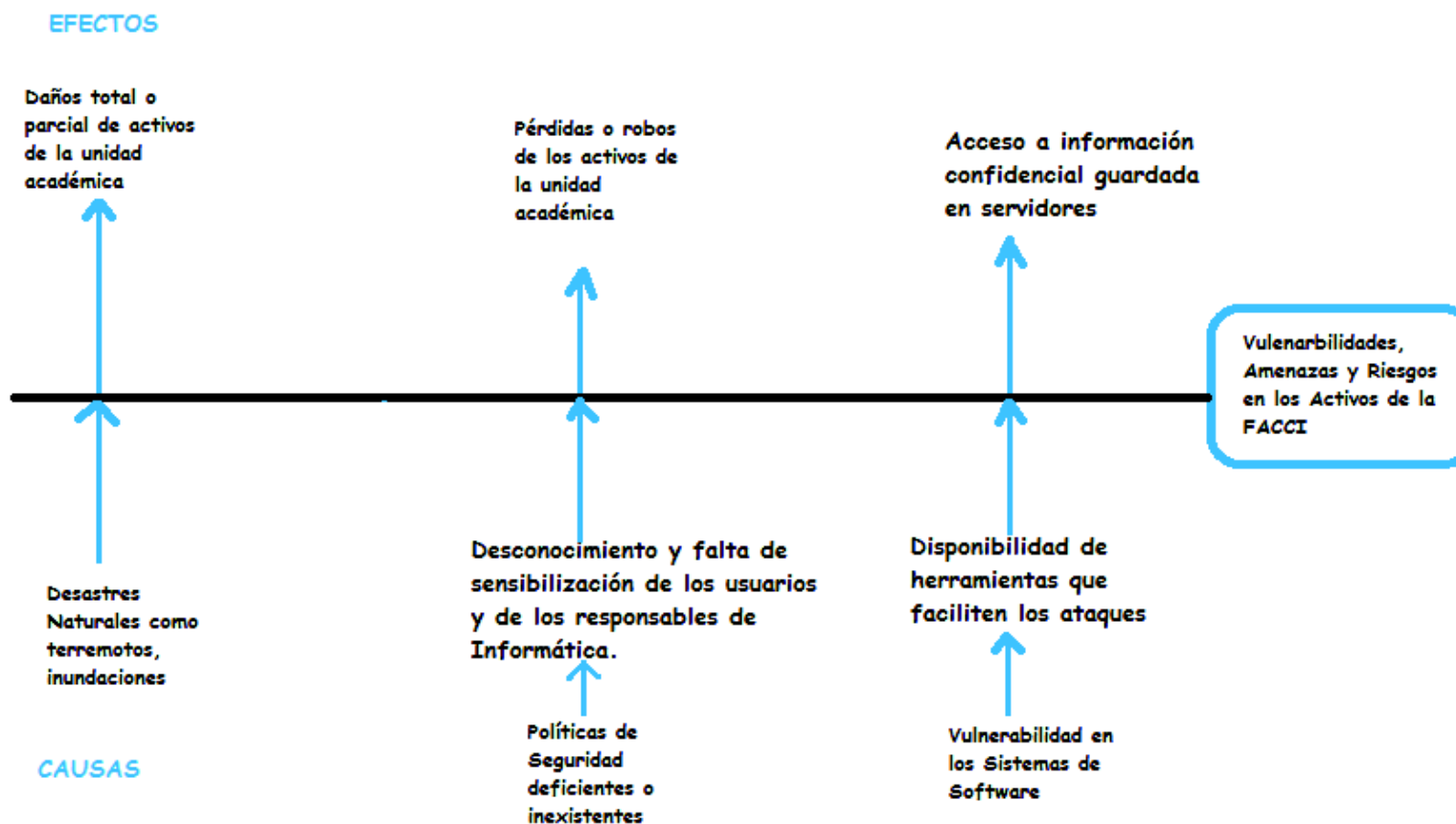


Ilustración 1: Diagrama Causa-Efecto

Fuente: Autores

Objetivos

Objetivo general.

Desarrollar un sistema de gestión de riesgo informático, basado en la metodología MAGERIT, para evaluar, controlar y mitigar las vulnerabilidades y amenazas de los sistemas de información y la infraestructura informática de la Facultad de Ciencias Informáticas.

Objetivos específicos de investigación y de resolución del problema

- Analizar y evaluar metodologías de Gestión de Riesgos.
- Obtener activos de la FACCI para su evaluación de riesgos.
- Diseñar software de escritorio basado en la metodología MAGERIT y NORMAS ISO/IEC 17799 e ISO/IEC 27001 para el análisis de riesgo en la FACCI.
- Implementar y evaluar Sistema de Gestión de Riesgo Informático en la FACCI

Justificación

La mayoría de organizaciones públicas o privadas en la actualidad se ven obligadas a actualizarse con las nuevas tecnologías, lo que conlleva a tener una gran cantidad de información, así como activos, y es aquí donde el análisis de riesgo es relevante realizarlo para poder mitigar las vulnerabilidades amenazas y riesgos que puedan sufrir.

En el terremoto del 16 A currido en Ecuador, se puedo verificar que la mayoría de organizaciones no tuvieron previsto lo ocurrido, y especificando concretamente en la facultad de Ciencias Informáticas los activos corren muchas amenazas, vulnerabilidades y un gran riesgo ya que no se aplica ninguna metodología que pueda mitigarlos, se podrían citar los robos ocurridos recientemente, por ello para poder evitar estos es necesario el análisis de riesgo.

CAPITULO I

1 MARCO TEORICO DE LA INVESTIGACIÓN

1.1 Antecedentes de investigaciones relacionadas al tema presentado

Existen algunas propuestas de tesis realizadas de Seguridad Informática tanto en nuestra alma mater, como en otras universidades, las cuales nos han servido de referencia y se citan a continuación:

Tema 1: “PROPUESTA DE UN SISTEMA DE GESTIÓN DE RIESGOS MEDIANTE LA METODOLOGÍA MAGERIT APLICADO A LOS ACTIVOS INFORMÁTICOS. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS”

Este tema se presentó en el año 2016 en la Universidad Laica “Eloy Alfaro de Manabí” en la Facultad de Ciencias Informáticas por Alcívar Zambrano Ginella Michelle en donde realizan una propuesta de la gestión de activos mediante la metodología MAGERIT aplicando el software PILAR para la obtención de resultados.

Tema 2: “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA COMPAÑÍA DE SEGUROS”

Este tema se presentó en Abril del 2011 en Lima-Perú en la Universidad Pontificia Católica del Perú en la Facultad de Ciencias e Ingeniería realizado por Ampuero Chang Carlos Enrique, donde realizan un estudio del diseño que debe de tener un sistema de gestión de seguridad específicamente para empresas de seguros.

Tema 3: “PLAN DE SEGURIDAD INFORMÁTICA PARA LA ESPE SEDE LATACUNGA”

Este tema fue presentado en el 2015 en Sangolquí en la Universidad de las Fuerzas Armadas ESPE, realizado por Aguirre Martínez Cristian Fabián y por Castellanos Campoverde Yinson Patricio, donde concluyen un plan de seguridad informático aplicado a la ESPE con sede en Latacunga.

Tema 4: “APLICACIÓN DE LA METODOLOGÍA MAGERIT PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A LA EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A EN LA CIUDAD DE MACHALA”

En el año 2013 se presentó este tema en la Universidad Politécnica Salesiana con Sede en Cuenca, en la Carrera de Ingeniería en Sistemas, realizado por Karina del Rocío Gaona Vásquez, donde realizan un análisis exhaustivo de la empresa citada mediante la metodología MAGERIT mediante el software PILAR

1.2 Definiciones conceptuales

1.2.1 Seguridad Informática

Según (Vieites, 2014) en la actualidad las actividades cotidianas de las empresas y de las distintas Administraciones Públicas e, incluso, las de muchas otras instituciones y organismos, así como las de los propios ciudadanos, requieren del correcto funcionamiento de los sistemas y redes informáticas que las soportan y, en especial, de su seguridad.

Por ello indica el autor del libro que a todos los aspectos relacionados con la seguridad informática se le debe de dar una gran importancia en una organización, y la de los virus y códigos malignos y su rápida distribución a través de redes como Internet, así como los miles de ataques e incidentes de seguridad que se producen todos los años han contribuido a despertar un mayor interés por esta cuestión.

Este autor define la Seguridad Informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Nos dice el autor (Vieites, 2014), que se puede mencionar otra definición propuesta por el INFOSEC Glossary 2000: Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos

de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican.

Concluye el autor indicando que hoy en día uno de los principios de las buenas prácticas de la gestión corporativa es el de la seguridad de la información, siendo responsabilidad de la Alta Dirección el poner los recursos y medios necesarios para implantación de un adecuado sistema de Gestión de la Seguridad de la Información en el conjunto de la organización (Vieites, 2014).

Por otro lado (Escrivá Gascó, 2013) indica que la seguridad informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida. Distingue los siguientes tipos:

En función de lo que se quiere proteger:

- Seguridad física: se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.
- Seguridad lógica: mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.

En función del momento en que tiene lugar la protección:

- Seguridad activa: se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas).

Por ejemplo, utilización de contraseñas.

- Seguridad pasiva: comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Por ejemplo, las copias de seguridad.

1.2.2 Seguridad de la Información

Para Escrivá Gascó, 2013 la seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información.

El autor (T., 2015) indica que la seguridad de la información es más que un problema de seguridad de datos en las computadoras, ya que debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas.

1.2.2.1 Confidencialidad

Según (Dirección General de Modernización Administrativa, 2012) es la propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

1.2.2.2 Integridad

Según (Dirección General de Modernización Administrativa, 2012) integridad es la propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el

punto de vista de integridad cuando su alteración no supone preocupación alguna (Dirección General de Modernización Administrativa, 2012).

1.2.2.3 Disponibilidad

Según (Dirección General de Modernización Administrativa, 2012) disponibilidad es la propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves. Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño. La disponibilidad es una característica que afecta a todo tipo de activos. A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada (Dirección General de Modernización Administrativa, 2012).

Para (Martínez, 2017) la disponibilidad de la información representa para los usuarios la garantía de posibilidad de utilización cuando sea requerida o necesitada.

1.2.2.4 Autenticación

Este término se refiere a los mecanismos de seguridad que posea los equipos que utilicemos para comunicarnos, permitiéndonos verificar si el origen de los datos es correcto, quien los envió y cuando fueron enviados y recibidos (Vásquez, 2013).

1.2.3 Activos

En una organización existen diferentes tipos de activos, según (Dirección General de Modernización Administrativa, 2012) los esenciales serían los siguientes:

Dícese de aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar aquellos que son imprescindibles para que la Organización supere una situación de emergencia, aquellos que permiten desempeñar o reconstruir las misiones críticas, aquellos sustancian la naturaleza legal o los derechos financieros de la Organización o sus usuarios.

Dícese de cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

Dícese de aquellos sometidos a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es especialmente relevante. La tipificación de qué datos deben ser clasificados y cuáles son las normas para su tratamiento, vienen determinadas por regulaciones sectoriales, por acuerdos entre organizaciones o por normativa interna.

Los autores (Escrivá Gascó, 2013) definen a un activo como aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no. Según esta definición, consideraremos como activos: los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc.

1.2.4 Vulnerabilidades

El autor (Baca Urbina, 2016) indica que vulnerabilidades son los puntos débiles que existen en los sistemas de información, y dependiendo del número de vulnerabilidades se tiene más o menos riesgos.

Según (Escrivá Gascó, 2013) se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc. Por ejemplo, no utilizar ningún tipo de protección frente a fallos eléctricos o carecer de mecanismos de protección frente a ataques informáticos, como antivirus o cortafuegos.

1.2.5 Amenazas

Se entiende por amenaza una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad (no cumplimiento de alguno de los aspectos mencionados), afectando parte de la información y de la TI de la organización (Baca Urbina, 2016).

Según (Costas Santos, 2014) las amenazas a un sistema informático pueden provenir desde un hacker remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Se pueden clasificar por tanto en amenazas provocadas por:

- Personas
- Amenazas lógicas
- Amenazas físicas.

Los autores (Escrivá Gascó, 2013) indican que una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño. Las amenazas se suelen dividir en pasivas y activas, en función de las acciones realizadas por parte del atacante:

Amenazas pasivas, también conocidas como “escuchas”. Su objetivo es obtener información relativa a una comunicación. Por ejemplo, los equipos informáticos portátiles que utilizan programas especializados para monitorizar el tráfico de una red WiFi.

Amenazas activas, que tratan de realizar algún cambio no autorizado en el estado del sistema, por lo que son más peligrosas que las anteriores. Como ejemplos se encuentran la inserción de mensajes ilegítimos, la usurpación de identidad, etc.

1.2.6 Riesgos

Las causas de riesgo de afectación de los recursos informativos de las entidades muchas veces se deben a la calidad deficiente de las aplicaciones informáticas en algunas de las fases de su ciclo de vida. Por ello es necesario que el diseño y la elaboración de los sistemas, así como las posibles adquisiciones de estos, tengan el más alto nivel de calidad posible (Blanco Encinosa, 2005).

Según (Álvarez Maraño, Seguridad informática para empresas y particulares, 2004) los riesgos no se pueden eliminar por completo, lo que hacen es reducirse de manera aceptable.

En términos generales, (Baca Urbina, 2016) define el riesgo como la posibilidad de que no se obtengan los resultados deseados. En informática, las empresas nunca desean sufrir un ataque externo o interno a sus sistemas de información, pero los ataques siempre suceden, de manera que esa posibilidad o probabilidad se materializa. La empresa siempre está amenazada de sufrir algún daño en su sistema informático. Los clasifica en riesgos tecnológicos y externos.

1.2.7 Análisis de Riesgos

El análisis de riesgos es conocido como el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. Permite determinar cómo es, cuánto vale y cómo de protegido se encuentra un sistema, siguiendo los objetivos, estrategia y política de la organización para elaborar un plan de seguridad. Al implantar y operar este plan debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la Dirección de la organización. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos (Miranda, PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA, 2015).

1.2.8 Gestión de Riesgos

Según (Cárdenas, 2013) indica que las empresas o entidades que adoptan un criterio equilibrado ante la madurez de la gestión de riesgos de tecnologías de la información, no sólo tienen menos incidentes en este ámbito sino que obtienen

mayor rentabilidad del negocio y de tecnologías de la información respecto de la competencia, nos dice que el criterio idóneo es el que equilibra las tres disciplinas principales involucradas en la gestión de riesgos de tecnologías de la información: los procesos de gobierno de riesgos, un entorno sólido de tecnologías de la información y una cultura consciente de los riesgos. Todos aquellos que adopten este criterio no sólo evitarán la interrupción de sus operaciones, sino que además lograrán mayor eficacia y agilidad en la empresa. Pueden aprovechar las funciones de gestión de riesgos de tecnologías de la información para mejorar la gestión de tecnologías de la información en general.

Según (Gómez, 2010) la disciplina de gestión de riesgos de tecnologías de la información se enmarca no sólo dentro de los requerimientos regulatorios, sino también dentro de los de negocio. Un profesional de la gestión del riesgo en tecnologías de la información debe ser especialista en tecnología y sistemas de gestión de seguridad de la información, y también tener un amplio conocimiento del negocio de la empresa en la que desarrolla su actividad. El reto actual de gestión de riesgos de tecnologías de la información se basa en definir un programa continuo, objetivo, repetible y medible, en el que la evaluación de costos, la valoración de activos y las métricas de rendimiento convivan de manera integrada con el resto de requerimientos corporativos. La creación del programa debe realizarse desde una perspectiva de arriba hacia abajo, totalmente enmarcada en la gestión global de los riesgos y respondiendo a los diferentes requerimientos de las distintas unidades de negocio, consiguiendo gestionar y definir unos controles flexibles y adaptables a los distintos tipos de riesgos y de requerimientos regulatorios que no obliguen a la organización de tecnologías de la información a reinventar las tareas, y los controles y las evidencias de cumplimiento.

Se puede plantear de forma general que la gestión de riesgos en tecnologías de la información se basa en los siguientes pasos:

Estimación de Riesgos: La estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos:

- La identificación de riesgos.
- El análisis de riesgos.
- La asignación de prioridades a los riesgos.
- Administración de riesgos: su objetivo, es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestos las actividades, categorías o ramas que presentan cada empresa, organización o entidad.
- Monitorización de riesgos: la vida en el mundo informático sería más fácil si los riesgos apareciesen después de que hayamos desarrollado planes para tratarlos. Pero los riesgos aparecen y desaparecen dentro del entorno informático, por lo que se necesita una monitorización para comprobar cómo progresa el control de un riesgo e identificar como aparecen nuevos eventos perjudiciales en las actividades informáticas.

1.2.9 Ataque Informático

Según (T., 2015) indica que en la encuesta anual de Seguridad que realiza el FBI se muestra que los virus informáticos siguen siendo la principal fuente de pérdida financiera en las organizaciones, seguidos por los impactos derivados de accesos no autorizados a los sistemas, el robo de información de propiedad industrial, y la

pérdida de computadores personales o elementos de computación móvil, estas causas generan más de un 74% del total de pérdidas financieras.

1.2.10 Impacto

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal; estas consecuencias para la empresa reciben el nombre de impacto. Dicho de otra forma, el impacto sería el alcance producido o daño causado en caso de que una amenaza se materialice. Dos organizaciones pueden verse afectadas en diferente medida ante la materialización de la misma amenaza si han adoptado estrategias diferentes para solucionarla. Así, el impacto del borrado del disco duro ocasionado por un virus informático será muy escaso en una empresa que realiza periódicamente copias de seguridad de la información importante, pero será bastante grave en una empresa que no lleva a cabo copias de seguridad regularmente.

Un impacto leve no afecta prácticamente al funcionamiento de la empresa y se produce en organizaciones que han identificado las amenazas y han establecido las pautas a seguir en el caso de que se materialicen. Por otro lado, un impacto grave afecta seriamente a la empresa pudiendo ocasionar su quiebra y se produce en organizaciones que no han considerado las consecuencias que supone para ellas la materialización de esa amenaza. Las empresas deben, por tanto, identificar los impactos para la organización en el caso de que las posibles amenazas se produzcan. Esta tarea es uno de los objetivos del análisis de riesgos que debe realizar toda organización (Escrivá Gascó, 2013).

1.2.11 Desastres

Según ISO 27001, un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque (Escrivá Gascó, 2013).

1.2.12 Políticas de Seguridad

El autor (Álvarez Marañón, Seguridad informática para empresas y particulares, 2004) indica que las políticas de seguridad delimitan las reglas que la organización espera sean seguidas por sus miembros y las consecuencias derivadas de no cumplir constituyen la piedra angular para la implantación de la seguridad, indica que por lo general el número de políticas se corresponde con el número de áreas identificadas en los objetivos de seguridad, sobre todo el autor dice que se deben de implantar no solo dejarlas en papel.

1.2.13 ISO/IEC 17799

ISO/IEC 17799 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Técnicas de seguridad TI*.

La segunda edición cancela y reemplaza la primera edición (ISO/IEC 17799:2000), la cual ha sido revisada técnicamente.

El ISO/IEC JTC 1/SC 27 viene desarrollando una familia de Estándares Internacionales para el Sistema de Gestión de Seguridad de la Información (ISMS). La familia incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. La familia adoptará el esquema de numeración utilizando las series del número 27000 en secuencia.

A partir del 2007, se propone incorporar una edición nueva del ISO/IEC 17799 en este nuevo esquema de numeración con el nombre ISO/IEC 27002 (ISO/IEC, ESTÁNDAR INTERNACIONAL ISO/IEC 17799, 2005).

1.2.14 ISO/IEC 27001

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización: por ejemplo, una situación simple requiere una solución SGSI simple (ISO/IEC, ESTÁNDAR INTERNACIONAL ISO/IEC 27001, 2005).

1.2.15 Controles Informáticos

Nos dice (Blanco Encinosa, 2005) en su libro que *Un control informativo es una acción que se diseña en un sistema informático, o en un área de procesamiento de información, para eliminar o disminuir posibles causas de riesgos durante la explotación u operación.*

1.2.16 Herramientas de análisis de riesgos

Indica la autora (Chicano Tejada, 2014) que las herramientas de gestión de riesgos sirven para ayudar a identificar los recursos importantes en la organización, los

riesgos a los que están sometidos y el daño que pueden sufrir en caso de producirse una amenaza de cualquier tipo. A continuación vamos a citar algunas mas relevantes:

1.2.16.1 EAR/PILAR Entorno de análisis de riesgos

PILAR es una herramienta desarrollada para soportar el análisis y la gestión de riesgos de sistemas de información siguiendo la metodología MAGERIT. Las siglas de PILAR provienen de “Procedimiento Informático Lógico para el Análisis de Riesgos” creado por el Centro Nacional de Inteligencia, actualmente se encuentra disponible la versión 5.4.

Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para tratar el riesgo se proponen: salvaguarda o contramedidas, normas y procedimientos de seguridad.

Esta herramienta soporta las fases del método MAGERIT:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

Evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

PILAR presenta los resultados en varias formas, ya sea en informes RTF, gráficas o tablas que se pueden agregar a una hoja de cálculo, logrando elaborar diferentes tipos de informes y presentaciones de los resultados.

Finalmente, la herramienta calcula calificaciones de seguridad respecto a normas ampliamente conocidas, como son UNE-ISO/IEC 27002:2009: sistemas de gestión de seguridad, RD 1720/2007: datos de carácter personal y RD 3/2010: Esquema Nacional de Seguridad.

Cabe destacar que esta herramienta incorpora tanto los modelos cualitativos como cuantitativos, logrando alternarse entre estos para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos.

PILAR puede realizar un análisis cualitativo, usando una serie de niveles discretos para la valoración de los activos.

Un análisis cualitativo se recomienda siempre en primer lugar, antes de que se intente un análisis cuantitativo detallado. Un análisis cualitativo permite:

- identificar los activos más significativos
- identificar el valor relativo de los activos
- identificar las amenazas más relevantes
- identificar las salvaguardas presentes en el sistema
- establecer claramente los activos críticos (los que están sujetos a un riesgo máximo)

Un análisis cualitativo permite el centrarse en esos aspectos que sean difíciles de cuantificar exactamente, o no sea fácil de explicar con medidas cuantitativas (es decir, para esas cosas que “no tienen precio”). Además, proporciona un primer acercamiento a esas cosas que sí tienen un precio, pero no estamos interesados ni

podemos indicar... de momento. Un análisis cuantitativo posterior entrará en más profundidad.

PILAR puede realizar un análisis cuantitativo detallado:

- detalla las consecuencias económicas de la materialización de una amenaza en un activo
- estima la tasa anual de ocurrencia (ARO) de amenazas (annual rate of occurrence)
- detalla el coste de despliegue y mantenimiento de las salvaguardas
- permite ser más preciso en la planificación de gastos de cara a un plan de mejora de seguridad.

Niveles y Valores

PILAR permite el asociar niveles cualitativos a valores cuantitativos. Esta asociación trabaja solamente si el usuario no proporciona información explícita para ambos.

En un análisis cualitativo, cuando varios servicios dependen de un solo equipo, el nivel acumulado en el equipo compartido es el máximo de los niveles requeridos por los activos soportados. Se pierde información cuando muchos servicios dependen de un punto compartido de fallo. El análisis cuantitativo muestra esta acumulación porque simplemente suma los valores individuales.

En análisis cuantitativo, cuando un servidor con un servicio altamente cualificado se compara a otro servidor con varios servicios cualificados más bajos, la adición de muchos valores pequeños puede alcanzar un alto valor, y el usuario puede verse tentado a proteger la cantidad antes que la calidad. El análisis cualitativo muestra la diferencia al quedarse con el nivel más alto.

El mismo modelo preparado con pilar, puede abrirse en modo cualitativo o cuantitativo; basta elegir la opción deseada al arrancar PILAR. PILAR, abierto en

modo cualitativo, utiliza valores cualitativo, bien los que se hayan introducido directamente, bien valores estimados a partir de la valoración cuantitativa. Igualmente, PILAR abierto en modo cuantitativo, trabaja con cantidades numérica, bien las que se hayan introducido directamente, bien valores derivados a partir de los niveles cualitativos (Servicio Nacional de Aprendizaje -SENA, 2012).

1.2.16.2 HERRAMIENTA DE EVALUACIÓN DE SEGURIDAD DE MICROSOFT (MSAT)

Según (Miranda, Universidad Politécnica de Madrid, 2015) esta herramienta gratuita de Microsoft emplea un enfoque integral para la medición de la seguridad para temas que abarcan tanto personas, procesos y tecnología; ofreciendo información y recomendaciones para la seguridad del ambiente informático de empresa con menos de 1000 empleados, a fin de ayudarles a comprender los riesgos potenciales que afrontan y el nivel de madurez de seguridad de la organización. Utiliza el concepto de defensa en profundidad para implementar capas de defensa que incluyen controles técnicos, estándares organizativos y operativos, basándose en las mejores prácticas aceptas para reducir el riesgo en ambientes de TI como son ISO 17799 y NIST -800.x.

MSAT proporciona:

Conocimiento constante, complejo y fácil de utilizar acerca del nivel de seguridad.

Marco de defensa de profundidad con análisis comparativos del sector.

Informes detallados y actuales comparando el plan inicial con los avances obtenidos.

Recomendaciones comprobadas y actividades prioritarias para mejorar la seguridad.

Consejos estructurados de Microsoft y de la industria.

La evaluación de riesgos consiste en dos partes:

Un perfil de los riesgos comerciales (BRP).- Consta de alrededor 200 preguntas distribuidas sobre el modelo de la empresa para calcular el riesgo.

Una evaluación para determinar las medidas de seguridad formadas por capas de defensa compuesta por cuatro áreas de análisis: infraestructura, aplicaciones, operaciones y usuarios

Su funcionalidad según (JGAIPro, 2012) la primera fase de la evaluación consiste en generar un perfil para la empresa y los posibles riesgos empresariales, los cual nos pedirá información como Nombre de la empresa, número de trabajadores, numero de servidores y estaciones clientes todas distribuidas en 6 nodos.

Ya completada la primera fase de la encuesta, seguirá la segunda parte en la cual la completaremos haciendo clic en Crear nueva evaluación hay nos pedirá crear un nuevo sub perfil el cual nos separara de la primera fase.

La parte más importante de las preguntas en las cuales se nos divide en cuatro aéreas de análisis Infraestructura – Aplicaciones – Operaciones – Personal y tendremos una serie de preguntas más técnicas y aplicadas a nuestra infraestructura

Habiendo completado todas las preguntas veremos la opción de generar el informe del estado de seguridad de nuestra infraestructura IT Informes

Al final una serie de informes separados en tres ítems Informe resumido – Informe completo – Informe corporativo este último requiriendo obligatoriamente el envío de la información de forma anónima a Microsoft.

1.2.16.3 RISICARE

Para (Miranda, Universidad Politécnica de Madrid, 2015) esta es una herramienta basada en el método MEHARI que mejora la productividad y la precisión de un

enfoque de gestión de riesgos especialmente en contexto de empresas medianas.

RISICARE define un perímetro de procesos claves para optimizar el proceso y los recursos sean internos o externos; apoyado en los siguientes parámetros:

Utilizar el método MEHARI desarrollado dentro de CLUSIF.

Personalizar la base de conocimientos e incluso construir sus propias base de conocimiento.

Relacionar la cuantificación de los escenarios de riesgo con una posible auditoría.

Desarrollar planes coherentes para optimizar la reducción de riesgos generales.

Ser una herramienta potente y de fácil uso integrándose con Windows.

RISICARE consta de 4 fases:

Establecimiento del contexto.-Primero se identifican y se clasifican los activos, luego se establece un vínculo entre los procesos del negocio y finalmente se cuantifican las vulnerabilidades de los activos.

Análisis de lo Existente.- Se mide el nivel de madurez de la empresa en función de la taxonomía de temas de auditoría de CLUSIF 2010.

Tratamiento de Riesgos.- Se garantiza el cumplimiento de la norma ISO 27005, realizando planes de acción destinados a reducir la gravedad de los riesgos.

Aceptación del Riesgo.- Definir medios para evitar, transferir y reducir el riesgo.

1.2.17 Metodologías de análisis de riesgos

Para (Miranda, PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA, 2015) un método es un procedimiento o proceso sistemático y ordenada para alcanzar algún objetivo. Una metodología se materializa por un conjunto de métodos, técnicas y herramientas. No contiene métodos específicos; sin

embargo, lo especifica por procesos que conforman el marco de gestión de riesgo.

Indica que la metodología cualitativa es el más utilizado para el análisis de riesgos y cumple con los requisitos de ISO 27001.

Las metodologías más reconocidas son :

- MAGERIT
- OCTAVE
- Metodología NIST SP800-30
- CRAMM
- MEHARI
- CORAS

Según el autor (Martínez, 2017) también existen múltiples metodologías de análisis de riesgos.

1.2.17.1 MAGERIT

Empezando por la metodología MAGERIT, (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), la cual fue desarrollada por iniciativa del Ministerio de Administraciones Públicas a finales de los noventa y elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática. Su empleo está muy extendido en la Administración española.

1.2.17.1.1 Evolución de Magerit

La primera de Magerit, publicada en 1997 ha resistido en su mayor parte el paso del tiempo, ratificándose en lo fundamental. No obstante, el tiempo pasado permite mejorar notablemente aquella primera versión.

La segunda versión, publicada en 2005, se planteó como revisión constructiva, adaptándola al tiempo presente e incorporando la experiencia de estos años.

Esta tercera versión busca una nueva adaptación, teniendo en cuenta no solo la experiencia práctica sino también la evolución de las normas internacionales de ISO que constituyen un referente obligado (Electrónica, 2012).

1.2.17.1.2 Objetivos

Magerit persigue los siguientes objetivos:

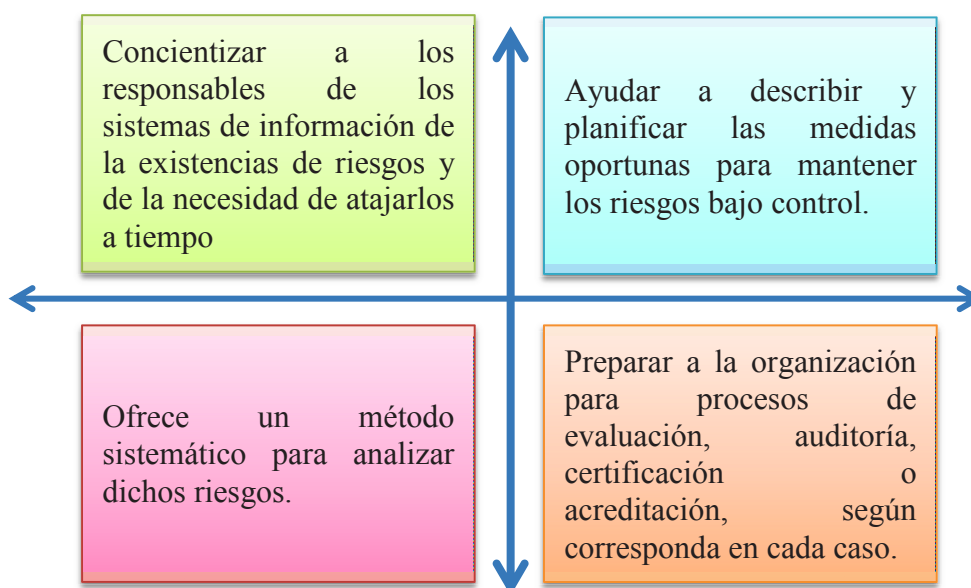


Ilustración 2: Objetivos de Magerit

Fuente: Autores

El modelo MAGERIT maneja tres submodelos, el de elementos de seguridad (actividades, amenazas, vulnerabilidades, impactos, riesgo y salvaguardias), el de eventos de seguridad (estático, dinámico organizativo y dinámico físico) y el de procesos de seguridad (planificación, análisis de riesgos, gestión de riesgos y gestión de salvaguardias).

CLUSIF (CLUb de la Sécurité des Systèmes d'Information Français), desarrolló MEHARI, (MÉthode Harmonisée d'Analyse des RISques), que clasifica los riesgos según sus causas, (accidentes, errores y actos malintencionados), según la característica de seguridad que vulneran, (confidencialidad, integridad y disponibilidad). Otras metodologías acometen el análisis de las amenazas en función del origen o la causa que las puede desencadenar, agrupándolas en orígenes homogéneos, por ejemplo, entorno físico (situación, edificios, gestión y funciones del negocio, entorno tecnológico, relaciones con el exterior, amenazas externas, etc.). Pero cualquiera que sea el método seguido, se hace imprescindible un análisis de la situación para poder detectar los riesgos existentes e implantar unas medidas que consigan un máximo de eficacia con el mínimo de inversión, y por ello, para un correcto Análisis de Riesgos, es siempre recomendable tomar como referencia un modelo de seguridad que nos permita tener la certeza de que hemos considerado todos los escenarios posibles.

Para (Chicano Tejada, 2014) la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas o Metodología Magerit fue diseñada por el CSAE (Consejo Superior de Administración Electrónica) y es de carácter público. Su primera versión data de 1997, la segunda de 2005 y la

tercera (que es la vigente en la actualidad) fue publicada en 2012, convirtiéndose en un referente para el desarrollo de planes de riesgo de las organizaciones a nivel nacional. Para este autor los principales objetivos de esta metodología, son los siguientes:

- La concienciación de los encargados de los sistemas de información de la existencia de riesgos y de la importancia de una gestión de riesgos adecuada.
- Facilitar una metodología que permita analizar sistemáticamente los riesgos de las organizaciones. Proporcionar un apoyo a las organizaciones para que sean capaces de diseñar sus propias medidas para combatir los riesgos de sus activos.

Además añade un objetivo indirecto: Magerit fue diseñada para que las organizaciones sean capaces de adaptar sus tareas a los procesos de evaluación, certificación, auditoría o acreditación necesarios, según el caso, para conseguir mantener unos estándares de calidad en sus actividades.

1.2.17.1.3 Pasos de la metodología MAGERIT

Según el libro (Electrónica, 2012) indica que MAGERIT sigue los siguientes pasos pautados:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Los pasos indicados se detallan en la siguiente gráfica:



Ilustración 3: Elementos del análisis de riesgos potenciales

Fuente: Libro I MAGERIT v3

Paso 1: Activos

En el paso uno es donde se identifican a todos los activos existentes son los bienes tanto tangibles como intangibles que son de importancia en la organización para lograr un mejor desempeño. Entre los activos se encuentran: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (Michelle, 2016) .

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

Tabla 1: Listado de Activos Magerit v3

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

Fuente: Libro II Magerit v3 1

Valoración de Activos

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

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

Paso 2: Amenazas

En el siguiente paso se debe determinar las amenazas que afectarían a cada activo.

Estas amenazas podrían causar daños potencialmente peligrosos a la organización.

Tabla 2: Clasificación de Amenazas

[N]	Desastres Naturales
[I]	De origen Industrial
[E]	Errores y fallos no intencionados
[A]	Ataques Intencionados

Fuente: Libro II Magerit v3

Valoración de Amenazas

Al momento de identificar las amenazas, éstas deben tener una valoración, mediante los siguientes parámetros:

Frecuencia: Cuánto perjudicado resulta el valor del activo.

Degradación: Impacto que tiene la materialización de la amenaza en el activo.

Impacto

Conociendo el valor de los activos y a degradación que causan las amenazas, se debe derivar el impacto que estas tendrían sobre el sistema.

Para el cálculo del impacto se utiliza la siguiente fórmula:

$$\text{Impacto acumulado} = \text{Valor Acumulado} \times \text{Degradación}$$

Riesgo

El riesgo es la medida del daño probable sobre un sistema. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

- Zona 1 – riesgos muy probables y de muy alto impacto
- Zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo.

- Zona 3 – riesgos improbables y de bajo impacto
- Zona 4 – riesgos improbables, pero de muy alto impacto

Para el cálculo del riesgo acumulado se utiliza la siguiente fórmula:

$$\text{Riesgo Acumulado} = \text{Impacto acumulado} \times \text{Degradación}$$

Paso 3: Salvaguardas

Las salvaguardas son medidas de protección frente a las amenazas convirtiéndose en procedimientos o mecanismos tecnológicos que disminuyen el riesgo.

Selección de salvaguardas

1. Tipo de activos a proteger, pues cada tipo se protege de una forma específica
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

La siguiente tabla relaciona cada uno de los tipos de protección con el modelo de degradación y de probabilidad:

Tabla 3: Tipos de Salvaguardas

EFEECTO	TIPO
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización

	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

Fuente: Libro I Magerit v3

MAGERIT consiste en 3 libros con versiones en inglés, español e italiano:

- Libro I: Método
- Libro II: Catálogo de Elementos
- Libro III: Guía de Técnicas

Tabla 4: Comparación de Metodologías

METODOLOGÍAS	MAGERIT	OCTAVE	NIST SP800-30	CRAMM	NEHARI
DESARROLLADA	Consejo Superior de Administración electrónica.	Computer Emergency Response Team (CERT).	Instituto Nacional de Estándares y Tecnología (NIST) fundado en 1901 el cual es parte del Ministerio de Comercio.	Por el Centro de informática y la Agencia Nacional de Telecomunicaciones (CCTA).	CLUSIF (CLUbe de la Sécurité de l'Information Français)
PAÍS	España	Estados Unidos	Estados Unidos	Reino Unido	Francia
OBJETIVOS	➤ Concientizar a responsables de los sistemas de información sobre los riesgos y la necesidad de gestionarlos. ➤ Ayuda a describir y planificar las medidas oportunas para mantener los riesgos bajo control. ➤ Ofrece un método sistemático para analizar dichos riesgos. ➤ Prepara a la organización para procesos de evaluación, auditoría, certificación o acreditación.	➤ Desmitificar la falsa creencia: la seguridad informática es un solamente un asunto técnico. ➤ Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.	➤ Aseguramiento de los sistemas de información que almacenan, procesan y transmiten información. ➤ Gestión de Riesgos. ➤ Optimizar la Administración de Riesgos a partir del resultado en el análisis de riesgos. ➤ Proteger las habilidades de la organización para alcanzar su misión (no solamente relacionada a la IT, sino de toda la empresa). ➤ Ser una función esencial de la administración (no solo limitada a funciones técnicas de IT).	Proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos.	El primer objetivo de MEHARI es proporcionar un método para la evaluación y gestión de los riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005, proporcionando el conjunto de herramientas y elementos necesarios para su implementación.
VERSIONES	➤ VERSIÓN 1: publicada en 1997 ➤ VERSIÓN 2: publicada en 2005 ➤ VERSIÓN 3: publicada en el 2012	➤ OCTAVE:+300 empleados ➤ OCTAVE –S: hasta 100 empleados ➤ OCTAVE Allegro(2007):enfoque en los activos de información	800-30 Rev.1 (2012)	Su versión inicial data de 1987 y la versión vigente es la 5.3 (2003) ➤ CRAMM Expert ➤ CRAMM Express ➤ BS7799	Su versión inicial es de 1995 y se deriva de las metodologías previas Melissa y Marion.

VENTAJAS	Se considera un alcance completo, tanto en el análisis como en la gestión de riesgos. Posee un extenso archivo de inventarios en lo referente a Recursos de Información, Amenazas y tipo de Activos. Su utilización no requiere autorización del Ministerio de Hacienda y Administraciones Públicas. Facilita la certificación ISO/IEC 27001	La ventaja clave que OCTAVE Allegro proporciona una organización es la flexibilidad para implementarlo por partes. Involucra a todo el personal de la entidad. Facilita la certificación ISO 27001	Otorga gran importancia a los controles, habla de perfiles claves dentro de la organización respecto a la responsabilidad de la administración del riesgo. Facilita la certificación ISO 27001	Se puede aplicar a nivel internacional, la v 5.1 ha sido usado en 23 países. Hay muchas herramientas para aplicarla. Facilita la certificación ISO 27001	Una un modelo de análisis de riesgos cualitativo y cuantitativo.
DESVENTAJAS	El hecho de tener que traducir en forma directa todas las valoraciones en valores económicos hace que esta metodología sea realmente costosa. No posee un inventario completo en lo referente a Políticas.	Costos	Costos licencia, implementación y análisis.	Costos licencia, implementación y análisis.	Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad, y deja a un lado el no repudio. La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de los riesgos.
COSTE	No tiene coste, ya que es una normativa de libre aplicación.	Industria \$2500 Gobierno \$2040	Habla del costo relacionado con el beneficio, otorgando una condición relativa al costo de un plan director de seguridad, siempre que el costo sea menor al costo del riesgo analizado y solventado, el costo será bajo.	La versión 4 costaba por año: Compañía comercial \$3900 + \$1200 de mantenimiento Estado británico: \$2200 + \$1200 de mantenimiento	~\$600 + \$9500 de formación en el extranjero.

Fuente: Análisis Comparativo: Metodologías de análisis de Riesgos (Mogollón, 2013)

CAPITULO II

2 MARCO INVESTIGATIVO

2.1 Introducción

Para realizar una investigación es necesario analizar bien la situación que ha llevado al problema para después poder brindar una solución, en nuestro caso hemos realizado una investigación sobre la seguridad de los activos en la Facultad de Ciencias Informáticas, donde hemos comprobado que actualmente no existe un plan de seguridad ni ningún método para cuidar estos activos, lo cual están muy propensos a sufrir ataques, robos y demás que se han venido dando a lo largo de los años.

La información que mantienen las instituciones es un activo que puede ser vulnerado por cibernautas para sacar algún beneficio o incluso dañar la organización o persona, lo que conlleva a pérdidas o confusiones que pueden dañar o desprestigiar a la empresa o persona. Por ello en el presente proyecto integrador diseñaremos un software para mitigar las vulnerabilidades de los activos de las organizaciones específicamente de nuestra facultad.

2.2 Tipo(s) de Investigación

Los tipos de investigaciones que hemos realizado son las siguientes:

- Investigación descriptiva
- Investigación exploratoria
- Investigación documental

2.2.1 Por el nivel de conocimientos que se adquieren:

2.2.1.1 Investigación Descriptiva

Esta investigación se realizó ya que se necesitó obtener información sobre la seguridad de los activos informáticos de la FACCI, se observó la situación en que los

responsables manejan la seguridad de los activos, así como la funcionalidad, metodología y políticas que se aplican, con el fin de dar soluciones al respecto.

2.2.2 Por las características de los medios utilizados para obtener los datos:

2.2.2.1 Investigación Exploratoria

Se realizó esta investigación para obtener toda la información para el desarrollo de este trabajo, se observaron todos los activos que posee la FACCI, el funcionamiento y los procesos que manejan, para así realizar un análisis de riesgo y ver las amenazas y vulnerabilidades que puede sufrir la Unidad Superior.

2.2.3 Según el propósito o finalidad que se persigue:

2.2.3.1 Investigación Documental

Para realizar este trabajo hemos revisado otros proyectos, trabajos, artículos relacionados con nuestro tema, para así poder abarcar las necesidades requeridas y poder desarrollar un producto eficaz.

2.3 Método de Investigación

2.3.1 Observación

Se utilizó este método, ya que se hizo la recolección de información de todos los activos de la facultad de forma directa, para conocer los riesgos de seguridad que sufren los activos de la FACCI, y así conocer en profundidad las vulnerabilidades de los mismos.

2.3.2 Hipotético-Deductivo

Este método se ha utilizado como consecuencias de la realización de la encuesta a toda la comunidad de la FACCI, y la entrevista al jefe de laboratorios, con lo que se llegó a la hipótesis que todos los activos de esta unidad superior sufren un riesgo el cual no es controlado, y dada esta hipótesis se va a llegar a conclusión comprobada experimentalmente mediante el software realizado.

2.4 Herramienta(s) de recolección de datos

2.4.1 Encuesta

Se utilizó esta herramienta en la fase inicial de la investigación para conocer en profundidad sobre la problemática tratada, en donde se concluyó que la FACCI carece de seguridad en los activos.

2.4.2 Entrevista

Para llevar a cabo este proyecto se realizó una entrevista al jefe de Laboratorios de la FACCI, con la cual conocimos que no existe un plan de seguridad, ni de contingencia, ni de gestión de riesgos o algún proceso establecido para gestionarlos, tampoco existe algún seguro que resguarde la pérdida de activos.

2.4.3 Observación

Se utilizó para obtener un análisis general de la problemática que ocurre en la FACCI.

2.5 Fuentes de Información de datos

Las fuentes de información de datos se dividen en dos que son las siguientes:

- Fuentes de Información Primarias

- Fuentes de Información Secundarias

2.5.1 Fuentes Primarias

Como fuentes primarias se tuvo en consideración a toda la comunidad de la FACCI a los cuales se les hizo una encuesta, y específicamente al jefe de Laboratorios al cual se entrevistó sobre la seguridad implementada y los riesgos existentes en los activos informáticos.

2.5.2 Fuentes Secundarias

Como fuentes secundarias se necesitaron conocer algunas terminologías a través de la web, en artículos científicos, etc., que nos ayudaron con definiciones e información adicional. Entre esos documentos se tienen:

- ISO/IEC 27001
- ISO/IEC 17799
- Libro de Magerit V3, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- Trabajos de Titulación realizados referente a la problemática
- Páginas de Internet referente a la temática verificando que el contenido sea completo y legitimo para conocer las bases teóricas.

2.6 Instrumental Operacional

2.6.1 Estructura y características de lo(s) instrumento(s) de recolección de datos.

2.6.1.1 Encuesta

La encuesta la realizamos como un dato de investigación, y colaborando con el equipo de Investigación, se realizaron 35 preguntas para conseguir datos verídicos, se envió por medio de los correos institucionales a toda la comunidad de la FACCI de manera online. El objetivo de esta encuesta fue conocer el estado actual de la seguridad informática en laboratorios, la mano de obra especializada del personal de laboratorio, los elementos de seguridad informática, y los tipos y aplicabilidad de la seguridad informática en Instituciones de Educación Superior. Las preguntas se realizaron a través de formulario de google forms, con 7 opciones a elegir, esto se realizó para que la encuesta sea rápida y más precisa tanto para el encuestado como para el encuestador a la hora de tabular los datos.

La encuesta se encuentra en anexo # 1.

2.6.1.2 Entrevista

La entrevista que realizamos fue con el Ing. Gilbert Loor Muñoz el cual es el jefe de laboratorios de la FACCI, se realizó con el propósito de conocer de forma clara la información que necesitábamos, así obtuvimos la opinión de la administración de la seguridad de los activos de la FACCI.

La entrevista se encuentra en el anexo #2.

2.6.1.3 Observación

La observación se realizó tanto en los laboratorios como departamentos administrativos, y la infraestructura en general para determinar los riesgos que puedan sufrir los activos informáticos, por ello con el software se podrá conocer la cantidad de riesgo y los controles a aplicar en los mismos.

2.7 Estrategia Operacional para la recolección y tabulación de datos

2.7.1 Plan de recolección

En este trabajo de investigación las herramientas de recolección de datos que hemos utilizado han sido encuestas, entrevistas y observaciones, para lo cual se determinó lo siguiente:

- Se encargó la recolección de datos a la Sra. Fátima Carrillo una de los integrantes de este proyecto, por lo que se considera apta para lograr obtener los resultados que se necesitan.
- Se establecieron los laboratorios y departamentos en los que se encuentran los activos informáticos como lugar para resolver la problemática planteada en este proyecto.
- Se ha realizado recolección de datos, recopilando información directamente con el personal de administración del centro de cómputo y el responsable del mismo que es el Ing. Gilbert Loor, nos facilitaron un listado de activos los cuales tuvimos que verificar su existencia y actualizarlos.

2.7.2 Tabulación y Análisis e interpretación de los datos

Mediante el análisis de la encuesta realizada nos permitió conocer la situación actual en que se encuentran los activos informáticos de la FACCI, por lo que se realizó lo siguiente:

- Todas las preguntas de la encuesta se pasaron a un documento de Excel para poder manipularlas mediante la tabulación.
- Se agruparon los datos en tablas de frecuencias absolutas
- Se presentó la información mediante gráficos de tipo circular.
- Como último punto, se realizó análisis de los resultados obtenidos.

2.8 PLAN DE MUESTREO

2.8.1 Segmentación

Para conocer la información de la seguridad que existe en la facultad, han intervenido un universo de toda la comunidad de la FACCI, como son los docentes, personal administrativo y de servicio, y los estudiantes matriculados en el periodo 2017(2).

2.8.2 Técnica de muestreo

En la encuesta a toda la comunidad de la FACCI, se utilizó la técnica de muestreo aleatoria simple, donde cada elemento de la población, en nuestro caso 690, tiene la misma probabilidad de ser seleccionado para integrar la muestra, ya que todos los que pertenecemos a la FACCI hacemos uso de los activos informáticos, servicios, e infraestructura de la institución. Al ser la encuesta online, la muestra la conforma quienes accedieron a realizar la encuesta.

2.8.3 Tamaño de la muestra

El tamaño de la muestra es el número de personas que realizaron la encuesta, al haberla realizado a través de un formulario de Google nos facilitó el conocimiento de personas encuestadas, con exactitud se encuestaron 321 personas de la comunidad de la FACCI.

Personas encuestadas en anexo # 3.

El tamaño de la muestra se calculó con la siguiente fórmula, utilizando una hoja de Excel:

$$n = \frac{\frac{Z^2 (P) (1 - q) * N}{2}}{e (N - 1) + \frac{Z^2 (P) (1 - q)}{2}}$$

Ecuación 1: Fórmula del Tamaño de Muestra

Significado de cada una de las variables:

Tabla 5: Significado de Variables de Fórmula de Tamaño de Muestra

VARIABLES	DESCRIPCIÓN
n=	Tamaño de la muestra
N=	Tamaño de la población
P=	% de veces que se supone que ocurre (éxito) un fenómeno en la población = 0.5
e=	Error
q=	% de veces de la no ocurrencia (fracaso) del fenómeno (1 - q) = 0,5
Z=	Nivel de confianza

Fuente: (Carlos Eduardo Valdivieso Tabora, 2011)

Tabla 6: Resultado de Muestreo

COMPROBACIÓN		.2	.2
		e (N - 1)	Z (P) (1 - q)
NUMERADOR	690,17	4,19	0,93
DENOMINADOR	5,11		5,11
n	135,03		

Fuente: Autores

2.9 PRESENTACIÓN Y ANALISIS DE LOS RESULTADOS

2.9.1 Presentación y Descripción de los Resultados Obtenidos

Pregunta 1:

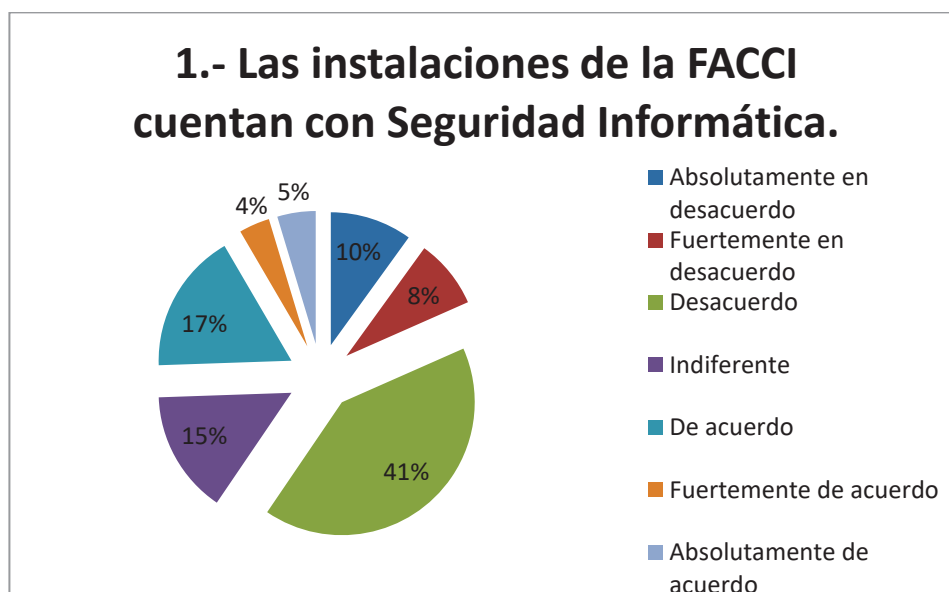


Gráfico 1: Frecuencia de la Pregunta #1

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 7: Frecuencia de pregunta #1

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	32	10,0%
Fuertemente en desacuerdo	27	8,4%
Desacuerdo	132	41,1%
Indiferente	48	15,0%
De acuerdo	55	17,1%
Fuertemente de acuerdo	12	3,7%
Absolutamente de acuerdo	15	4,7%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

En el gráfico #1 se puede observar claramente los resultados a igual que en la tabla de frecuencia, donde se indica que un 41,1% de los encuestados indican que están en desacuerdo con que la FACCI cuenta con Seguridad Informática, un 17% está de acuerdo, un 15% es indiferente a esta pregunta, y el resto de porcentajes son mínimos referentes a los indicados.

Análisis

La mayoría de la comunidad de la FACCI con sus respuesta nos indica que en la instalaciones no se cuenta con Seguridad Informática, seguido del porcentaje que es indiferente porque no sabe o porque no entiende el significado de la pregunta.

Pregunta 2:

2.- La red eléctrica y la de telecomunicaciones están debidamente normalizadas, con protección contra fallos adecuados y etiquetados en todos los departamentos, laboratorios y dependencias de la FACCI.

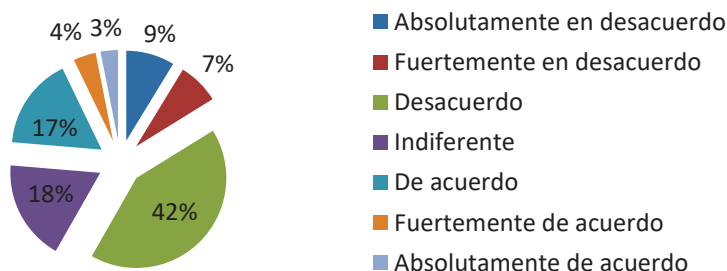


*Gráfico 2: Frecuencia de la Pregunta #2
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 8: Frecuencia de Pregunta #2

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	28	8,7%
Fuertemente en desacuerdo	24	7,5%
Desacuerdo	135	42,1%
Indiferente	58	18,1%
De acuerdo	53	16,5%
Fuertemente de acuerdo	13	4,0%
Absolutamente de acuerdo	10	3,1%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

En el gráfico #2 se puede observar que un 42 % está en desacuerdo con que la red eléctrica y de telecomunicaciones están debidamente normalizadas con protección contra fallos adecuados y etiquetados en todos los departamentos, laboratorios y dependencias de la FACCI, un 18% indica que es indiferente un 16,5% está de acuerdo, y un 8,7% contestó que está absolutamente en desacuerdo.

Análisis

La mayoría de los encuestados está en desacuerdo con la existencia de normalización en la red eléctrica y de telecomunicaciones, por lo que se determina que esta falencia existe en la Facultad de Ciencias Informáticas.

Pregunta 3:

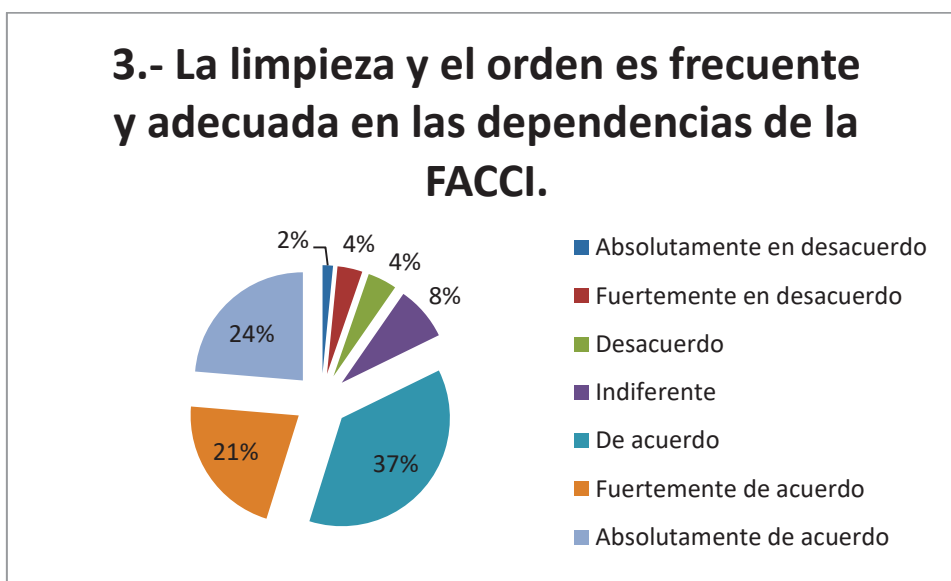


Gráfico 3: Frecuencia de la Pregunta #3
Fuente: Comunidad FACCI
Elaboración: Autores

Tabla 9: Frecuencia de pregunta #3

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	5	1,6%
Fuertemente en desacuerdo	12	3,7%
Desacuerdo	14	4,4%
Indiferente	26	8,1%
De acuerdo	119	37,1%
Fuertemente en acuerdo	69	21,5%
Absolutamente de acuerdo	76	23,7%

Fuente: Comunidad FACCI
Elaboración: Autores

Interpretación

En el grafico #3 se puede observar que están de acuerdo UN 37,1%, fuertemente de acuerdo UN 21,5% y absolutamente de acuerdo UN 23,7%, en que la limpieza y el orden es frecuente y adecuada en las dependencias de la FACCI.

Análisis

Según el porcentaje de respuesta se puede indicar que en las dependencias de las FACCI es frecuente el orden y la limpieza.

Pregunta 4:

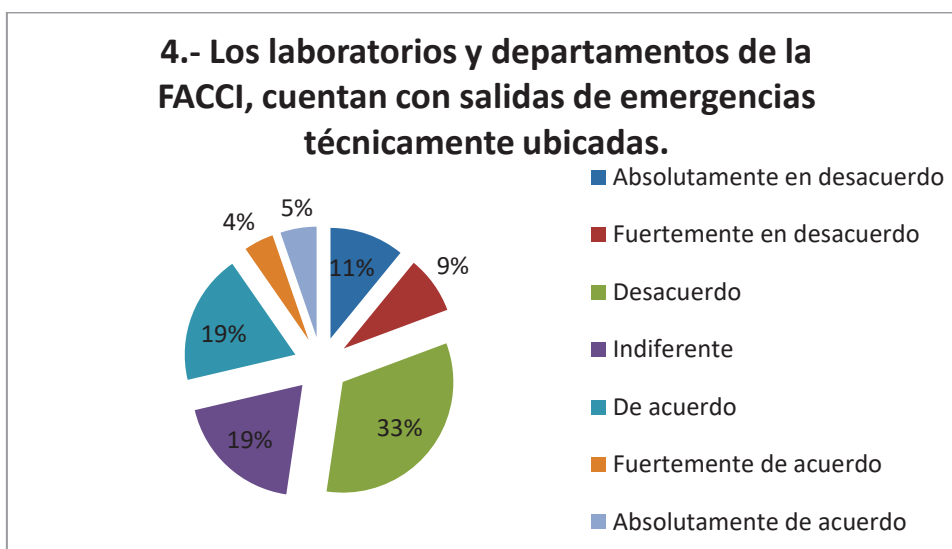


Gráfico 4: Frecuencia de la Pregunta #4
Fuente: Comunidad FACCI
Elaboración: Autores

Tabla 10: Frecuencia de Pregunta #4

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	35	11%
Fuertemente en desacuerdo	27	8%
Desacuerdo	106	33%
Indiferente	61	19%
De acuerdo	61	19%
Fuertemente en acuerdo	14	4%
Absolutamente de acuerdo	17	5,3%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

En el grafico #4 se puede observar que están en desacuerdo un 33%, indiferente un 19% y de acuerdo también un 19%, en que los laboratorios y departamentos de la FACCI cuentan con salidas de emergencias técnicamente ubicadas.

Análisis

En toda institución se debe de contar con salidas de emergencia que estén técnicamente ubicadas, la mayoría de encuestados al estar en desacuerdo con esta pregunta indican no hay salidas de emergencias técnicamente ubicadas.

Pregunta 5:

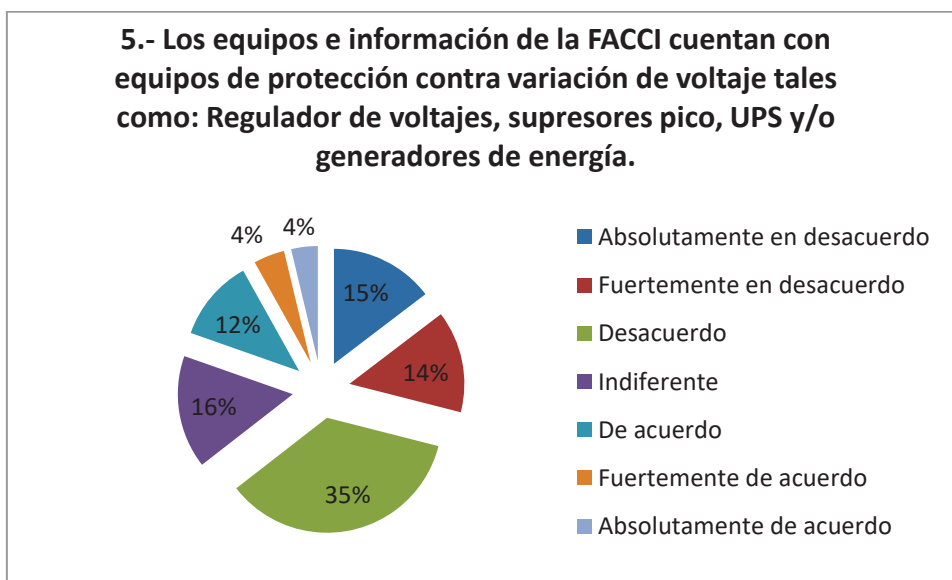


Gráfico 5: Frecuencia de la Pregunta #5
Fuente: Comunidad FACCI
Elaboración: Autores

Tabla 11: Frecuencia de Pregunta #5

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	47	15%
Fuertemente en desacuerdo	46	14%
Desacuerdo	114	36%
Indiferente	51	16%
De acuerdo	37	12%
Fuertemente en acuerdo	14	4%
Absolutamente de acuerdo	12	4%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el grafico #5 se puede observar que un 35% ha indicado que está en desacuerdo, un 16% que es indiferente, un 15% que está Absolutamente en desacuerdo, y un 14% que está fuertemente en desacuerdo.

Análisis

Se puede observar que la mayor parte de la comunidad de la FACCI indica que no se cuenta con equipos de protección de voltaje, un porcentaje es indiferente a esta pregunta, junto con los que están fuertemente en desacuerdo.

Pregunta 6:

6.- Los sistemas operativos y el software de aplicación instalados en los laboratorios de la FACCI, cuentan con Licencias debidamente legalizadas.

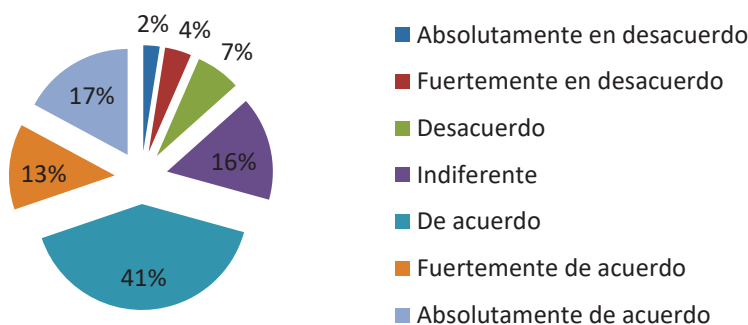


*Gráfico 6: Frecuencia de la Pregunta #6
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 12: Frecuencia de Pregunta #6

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	8	2%
Fuertemente en desacuerdo	13	4%
Desacuerdo	22	7%
Indiferente	51	16%
De acuerdo	130	40%
Fuertemente en acuerdo	42	13%
Absolutamente de acuerdo	55	17%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según la tabulación en el gráfico #6 se observa que un 40,5% han indicado que está de acuerdo, un 17,1% que está absolutamente de acuerdo, un 15,9% es indiferente, y un 13,1% está fuertemente de acuerdo.

Análisis

La mayoría de los encuestados indican que los sistemas operativos y el software instalados en laboratorios de la FACCI si cuentan con licencia legalizadas, pero hay una minoría que no está de acuerdo, por lo que se entiende que hay laboratorios con máquinas que no cumplen lo indicado.

Pregunta 7:

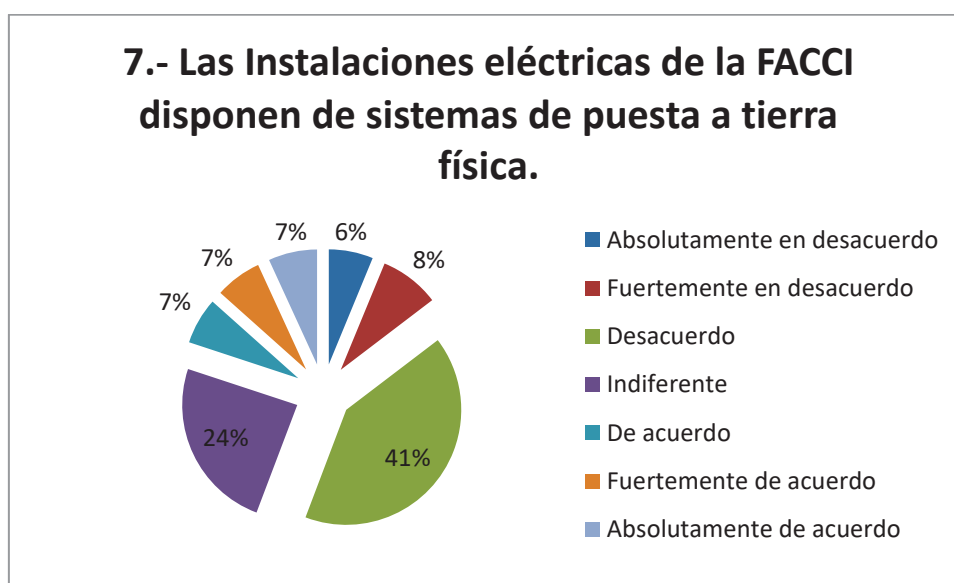


*Gráfico 7: Frecuencia de la Pregunta #7
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 13: Frecuencia de Pregunta #7

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	20	6%
Fuertemente en desacuerdo	27	8%
Desacuerdo	132	41%
Indiferente	78	24%
De acuerdo	21	7%
Fuertemente de acuerdo	21	7%
Absolutamente de acuerdo	22	7%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #7 se observa que un 41,1 % está en desacuerdo, un 24,3% es indiferente, un 11,5% está fuertemente de acuerdo, y un 8% está fuertemente en desacuerdo.

Análisis

Los encuestados en su mayoría indican que la FACCI no consta con sistemas de puesta a tierra física, otros no tienen claro el tema, y una minoría indica que si hay.

Pregunta 8:

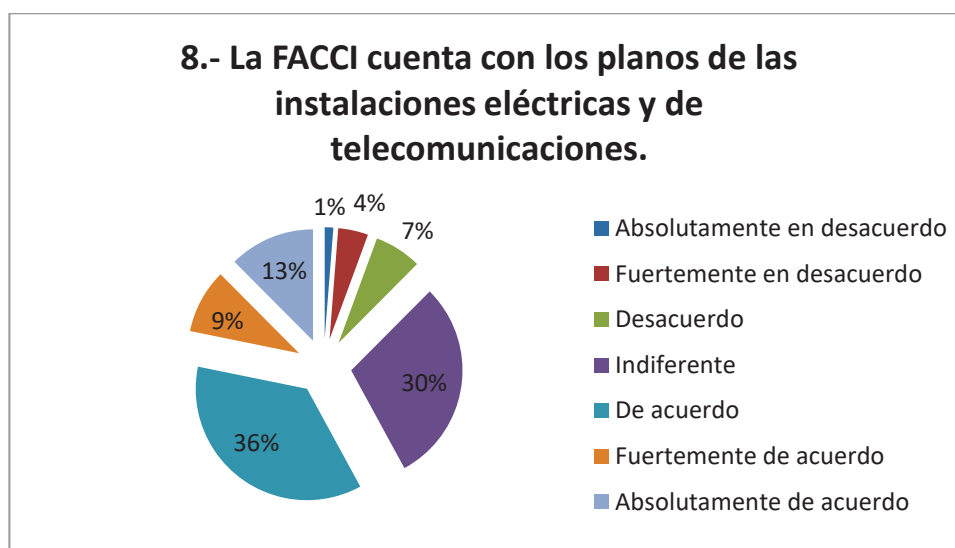


*Gráfico 8: Frecuencia de la Pregunta #8
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 14: Frecuencia de Pregunta #8

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	4	1%
Fuertemente en desacuerdo	14	4%
Desacuerdo	22	7%
Indiferente	95	30%
De acuerdo	116	36%
Fuertemente en acuerdo	30	9%
Absolutamente de acuerdo	40	12%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #8, un 36,1% está de acuerdo, un 29,6% es indiferente, 12,5% está absolutamente de acuerdo, y un 9,3% está fuertemente de acuerdo, los demás son cifras menos significativas.

Análisis

La mayoría de la comunidad de la FACCI indica que si se cuenta con planos de instalaciones eléctricas y de telecomunicaciones, y un porcentaje importante lo desconoce.

Pregunta 9:

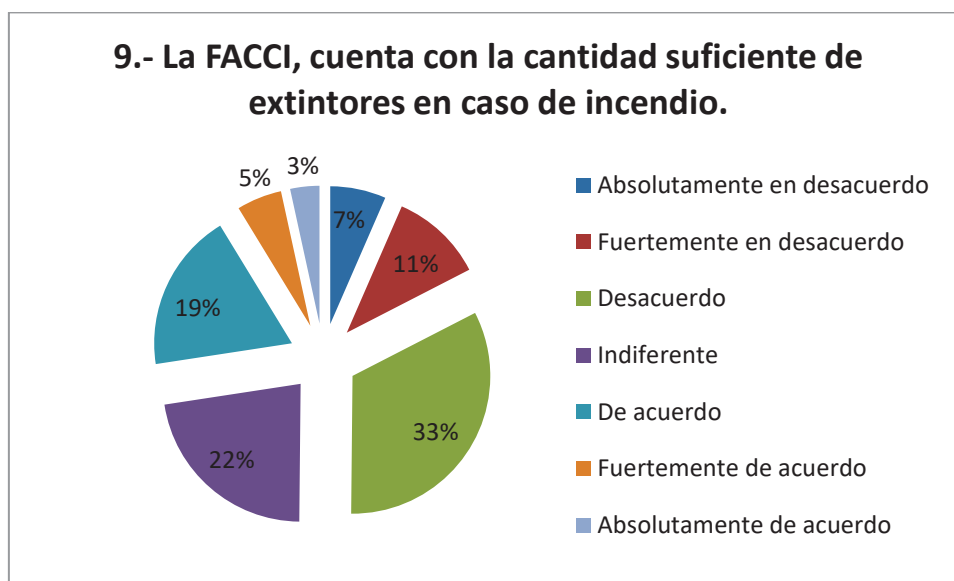


*Gráfico 9: Frecuencia de la Pregunta #9
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 15: Frecuencia de Pregunta #9

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	21	7%
Fuertemente en desacuerdo	35	11%
Desacuerdo	105	33%
Indiferente	72	22%
De acuerdo	60	19%
Fuertemente en acuerdo	17	5%

Absolutamente de acuerdo	11	3%
---------------------------------	-----------	-----------

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el grafico #9, un 33% está en desacuerdo con esta pregunta, un 22% está es indiferente, y un 19% está de acuerdo, los demás porcentajes son minoritarios.

Análisis

La mayoría de los encuestados indican que la FACCI no cuenta con los extintores necesarios en caso de algún incendio.

Pregunta 10:

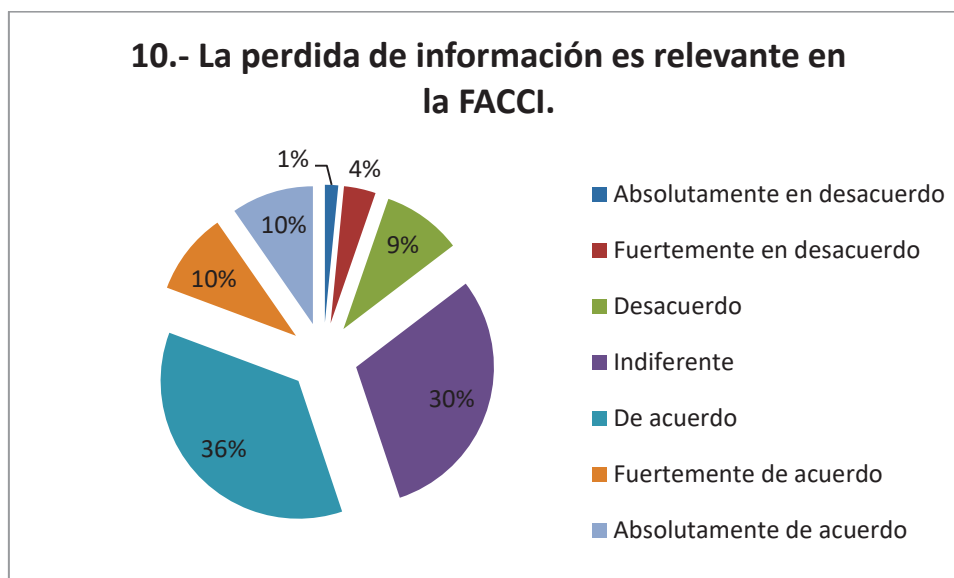


*Gráfico 10: Frecuencia de la Pregunta #10
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 16: Frecuencia de Pregunta #10

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	5	2%
Fuertemente en desacuerdo	12	4%
Desacuerdo	30	9%

Indiferente	97	30%
De acuerdo	115	36%
Fuertemente de acuerdo	31	10%
Absolutamente de acuerdo	31	10%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico #10, un 35,8% está de acuerdo, un 30,2 es indiferente, un 9,7% está fuertemente de acuerdo, también un 9,7% está absolutamente de acuerdo, y un 9,3% está en desacuerdo, las demás cifras son minoritarias.

Análisis

La mayoría de los encuestados indican que la perdida de información de la FACCI es relevante, y una minoría no está de acuerdo con lo indicado. Toda información de instituciones es importante para llevar acabo los procesos internos.

Pregunta 11:

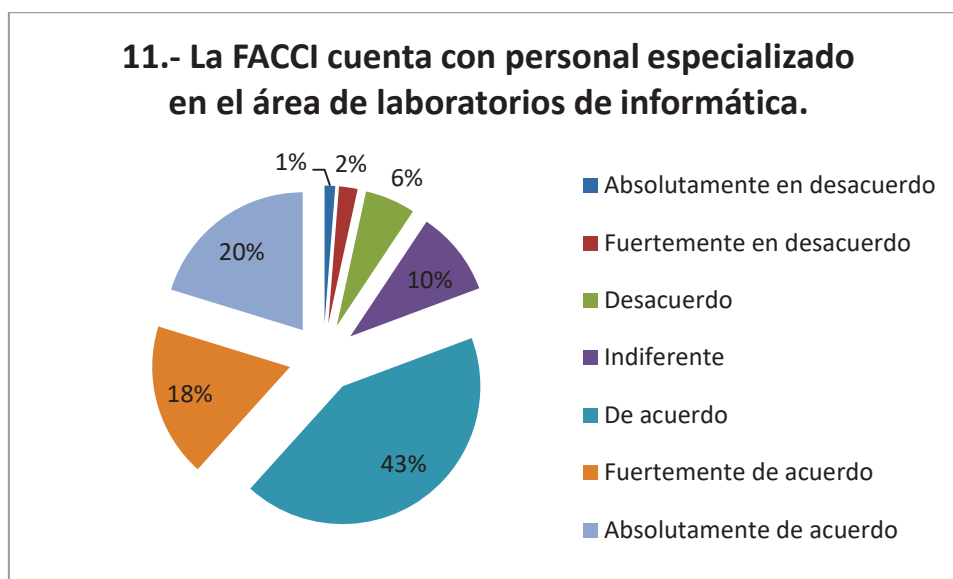


Gráfico 11: Frecuencia de la Pregunta #11

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 17: Frecuencia de Pregunta #11

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	4	1%
Fuertemente en desacuerdo	7	2%
Desacuerdo	19	6%
Indiferente	32	10%
De acuerdo	136	42%
Fuertemente en acuerdo	58	18%
Absolutamente de acuerdo	65	20%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #11, un 42,4% está de acuerdo, un 20,2% está absolutamente de acuerdo, un 18,1% está fuertemente de acuerdo, y un 10% es indiferente, las demás cifras son mínimas.

Análisis

La mayoría de encuestados indican que si se cuenta con personal especializado en el área de laboratorios de informática, en contra de un mínimo que no está de acuerdo.

Pregunta 12:

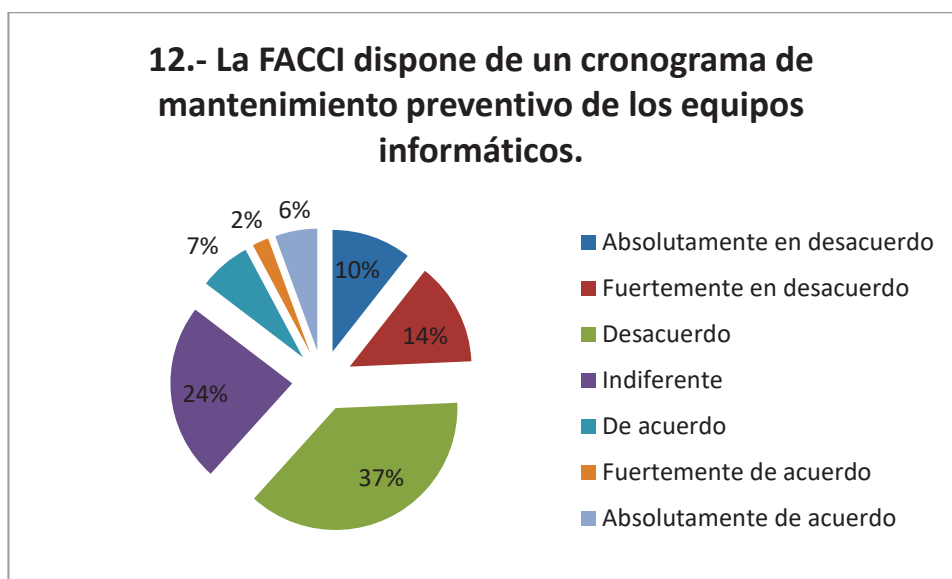


*Gráfico 12: Frecuencia de la Pregunta #12
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 18: Frecuencia de Pregunta #12

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	34	11%
Fuertemente en desacuerdo	44	14%
Desacuerdo	120	37%
Indiferente	76	24%
De acuerdo	22	7%
Fuertemente en acuerdo	7	2%
Absolutamente de acuerdo	46	14,33%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el grafico #12, un 37% está en desacuerdo, un 24% es indiferente, un 14% está fuertemente en desacuerdo, y un 14% también está absolutamente de acuerdo, frente a los otros porcentajes mínimos.

Análisis

La mayoría de los encuestados están en desacuerdo en que la FACCI dispone de un cronograma de mantenimiento preventivo de los equipos informáticos, frente a una minoría que está de acuerdo que lo haya.

Pregunta 13:

13.- Los mantenimientos preventivos de los equipos informáticos se los realiza periódicamente en forma trimestral.

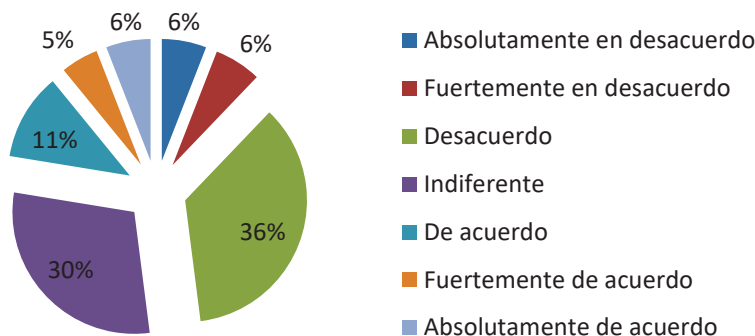


Gráfico 13: Frecuencia de la Pregunta #13

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 19: Frecuencia de Pregunta #13

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	19	6%
Fuertemente en desacuerdo	20	6%
Desacuerdo	115	36%
Indiferente	95	30%
De acuerdo	37	12%
Fuertemente de acuerdo	16	5%
Absolutamente de acuerdo	19	6%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico #13, un 36% está en desacuerdo, un 30% lo desconoce, un 12% está de acuerdo, junto con otros porcentajes mínimos.

Análisis

La mayoría de los encuestados indican que no se realizan mantenimientos preventivos de los equipos informáticos de forma periódica trimestralmente, frente a una minoría que está de acuerdo.

Pregunta 14:

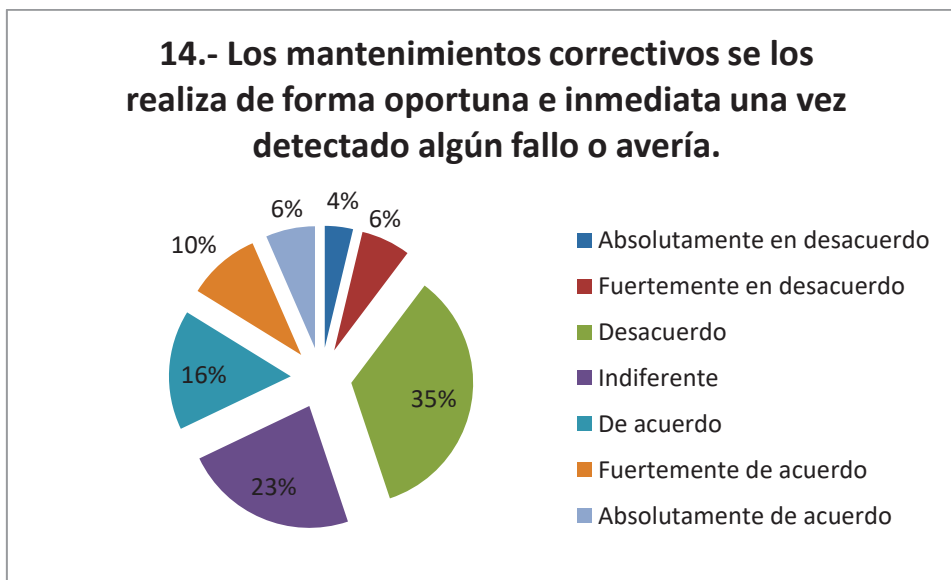


*Gráfico 14: Frecuencia de la Pregunta #14
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 20: Frecuencia de Pregunta #14

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	12	4%
Fuertemente en desacuerdo	21	7%
Desacuerdo	111	35%
Indiferente	74	23%
De acuerdo	51	16%
Fuertemente de acuerdo	31	10%
Absolutamente de acuerdo	21	7%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico # 14, un 35% está en desacuerdo, un 23% es indiferente, un 16% está de acuerdo, y un 10% fuertemente de acuerdo, frente a otros porcentajes mínimos especificados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo que los mantenimientos correctivos se realizan de forma oportuna e inmediata una vez detectado algún fallo o avería, existe un porcentaje que lo desconoce, y otro porcentaje inferior que está de acuerdo.

Pregunta 15:

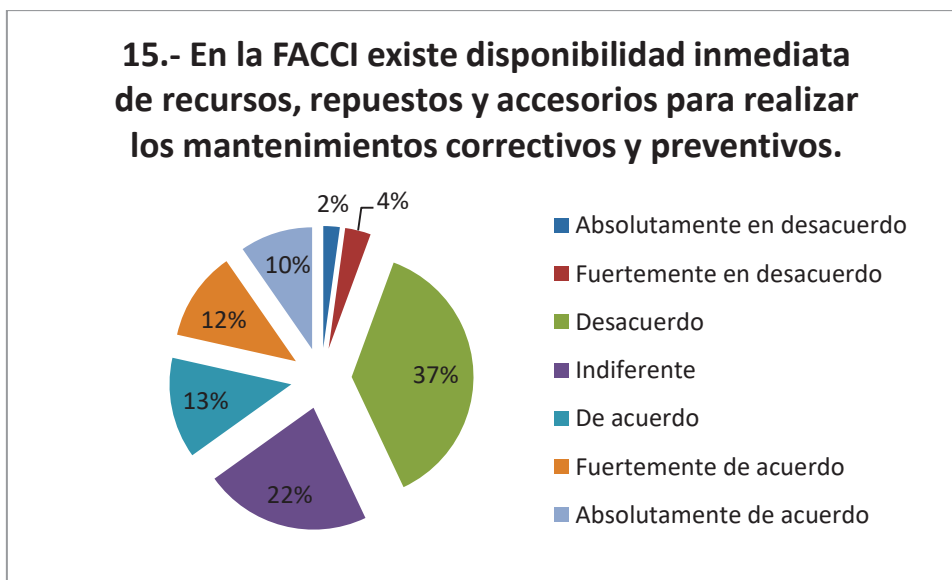


*Gráfico 15: Frecuencia de la Pregunta #15
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 21: Frecuencia de Pregunta #15

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	7	2%
Fuertemente en desacuerdo	11	3%
Desacuerdo	120	37%
Indiferente	71	22%
De acuerdo	43	13%
Fuertemente de acuerdo	38	12%
Absolutamente de acuerdo	31	10%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #15, un 37% está en desacuerdo, un 22% es indiferente, un 13% está en de acuerdo, un 12% está fuertemente de acuerdo, frente a los demás porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados de la FACCI indican que no existe inmediata disponibilidad de recursos, repuestos, y accesorios para la realización de mantenimientos correctivos y preventivos, existe un porcentaje importante de acuerdo y otros que desconocen el proceso.

Pregunta 16:

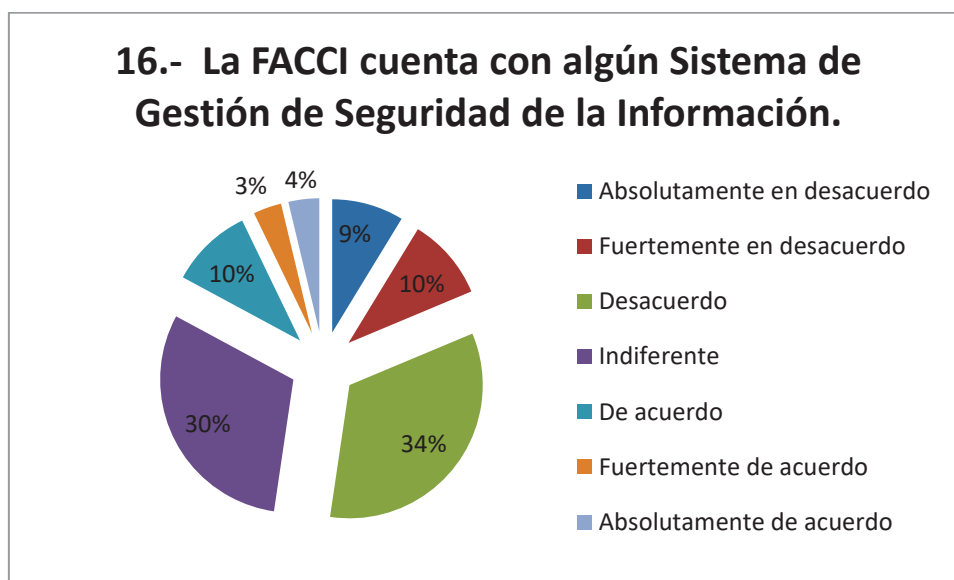


Gráfico 16: Frecuencia de la Pregunta #16
Fuente: Comunidad FACCI
Elaboración: Autores

Tabla 22: Frecuencia de Pregunta #16

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	28	9%
Fuertemente en desacuerdo	32	10%
Desacuerdo	108	34%
Indiferente	98	31%
De acuerdo	32	10%
Fuertemente en acuerdo	11	3%
Absolutamente de acuerdo	12	4%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según gráfico # 16, un 34% está en desacuerdo, un 30% es indiferente, un 10% está de acuerdo, un 10% está fuertemente en desacuerdo, frente a los demás porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, y con un porcentaje alto desconocen si existe un sistema de gestión de seguridad de la información, con otro porcentaje relevante que indica que si lo hay.

Pregunta 17:

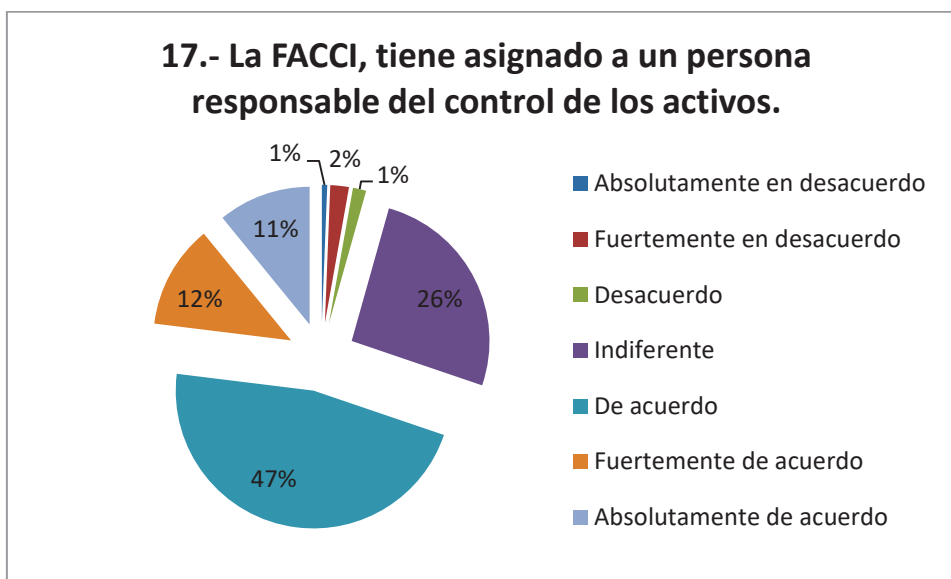


*Gráfico 17: Frecuencia de la Pregunta #17
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 23: Frecuencia de Pregunta #17

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	2	1%
Fuertemente en desacuerdo	7	2%
Desacuerdo	5	2%
Indiferente	83	26%
De acuerdo	150	47%
Fuertemente de acuerdo	39	12%
Absolutamente de acuerdo	35	11%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico # 17, un 47% está de acuerdo, un 26% es indiferente, un 12% está fuertemente de acuerdo, y un 11% absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados de la FACCI, indican que están de acuerdo con la pregunta, un porcentaje importante desconoce si existe una persona responsable del

control de los activos, frente a un porcentaje que tiene claro que no existe este responsable.

Pregunta 18:

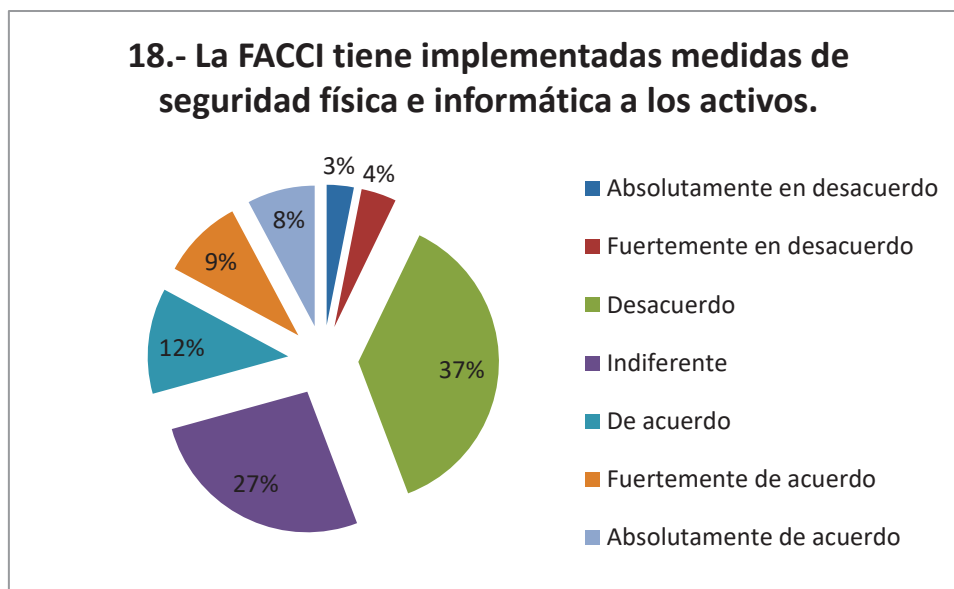


Gráfico 18: Frecuencia de la Pregunta #18

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 24: Frecuencia de Pregunta #18

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	10	3%
Fuertemente en desacuerdo	13	4%
Desacuerdo	119	37%
Indiferente	85	26%
De acuerdo	39	12%
Fuertemente de acuerdo	30	9%
Absolutamente de acuerdo	25	8%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico #18, un 37% está en desacuerdo, un 27% es indiferente, un 12% está de acuerdo, y un 9% fuertemente de acuerdo, junto con otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de encuestados está en desacuerdo con esta pregunta, un porcentaje importante desconoce si existen medidas de seguridad física e informática aplicadas a los activos.

Pregunta 19:

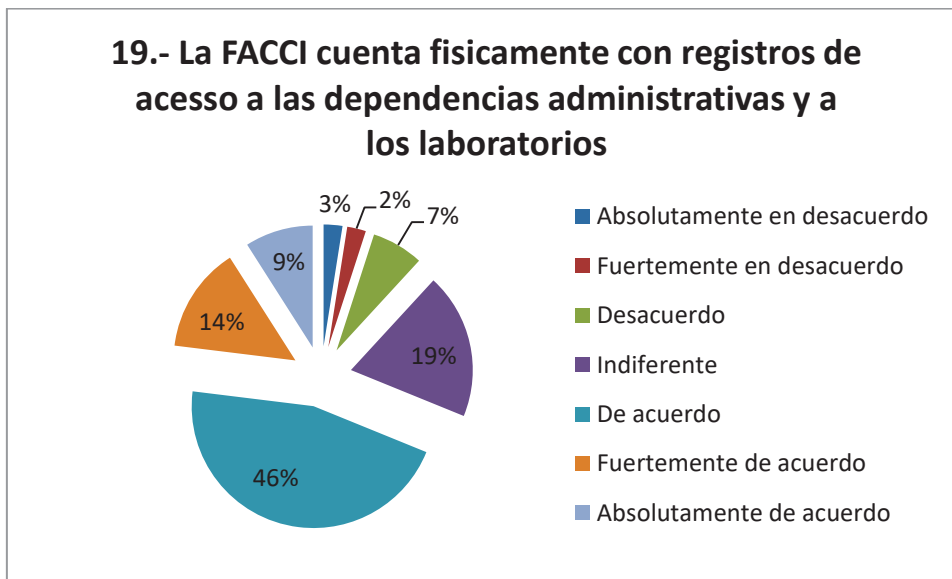


*Gráfico 19: Frecuencia de la Pregunta #19
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 25: Frecuencia de Pregunta #19

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	8	2%
Fuertemente en desacuerdo	8	2%
Desacuerdo	22	7%
Indiferente	62	19%
De acuerdo	147	46%
Fuertemente de acuerdo	45	14%
Absolutamente de acuerdo	29	9%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #19, un 46% está de acuerdo, un 19% es indiferente, un 14% está fuertemente de acuerdo, y un 9% está absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados está de acuerdo con esta pregunta, un porcentaje importante desconoce si existe físicamente registro de accesos a las dependencias administrativas y laboratorios, existe también un porcentaje importante que indica que no existen tales registros.

Pregunta 20:

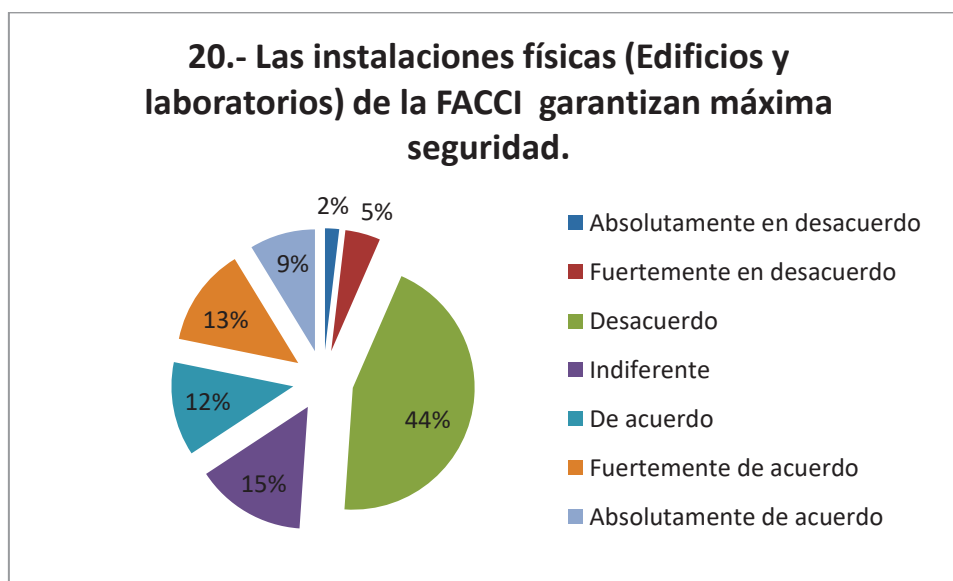


*Gráfico 20: Frecuencia de la Pregunta #20
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 26: Frecuencia de Pregunta #20

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	6	2%
Fuertemente en desacuerdo	15	5%
Desacuerdo	143	45%
Indiferente	47	15%
De acuerdo	40	12%
Fuertemente de acuerdo	42	13%

Absolutamente de acuerdo	28	9%
--------------------------	----	----

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el grafico #20, un 44% está en desacuerdo, un 15% es indiferente, y un 13% está fuertemente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, un porcentaje importante han indicado que las instalaciones físicas de la FACCI no garantizan máxima seguridad, aunque otros desconocen el tema.

Pregunta 21:

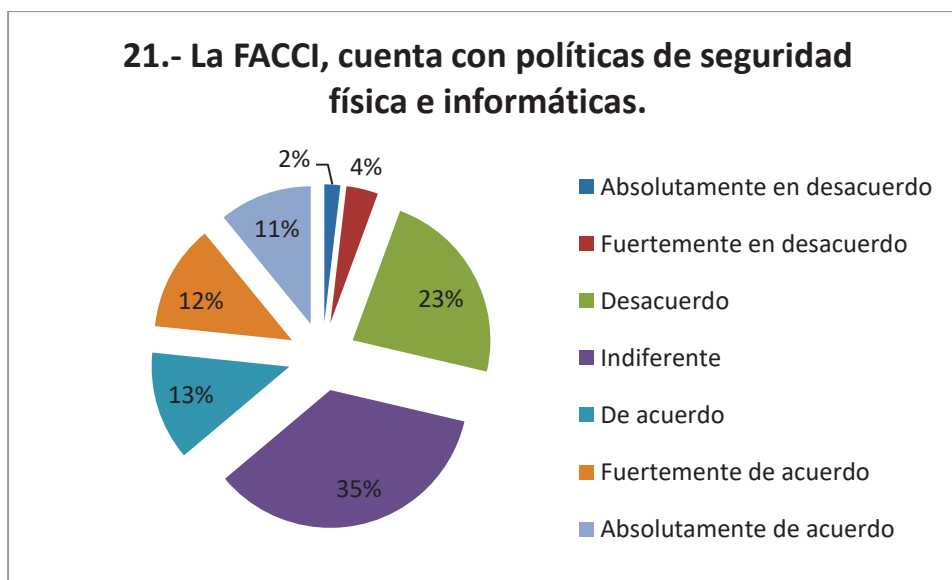


*Gráfico 21: Frecuencia de la Pregunta #21
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 27: Frecuencia de Pregunta #21

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	6	2%
Fuertemente en desacuerdo	12	4%
Desacuerdo	74	23%
Indiferente	113	35%
De acuerdo	41	13%
Fuertemente en acuerdo	40	12%
Absolutamente de acuerdo	35	11%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #21, un 35% es indiferente a esta pregunta, un 23% está en desacuerdo, y un 13% está de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados desconocen si en la FACCI se cuenta con políticas de seguridad física e informáticas, seguidos de un porcentaje importante que está en desacuerdo.

Pregunta 22:

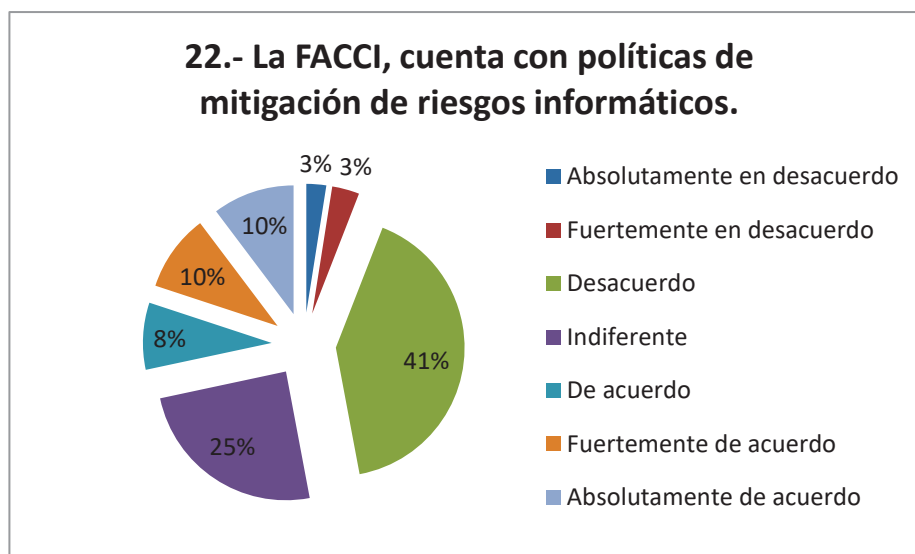


*Gráfico 22: Frecuencia de la Pregunta #22
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 28: Frecuencia de Pregunta #22

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	8	2%
Fuertemente en desacuerdo	11	3%
Desacuerdo	132	41%
Indiferente	79	25%
De acuerdo	27	8%
Fuertemente en acuerdo	31	10%
Absolutamente de acuerdo	33	10%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el grafico #22, un 41% está en desacuerdo, un 25% es indiferente, y un 10% está absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados está en desacuerdo con esta pregunta, existen una gran cantidad de personas que realizaron la encuesta que desconocen si la FACCI cuenta con políticas de mitigación de riesgos informáticos.

Pregunta 23:

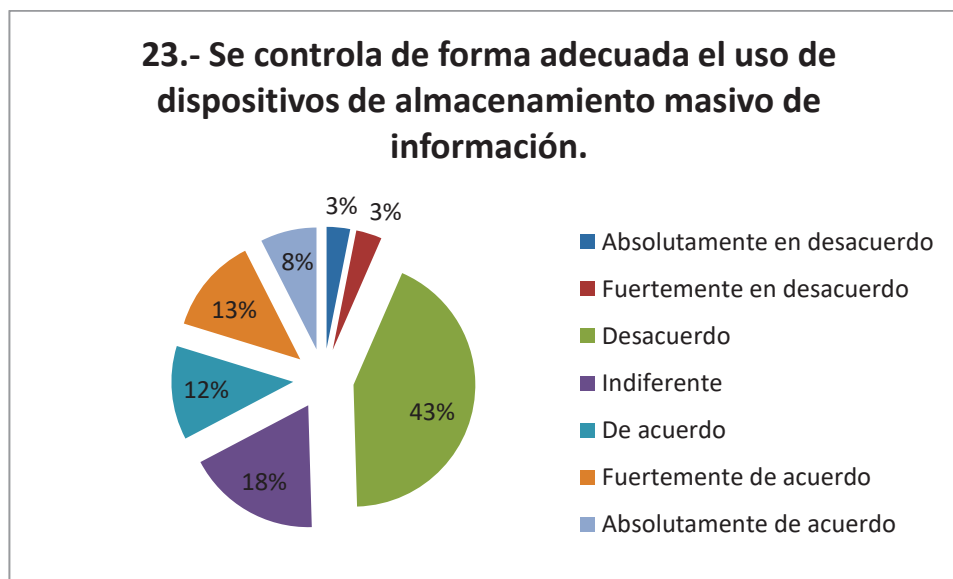


Gráfico 23: Frecuencia de la Pregunta #23

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 29: Frecuencia de Pregunta #23

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	10	3%
Fuertemente en desacuerdo	11	3%
Desacuerdo	138	43%
Indiferente	57	18%
De acuerdo	40	12%
Fuertemente de acuerdo	41	13%
Absolutamente de acuerdo	24	7%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el grafico # 23, un 43% está en desacuerdo, un 18% es indiferente, un 13% está fuertemente de acuerdo, y un 12% en desacuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados está en desacuerdo con esta pregunta, seguidos de los que desconocen si se controla de forma adecuada el uso de dispositivos de almacenamiento masivo de información, seguido de un porcentaje que indica que si se realiza tal control.

Pregunta 24:

**24.- La comunidad académica de la FACCI
(personal docente, administrativos y
estudiantes) está capacitado en Seguridad
Industrial y Salud Ocupacional.**

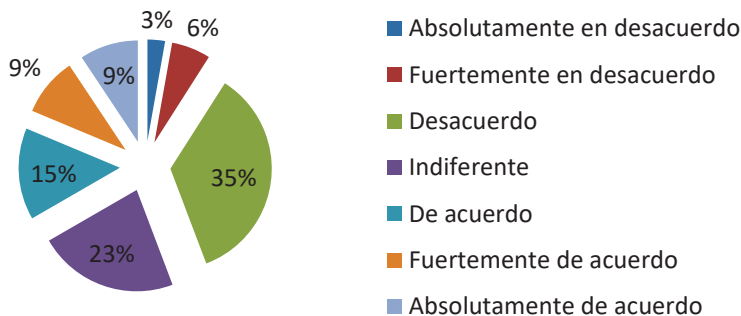


*Gráfico 24: Frecuencia de la Pregunta #24
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 30: Frecuencia de Pregunta #24

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	9	3%
Fuertemente en desacuerdo	20	6%
Desacuerdo	113	35%
Indiferente	72	22%
De acuerdo	47	15%
Fuertemente en acuerdo	30	9%
Absolutamente de acuerdo	30	9%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico # 24, un 35% está en desacuerdo, un 23% es indiferente, un 15% está en desacuerdo, frente a otros porcentajes inferiores que se indican en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, seguido de los que desconocen si la comunidad académica de la FACCI está capacitado en Seguridad Industrial y Salud Ocupacional.

Pregunta 25:

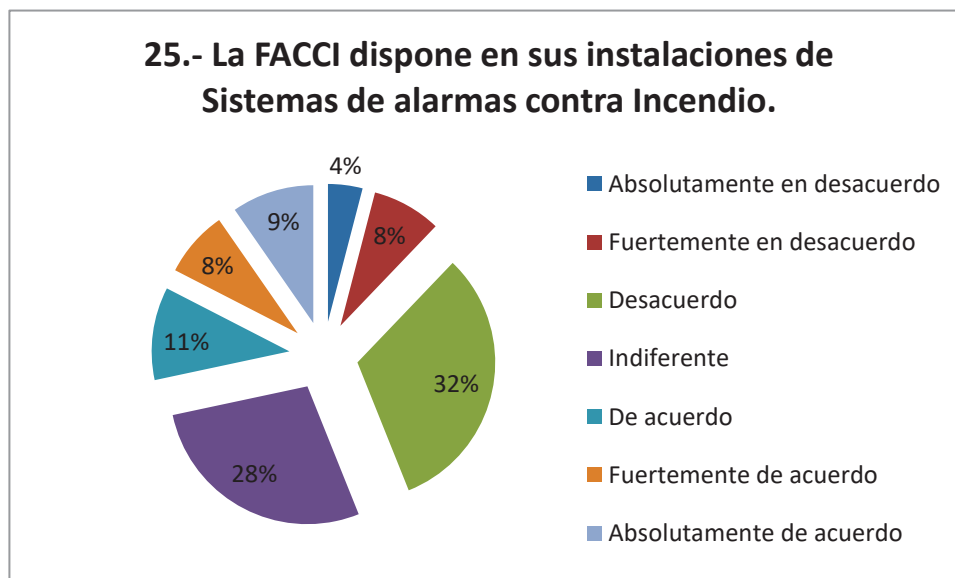


*Gráfico 25: Frecuencia de la Pregunta #25
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 31: Frecuencia de Pregunta #25

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	13	4%
Fuertemente en desacuerdo	26	8%
Desacuerdo	102	32%
Indiferente	89	28%
De acuerdo	35	11%
Fuertemente en acuerdo	25	8%
Absolutamente de acuerdo	31	10%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #25, un 32% está en desacuerdo, un 28% es indiferente, un 11% está de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, seguidos de los que desconocen si en la FACCI se dispone de instalaciones de sistemas de alarmas contra incendio.

Pregunta 26:

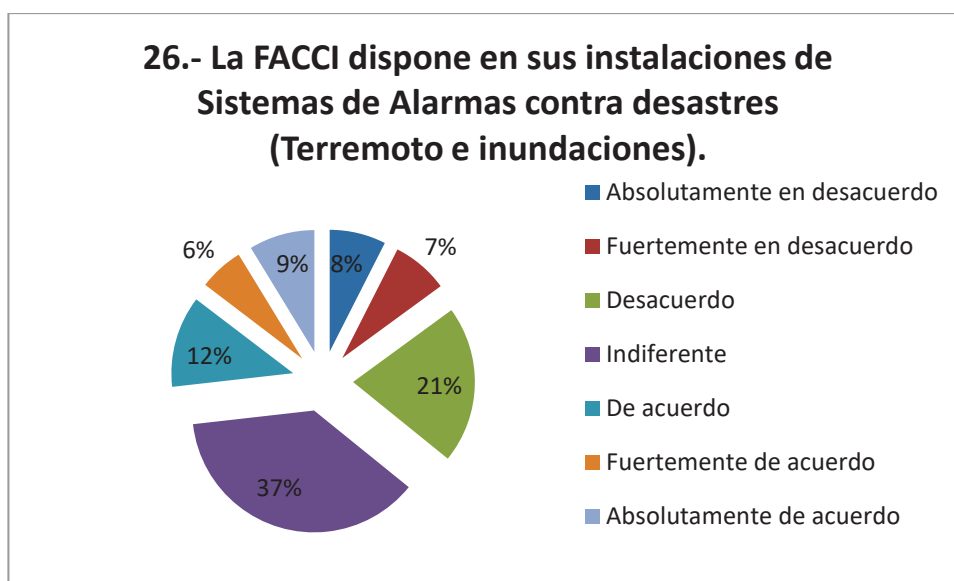


*Gráfico 26: Frecuencia de la Pregunta #26
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 32: Frecuencia de Pregunta #26

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	24	7%
Fuertemente en desacuerdo	24	7%
Desacuerdo	67	21%
Indiferente	120	37%
De acuerdo	39	12%
Fuertemente en acuerdo	19	6%
Absolutamente de acuerdo	28	9%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #26, un 37% es indiferente, un 21% está en desacuerdo, un 12% está de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados desconocen si en la FACCI se dispone en sus instalaciones de sistemas de alarmas contra desastres naturales, y un gran porcentaje está en desacuerdo que no existen tales instalaciones.

Pregunta 27:

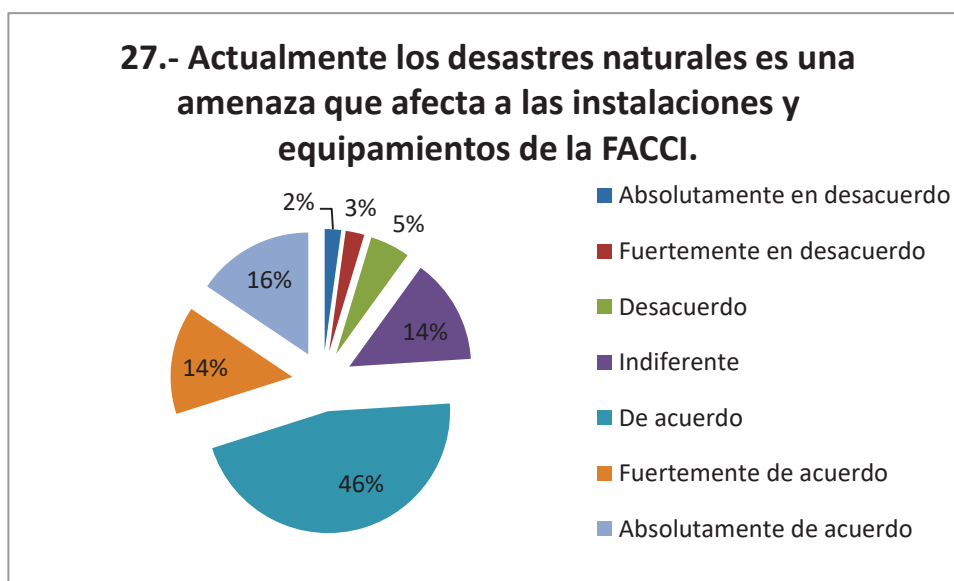


*Gráfico 27: Frecuencia de la Pregunta #27
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 33: Frecuencia de Pregunta #27

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	7	2%
Fuertemente en desacuerdo	8	2%
Desacuerdo	17	5%
Indiferente	45	14%
De acuerdo	148	46%
Fuertemente en acuerdo	46	14%
Absolutamente de acuerdo	50	16%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico #27, un 46,1% está de acuerdo, un 15,6% absolutamente de acuerdo, y un 14,3% fuertemente de acuerdo, frente a otros porcentajes mínimos que se indican en la tabla anterior.

Análisis

Casi la mitad de los encuestados están de acuerdo con esta pregunta, seguidos de un porcentaje que desconoce si actualmente los desastres naturales son una amenaza que afectan a las instalaciones y equipamiento de la FACCI.

Pregunta 28:

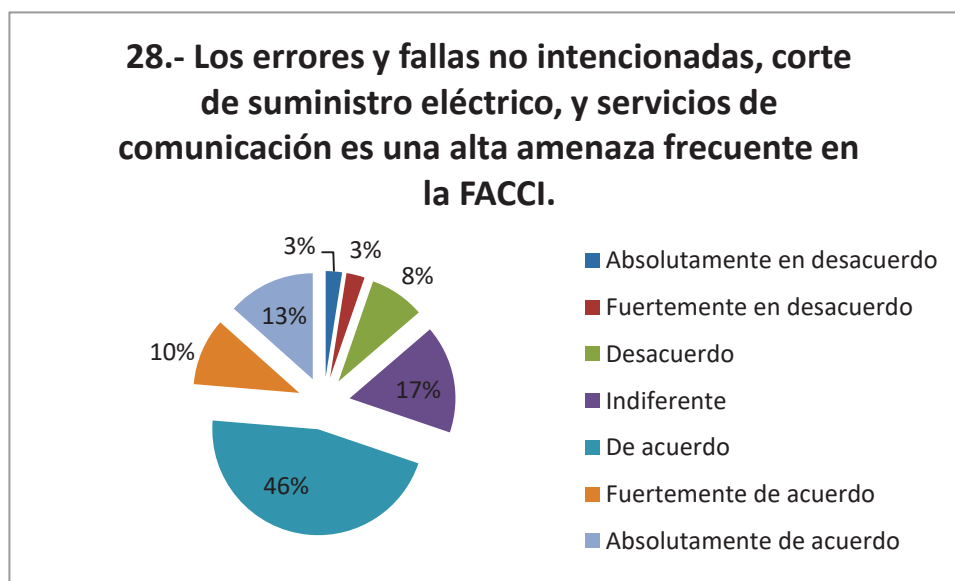


*Gráfico 28: Frecuencia de la Pregunta #28
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 34: Frecuencia de Pregunta #28

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	8	2%
Fuertemente en desacuerdo	9	3%
Desacuerdo	27	8%
Indiferente	53	17%
De acuerdo	148	46%
Fuertemente en acuerdo	33	10%
Absolutamente de acuerdo	43	13%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el grafico # 28, un 46% está de acuerdo, un 16,5% es indiferente, y un 13,4% está absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La gran mayoría de los encuestados están de acuerdo con esta pregunta, seguidos de los que desconocen si los errores y fallas no intencionadas, cortes de suministro eléctrico y servicios de comunicación es una alta amenaza frecuente en la FACCI.

Pregunta 29:

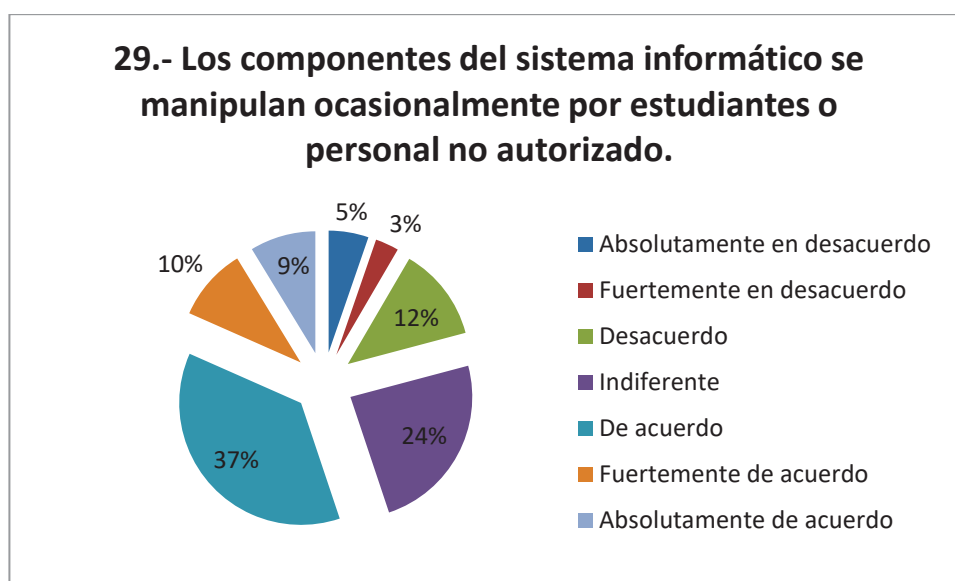


*Gráfico 29: Frecuencia de la Pregunta #29
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 35: Frecuencia de Pregunta #29

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	17	5%
Fuertemente en desacuerdo	10	3%

Desacuerdo	40	12%
Indiferente	77	24%
De acuerdo	118	37%
Fuertemente en acuerdo	31	10%
Absolutamente de acuerdo	28	9%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico #29, un 36,7% está de acuerdo, un 24% es indiferente, y un 12,5 está en desacuerdo, frente a los otros porcentajes mínimos que se indican en la tabla anterior.

Análisis

La mayoría de los encuestados están de acuerdo con esta pregunta, seguido de los que desconocen si los componentes del sistema informático se manipula ocasionalmente por estudiantes o personal no autorizado, existe también una gran parte de los encuestados que indican que no son manipulados.

Pregunta 30:

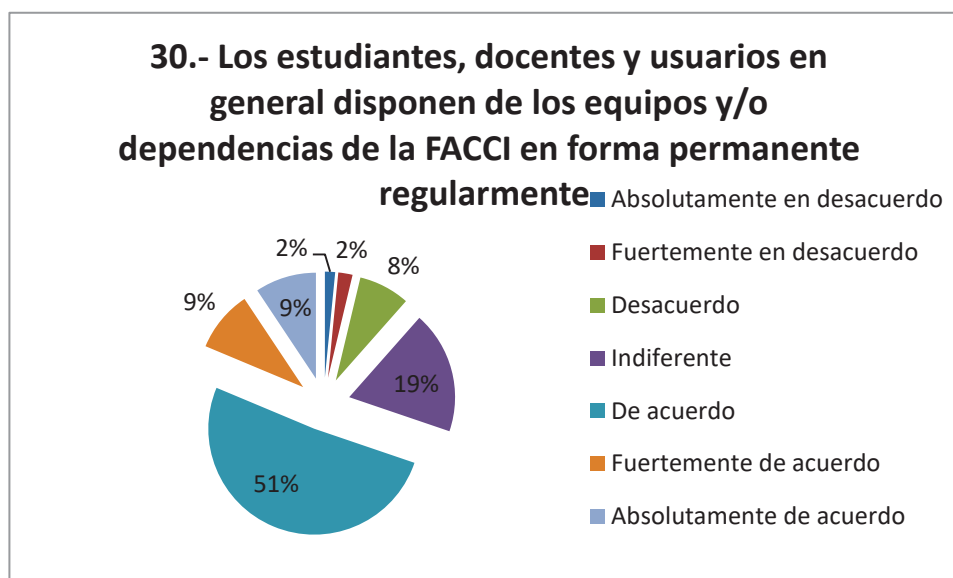


Gráfico 30: Frecuencia de la Pregunta #30

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 36: Frecuencia de Pregunta #30

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	5	2%
Fuertemente en desacuerdo	7	2%
Desacuerdo	25	8%
Indiferente	60	19%
De acuerdo	164	51%
Fuertemente en acuerdo	30	9%
Absolutamente de acuerdo	30	9%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico #30, un 51,1% está de acuerdo, un 18,7 es indiferente, y un 9,35 está fuertemente de acuerdo y absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

Más de la mitad de encuestados están de acuerdo con esta pregunta, con un porcentaje que desconoce si los estudiantes, docentes y usuarios en general disponen de los equipos y dependencias De la FACCI de forma permanente regularmente.

Pregunta 31:

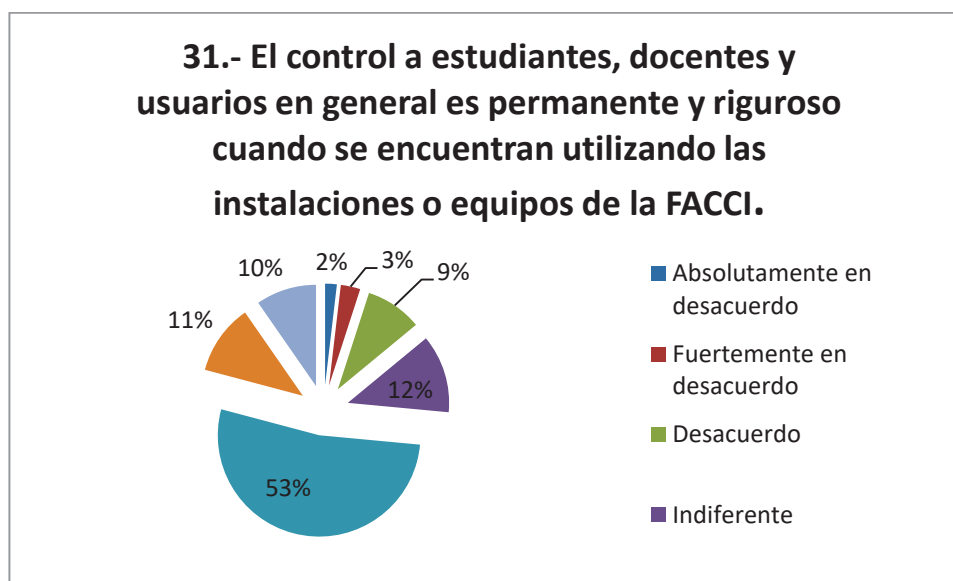


Gráfico 31: Frecuencia de la Pregunta #31

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 37: Frecuencia de Pregunta #31

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	6	2%
Fuertemente en desacuerdo	10	3%
Desacuerdo	29	9%
Indiferente	40	12%
De acuerdo	169	53%
Fuertemente en acuerdo	36	11%
Absolutamente de acuerdo	31	10%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico # 31, un 52,6% está de acuerdo, un 12,5% es indiferente, y un 11,2% está fuertemente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados está de acuerdo con esta pregunta, seguidos de un porcentaje que desconocen si el control es riguroso cuando se utilizan las instalaciones.

Pregunta 32:

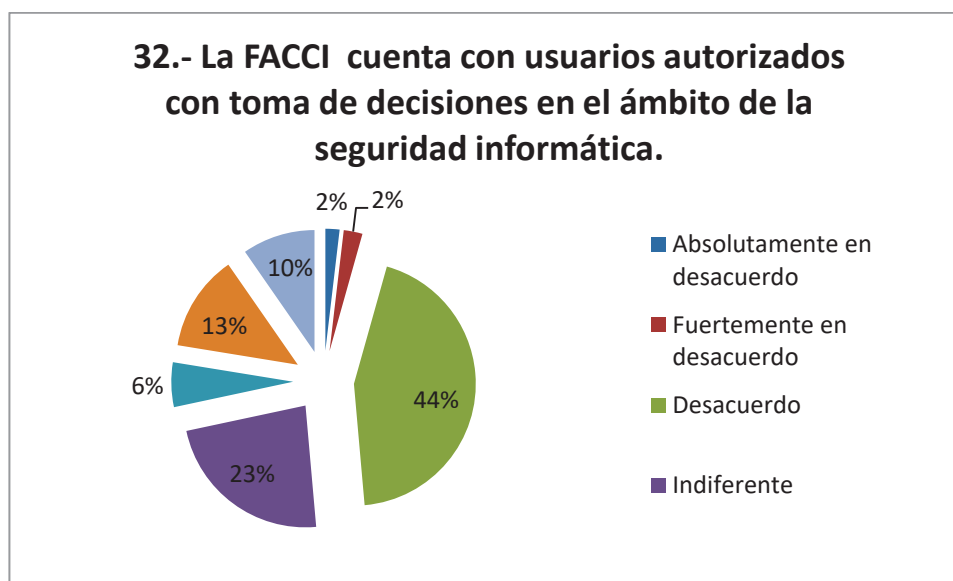


Gráfico 32: Frecuencia de la Pregunta #32

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 38: Frecuencia de Pregunta #32

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	6	2%
Fuertemente en desacuerdo	8	2%
Desacuerdo	142	44%
Indiferente	74	23%
De acuerdo	19	6%
Fuertemente en acuerdo	41	13%
Absolutamente de acuerdo	31	10%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico # 31, un 44,6% está en desacuerdo, un 23% es indiferente, y un 113% está fuertemente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, seguido de los que desconocen si en la FACCI existen usuarios autorizados en la toma de decisiones de seguridad informática.

Pregunta 33:

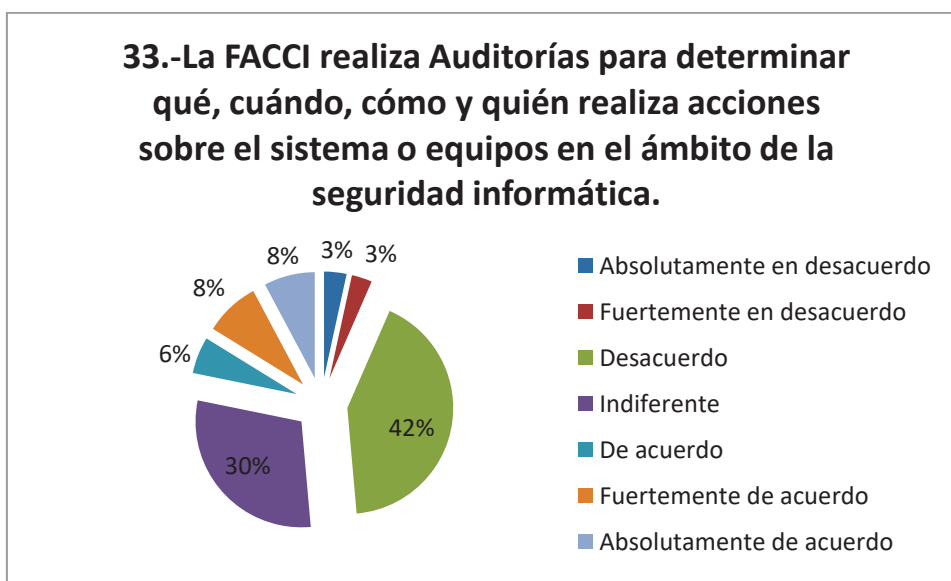


Gráfico 33: Frecuencia de la Pregunta #33

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 39: Frecuencia de Pregunta #33

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	11	3%
Fuertemente en desacuerdo	10	3%
Desacuerdo	135	42%
Indiferente	95	30%
De acuerdo	18	6%
Fuertemente en acuerdo	27	8%
Absolutamente de acuerdo	25	8%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico # 33, un 42% está en desacuerdo, un 30% es indiferente, y un 8% está Absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, seguidos de los que desconocen si en la FACCI se realizan auditorías para determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema o equipos en el ámbito de la seguridad informática, existe un porcentaje de encuestados que indica que si se realizan estas auditorías.

Pregunta 34:

**34.-En la FACCI es obligatorio el uso de las
Normas Técnicas Ecuatorianas NTE INEM-
ISO/IEC 27000 para la Gestión de Seguridad de
la Información tal como lo establece la SNAP**

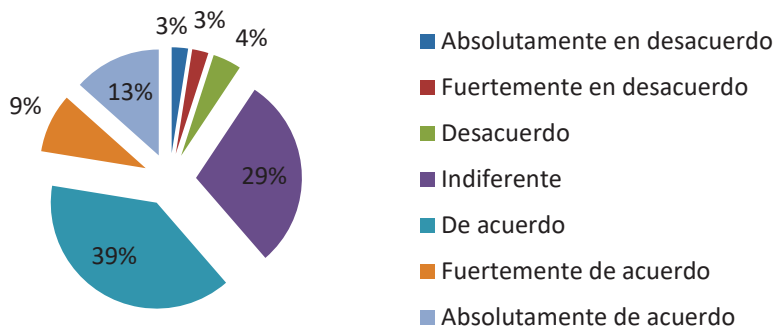


Gráfico 34: Frecuencia de la Pregunta #34

Fuente: Comunidad FACCI

Elaboración: Autores

Tabla 40: Frecuencia de Pregunta #34

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	8	2%
Fuertemente en desacuerdo	8	2%
Desacuerdo	14	4%
Indiferente	94	29%
De acuerdo	125	39%
Fuertemente de acuerdo	29	9%
Absolutamente de acuerdo	43	13%

Fuente: Comunidad FACCI

Elaboración: Autores

Interpretación

Según el gráfico # 34, un 38,9% está de acuerdo, un 29,3% es indiferente, y un 13,4% está absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de encuestados están de acuerdo con esta pregunta, seguidos de los que desconocen si en la FACCI es obligatorio el uso de las Normas Técnicas Ecuatorianas

NTE INEM-ISO/IEC 27000 para la Gestión de Seguridad de la Información tal como lo establece la Secretaría Nacional de Administración Pública del Ecuador (SNAP).

Pregunta 35:

35.- En la FACCI se realiza evaluación de riesgos en base a la norma INEN ISO/IEC 27005 como establece la Secretaría Nacional de...

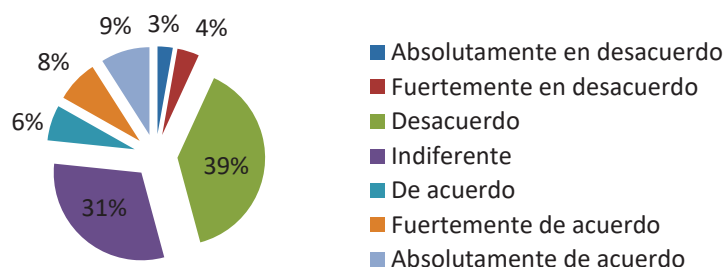


*Gráfico 35: Frecuencia de la Pregunta #35
Fuente: Comunidad FACCI
Elaboración: Autores*

Tabla 41: Frecuencia de Pregunta #35

Alternativas	Frecuencia	Porcentaje
Absolutamente en desacuerdo	9	3%
Fuertemente en desacuerdo	13	4%
Desacuerdo	125	39%
Indiferente	99	31%
De acuerdo	21	7%
Fuertemente en acuerdo	25	8%
Absolutamente de acuerdo	29	9%

*Fuente: Comunidad FACCI
Elaboración: Autores*

Interpretación

Según el gráfico # 33, un 39% está en desacuerdo, un 31% es indiferente, y un 9% está en Absolutamente de acuerdo, frente a otros porcentajes mínimos indicados en la tabla anterior.

Análisis

La mayoría de los encuestados están en desacuerdo con esta pregunta, y un porcentaje importante desconoce si en la FACCI se realiza evaluación de riesgos en base a la norma INEN ISO/IEC 27005 como establece la Secretaría Nacional de Administración Pública (SNAP).

2.9.2 Análisis de los Resultados

2.9.2.1 Análisis de Resultados de Encuesta a toda la comunidad de la FACCI (Docentes, estudiantes y personal administrativo y de servicio)

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

- Existe desconocimiento de la aplicabilidad de la seguridad informática en los laboratorios de la FACCI, lo que perjudica al momento de ocurrir pérdidas de activos.
- La mano de obra en los laboratorios es especializada, pero carece de planificación en sus procesos.
- La FACCI carece de elementos de seguridad informática, según la encuesta y entrevista realizada al Jefe de laboratorios.
- Se conoce la obligatoriedad de las normas (SNAP), pero no su aplicabilidad.

2.9.2.2 Análisis de Resultados de Entrevista

La entrevista se realizó al jefe de laboratorios de la FACCI como se indicó anteriormente, con el objetivo de conocer las políticas y procedimientos relacionados con la evaluación de riesgos de activos y seguridad informática de dichos laboratorios. Véase [Anexo B](#) y [Anexo C](#).

Las preguntas que se realizaron fueron las siguientes, con sus respectivas respuestas:

Entrevistador: ¿Conoce lo que es un plan de seguridad informática?

Jefe de Laboratorios: SI

Entrevistador: ¿Se cuenta actualmente con un plan de seguridad informática en la FACCI?

Jefe de Laboratorios: NO

Entrevistador: ¿Se cuenta con inventario de activos de la FACCI?

Jefe de Laboratorios: SI

Entrevistador: ¿Existe algún plan de contingencia en la FACCI?

Jefe de Laboratorios: NO

Entrevistador: ¿Existe algún documento de gestión de riesgos o algún proceso establecido para gestionarlos?

Jefe de Laboratorios: NO

Entrevistador: ¿Si en este momento ocurriera alguna amenaza para los activos informáticos de la FACCI como reaccionaria?

Jefe de Laboratorios: NORMAL

Entrevistador: ¿Existe en la actualidad algún seguro para proteger los sistemas ante posibles pérdidas causadas por robos o desastres naturales?

Jefe de Laboratorios: NO

Por las respuestas de esta entrevista, se conoce que la FACCI carece de un sistema de gestión de seguridad, de un plan de contingencia que permita una continuidad en los servicios informáticos en el caso de ocurrir una emergencia, robo, desastre natural, etc.

CAPITULO III

3 MARCO PROPOSITIVO (PROPUESTA)

3.1 Introducción

En este capítulo vamos a realizar la descripción de la propuesta de este trabajo de titulación, detallando su alcance, los recursos como es el humano, tecnológico, así como la factibilidad, los riesgos y la selección de las herramientas de desarrollo.

3.2 Descripción de la propuesta

Según el análisis realizado en el capítulo anterior nos ha permitido conocer que la FACCI no contempla los riesgos que pueden sufrir sus activos ante muchas amenazas a las que están sometidos.

En la actualidad no existen muchas herramientas de análisis de riesgos informáticos, al realizar su valoración se puede observar que no todas las empresas utilizan este tipo de herramientas, a no ser que les haya ocurrido ya algún desastre, como lo que ocurrió en nuestro país el 16 de abril del 2016. Falta concienciación en la mayoría de organizaciones para la utilización de herramientas de análisis de riesgos.

También se puede indicar que algunas organizaciones no utilizan estas herramientas debido al costo que presentan, y al desconocer el manejo de las mismas.

De las herramientas de análisis de riesgo citadas, se puede decir que la herramienta Pilar se basa en las ISO/IEC 17799 -27002 y al ser de pago es muy difícil y costoso para una empresa acceder a esta aunque tenga muy buenas funcionalidades, referente a la herramienta MSAT está realizada para empresas que no superen los 1000 empleados, aunque se basa en la ISO/IEC 17799 se encuentra limitada por el tamaño de la organización y el Sistema Operativo, y por último la herramienta RISICARE utiliza el método NEHARI basado en las normas ISO/IEC 27001 pero al ser una herramienta de pago también es poco asequible a las organizaciones.

Tras lo indicado surge la necesidad de un software de análisis de riesgo para poder controlar las vulnerabilidades de los activos de las Instituciones, en nuestro caso específicamente de la FACCI, por ello se manifiesta la siguiente temática: “SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS”

3.3 Determinación de Recursos

3.3.1 Humanos

Como recursos humanos se consideran a las personas que han colaborado con la realización de este proyecto integrador.

Tabla 42: Recursos Humanos

Recursos Humanos	
Autores	Acosta Alvarado Nexar Jesús
	Carrillo Morán Fátima Guadalupe
Tutores del Trabajo de Titulación	Ing. Robert Moreira, Mg
	Ing. Denise Vera Navarrete, Mg
Recursos Humanos de la FACCI	Estudiantes
	Docentes
	Personal Administrativo

Fuente: Autores

3.3.2 Tecnológicos

Los recursos tecnológicos que hemos utilizado en este trabajo de titulación se detallan a continuación:

3.3.2.1 Hardware

Tabla 43: Recursos Tecnológicos - Hardware

ítem	Recursos de Hardware
-------------	-----------------------------

1	Descripción	Cantidad
1.1	Acer E1-571G 8GB de RAM, 3.2GHz: Procesador Intel Core i5-3230M	1
1.2	Asus Procesador Intel Core i5, 8 GB de RAM	1
1.3	Impresora Canon	1
1.4	Tinta Impresora	1
1.4	Memorias USB	2

Fuente: Autores

3.3.2.2 Software

Tabla 44: Recursos Tecnológicos - Software

Ítem	Recursos de Software	
2	Descripción	Cantidad
2.1	Sistema Operativo Windows 10	1
2.2	Office 2010: Microsoft Word 2010, Microsoft Excel 2010, Microsoft Power Point	3
2.3	Software de Programación: Netbeans	2
2.4	Base de datos: MySQL	
3	Servicio	
3.1	Internet	8(meses, 4 meses cada uno)

Fuente: Autores

3.3.2.3 Materiales y otros

En este apartado vamos a mencionar otros recursos que no son ni tecnológicos ni humanos y que se ha necesitado para el desarrollo de este Proyecto.

Tabla 45: Recursos Materiales y otros

ítem	Recursos de Materiales y otros
-------------	---------------------------------------

1	Descripción	Cantidad
1.1	Resmas de Papel	2
1.2	Anillados	1
1.3	Empastado	1
1.4	CDs	2
1.5	Bolígrafos	3
1.6	Cuaderno	2
2	Libros PDF	
2.1	Magerit libro 1 Método	2
2.2	Magerit libro 2 Catálogo de elementos	2
2.3	Magerit libro 3 Guía de técnicas	2
2.4	ISO/IEC 27001	2
2.5	ISO/IEC 17799	2

Fuente: Autores

3.3.3 Económicos (presupuesto)

En este apartado vamos a considerar todos los gastos que ha habido para la realización de este trabajo de titulación, se va a detallar desde el presupuesto de recursos humanos, tecnológicos y otros materiales

3.3.3.1 Presupuesto de Recursos Humanos

El presupuesto de los recursos humanos se detalla en la siguiente tabla:

Tabla 46: Presupuesto Recursos Humanos

Presupuesto Recursos Humanos					
Ítem	Descripción	Cantidad	Horas	Valor/Hora	Total
1	Grupo de Investigación				
1.1	Autores de	2	400	\$5,00	\$2.000,00

	trabajo de titulación				
2	Asesoría de Proyecto Integrador				
2.1	Tutores de trabajo de titulación	2	-	-	-
Total del presupuesto de Recursos Humanos					\$2.000,00

Fuente: Autores

3.3.3.2 Presupuesto de recursos tecnológicos

El presupuesto de los recursos tecnológicos se detalla en la siguiente tabla:

Tabla 47: Presupuesto Recursos Tecnológicos

Presupuesto Recursos Tecnológicos				
Ítem	Descripción	Cantidad	Costo	Total
1	Hardware			
1.1	Acer E1-571G 8GB de RAM, 3.2GHz: Procesador Intel Core i5-3230M	1	\$800,00	\$800,00
1.2	Asus Procesador Intel Core i5, 8 GB de RAM	1	\$500	\$500
1.3	Sistema de tinta continua	1	\$50,00	\$50,00
1.4	Impresora	1	\$100	\$100
1.5	Memoria USB	2	\$8	\$16
2	Servicio			
2.1	Internet	8 (meses, entre los 2 autores)	\$25,00	\$50,00

Total del presupuesto de Recursos Tecnológicos	\$1516,00
---	------------------

Fuente: Autores

3.3.3.3 Presupuesto de otros recursos materiales

El presupuesto de otros recursos materiales se detalla en la siguiente tabla:

Tabla 48: Presupuesto Recursos Tecnológicos

Presupuesto Otros Recursos Materiales				
Ítem	Descripción	Cantidad	Costo	Total
2	Materiales de Oficina			
2.1	Resmas de Papel	2	\$3,25	\$6,50
2.2	Anillados	1	\$10,00	\$10,00
2.3	Empastado	1	\$20,00	\$20,00
2.4	CDs	2	\$1,50	\$3,00
2.5	Bolígrafos	3	\$0,75	\$2,25
2.6	Cuaderno	2	\$1,00	\$2,00
3	Servicios			
3.2	Energía Eléctrica	8 (meses 4 cada autor)	\$30,00	\$60,00
4	Viáticos			
4.1	Transporte Autor 1	20 (días)	\$0,60	\$12,00
4.2	Transporte Autor 2	20 (días)	\$5,00	\$100,00
Total Presupuesto de otros recursos materiales				\$215,75

Fuente: Autores

3.3.3.4 Presupuesto Total

El presupuesto total se detalla en la siguiente tabla:

Tabla 49: Presupuesto Total

PRESUPUESTO TOTAL

Ítem	Rubro	Total
1	Total del presupuesto de Recursos Humanos	\$2000,00
2	Total del presupuesto de Recursos Tecnológicos	\$1516,00
3	Total Presupuesto de otros recursos materiales	\$215,75
Subtotal		\$3731,75
4	5% Imprevistos	\$186,58
TOTAL PRESUPUESTO		\$3918,33

Fuente: Autores

Todos los gastos indicados en este presupuesto fueron asumidos por los autores de este proyecto, y se calcularon por los 4 meses que ha durado la realización de este proyecto.

3.4 Etapas de acción para el desarrollo de la propuesta

FASE DE INICIO

3.4.1 FASE I: ANÁLISIS DE LA INSTITUCIÓN

3.4.1.1 Antecedentes de la FACCI (Reseña Histórica)

La Unidad Académica inicia su proceso de formación de Tecnólogos en Computación Administrativa en 1982 en la Escuela de Computación Administrativa adscrita a la Facultad de Ciencias Administrativas.

Ante la aparición de nuevas tecnologías y necesidades del contexto, que implica formar profesionales altamente especializados, en el año 1991, se aplica un rediseño y se realizan los trámites respectivos para el cambio de titulación a Analista de Sistemas, bajo la misma modalidad.

El entorno social, el estado, la constitución y las nuevas leyes de educación, demandan que las instituciones de educación superior, atiendan las necesidades cada vez más crecientes del país. Ante esta exigencia en el año 1997 se oferta la carrera de Ingeniería en Sistemas con una duración de 6 años.

En el año 2001 basado en los principios de integralidad y siguiendo las tendencias de la educación superior, se implementa un rediseño curricular bajo la modalidad anual que contempla la duración de la carrera a 5 años. Rediseño acogido por la Comisión Académica de la ULEAM, y por los miembros del Honorable Consejo Universitario quienes en sesión del miércoles 11 de julio del 2001 autorizan la creación de la Facultad de Ciencias Informáticas, con titulación de Ingeniero/a en Sistemas.

En el año lectivo 2007-2008, la institución aprueba la implementación del sistema curricular con enfoque por competencias y créditos a la que se fueron sumando cada una de las unidades académicas, entre ellas la FACCI, quien lo hizo a partir del período académico 2011-2012 (MANABÍ, 2018).

3.4.1.2 Misión

Unidad académica de Educación Superior líder en el ámbito informático, con criterio creativo e innovador de reconocimiento local y nacional; en la formación integral de profesionales generadores de bienes y servicios (MANABÍ, 2018).

3.4.1.3 Visión

Proporcionar formación científica, tecnológica y cultural a los futuros profesionales en las ciencias informáticas, enmarcadas en la ética y la moral; con el fin de

garantizar la eficiencia y eficacia en la prestación de sus servicios y la producción de bienes a la sociedad.

3.4.1.4 Organigrama estructural de la FACCI

En la siguiente ilustración se muestra el organigrama funcional de la FACCI.



Ilustración 4: Organigrama funcional de la FACCI

Fuente: <http://carreras.uleam.edu.ec/facci/datos-generales/estructura-organica/>

3.4.1.5 Personal involucrado en el proyecto

En este apartado se va a indicar las personas que han intervenido en este proyecto:

Autores del Proyecto

- Acosta Alvarado Nexar Jesús
- Carrillo Morán Fátima Guadalupe

Personal Involucrado

- Ing. Denise Vera Navarrete
- Ing. Robert Moreira
- Ing. Gilber Loo Muñoz (Analista de Informática)
- Ing. José Bazurto (Asesor estadístico)

3.4.2 FASE II: ACTIVIDADES PRELIMINARES

3.4.2.1 Estudio de Oportunidad

Según las encuestas realizadas, y la entrevista se puede evidenciar las siguientes falencias en la FACCI:

- No existe en la actualidad ningún plan de seguridad informática.
- No todo el software utilizado se encuentra con licencia.
- Ante cualquier amenaza a los activos, no existe forma de actuar.

Por ello se ve en la necesidad de realizar un análisis de gestión de riesgos de los activos informáticos de la FACCI, para mitigar las amenazas y vulnerabilidades que estos pueden sufrir, así como mejorar la seguridad informática.

3.4.2.2 Determinación del alcance del proyecto

Este proyecto se va a realizar en la FACCI. Se detallan de forma general los activos con lo que cuenta la facultad:

- Datos e información: Inventarios General de los bienes.
- Servicios: Red Intranet/Extranet.
- Software: Ofimática, antivirus, sistema operativo y otro software.
- Hardware: Computadoras personales, computadoras de escritorio, impresoras, switch, router.

- Redes de comunicaciones: Red WI-FI, red LAN e internet.
- Soportes de información: CD, memorias USB y disco duro externo.
- Equipamiento auxiliar: UPS y cámaras de seguridad.
- Instalaciones: Instalaciones eléctricas.
- Personal: Personal Administrativo, docentes y directivos.

Se clasificaron los activos por el tipo, mediante la estructura de la metodología MAGERIT que se encuentra en su libro II- Catálogo de Elementos.

3.4.2.3 Identificación de los activos

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

La solicitud se encuentra en el anexo 4.

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

Tabla 50: Identificación de Activos Informáticos de la FACCI

ACTIVOS INFORMÁTICOS	
[DI] Datos/Información	Inventario General de los bienes
[S] Servicios	Red Intranet/Extranet
	Red Intranet/Extranet
[SW] Software-Aplicaciones Informáticas	Ofimática
	Antivirus
	Sistema Operativo
	Otros tipos de Software
[HW] Hardware-Equipamiento Informático	Ordenadores(Portátiles/Escritorio)
	Impresoras
	Switch
	Router
	WAP (Punto de acceso inalámbrico)
[COM] Redes de Comunicaciones	Red Wi-Fi
	Red Lan
	Internet

[Media] Soportes de Información	CD
	Memorias USB
	Disco Duro Externo
[AUX] Equipamiento Auxiliar	Ups
	Cámaras de Seguridad
	Aires Acondicionados
[INST] Instalaciones	Instalaciones eléctricas
[PSL] Personal	Personal Administrativo
	Docentes
	Directivos

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

Elaboración: Autores

3.4.3 FASE III: PLANIFICACIÓN

3.4.3.1 Descripción de la metodología de trabajo

Para el desarrollo del software se ha elegido la metodología ágil SCRUM, la cual facilita la administración de los proyectos de cualquier tamaño y complejidad, ya que facilita el flujo de información, y hay mucha comunicación entre el equipo de trabajo.

Las ventajas de elección de SCRUM son la transparencia, adaptabilidad, mejora continua, retroalimentación continua, y los procesos iterativos le dan una entrega continua de valor, lleva un ritmo de trabajo sostenible, tiene una anticipada entrega de valor con los entregables lo que con lleva a que los requisitos con más valor de los clientes sean los primeros en ser satisfechos, y por último es un proceso de desarrollo eficiente con periodos específicos lo que reduce al mínimo el trabajo que no es esencial.

3.4.3.2 Bosquejo de la Metodología de Trabajo SCRUM

En la metodología SCRUM la planificación es esencial, por ello se estableció un grupo de trabajo bien definido, así como establecer los objetivos de forma clara y concisa en el Product Backlog, los cuales son divididos en iteraciones de máximo 20 días, planificando la realización de cada una de las tareas en un Sprint Backlog. Se establecieron reuniones cortas de 10 minutos para verificar avances, realizar retroalimentación y determinar un plan de acción para solucionar los inconvenientes que se hayan dado.

3.4.3.2.1 Personas o roles del Proyecto.

El equipo de trabajo aplicando SCRUM se definió de la siguiente forma:

Tabla 51: Personas o roles del Proyecto

Persona	Contacto	Rol
Carrillo Morán Fátima Guadalupe	fattecm@hotmail.com 0990490186	[Coordinador / Scrum Manager...]
Ing. Vera Navarrete Denise Soraya	0987224890	[Gestor de producto / P. Owner ...]
Acosta Alvarado Nexar Jesús	0981773628	[Equipo técnico...]
Carrillo Morán Fátima Guadalupe	fattecm@hotmail.com 0990490186	[Equipo técnico...]

Fuente: Autores

Product Owner(Cliente): El puente entre clientes y grupo de trabajo, es desempeñado por la Ing. Denise Vera.

Scrum Master(Facilitador): El guía de la metodología SCRUM y organización de reuniones, estará a cargo de Fátima Carrillo.

Team (Equipo de desarrollo): Realizara el proceso de creación del producto, será desempeñado por Acosta Nexar, y Carrillo Fátima.

3.4.3.2.2 Descripción de los objetivos del producto (Product Backlog)

Tabla 52: Product Backlog

Id	Prioridad	Descripción	Estimación
1	Alta	Requisitos, Análisis	2
2	Muy Alta	Diseño y desarrollo de la base de datos	2
3	Alta	Configuración de Plataformas de desarrollo	1
4	Alta	Diseño y desarrollo de Interfaz de usuario	1
5	Alta	Inicio de Sesión - Home	2
6	Alta	Gestión Modulo Ingresos	3
7	Alta	Gestión Modulo Cruces	2
8	Alta	Gestión Modulo Análisis	1
9	Alta	Gestión Modulo Aplicación	1

Fuente: Autores

3.4.3.2.3 Planeación de Sprint

Para llevar acabo organizadamente los Sprint, se ha utilizado el software Sprintometer 6.54, el cual ayuda a llevar acabo la metodología SCRUM.

Nombre Sprint	Fecha de Inicio	Fecha Final
Totales:		
✓ <u>Requisitos y analisis</u>	13 Nov 2017	24 Nov 2017
✓ <u>Diseño y Desarrollo de la BD</u>	27 Nov 2017	06 Dec 2017
✓ <u>Configuracion de Plataformas D</u>	07 Dec 2017	08 Dec 2017
✓ <u>Inicio Sesion - Home</u>	11 Dec 2017	15 Dec 2017
✓ <u>Modulo Ingreso</u>	18 Dec 2017	12 Jan 2018
✓ <u>Modulo Cruces</u>	15 Jan 2018	02 Feb 2018
✓ <u>Modulo Analisis y Aplicación</u>	05 Feb 2018	14 Feb 2018
✓ <u>Testeo</u>	15 Feb 2018	16 Feb 2018
✓ <u>Implementacion</u>	19 Feb 2018	19 Feb 2018

Gráfico 36: Planeación de Sprint

Fuente: Sprintometer

Elaboración: Autores

3.4.4 FASE V: DISEÑO E IMPLEMENTACIÓN

3.4.4.1 Descripción de Sprints

3.4.4.1.1 Descripción Sprint 1

El Sprint 1 es de Requisitos y análisis:

ID Historia	Nombre Historia	Codificado	Probado	Hecho	▽
✓ 1.1	Reconocimiento del problema	n/a	n/a	✓ 100%	
✓ 1.2	Evaluación y síntesis	n/a	n/a	✓ 100%	
✓ 1.3	Especificación de Requisitos	n/a	n/a	✓ 100%	

*Gráfico 37: Sprint 1
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.1.2 Descripción Sprint 2

El Sprint 2 es de Diseño y desarrollo de la BD:

ID Historia	Nombre Historia	Codificado	Probado	Hecho	▽
✓ 2.1	Modelo ER y Relaciones de Tablas	✓ 100%	n/a	✓ 100%	
✓ 2.2	Creación de BD	✓ 100%	n/a	✓ 100%	

*Gráfico 38: Sprint 2
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.1.3 Descripción Sprint 3

El Sprint 3 es de Configuración de la Plataforma

ID Historia	Nombre Historia	Codificado	Probado	Hec...	▽
✓ 3.1	Instalación Netbeans	n/a	✓ 100%	✓ 100%	
✓ 3.2	Instalar IDE de MySQL	✓ 100%	n/a	✓ 100%	
✓ 3.3	Conexión de Netbeans y Mysql	✓ 100%	n/a	✓ 100%	

*Gráfico 39: Sprint 3
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.1.4 Descripción Sprint 4

El Sprint 4 es de Inicio de Sesión –Home:

ID Historia	Nombre Historia	Codificado	Probado	Hec... ▾
✓ 4.1	Creacion de Interfaz	✓ 100%	n/a	✓ 100%
✓ 4.2	Crecion de Login	✓ 100%	n/a	✓ 100%
✓ 4.3	Creacion de Informacion- Contacto	✓ 100%	n/a	✓ 100%

*Gráfico 40: Sprint 4
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.1.5 Descripción Sprint 5

El Sprint 5 es del Módulo de Ingreso:

ID Historia	Nombre Historia	Codificado	Probado	Hec... ▾
✓ 5.1	Ingreso de Activos	✓ 100%	n/a	✓ 100%
✓ 5.2	Ingreso de Amenazas	✓ 100%	n/a	✓ 100%

*Gráfico 41: Sprint 5
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.1.6 Descripción Sprint 6

El Sprint 6 es del Módulo de Cruces:

ID Historia	Nombre Historia	Codificado	Probado	Hec... ▾
✓ 6.1	Creacion de Interfaz	✓ 100%	n/a	✓ 100%
✓ 6.2	Cruce Amenaza-Activo	✓ 100%	n/a	✓ 100%
✓ 6.3	Reporte	✓ 100%	n/a	✓ 100%

*Gráfico 42: Sprint 6
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.1.7 Descripción Sprint 7

El Sprint 7 es del Módulo de Análisis y Aplicación:

ID Historia	Nombre Historia	Codificado	Probado	Hec... ▾
✓ 7.1	Creacion de Interfaz	✓ 100%	n/a	✓ 100%
✓ 7.2	Probabilidad Impacto	✓ 100%	n/a	✓ 100%
✓ 7.3	Aplicación ISO 17799	✓ 100%	n/a	✓ 100%
✓ 7.4	Aplicación ISO 27001	✓ 100%	n/a	✓ 100%

Gráfico 43: Sprint 7
Fuente: Sprintometer
Elaboración: Autores

3.4.4.1.8 Descripción Sprint 8

El Sprint 8 es el Testeo:

ID Historia	Nombre Historia	Codificado	Probado	Hec... ▾
✓ 8.1	Realizar Prueba de errores	✓ 100%	n/a	✓ 100%

Gráfico 44: Sprint 8
Fuente: Sprintometer
Elaboración: Autores

3.4.4.1.9 Descripción Sprint 9

El Sprint 8 es la Implementación:

ID Historia	Nombre Historia	Codificado	Probado	Hec... ▾
✓ 8.1	Caso de estudio	n/a	✓ 100%	✓ 100%

Gráfico 45: Sprint 9
Fuente: Sprintometer
Elaboración: Autores

3.4.4.2 Detalle de cada Sprint

En este apartado se va a detallar las tareas que se hicieron en cada uno de los Sprint durante todo el Proyecto.

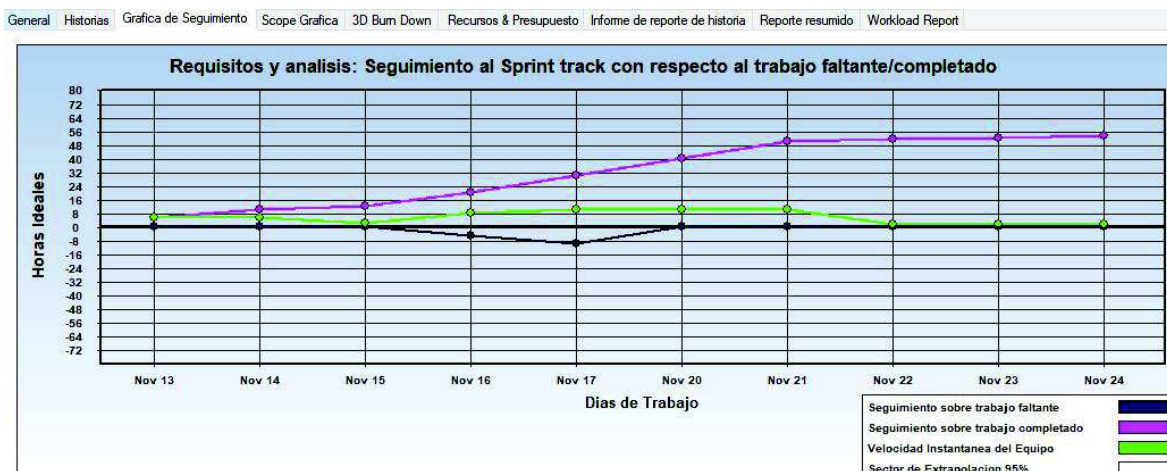


*Gráfico 47: Seguimiento Sprint 1
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.2.1.1 Requisitos Funcionales

- Roles de Usuarios
- Registro de Activos
- Registro de Amenazas
- Reporte de Cruce Activos-Amenazas
- Aplicación de Controles para cada cruce

3.4.4.2.1.2 Requisitos no Funcionales

- IDE Netbeans 8.0
- MySQL Workbench
- Lenguaje Java

3.4.4.2.2 Diseño y Desarrollo de Base de Datos (Sprint 2)

En este segundo Sprint se realiza el modelo Entidad Relación, relaciones de las tablas y la creación de la base de datos.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Burn Down	Recursos & Presupuesto	Informe de reporte de historia	Reporte resumido	Workload Report					
						Estimacion/Fecha:	Nov 28	Nov 29	Nov 30	Dec 01	Dec 04	Dec 05	Dec 06
						Hecho %:	25% (6)	38% (9)	58% (14)	75% (18)	79% (19)	88% (21)	✓ 100% (24)
						Codificado %:	-	11% (1)	33% (3)	33% (3)	44% (4)	67% (6)	✓ 100% (9)
						Probado %:	n/a	n/a	n/a	n/a	n/a	n/a	n/a
						Hecho hoy/Para hacer:	1/4	3/4	5/2	4/1	1/2	2/1	3/0
						Codificado hoy/para hacer:	0/0	1/1	2/0	0/0	1/2	2/1	3/0
						Probado hoy/Para hacer:	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea	Asignado 1	Asignado 2			Hecho %:	33% (6)	50% (9)	78% (14)	✓ 100% (18)	✓ 100% (18)	✓ 100% (18)	✓ 100% (18)
✓ 2.1	Modelo ER y Relaciones de Tablas					15	1/4	2/3	3/2	4/1	0/0	0/0	0/0
✓ 2	Relaciones entre tablas					3		1/1	2/0	0/0	0/0	0/0	0/0
✓ 2.2	Creación de BD					Hecho %:					17% (1)	50% (3)	✓ 100% (6)
✓ 1	Creacion de Script para MySQL					6					1/2	2/1	3/0

Gráfico 48: Historia Sprint 2
Fuente: Sprintometer
Elaboración: Autores

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #49 se muestra las fechas del Sprint de inicio (27/11/2017) y fin (06/12/2017) del Sprint con respecto al trabajo faltante/completado.

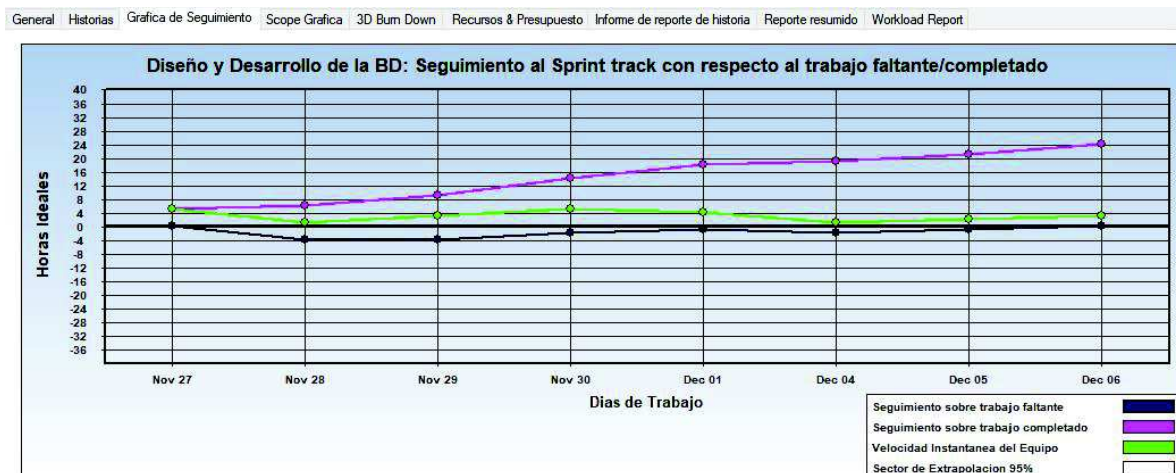


Gráfico 49: Seguimiento Sprint 2
Fuente: Sprintometer
Elaboración: Autores

MODELO ENTIDAD /RELACIÓN

El modelo ER se realizó en el IDE MySQL Workbench, junto con los atributos y relaciones entre las tablas.

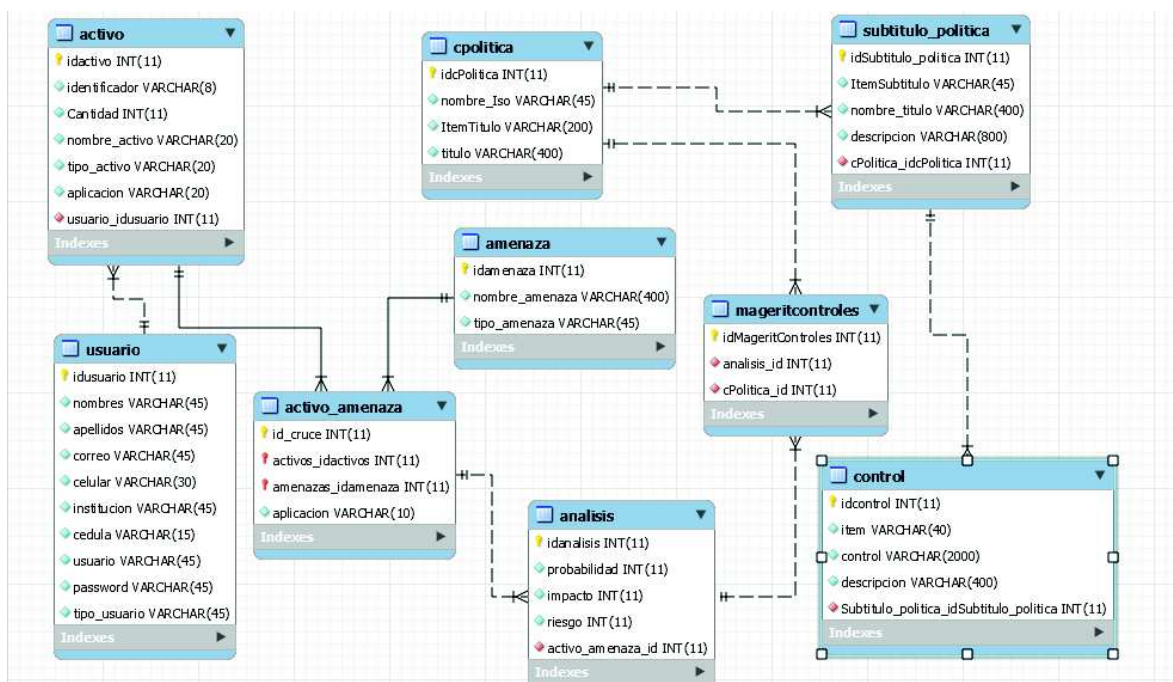


*Gráfico 50: Modelo Entidad /Relación
Fuente: Workbench
Elaboración: Autores*

Creación de Base de datos y tablas

MySQL Workbench

Local instance MySQL57 x MySQL Model (modelof.mwb) x EER Diagram x

File Edit View Query Database Server Tools Scripting Help

Navigator

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

SCHEMAS

Filter objects

- riskman
- sys

Information

Query 1 activo amenaza activo_amenaza amenaza amenaza amenaza usuario

```

16
17
18 CREATE SCHEMA IF NOT EXISTS `riskman` DEFAULT CHARACTER SET utf8 ;
19 USE `riskman` ;
20
21 -- Table `riskman`.`usuario`
22
23 CREATE TABLE IF NOT EXISTS `riskman`.`usuario` (
24   `idusuario` INT(11) NOT NULL,
25   `nombres` VARCHAR(45) NOT NULL,
26   `apellidos` VARCHAR(45) NOT NULL,
27   `correo` VARCHAR(45) NOT NULL,
28   `celular` VARCHAR(30) NOT NULL,
29   `institucion` VARCHAR(45) NOT NULL,
30   `cedula` VARCHAR(15) NOT NULL,
31   `usuario` VARCHAR(45) NOT NULL,
32   `password` VARCHAR(45) NOT NULL,
33   `tipo_usuario` VARCHAR(45) NOT NULL,
34   PRIMARY KEY (`idusuario`))
35 ENGINE = InnoDB
36 DEFAULT CHARACTER SET = utf8;
37
38
39 -- Table `riskman`.`activo`
40
41 CREATE TABLE IF NOT EXISTS `riskman`.`activo` (
42   `idactivo` INT(11) NOT NULL,
43   `identificador` VARCHAR(8) NOT NULL,
44   `Cantidad` INT(11) NOT NULL,
45   `nombre_activo` VARCHAR(20) NOT NULL,
46   `tipo_activo` VARCHAR(20) NOT NULL,
47   `aplicacion` VARCHAR(20) NOT NULL,
48   `usuario_idusuario` INT(11) NOT NULL,

```

Gráfico 51: Script de creación de BD y tablas

*Fuente: Workbench
Elaboración: Autores*

3.4.4.2.3 Configuración de Plataformas de desarrollo (Sprint 3)

En este tercer Sprint se realiza la configuración del IDE Netbeans 8.0, con el IDE de la base de datos MySQL Workbench.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Burn Down	Recursos & Presupuesto	Informe de reporte de historia	Reporte resumido	Workload
						Estimacion\Fecha:	Dec 07	Dec 08
						Hecho %:	67% (2)	✓ 100% (3)
						Codificado %:	50% (1)	✓ 100% (2)
						Probado %:	✓ 100% (1)	✓ 100% (1)
						Hecho hoy/Para hacer:	2/0	1/0
						Codificado hoy/para hacer:	1/0	1/0
						Probado hoy/Para hacer:	1/0	0/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea		Asignado 1	Asignado 2	Probado hoy/Para hacer:			
✓ 3.1	Instalación Netbeans				Hecho %:	✓ 100% (1)	✓ 100% (1)	
✓ 1	Descarga de IDE				1	✓ 1/0	✓ 0/0	
✓ 3.2	Gestión de MySQL				Hecho %:	✓ 100% (1)	✓ 100% (1)	
✓ 1	Funcionamiento con Netbeans de MySQL Workbench				1	✓ 1/0	✓ 0/0	
✓ 3.3	Conexión de Netbeans y Mysql				Hecho %:		✓ 100% (1)	
✓ 1	Realizar Conexión				1		✓ 1/0	

*Gráfico 52: Historia Sprint 2
Fuente: Sprintometer
Elaboración: Autores*

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #54 se muestra las fechas del Sprint de inicio (07/12/2017) y fin (08/12/2017) del Sprint con respecto al trabajo faltante/completado.

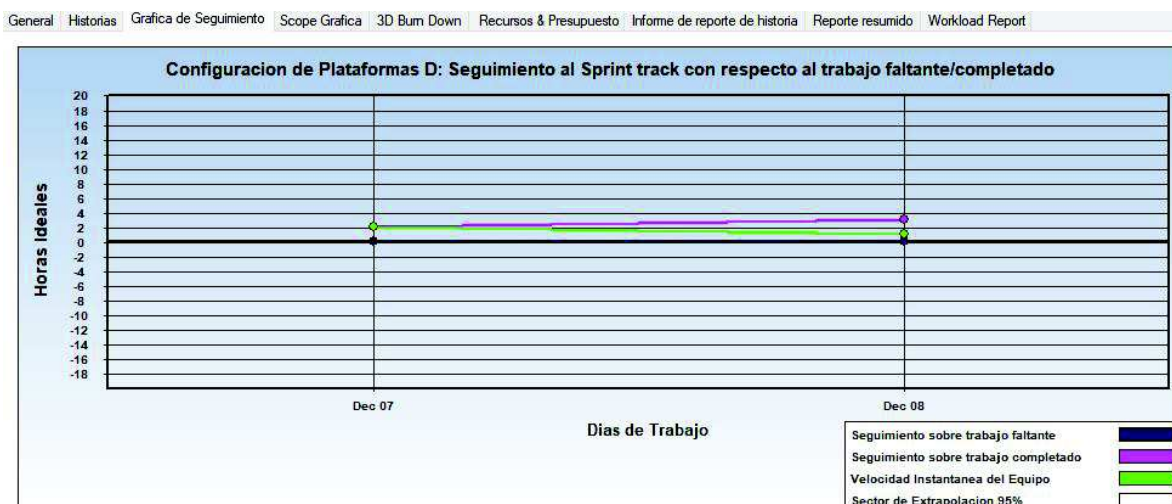


*Gráfico 54: Seguimiento Sprint 3
Fuente: Sprintometer
Elaboración: Autores*

Netbeans 8.0

Ejecutable:

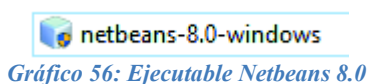


Gráfico 56: Ejecutable Netbeans 8.0

Una vez ya instalado:

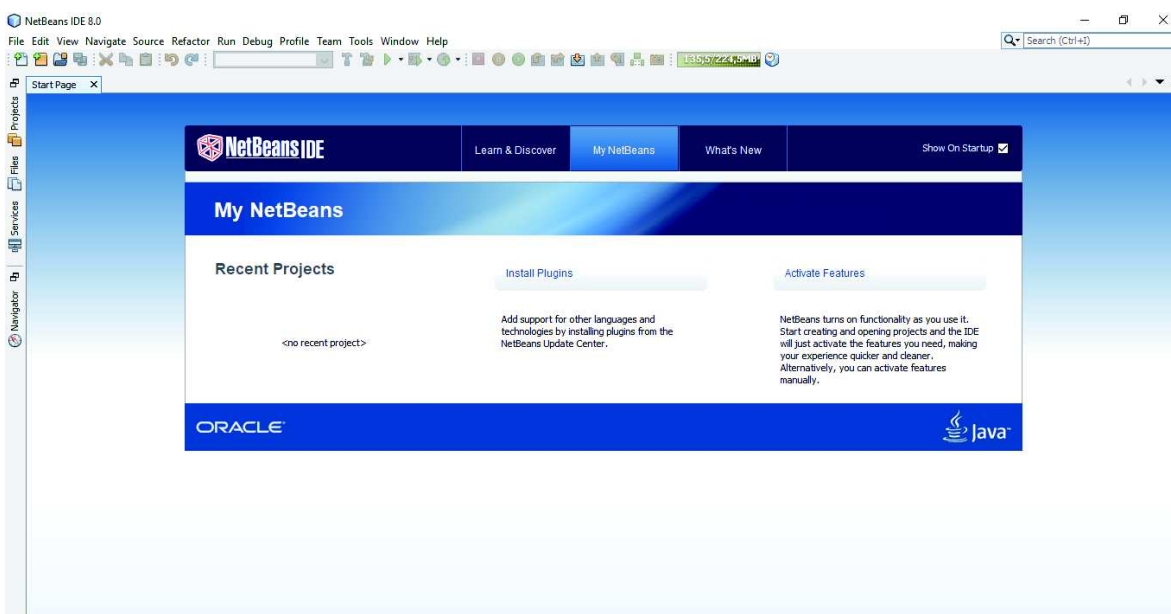


Gráfico 55: Netbeans 8.0

Se crea el proyecto Riskman, y a continuación se añaden las librerías para conexión con MySQL.

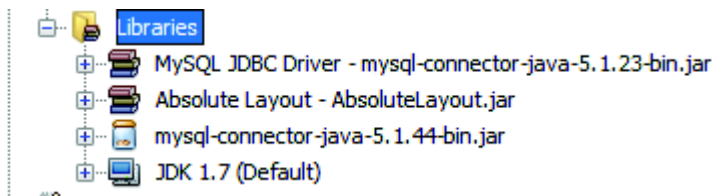


Gráfico 57: Librerías en Netbeans 8.0

Métodos de conexión de Netbeans con Workbench

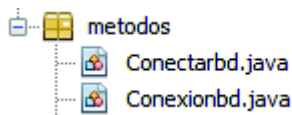


Gráfico 58: Métodos de Conexión de Netbeans con MySQL

3.4.4.2.4 Inicio Sesión –Home (Sprint 4)

En este cuarto Sprint se realiza creación de interfaz de login, funcionalidad del acceso, y las pestañas de información y contacto.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Bum Down	Recursos & Presupuesto	Informe de reporte de historia	Reporte resumido	Workload Report			
						Estimacion\Fecha:	Dec 11	Dec 12	Dec 13	Dec 14	Dec 15
						Hecho %:	14% (1)	29% (2)	57% (4)	71% (5)	✓ 100% (7)
						Codificado %:	14% (1)	29% (2)	57% (4)	71% (5)	✓ 100% (7)
						Probado %:	n/a	n/a	n/a	n/a	n/a
						Hecho hoy/Para hacer:	1/0	1/1	2/0	1/1	2/0
						Codificado hoy/para hacer:	1/0	1/1	2/0	1/1	2/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea		Asignado 1	Asignado 2	Probado hoy/Para hacer:		0/0	0/0	0/0	0/0	0/0
✓ 4.1	Creacion de Interfaz				Hecho %:		✓ 100...	✓ 100...	✓ 100% (1)	✓ 100% (1)	✓ 100% (1)
✓ 1	Crear Interfaz			1			✓ 1/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0
✓ 4.2	Creacion de Login				Hecho %:			33% (1)	✓ 100% (3)	✓ 100% (3)	✓ 100% (3)
✓ 1	Crear Acceso al sistema			3				1/1	✓ 2/0	✓ 0/0	✓ 0/0
✓ 4.3	Creacion de Informacion- Contacto				Hecho %:					33% (1)	✓ 100% (3)
✓ 1	Creación de Pestañas			3						1/1	✓ 2/0

Gráfico 59: Historia Sprint 4

Fuente: Sprintometer

Elaboración: Autores

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #60 se muestra las fechas del Sprint de inicio (11/12/2017) y fin (15/12/2017) del Sprint con respecto al trabajo faltante/completado.

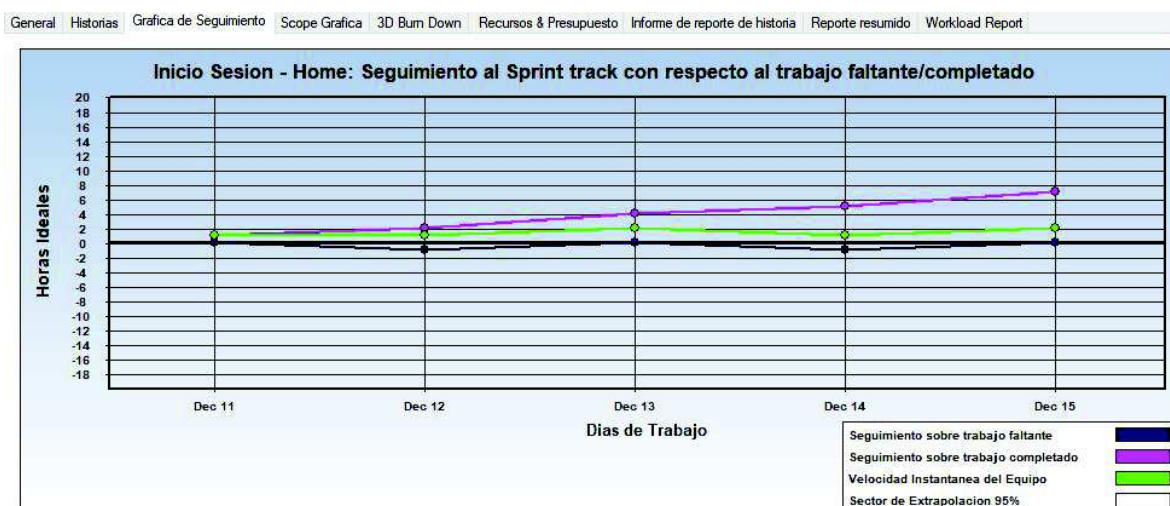


*Gráfico 60: Seguimiento Sprint 4
Fuente: Sprintometer
Elaboración: Autores*

Creación de Interfaz: Como se puede visualizar es la primera pantalla del sistema, el cual no permite la creación de ningún usuario, ya que debe de existir uno por defecto.

Gráfico 61: Interfaz Login

Información y contacto

*Gráfico 62: Interfaz Información y Contacto
Fuente: IDE Netbeans*

3.4.4.2.5 Módulo de Ingreso (Sprint 5)

En este quinto Sprint se realiza creación la interfaz de ingreso de activos y amenazas, que permite además de ingreso, modificación y eliminación.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Burn Down	Recursos & Presupuesto	Informe de reporte de historia	Reporte resumido	Workload Report					
						Estimacion\Fecha:	Jan 06	Jan 07	Jan 08	Jan 09	Jan 10	Jan 11	Jan 12
						Hecho %:	42% (8)	42% (8)	53% (10)	53% (10)	58% (11)	74% (14)	✓ 100% (19)
						Codificado %:	42% (8)	42% (8)	53% (10)	53% (10)	58% (11)	74% (14)	✓ 100% (19)
						Probado %:	n/a	n/a	n/a	n/a	n/a	n/a	n/a
						Hecho hoy/Para hacer:	0/0	0/0	2/0	0/0	1/0	3/0	5/0
						Codificado hoy/para hacer:	0/0	0/0	2/0	0/0	1/0	3/0	5/0
						Probado hoy/Para hacer:	0/0	0/0	0/0	0/0	0/0	0/0	0/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea	Asignado 1	Asignado 2			Hecho %:	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100% (8)
✓ 5.1	Ingreso de Activos					Hecho %:	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0
✓ 1	Ingreso Activos					Hecho %:	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0
✓ 2	Modificar Activo					Hecho %:	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0
✓ 3	Eliminar Activos					Hecho %:	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0
✓ 5.2	Ingreso de Amenazas					Hecho %:			18% (2)	18% (2)	27% (3)	55% (6)	✓ 100% (11)
✓ 1	Ingreso Amenazas					Hecho %:			2/0	0/0	0/0	2/0	2/0
✓ 2	Modificar Amenazas					Hecho %:					1/0	1/0	1/0
✓ 3	Eliminar Amenazas					Hecho %:							2/0

Gráfico 63: Historia Sprint 5

Fuente: Sprintometer

Elaboración: Autores

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #64 se muestra las fechas del Sprint de inicio (18/12/2017) y fin (12/1/2018) del Sprint con respecto al trabajo faltante/completado.

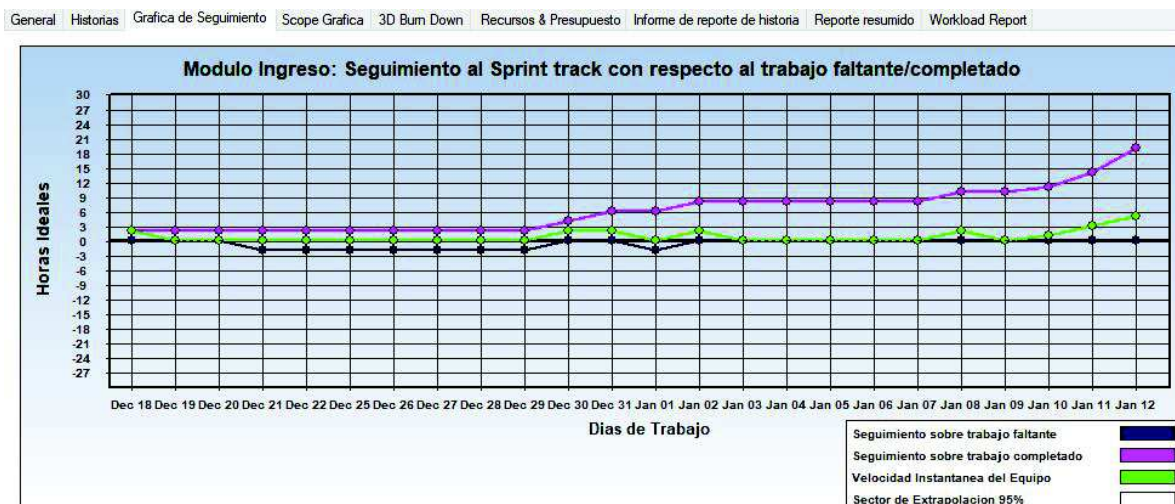


Gráfico 64: Seguimiento Sprint 5

Fuente: Sprintometer

Elaboración: Autores

Ingreso Activos Administrador

Tiene todas las funcionalidades de usuario Administrador.

Registro Activo

Area:

Identificador:

Cantidad:

Nombre Activo:

Tipo Activo: **DI** Aplicacion: **SI**

Buscar Activos

Buscar por: **Id**

Tabla de Activos

Area	Identificador	Cantidad	Activo	Tipo Activo	Aplicacion
LAB201	A1	90	TECLADOS DELL	HW	SI
LAB201	A2	29	TECLADOS DELL	HW	SI
LAB201	A3	12	sd	DI	SI
LAB202	B1	123	asd	HW	NO
LAB206	C3	20	MONITORES LG	HW	NO
LAB206	C4	20	RATON	HW	NO
LAB206	C3	18	MONITORES LG	HW	SI

Nuevo **Guardar** **Modificar** **Eliminar**

Gráfico 66: Ingreso Activos usuario Administrador

Fuente: IDE Netbeans

Ingreso Activos Usuario Auxiliar

A este usuario no se le permite eliminar activos.

Registro Activo

Area:

Identificador:

Cantidad:

Nombre Activo:

Tipo Activo: **DI** Aplicacion: **SI**

Buscar Activos

Buscar por: **Id**

Tabla de Activos

Area	Identificador	Cantidad	Activo	Tipo Activo	Aplicacion
LAB201	A1	90	TECLADOS DELL	HW	SI
LAB201	A2	29	TECLADOS DELL	HW	SI
LAB201	A3	12	sd	DI	SI
LAB202	B1	123	asd	HW	NO
LAB206	C3	20	MONITORES LG	HW	NO
LAB206	C4	20	RATON	HW	NO
LAB206	C3	18	MONITORES LG	HW	SI

Nuevo **Guardar** **Modificar**

Gráfico 67: Ingreso Activos usuario Auxiliar

Fuente: IDE Netbeans

Ingreso amenazas Administrador

*Gráfico 68: Ingreso Amenazas Usuario Administrador
Fuente: IDE Netbeans*

Ingreso Amenaza usuario Auxiliar

A este usuario no se le permite eliminar las amenazas

*Gráfico 69: Ingreso Amenazas Usuario Auxiliar
Fuente: IDE Netbeans*

3.4.4.2.6 Módulo de Cruces (Sprint 6)

En este sexto Sprint se realiza creación de interfaz de cruces, funcionalidad del cruce Activo-Amenazas, y reporte.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Bum Down	Recursos & Presupuesto	Informe de reporte de historia	Reporte resumido	Workload Report					
						Estimacion\Fecha:	Jan 27	Jan 28	Jan 29	Jan 30	Jan 31	Feb 01	Feb 02
						Hecho %:	46% (12)	54% (14)	62% (16)	65% (17)	73% (19)	85% (22)	✓ 100% (26)
						Codificado %:	46% (12)	54% (14)	62% (16)	65% (17)	73% (19)	85% (22)	✓ 100% (26)
						Probado %:	n/a	n/a	n/a	n/a	n/a	n/a	n/a
						Hecho hoy/Para hacer:	2/0	2/0	2/0	1/3	2/2	3/1	4/0
						Codificado hoy/para hacer:	2/0	2/0	2/0	1/3	2/2	3/1	4/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea	Asignado 1	Asignado 2	Probado hoy/Para hacer:	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
✓ 6.1	Creacion de Interfaz			Hecho %:	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100% (1)
✓ 1	Creacion de Interfaz			1	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	0/0
✓ 6.2	Cruce Amenza-Activo			Hecho %:	73% (11)	87% (13)	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100% (15)
✓ 1	Recorrer ambas tablas			15	2/0	2/0	2/0	0/0	0/0	0/0	0/0	0/0	0/0
✓ 6.3	Reporte			Hecho %:				10% (1)	30% (3)	60% (6)	✓ 100% (10)		
✓ 1	Reporte de Cruce			10				1/3	2/2	3/1	4/0		

*Gráfico 70: Historia Sprint 6
Fuente: Sprintometer
Elaboración: Autores*

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #71 se muestra las fechas del Sprint de inicio (15/01/2018) y fin (02/02/2018) del Sprint con respecto al trabajo faltante/completado.



Gráfico 71: Seguimiento Sprint 6

Fuente: Sprintometer

Elaboración: Autores

Interfaz Cruce Activos-Amenazas de Usuario Administrador

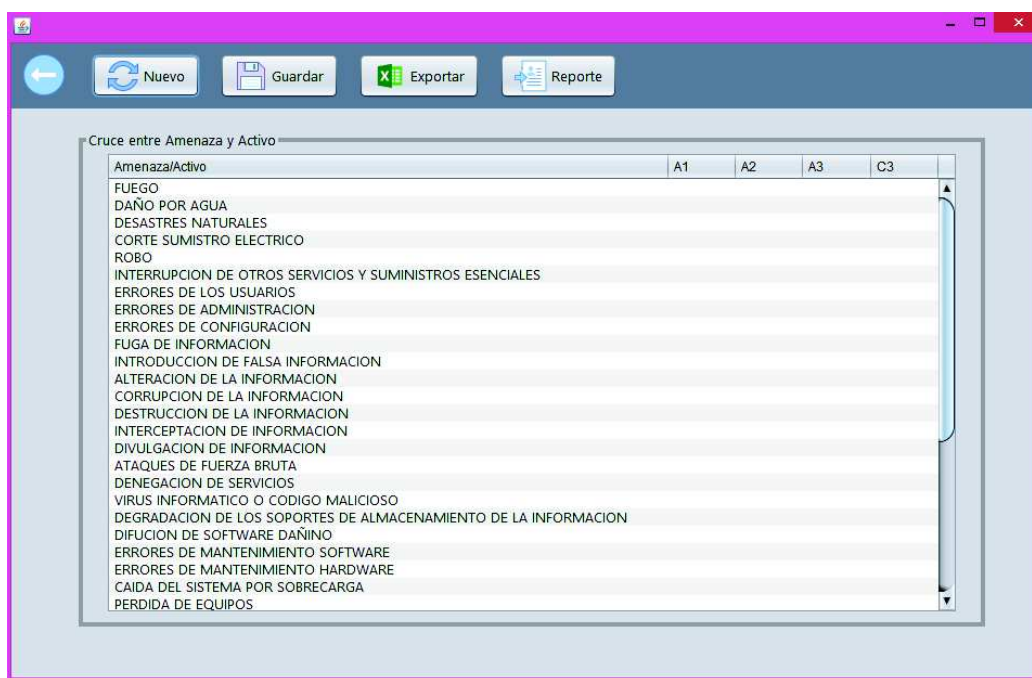


Gráfico 72: Cruce Activo-Amenaza Usuario Administrador

Fuente: IDE Netbeans

Interfaz Cruce Activos-Amenazas de Usuario Auxiliar

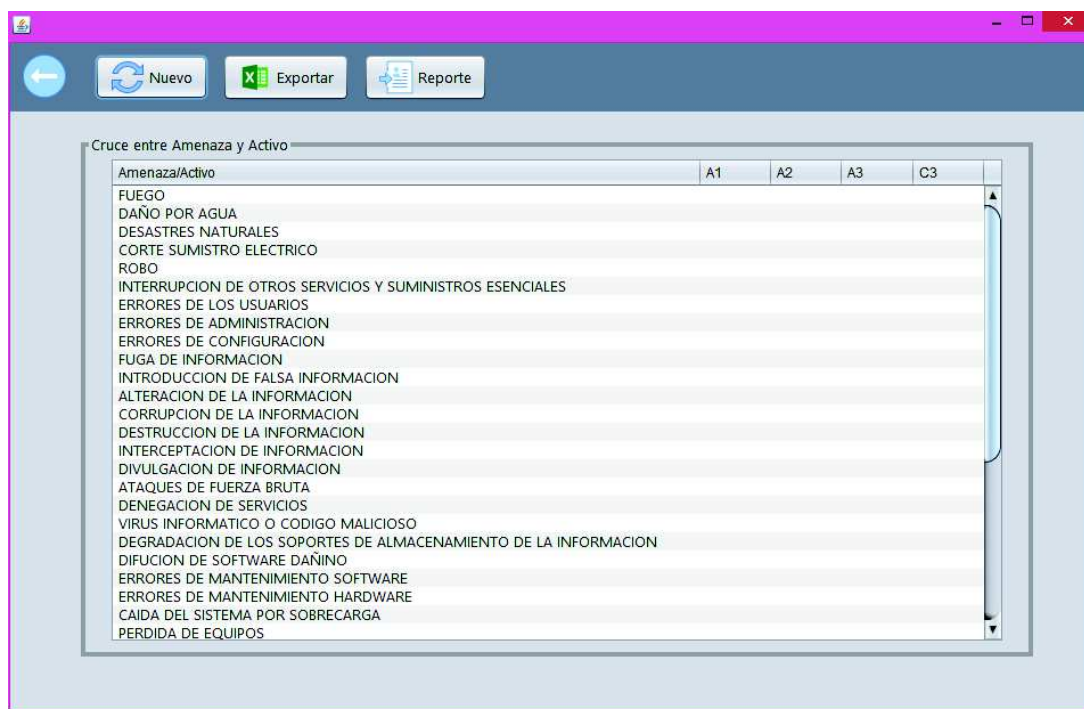


Gráfico 73: Cruce Activos-Amenazas de Usuario Auxiliar
Fuente: IDE Netbeans

3.4.4.2.7 Módulo de Análisis y Aplicación (Sprint 7)

En este séptimo Sprint se realiza los módulos de análisis y aplicación, con las tareas de creación de interfaz, la probabilidad y el impacto de activo con las amenazas, y las aplicaciones de las ISO/IEC 17799 y 27001.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea	Asignado 1	Asignado 2	Probado hoy/Para hacer:	0/0	0/0	0/0	0/0	0/0	0/0	0/0
✓ 7.1	Creacion de Interfaz			Hecho %:	✓ 10...	✓ 10...	✓ 100...	✓ 100...	✓ 100...	✓ 100...	✓ 100% (1)
✓ 1	Creacion de Interfaz			1	✓ 1/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0	✓ 0/0
✓ 7.2	Probabilidad Impacto			Hecho %:	- 5% (1)	15% (3)	30% (6)	50% (10)	75% (15)	✓ 100% (20)	
✓ 1	Recorrer ambas tablas			20	0/2	1/4	2/3	3/2	4/1	5/0	5/0
✓ 7.3	Aplicación ISO 17799			Hecho %:				42% (5)	75% (9)	✓ 100...	✓ 100% (12)
✓ 1	Valoración de Riesgo			12				5/4	4/3	✓ 3/2	✓ 0/0
✓ 7.4	Aplicación ISO 27001			Hecho %:					57% (4)	✓ 100...	✓ 100% (7)
✓ 1	Valoración de Riesgo			7					4/3	✓ 3/1	✓ 0/0

Gráfico 74: Historia Sprint 7
Fuente: Sprintometer
Elaboración: Autores

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #75 se muestra las fechas del Sprint de inicio (05/02/2018) y fin (14/02/2018) del Sprint con respecto al trabajo faltante/completado.

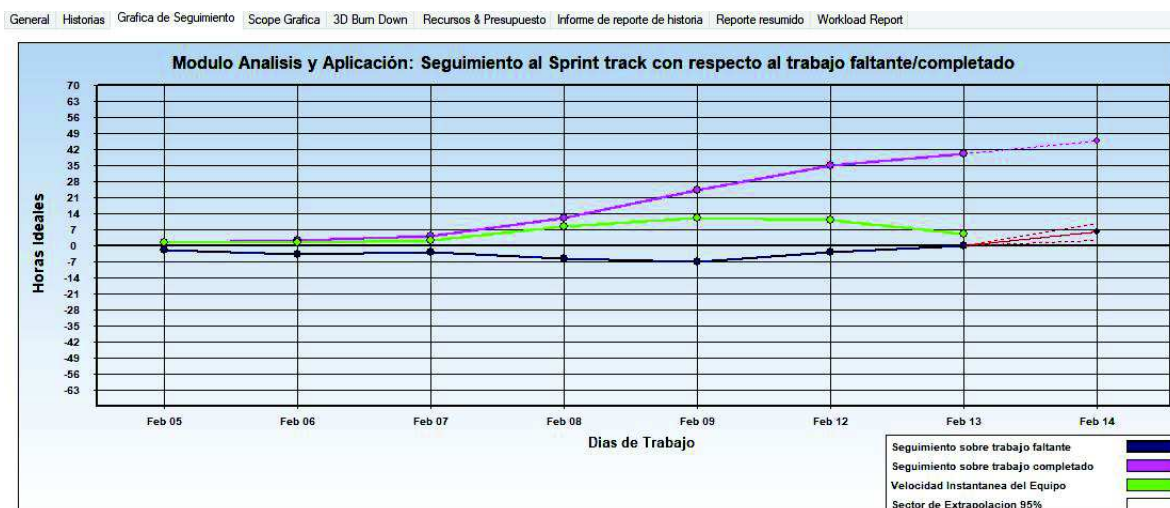


Gráfico 75: Seguimiento Sprint 7
Fuente: Sprintometer
Elaboración: Autores

Análisis de Usuario Administrador

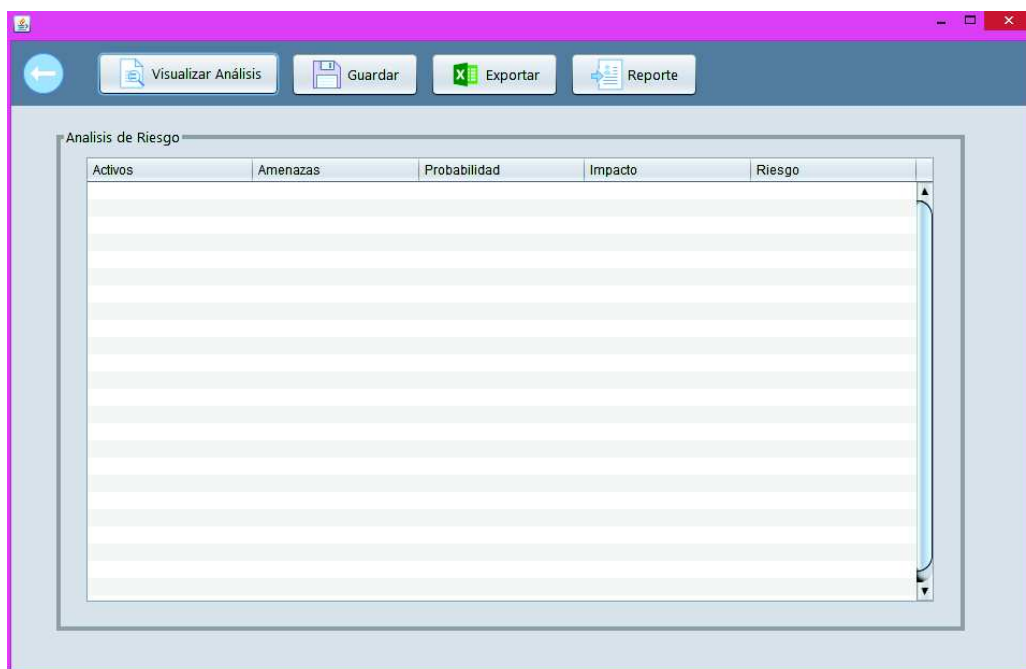


Gráfico 76: Interfaz de Análisis de Usuario Administrador
Fuente: IDE Netbeans
Elaboración: Autores

A este usuario no se le permite guardar

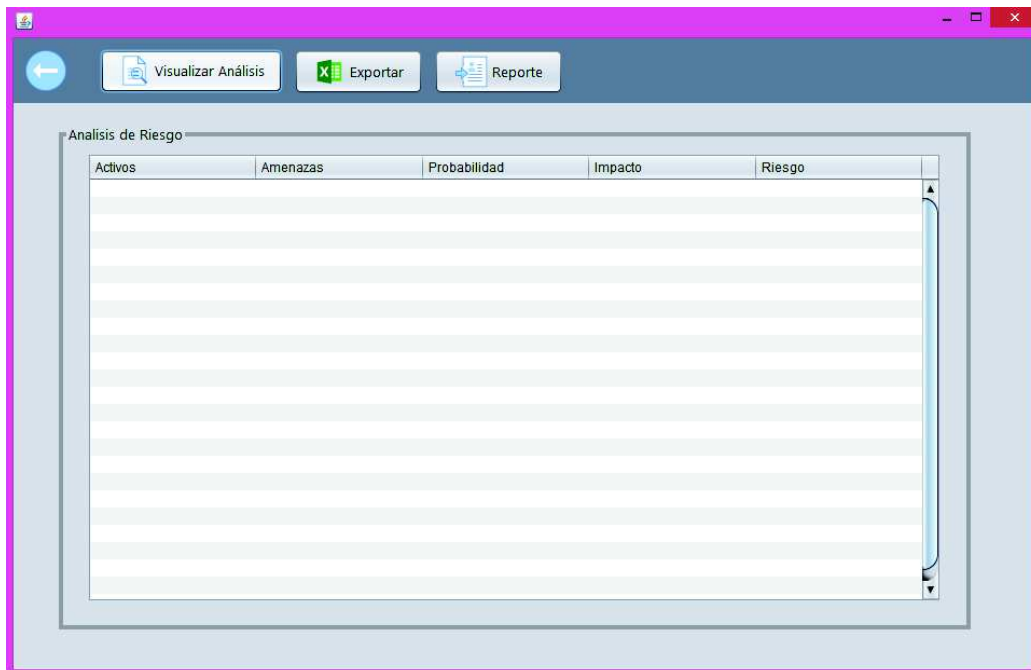


*Gráfico 77: Interfaz Análisis Usuario Auxiliar
Fuente: IDE Netbeans
Elaboración: Autores*

Aplicación de Usuario Administrador

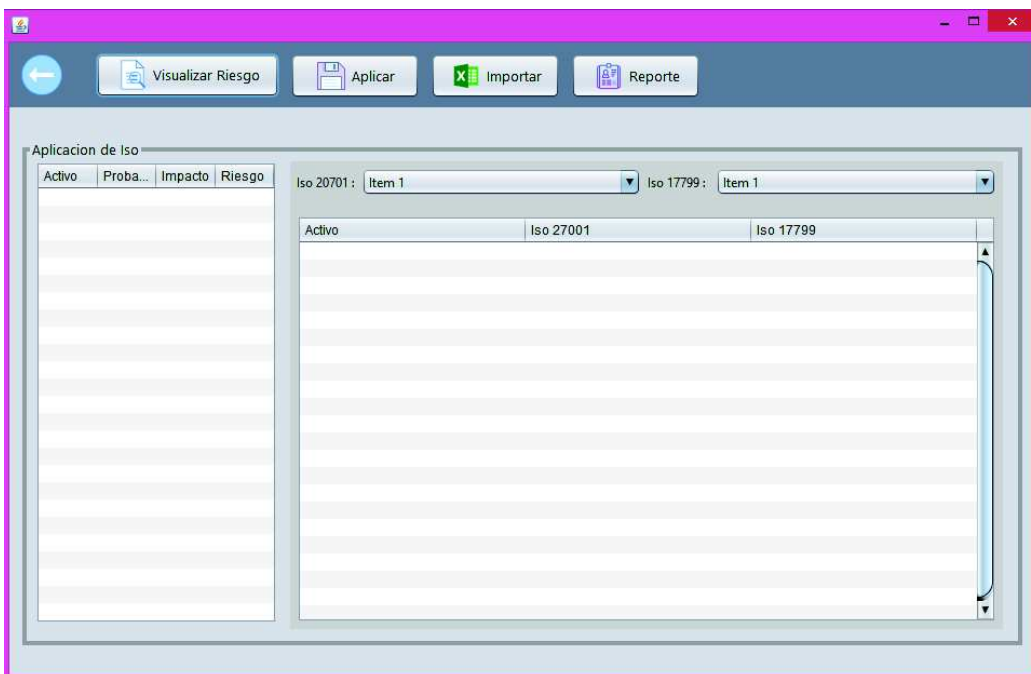


*Gráfico 78: Interfaz de Aplicación Usuario Administrador
Fuente: IDE Netbeans
Elaboración: Autores*

Aplicación de Usuario Auxiliar

A diferencia del usuario Administrador, el usuario auxiliar no puede aplicar los cambios.

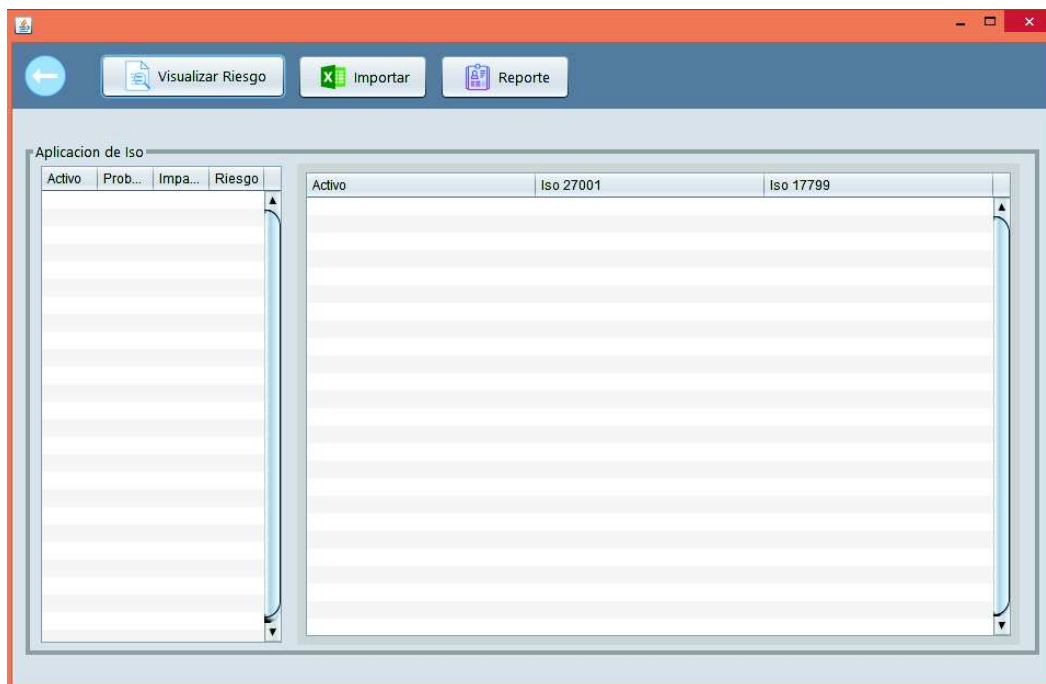


*Gráfico 79: Interfaz de Aplicación Usuario Auxiliar
Fuente: IDE Netbeans
Elaboración: Autores*

3.4.4.2.8 Testeo (Sprint 8)

En este octavo Sprint se realiza testeo para comprobar funcionamiento de software y posibles errores.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Burn Down	Recursos & Presupuesto	Informe de reporte de historia	Rep
					Estimacion\Fecha:	Feb 15	Feb 16
					Hecho %:	33% (1)	✓ 100% (3)
					Codificado %:	33% (1)	✓ 100% (3)
					Probado %:	n/a	n/a
					Hecho hoy/Para hacer:	1/1	2/0
					Codificado hoy/para hacer:	1/1	2/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea	Asignado 1	Asignado 2	Probado hoy/Para hacer:	0/0	0/0	
✓ 8.1	Realizar Prueba de errores			Hecho %:	33% (1)	✓ 100% (3)	
✓ 1	Comprobacion de errores			3	1/1	✓ 2/0	

*Gráfico 80: Historia Sprint 8
Fuente: Sprintometer
Elaboración: Autores*

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #81 se muestra las fechas del Sprint de inicio (15/02/2018) y fin (16/02/2018) del Sprint con respecto al trabajo faltante/completado.

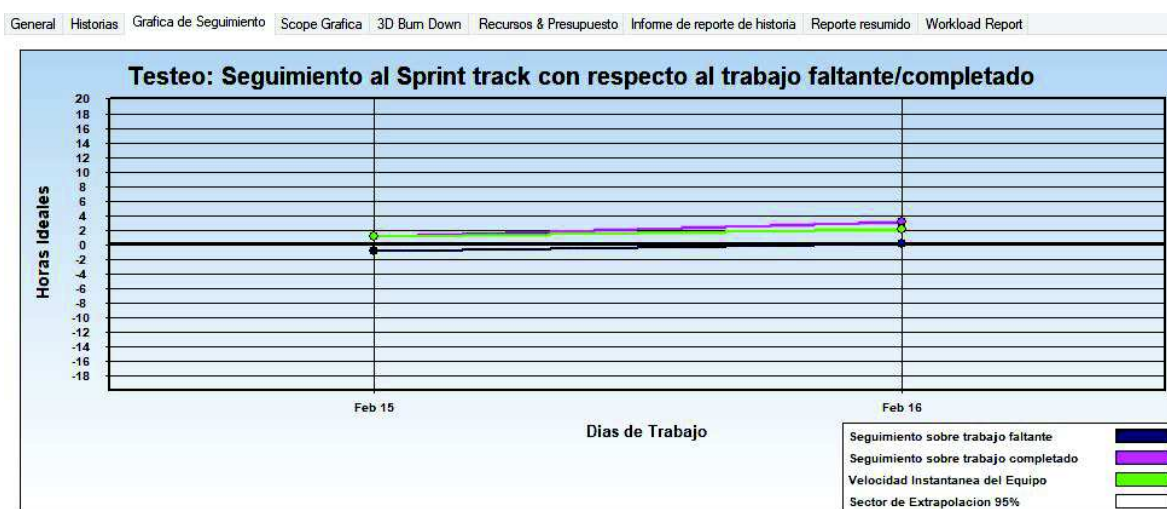


*Gráfico 81: Seguimiento Sprint 8
Fuente: Sprintometer
Elaboración: Autores*

3.4.4.2.9 Implementación (Sprint 9)

En este noveno Sprint se realiza implementación del software realizando análisis de riesgos de laboratorios de la FACCI.

Se presenta a continuación la gráfica de la historia de este Sprint realizado con el software Sprintometer.

General	Historias	Grafica de Seguimiento	Scope Grafica	3D Bum Down	Recursos & Presupuesto	Informe de reporte de histo
					Estimacion\Fecha:	Feb 19
					Hecho %:	✓ 100% (1)
					Codificado %:	n/a
					Probado %:	✓ 100% (1)
					Hecho hoy/Para hacer:	1/0
					Codificado hoy/para hacer:	0/0
					Probado hoy/Para hacer:	1/0
Nº Historia, Nº tarea	Nombre Historia, Nombre Tarea	Asignado 1	Asignado 2			
✓ 8.1	Caso de estudio				Hecho %:	✓ 100% (1)
✓ 1	Analisis de riesgo				1	✓ 1/0

Gráfico 82: Historia Sprint 9

Fuente: Sprintometer

Elaboración: Autores

En este grafico se muestran las historias y las tareas realizadas en cada historia, así como el cumplimiento de las mismas.

En el gráfico #83 se muestra las fecha (19/02/2018) del Sprint con respecto al trabajo faltante/completado.

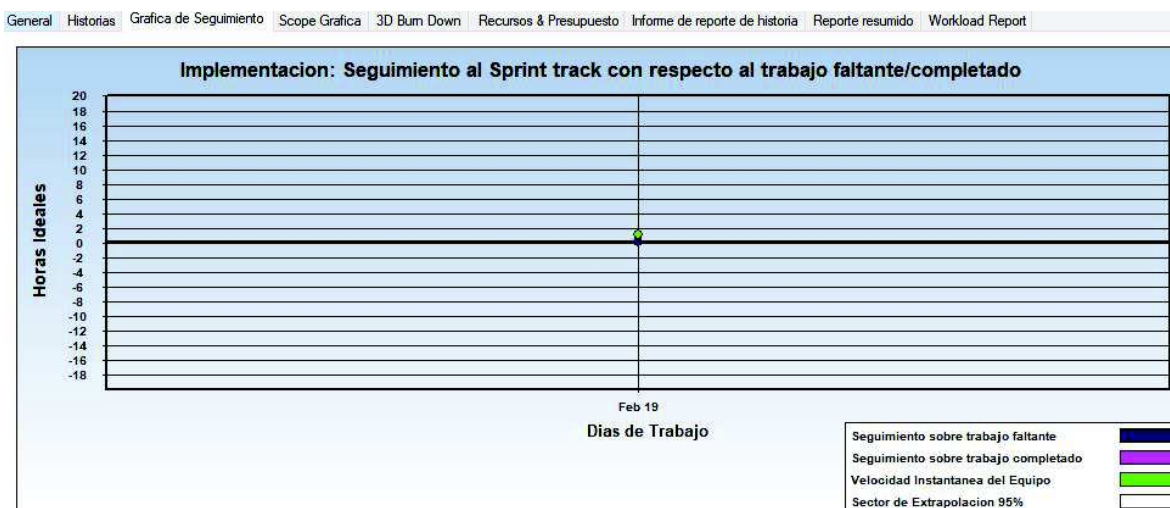


Gráfico 83: Seguimiento Sprint 9

Fuente: Sprintometer

Elaboración: Autores

CAPITULO IV

4 EVALUACIÓN DE RESULTADOS

4.1 Introducción

Mediante la implementación del software en la Facultad de Ciencias Informáticas se pueden visualizar las amenazas en que se ven afectados los activos, e introduciendo la probabilidad y el impacto de cada uno de ellos se puede observar la gravedad en que afectaría a estos.

Cumpliendo con los controles que se indican de las ISO/IEC 17799 E ISO/IEC 27001 se puede llegar a mitigar y controlar los riesgos que sufren los activos de la FACCI.

Al tratarse de un prototipo realizado a primera instancia para presentación de este proyecto, se va a seguir mejorando para mejor rentabilidad.

4.2 Seguimiento y Monitoreo de Resultados

El seguimiento y monitoreo se va a llevar a cabo por las auditorías internas que se implementaran en el proyecto de investigación SGSI, quienes verificaran los controles de las normas ISO/IEC a las cuales hace referencia este proyecto.

Conclusiones

Se estudiaron metodologías de análisis de riesgos informáticos, señalando como la más conveniente a MAGERIT.

Se solicitó y se obtuvieron los activos de la Facultad de Ciencias Informáticas para realizar análisis de riesgos.

Se llevó acabo el desarrollo de prototipo de software de análisis de riesgos basado en la metodología MAGERIT e implementación de controles de las ISO/IEC 27001 e ISO/IEC 17799.

Se realizaron encuestas a toda la comunidad de la Facultad de Ciencias Informáticas, así como entrevista al Jefe de Informática de los laboratorios para identificar falencias en la seguridad de activos.

Se cumplió con las actividades encomendadas en el proyecto de investigación “Sistema de Gestión de Seguridad de la Información bajo normas ISO/IEC 27001”

Recomendaciones

Se recomienda realizar análisis de riesgos de todos los laboratorios y departamentos de la Facultad de Ciencias Informáticas mediante el software desarrollado en este proyecto.

Designar y capacitar personal especializado encargado de los activos de la FACCI y manejo de software de análisis de riesgos.

Cumplir y hacer cumplir con los controles y recomendaciones que resultan del análisis de riesgo de la herramienta RISKMANAGEMENT 1.0.

Bibliografía

Álvarez Maraño, G. P. (2004). *Seguridad informática para empresas y particulares*.

Madrid: McGraw-Hill España.

Álvarez Maraño, G. P. (2004). *Seguridad informática para empresas y particulares*.

Madrid: McGraw-Hill España.

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. México: Grupo Editorial Patria.

Blanco Encinosa, L. J. (2005). *Auditoria y Sistemas Informáticos*. La Habana: Editorial Félix Varela.

Cárdenas, L. L. (2013). *Monografías*. Obtenido de

<http://www.monografias.com/trabajos99/herramienta-informatica-gestion-riesgos-tecnologias-informacion/herramienta-informatica-gestion-riesgos-tecnologias-informacion3.shtml>

Carlos Eduardo Valdivieso Taborga, R. V. (2011). *Universidad Privada Boliviana*. Obtenido de <ftp://ftp.repec.org/opt/ReDIF/RePEc/iad/wpaper/0311.pdf>

Carmona, E. J. (2013). OCTAVE, metodología para el análisis de riesgos de TI. pág.

https://www.uv.mx/universo/535/infgral/infgral_08.html.

Chicano Tejada, E. (2014). *Auditoría de seguridad informática (MF0487_3)*. Málaga: IC Editorial.

CLUSIF. (2010). *NEHARI*.

Costas Santos, J. (2014). *Seguridad Informática*. Madrid: RA-MA.

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT 3.0*. Madrid: Ministerio de Hacienda y Administraciones Públicas.

- Electrónica, C. d. (2012). *MAGERIT v3 Libro1 Método*.
- Escrivá Gascó, G. R. (2013). *Seguridad Informática*. Madrid: Macmillan Iberia, S.A.
- Esquema Nacional de Seguridad. (2012). *MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. España: Ministerio de Hacienda y Administraciones Públicas.
- Gómez, C. (2010). La gestión de riesgos en TI en el marco corporativo Marco para la Auditoría de los Sistemas de Información.
- ISO/IEC. (2005). ESTÁNDAR INTERNACIONAL ISO/IEC 17799.
- ISO/IEC. (2005). ESTÁNDAR INTERNACIONAL ISO/IEC 27001.
- JGAIPro. (2012). Obtenido de <http://jaigomezit.blogspot.com/2012/01/utilizando-herramienta-de-evaluacion-de.html>
- MANABÍ, U. L. (2018). Obtenido de <http://carreras.uleam.edu.ec/facci/datos-generales/personal-docente-2/>
- Martínez, J. G. (2017). *Planes de contingencia: la continuidad del negocio en las organizaciones*. Madrid: Ediciones Díaz de Santos.
- Michelle, A. Z. (2016). Propuesta de un Sistema de Gestión de Riesgos Mediante la metodología Magerit aplicado a los activos informáticos.
- Miranda, M. F. (2015). *PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA*. Madrid.
- Miranda, M. F. (2015). *Universidad Politécnica de Madrid*. Obtenido de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf
- Mogollón, A. (2013). *Análisis Comparativo: Metodologías de análisis de Riesgos*.
- R. Caralli, J. S. (2007). *Introducing OCTAVE Allegro*.
- Roa Buendía, J. F. (2013). *Seguridad informática*. Madrid: McGraw-Hill España.

Servicio Nacional de Aprendizaje -SENA. (2012). Obtenido de

https://docs.google.com/document/d/15TYUCIkxF_WYA1kTqCJa6bwQaCLlaEkwAQ-8EvFO7js/edit?pli=1

T., C. H. (2015). La gestión de riesgos en TI en el marco corporativo Marco para la Auditoría de los Sistemas de Información.

Vásquez, K. d. (2013). Aplicación de la metodología MAGERIT para el Análisis y Gestion de Riesgos de la Seguridad de la Información. MACHALA.

Vieites, A. G. (2014). Seguridad en Equipos Informáticos. Madrid: RA-MA.

Watkins, A. C. (2012). Information Security Risk Management forISO27001/ISO27002.

ANEXOS

ANEXO A

Anexo A: Encuesta en google forms

ENCUESTA PARA LA DETERMINACIÓN DE LA PROBLEMÁTICA DE SEGURIDAD INFORMÁTICA EN LA FACULTAD DE CIENCIAS INFORMÁTICAS DE LA ULEAM PROYECTANDO LA APLICACIÓN DE UN “SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS”

Estimado participante, se solicita su respuesta con responsabilidad para la obtención de resultados confiables; si vase seleccionar la opción que considere más pertinente y se aproxime a la realidad de la situación actual de la Facultad de Ciencias Informáticas. Gracias por su atención. La encuesta es anónima.

**Obligatorio*

Dirección de correo electrónico *

Tu dirección de correo electrónico

Ilustración 5: Título de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

FACCI
FACULTAD DE CIENCIAS INFORMÁTICAS

DIMENSIÓN 1: SITUACIÓN ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LABORATORIO DE LA FACCI.- ANTECEDENTES.

1.- Las instalaciones de la FACCI cuentan con Seguridad Informática. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

2.- La red eléctrica y la de telecomunicaciones están debidamente normalizadas, con protección contra fallos adecuados y etiquetados en todos los departamentos, laboratorios y dependencias de la FACCI. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

Ilustración 6: Preguntas 1 y 2 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

3.- La limpieza y el orden es frecuente y adecuada en las dependencias de la FACCI. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

4.- Los laboratorios y departamentos de la FACCI, cuentan con salidas de emergencias técnicamente ubicadas. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

5.- Los equipos e información de la FACCI cuentan con equipos de protección contra variación de voltaje tales como: Regulador de voltajes, supresores pico, UPS y/o generadores de energía. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

Ilustración 7: Preguntas 3, 4 y 5 de encuesta

Fuente: <https://docs.google.com/forms>

Elaboración: Autores

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

6.- Los sistemas operativos y el software de aplicación instalados en los laboratorios de la FACCI, cuentan con Licencias debidamente legalizadas. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

7.- Las Instalaciones eléctricas de la FACCI disponen de sistemas de puesta a tierra física. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

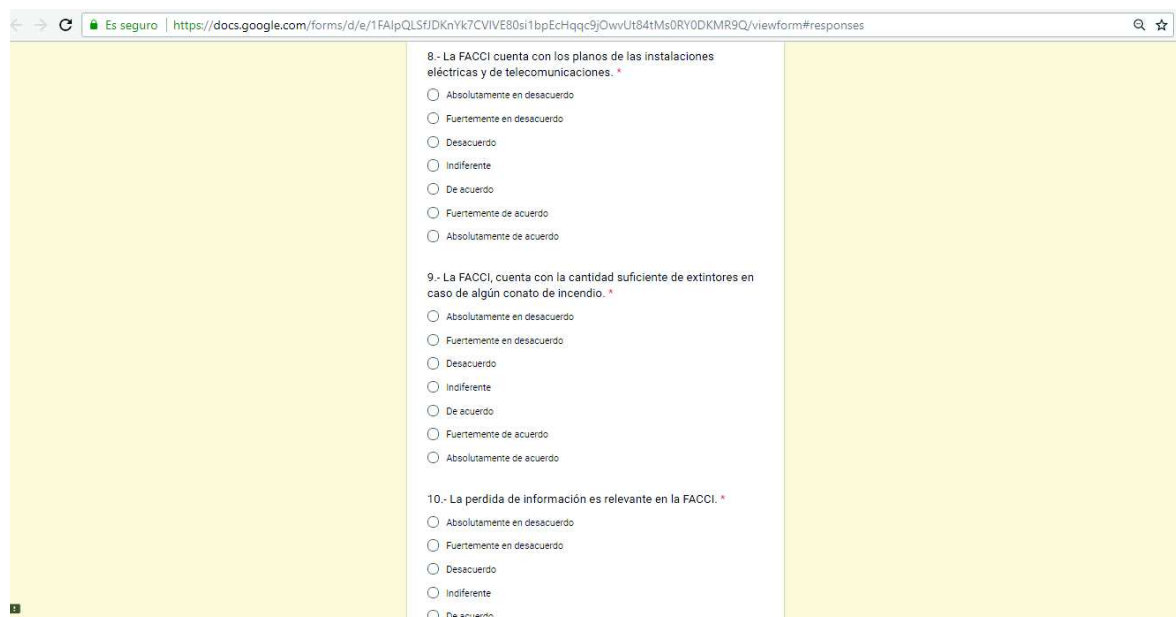
☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

Ilustración 8: Preguntas 6 y 7 de encuesta

Fuente: <https://docs.google.com/forms>

Elaboración: Autores



Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfjDKnYk7CVIVE80si1bpEchHqc9jOwvUt84tMs0RY0DKMR9Q/viewform#responses>

8.- La FACCI cuenta con los planos de las instalaciones eléctricas y de telecomunicaciones. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

9.- La FACCI, cuenta con la cantidad suficiente de extintores en caso de algún conato de incendio. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

10.- La pérdida de información es relevante en la FACCI. *

☐ Absolutamente en desacuerdo

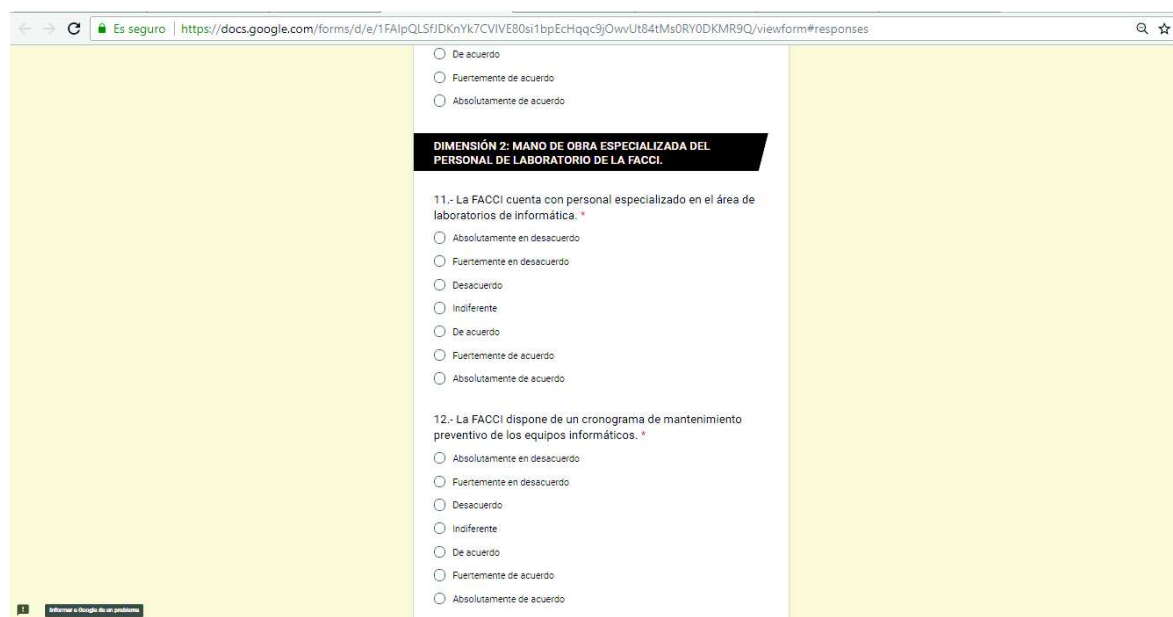
☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

Ilustración 9: Preguntas 8, 9 y 10 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores



Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfjDKnYk7CVIVE80si1bpEchHqc9jOwvUt84tMs0RY0DKMR9Q/viewform#responses>

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

DIMENSIÓN 2: MANO DE OBRA ESPECIALIZADA DEL PERSONAL DE LABORATORIO DE LA FACCI.

11.- La FACCI cuenta con personal especializado en el área de laboratorios de informática. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

12.- La FACCI dispone de un cronograma de mantenimiento preventivo de los equipos informáticos. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

Ilustración 10: Preguntas 11 y 13 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

13.- Los mantenimientos preventivos de los equipos informáticos se los realiza periódicamente en forma trimestral. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

14.- Los mantenimientos correctivos se los realiza de forma oportuna e inmediata una vez detectado algún fallo o avería. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

15.- En la FACCI existe disponibilidad inmediata de recursos, repuestos y accesorios para realizar los mantenimientos correctivos y preventivos. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

Ilustración 11: Preguntas 13, 14 y 15 de encuesta

Fuente: <https://docs.google.com/forms>

Elaboración: Autores

16.- La FACCI cuenta con algún Sistema de Gestión de Seguridad de la Información. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

DIMENSIÓN 3: ELEMENTOS DE SEGURIDAD INFORMÁTICA

17.- La FACCI, tiene asignado a un persona responsable del control de los activos. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

Ilustración 12: Preguntas 16 y 17 de encuesta

Fuente: <https://docs.google.com/forms>

Elaboración: Autores

18.- La FACCI tiene implementadas medidas de seguridad física e informática a los activos. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

19.- La FACCI cuenta físicamente con registros de acceso a las dependencias administrativas y a los laboratorios *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

20.- Las instalaciones físicas (Edificios y laboratorios) de la FACCI garantizan máxima seguridad. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

Ilustración 13: Preguntas 18,19 y 20 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

21.- La FACCI, cuenta con políticas de seguridad física e informáticas. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

22.- La FACCI, cuenta con políticas de mitigación de riesgos informáticos. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

23.- Se controla de forma adecuada el uso de dispositivos de almacenamiento masivo de información. *

☐ Absolutamente en desacuerdo

Ilustración 14: Preguntas 21,22 y 23 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfjDKnYk7CVIVE80si1bpEChqqc9jOwvUt84tMs0RY0DKMR9Q/viewform#responses>

☐ Faltan medidas de prevención

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

24.- La comunidad académica de la FACCI (personal docente, administrativos y estudiantes) está capacitado en Seguridad Industrial y Salud Ocupacional. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

25.- La FACCI dispone en sus instalaciones de Sistemas de alarmas contra incendio. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

Informe a través de un problema

Ilustración 15: Preguntas 24 y 25 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfjDKnYk7CVIVE80si1bpEChqqc9jOwvUt84tMs0RY0DKMR9Q/viewform#responses>

☐ Faltan medidas de prevención

26.- La FACCI dispone en sus instalaciones de Sistemas de Alarmas contra desastres (Terremoto e inundaciones). *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

27.- Actualmente los desastres naturales es una amenaza que afecta a las instalaciones y equipamientos de la FACCI. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

☐ Indiferente

☐ De acuerdo

☐ Fuertemente de acuerdo

☐ Absolutamente de acuerdo

28.- Los errores y fallas no intencionadas, corte de suministro eléctrico, y servicios de comunicación es una alta amenaza frecuente en la FACCI. *

☐ Absolutamente en desacuerdo

☐ Fuertemente en desacuerdo

☐ Desacuerdo

Informe a través de un problema

Ilustración 16: Preguntas 26, 27 y 28
Fuente: <https://docs.google.com/forms>
Elaboración: Autores

Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfJDkNkYk7CVIVE80si1bpEhHqc9jOwvUt84tMs0RY0DKMR9Q/viewform#responses>

Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

29.- Los componentes del sistema informático se manipulan ocasionalmente por estudiantes o personal no autorizado. *

Absolutamente en desacuerdo
Fuertemente en desacuerdo
Desacuerdo
Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

30.- Los estudiantes, docentes y usuarios en general disponen de los equipos y/o dependencias de la FACCI en forma permanente regularmente. *

Absolutamente en desacuerdo
Fuertemente en desacuerdo
Desacuerdo
Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

*Ilustración 17: Preguntas 29 y 30 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores*

Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfJDkNkYk7CVIVE80si1bpEhHqc9jOwvUt84tMs0RY0DKMR9Q/viewform#responses>

Absolutamente en desacuerdo
Fuertemente en desacuerdo
Desacuerdo
Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

31.- El control a estudiantes, docentes y usuarios en general es permanente y riguroso cuando se encuentran utilizando las instalaciones o equipos de la FACCI. *

Absolutamente en desacuerdo
Fuertemente en desacuerdo
Desacuerdo
Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

32.- La FACCI cuenta con usuarios autorizados con toma de decisiones en el ámbito de la seguridad informática. *

Absolutamente en desacuerdo
Fuertemente en desacuerdo
Desacuerdo
Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

33.- La FACCI realiza Auditorías para determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema o equipos en el ámbito de la seguridad informática. *

Absolutamente en desacuerdo
Fuertemente en desacuerdo
Desacuerdo
Indiferente
De acuerdo
Fuertemente de acuerdo
Absolutamente de acuerdo

*Ilustración 18: Preguntas 31, 32 y 33 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores*

← → Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfJDKnYk7CVIVE80si1bpEchHqc9jOvwUt84tMs0RY0DKMR9Q/viewform#responses> 🔍 ☆ ⋮

☐ Desacuerdo
☐ Indiferente
☐ De acuerdo
☐ Fuertemente de acuerdo
☐ Absolutamente de acuerdo

DIMENSIÓN 4: TIPOS Y APLICABILIDAD DE LA SEGURIDAD INFORMÁTICA EN INSTITUCIONES DE EDUCACIÓN SUPERIOR (CERTIFICACIÓN).

34.- En la FACCI es obligatorio el uso de las Normas Técnicas Ecuatorianas NTE INEM-ISO/IEC 27000 para la Gestión de Seguridad de la Información tal como lo establece la Secretaría Nacional de Administración Pública del Ecuador (SNAP). *

☐ Absolutamente en desacuerdo
☐ Fuertemente en desacuerdo
☐ Desacuerdo
☐ Indiferente
☐ De acuerdo
☐ Fuertemente de acuerdo
☐ Absolutamente de acuerdo

35.- En la FACCI se realiza evaluación de riesgos en base a la norma INEN ISO/IEC 27005 como establece la Secretaría Nacional de Administración Pública (SNAP). *

☐ Absolutamente en desacuerdo
☐ Fuertemente en desacuerdo
☐ Desacuerdo
☐ Indiferente
☐ De acuerdo
☐ Fuertemente de acuerdo
☐ Absolutamente de acuerdo

1 Informar a Google de un problema

*Ilustración 19: Preguntas 34 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores*

← → Es seguro | <https://docs.google.com/forms/d/e/1FAIpQLSfJDKnYk7CVIVE80si1bpEchHqc9jOvwUt84tMs0RY0DKMR9Q/viewform#responses> 🔍 ☆ ⋮

☐ Absolutamente de acuerdo

35.- En la FACCI se realiza evaluación de riesgos en base a la norma INEN ISO/IEC 27005 como establece la Secretaría Nacional de Administración Pública (SNAP). *

☐ Absolutamente en desacuerdo
☐ Fuertemente en desacuerdo
☐ Desacuerdo
☐ Indiferente
☐ De acuerdo
☐ Fuertemente de acuerdo
☐ Absolutamente de acuerdo

GRACIAS POR SU COLABORACIÓN

ENVIAR

Este contenido no ha sido creado ni aprobado por Google. Informar sobre abusos · Condiciones del servicio · Otras opciones

Google Formularios

2 Informar a Google de un problema

*Ilustración 20: Pregunta 35 de encuesta
Fuente: <https://docs.google.com/forms>
Elaboración: Autores*

ANEXO B

Anexo B: Entrevista con Jefe de Laboratorios

ENTREVISTA CON JEFE DE LABORATORIOS DE LA FACCI

[14/08/2017]

[10:30]

[FACCI]

REUNIÓN CONVOCADA POR	FÁTIMA GUADALUPE CARRILLO MORÁN
TIPO DE REUNIÓN	ENTREVISTA CON JEFE DE LABORATORIOS DE LA FACCI
ORGANIZADOR	FÁTIMA GUADALUPE CARRILLO MORÁN
APUNTADOR	FÁTIMA GUADALUPE CARRILLO MORÁN
ASISTENTES	FÁTIMA GUADALUPE CARRILLO MORÁN Y ING GILBERT LOOR MUÑOZ

Temas del orden del día

[TIEMPO ASIGNADO]

[TEMA DEL ORDEN DEL DÍA]

[MODERADOR]

OBJETIVO	Conocer las políticas y procedimientos relacionados con la evaluación de riesgos de los activos de los laboratorios de la FACCI.
FRAGMENTOS DE LA ENTREVISTA	
¿Conoce lo que es un plan de seguridad informática?	Si
¿Se cuenta actualmente con un plan de seguridad informática en la FACCI?	No
¿Se cuenta con inventario de activos de la FACCI?	Si
¿Existe algún plan de contingencia en la FACCI?	No
Existe algún documento de gestión de riesgos o algún proceso establecido para gestionarlos?	No
¿Si en este momento ocurriera alguna amenaza para los activos informáticos de la FACCI como reaccionaria?	Normal

Ilustración 21: Documento 1 de entrevista con Jefe de Informática de la FACCI

Elaboración: Autores

¿Existe en la actualidad algún seguro para proteger los sistemas ante posibles pérdidas causadas por robos o desastres naturales?

No

SÍNTESIS DE LA ENTREVISTA

En la actualidad en la Facci no existe pbn de seguridad, ni de contingencia, ni de gestión de riesgos o algún proceso establecido para gestionarlo, tampoco existe algún seguro que resguarde la pérdida de activos.

Se firma en Manta el día 14 del mes de Agosto del 2017

Fátima Carrillo M.

Entrevistador

Fátima Carrillo M.

C.I.: 130947803-8

Ing. Gilber Loor Muñoz

Jefe de Laboratorios de la FACCI

Ing. Gilber Loor Muñoz

C.I.: 130382500-2

Ilustración 22: Documento 2 de entrevista con Jefe de Informática de la FACCI

Elaboración: Autores

ANEXO C

Anexo C: Entrevista con Jefe de Laboratorios de la FACCI



Ilustración 23: Fotografía realizando entrevista a Jefe de Laboratorios

Elaboración: Autores

ANEXO D

Anexo D: Solicitud de Activos a la FACCI

	NOMBRE DEL DOCUMENTO: Solicitud de activos.	CÓDIGO: PAM-02-F-010	
	PROCEDIMIENTO: ANÁLISIS DE RIESGOS	REVISIÓN: 1 Página 1 de 1	

Manta, 14 de Agosto 2017

Licenciada
Dolores Muñoz Verduga
Decana Facultad de Ciencias Informáticas
Universidad Laica "Eloy Alfaro" de Manabí
Ciudad: -

De mi consideración:

Yo, CARRILLO MORÁN FÁTIMA GUADALUPE, con cédula de ciudadanía No 130947803-8, estudiante del noveno nivel de la Carrera de Ingeniería en Sistemas, con la finalidad de realizar análisis de riesgos informáticos de nuestra prestigiosa Facultad, solicito que por su digno intermedio se me haga la entrega de toda la información de los activos que existen en la actualidad, información que servirá de insumo para el proyecto de investigación de seguridad informática.

En espera de una pronta respuesta a mi requerimiento, quedo de usted,

Atentamente,

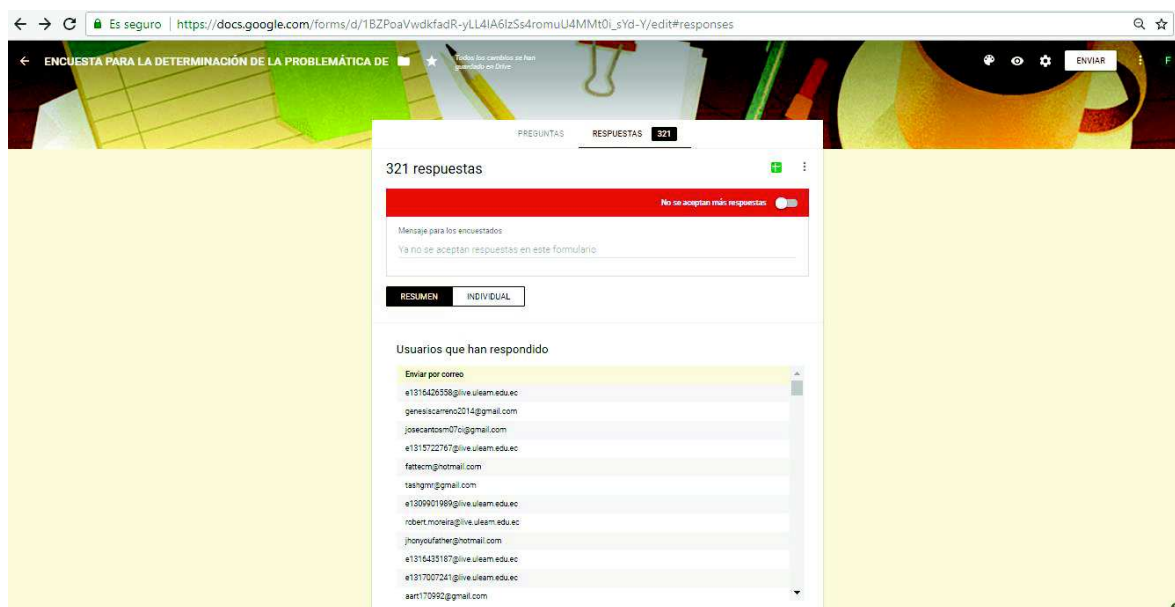
CARRILLO MORÁN FÁTIMA GUADALUPE
Cédula :130947803-8
Correo electrónico: fattecm@hotmail.com

14-08-2017
18:11
FACCI
FACULTAD DE CIENCIAS INFORMÁTICAS

*Ilustración 24: Oficio de solicitud de Activos
Elaboración: Autores*

ANEXO E

Anexo E: Resultados de Encuesta en Google Forms



The screenshot displays the Google Forms interface for a survey titled "ENCUESTA PARA LA DETERMINACIÓN DE LA PROBLEMÁTICA DE". The form is in the "RESPUESTAS" (Responses) tab, showing 321 responses. A red banner at the top of the response area states "No se aceptan más respuestas" (No more responses accepted). Below this, a message for respondents says "Ya no se aceptan respuestas en este formulario" (No more responses are accepted in this form). The "RESUMEN" (Summary) tab is selected, showing a list of users who have responded. The list includes email addresses such as e1315426558@live.uleam.edu.ec, genesacamero2014@gmail.com, josecantosm07ci@gmail.com, e1315722767@live.uleam.edu.ec, fatetcm@hotmail.com, tasghmr@gmail.com, e1309901989@live.uleam.edu.ec, robert.moreira@live.uleam.edu.ec, jhonyufather@hotmail.com, e1315435167@live.uleam.edu.ec, e1317007241@live.uleam.edu.ec, and aarti70992@gmail.com.

Ilustración 25: Resumen de participantes de la encuesta

Fuente: <https://docs.google.com/forms>

Elaboración: Autores

ANEXO F

Anexo F: Listado de Activos de la FACCI

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABI												
FACULTAD DE CIENCIAS INFORMÁTICAS												
Laboratorio de Prácticas Lcd. Blanca Gilbert												
13/09/2016												
Ubicación	Nombre-Pc	Responsable	Cantidad	Detalle	Fecha Adquisición	Marca	MODELO	SERIE	Observación	No. de Acto de Entrega	Tipo de elemento	Estado
ADMIN 205		ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO		HP	PAVILION SLIMLINE,5304	3C09240SD3	ASIG. 2015 EO ANTERIOR DE BAJA DELL E520		EQUIPO-PC	Operativa
ADMIN 205	PC07	FRANCISCO TOALA	1	MONITOR		HP	2009M20*	3C09270H0J	MONITOR EN PC07		PERIFERICO/MONITOR	Operativa
ADMIN 205		ING. DAHIANA ALVIA	1	MONITOR		HP	2009M20*	3C09270G29	FUNCION ADMINISTRATIVA		PERIFERICO/MONITOR	Operativa
ADMIN 205	ADM. SERVIDOR	ING. DONNY CORDERO	1	MONITOR		HP	2009M24*	3C095100TB	AREA DE ADMINISTRACION DE SERVIDORES		PERIFERICO/MONITOR	Operativa
LAB REDES		ING. JUAN CARLOS SENDON	1	MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5241557	ASIGNADO EL 3 DE AGOSTO 2016	04-2016	EQUIPO	Operativa
ADMIN 205	PC25	ING. GILBER LOOR		UPS		THOR	411631EC01	1307201033		25-2014		
ADMIN 205	PC25	ING. GILBER LOOR		CPU		LENOVO	THINKCENTRE M93P	MJ010DBT		25-2014		
LAB REDES		ING. JUAN CARLOS SENDON	1	MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5241726	ASIGNADO EL 3 DE AGOSTO 2016	04-2016	EQUIPO	Operativa
ADMIN 205	PC25	ING. GILBER LOOR		MOUSE		LENOVO	USB	HS417HA2FNC		25-2014		
ADMIN 205	PC25	ING. GILBER LOOR		TECLADO		LENOVO	USB	05875057		25-2014		
AUDITORIO	PC08	PERICLES	1	UNIDAD CENTRAL DE PROCESO		HP	PAVILION SLIMLINE,5304	3C09240SB5	UC EN PC08		EQUIPO-PC	Operativa
AUDITORIO		PERICLES	2	PORTA MICROFONOS								Operativa
AUDITORIO		PERICLES	1	UPS		ODP		110324-0220208				Operativa
AUDITORIO		PERICLES	1	CONSOLA		PHONIC		TE7112319	004-1425-00037			Operativa
AUDITORIO		PERICLES	1	WIRELESS RECEIVER OF MICROFONO		SHURE	J10-554-600MHZ	IME2196961-04				Operativa
AUDITORIO		PERICLES	1	TECLADO		GENIUS	USB	7B47C1U06044				Operativa
AUDITORIO		PERICLES	2	PARLANTES		CAMBRIDGE	SOUNDWORKS	MC155				Operativa
AUDITORIO		PERICLES	1	MOUSE		GENIUS	USB	X3684351706140				Operativa
AUDITORIO		PERICLES	1	CAMARA DE VIDEO CONFERENCIA		POLYCOM	0D06000	061021BE47CBA30				Operativa
AUDITORIO		PERICLES	1	CONSOLA DE CAMARA DE VIDEO CONFERENCIA		POLYCOM	0D06000	061021BE47CBA30				Operativa
AUDITORIO		PERICLES	4	PARLANTES DE ALTA PROYECCION DE SONIDO		HT HITANO	NO	NO	1 DE ELLOS ESTA DAÑADO			Operativa
AUDITORIO		PERICLES	1	MICROFONO DE MANO		SHURE	PG58	IME2196961-01				Operativa
AUDITORIO		PERICLES	1	MICROFONO DE OREJA		SHURE	PG30	DD4BLX1B				Operativa
AUDITORIO		PERICLES	1	PANTALLA DE PROYECTO			NO	NO				Operativa
AUDITORIO	PC01	FERMIN ALEXANDRA	1	MONITOR		HP	2009M20*	3C09270H0G	MONITOR AUDITORIO 13/09/2016		PERIFERICO/MONITOR	Operativa
LAB REDES		ING. JUAN CARLOS SENDON	1	MONITOR		DELL		CN-0F5035-64180-551-Y05	ASIG. 3 AGOSTO	04-2016	PERIFERICO/MONITOR	Operativa
DECANATO	6	LCD. DOLORES MUÑOZ	1	TECLADO		DELL		CN-0J4628-71616-59Y-0KF8			PERIFERICO/TECLADO	Operativa
DECANATO	6	LCD. DOLORES MUÑOZ	1	IMPRESORA		EPSON L555		S49V071251			PERIFERICO/IMPRESORA	Operativa
DECANATO	6	LCD. DOLORES MUÑOZ	1	UPS		THOR		1307201136			PERIFERICO/UPS	Operativa

*Ilustración 26: Hoja 1 Activos de la FACCI
Elaboración: Centro Computo de la FACCI*

Ubicación	Nombre-F	Responsable	Canti	Detalle	Fecha Adquis	Marca	MODELO	SERIE	Observación	No. de Acta de En	Tipo de elemento	Estado
DECANATO	6	LCD.A. DOLORES MUÑOZ	1	IMPRESORA		EPSON L555		S4V9071351			PERIFERICO/IMPRESORA	Operativa
DECANATO	6	LCD.A. DOLORES MUÑOZ	1	UPS		THOR		1367201136			PERIFERICO/UPS	Operativa
DECANATO	6	LCD.A. DOLORES MUÑOZ	1	PARLANTES		DELL		S/N			PERIFERICO/PARLANTES	Operativa
DECANATO	6	LCD.A. DOLORES MUÑOZ	1	WEBCAM		GENIUS		S/N			PERIFERICO/WEBCAM	Operativa
DECANATO	-		1	AIRE ACONDICIONADO		PANASONIC					EQUIPO/ACONDICIONAMIENTO	Operativa
DECANATO	DECANATO	LCD.A. DOLORES MUÑOZ	1	MOUSE		GENIUS	XISOROLL USB	X5K92033200JH7	NUEVO ASIG.		PERIFERICO	Operativa
DECANATO	PC22	ANTES JORGE MOYA VINCULADO	1	UNIDAD CENTRAL DE PROCESO		LENOVO	THINKCENTRE M93P	MJ010DDX	ANTES PROFESORES AHORA DECANATO	23-2014	EQUIPO	Operativa
TOACAN	PC22	FRANCISCO TOALA	1	MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5241144	LO TIENE DON FRANCISCO ASIGNADO EL VIERNES 9 DE SEPTIEMBRE DEL 2016		EQUIPO	Operativa
LAB-201	PC01	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600ST	UC CAMBIO DE PC02 a PC01		EQUIPO-PC	Operativa
LAB-201	PC02	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600CQ	UC CAMBIO DE PC19 a PC02		EQUIPO-PC	Operativa
LAB-201	PC04	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600BC	UC CAMBIO DE PC17 a PC04		EQUIPO-PC	Operativa
LAB-201	PC05	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600SH	UC CAMBIO DE PC15 a PC05		EQUIPO-PC	Operativa
LAB-201	PC06	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600C4	UC CAMBIO DE PC04 a PC06		EQUIPO-PC	Operativa
LAB-201	PC07	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML2151B6Y			EQUIPO-PC	Operativa
LAB-201	PC08	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600BJ	UC CAMBIO DE PC13 a PC08		EQUIPO-PC	Operativa
LAB-201	PC09	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML216009T	UC CAMBIO DE PC16 a PC09		EQUIPO-PC	Operativa
LAB-201	PC10	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML216009D	UC CAMBIO DE PC08 a PC10		EQUIPO-PC	Operativa
LAB-201	PC11	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600B2	UC CAMBIO DE PC14 a PC11		EQUIPO-PC	Operativa
LAB-201	PC12	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML2160007	PROBLEMAS DE FALLAS EN DISCO DURO		EQUIPO-PC	Operativa
LAB-201	PC13	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML216009L	NO RECONOCE MOUSE		EQUIPO-PC	Operativa
LAB-201	PC14	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML2160021	UC CAMBIO DE PC10 a PC14		EQUIPO-PC	Operativa
LAB-201	PC15	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600BG	UC CAMBIO DE PC03 a PC15		EQUIPO-PC	Operativa
LAB-201	PC16	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600SR	UC CAMBIO DE PC09 a PC16		EQUIPO-PC	Operativa
LAB-201	PC18	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600BH	UC CAMBIO DE PC05 a PC18		EQUIPO-PC	Operativa
LAB-201	PC19	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML21600D4	UC CAMBIO DE PC10 a PC19		EQUIPO-PC	Operativa
LAB-201	PC20	ING. DAHIANA ALVIA	1	UNIDAD CENTRAL DE PROCESO	41075	HP		MML2160095	UC CAMBIO DE PC11 a PC20		EQUIPO-PC	Operativa
LAB-201	PC01	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D69L			PERIFERICO/TECLADO	Operativa
LAB-201	PC02	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D69Q			PERIFERICO/TECLADO	Operativa
LAB-201	PC03	ING. DAHIANA ALVIA	1	TECLADO	41075	RLIP EXTREME	USB	KK561614001502751	SE REEMPLAZO TECLADO POR UN RLIP EXTREME CON SERIE KK561614001502751 POR MOTIVO DE FALLA		PERIFERICO/TECLADO	Operativa
ADMIN 205	STOCK	STOCK	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D69S	SE RETIRO DE LA PC03 DEL LAB 201 ESTA EN BUENAS CONDICIONES		PERIFERICO/TECLADO	Operativa
LAB-201	PC04	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D54J			PERIFERICO/TECLADO	Operativa
LAB-201	PC05	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D34N			PERIFERICO/TECLADO	Operativa
LAB-201	PC06	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D588			PERIFERICO/TECLADO	Operativa
LAB-201	PC07	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D96R			PERIFERICO/TECLADO	Operativa
LAB-201	PC08	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D572			PERIFERICO/TECLADO	Operativa
LAB-201	PC09	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D52B			PERIFERICO/TECLADO	Operativa
LAB-201	PC10	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D64V			PERIFERICO/TECLADO	Operativa
LAB-201	PC11	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012E	BAUDU00VB2D586			PERIFERICO/TECLADO	Operativa
LAB-201	PC12	ING. DAHIANA ALVIA	1	TECLADO	SN	GENIUS		2H9302226422			PERIFERICO/TECLADO	Operativa

*Ilustración 27: Hoja 2 Activos de la FACCI
Elaboración: Centro Computo de la FACCI*

“SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001. CASO DE APLICACIÓN EN LA FACULTAD DE CIENCIAS INFORMÁTICAS”

Ubicación	Nombre-F	Responsable	Canti	Detalle	Fecha Adquis	Marca	MODELO	SERIE	Observación	No. de Acta de En	Tipo de elemento	Estado
LAB-201	PC13	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	BAUDU000VB2D63H			PERIFERICO/TECLADO	Operativa
LAB-201	PC14	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	BAUDU000VB2D340			PERIFERICO/TECLADO	Operativa
LAB-201	PC15	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	BAUDU000VB2D8B0			PERIFERICO/TECLADO	Operativa
LAB-201	PC16	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	BAUDU000VB2D690			PERIFERICO/TECLADO	Operativa
LAB-201	PC17	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	BAUDU000VB2D59A			PERIFERICO/TECLADO	Operativa
LAB-201	PC18	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	PENDIENTE			PERIFERICO/TECLADO	Operativa
LAB-201	PC19	ING. DAHIANA ALVIA	1	TECLADO		FLIP EXTREME	USB	KKS56164081504679	SE UBICO EN ESTE PC POR QUE EL ANTERIOR SE ENCONTRABA EN MAL ESTADO ANTERIOR		PERIFERICO/TECLADO	Operativa
LAB-201	PC20	ING. DAHIANA ALVIA	1	TECLADO	41075	HP	MOD KB2012B	PENDIENTE			PERIFERICO/TECLADO	Operativa
LAB-201	PC01	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208PC0G		MONITOR CAMBIO DE PC13 A PC01		PERIFERICO/MONITOR	Operativa
LAB-201	PC02	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207004X		MONITOR CAMBIO DE PC11 A PC02		PERIFERICO/MONITOR	Operativa
LAB-201	PC03	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207005S		MONITOR CAMBIO DE PC17 A PC03		PERIFERICO/MONITOR	Operativa
LAB-201	PC04	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208P9WL		MONITOR CAMBIO DE PC09 A PC04		PERIFERICO/MONITOR	Operativa
LAB-201	PC05	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208P9T6				PERIFERICO/MONITOR	Operativa
LAB-201	PC06	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208PC2B		MONITOR CAMBIO DE PC08 A PC06		PERIFERICO/MONITOR	Operativa
LAB-201	PC07	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208P9V0		MONITOR CAMBIO DE PC07 A PC07		PERIFERICO/MONITOR	Operativa
LAB-201	PC08	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207004F		MONITOR CAMBIO DE PC01 A PC08		PERIFERICO/MONITOR	Operativa
LAB-201	PC09	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207P2MB		MONITOR CAMBIO DE PC16 A PC09		PERIFERICO/MONITOR	Operativa
LAB-201	PC10	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208PC2Q		MONITOR CAMBIO DE PC12 A PC10		PERIFERICO/MONITOR	Operativa
LAB-201	PC11	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207P2HC		MONITOR CAMBIO DE PC10 A PC11		PERIFERICO/MONITOR	Operativa
LAB-201	PC12	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC2070058		MONITOR CAMBIO DE PC14 A PC12		PERIFERICO/MONITOR	Operativa
LAB-201	PC13	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208PC29		MONITOR CAMBIO DE PC20 A PC13		PERIFERICO/MONITOR	Operativa
LAB-201	PC14	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207NWVK		MONITOR CAMBIO DE PC11 A PC14		PERIFERICO/MONITOR	Operativa
LAB-201	PC15	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207NW2Q		MONITOR CAMBIO DE PC12 A PC15		PERIFERICO/MONITOR	Operativa
LAB-201	PC16	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207NW30		MONITOR CAMBIO DE PC02 A PC16		PERIFERICO/MONITOR	Operativa
LAB-201	PC17	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC208P02P		MONITOR CAMBIO DE PC06 A PC17		PERIFERICO/MONITOR	Operativa
LAB-201	PC18	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC2070052		MONITOR CAMBIO DE PC19 A PC18		PERIFERICO/MONITOR	Operativa
LAB-201	PC19	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC207004K		MONITOR CAMBIO DE PC18 A PC19		PERIFERICO/MONITOR	Operativa
LAB-201	PC20	ING. DAHIANA ALVIA	1	MONITOR-17FG-E1914H	41075	HP	CNC2070041		MONITOR CAMBIO DE PC15 A PC20		PERIFERICO/MONITOR	Operativa
LAB-201	PC01	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200540			PERIFERICO/MOUSE	Operativa
LAB-201	PC02	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200504			PERIFERICO/MOUSE	Operativa
LAB-201	PC03	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200519			PERIFERICO/MOUSE	Operativa
LAB-201	PC04	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200513			PERIFERICO/MOUSE	Operativa
LAB-201	PC05	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200518			PERIFERICO/MOUSE	Operativa
LAB-201	PC06	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200518			PERIFERICO/MOUSE	Operativa
LAB-201	PC07	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200501			PERIFERICO/MOUSE	Operativa
LAB-201	PC08	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200535			PERIFERICO/MOUSE	Operativa
LAB-201	PC09	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK9203200503			PERIFERICO/MOUSE	Operativa
LAB-201	PC10	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK91658100913			PERIFERICO/MOUSE	Operativa
LAB-201	PC11	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	D8-120	3SK91658100993			PERIFERICO/MOUSE	Operativa

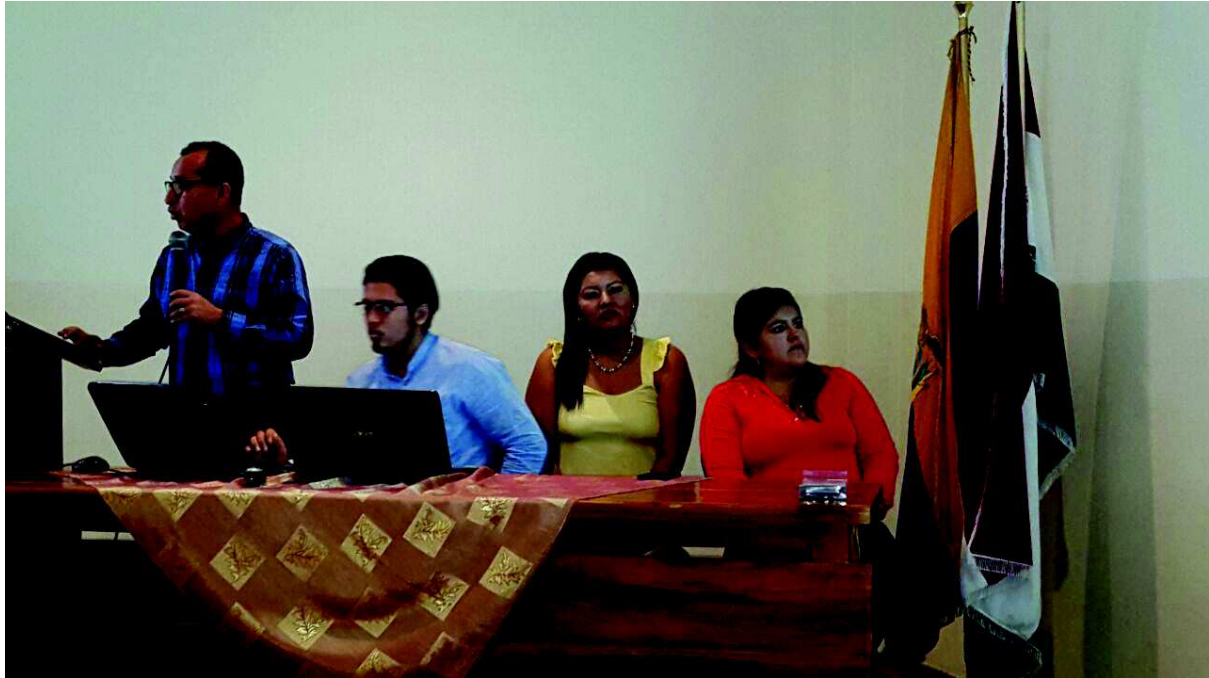
*Ilustración 28: Hoja 3 Activos de la FACCI
Elaboración: Centro Computo de la FACCI*

	Ubicación	Nombre-F	Responsable	Canti	Detalle	Fecha Adquisi	Marca	MODELO	SERIE	Observación	No. de Acta de En	Tipo de elemento	Estado
114	LAB-201	PC13	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK92032200511	NUEVO		PERIFERICO/MOUSE	Operativa
115	LAB-201	PC14	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK92032200514	NUEVO		PERIFERICO/MOUSE	Operativa
116	LAB-201	PC15	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK91658100057	NUEVO		PERIFERICO/MOUSE	Operativa
117	LAB-201	PC16	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK92032200508	NUEVO		PERIFERICO/MOUSE	Operativa
118	LAB-201	PC17	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK92032200523	NUEVO		PERIFERICO/MOUSE	Operativa
119	LAB-201	PC18	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK91658100097	NUEVO		PERIFERICO/MOUSE	Operativa
120	LAB-201	PC19	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK92032200523	NUEVO		PERIFERICO/MOUSE	Operativa
121	LAB-201	PC20	ING. DAHIANA ALVIA	1	MOUSE	42461	GENIUS	DS-120	ISK92032200521	NUEVO		PERIFERICO/MOUSE	Operativa
122	LAB-201	EQUIPO-LAB	ING. DAHIANA ALVIA	1	AIRE ACONDICIONADO	41075	LG					EQUIPO/ACONDICIONAM	Operativa
123	LAB-201	EQUIPO-LAB	ING. DAHIANA ALVIA	1	PROYECTOR	41075	EPSON					EQUIPO/PROYECTOR	Operativa
124	LAB-201	EQUIPO-LAB	ING. DAHIANA ALVIA	1	SWITCH	SN	D-LINK					EQUIPO/SWITCH	Operativa
125	LAB-201	EQUIPO-LAB	ING. DAHIANA ALVIA	41	SILLAS	SN	SILLAS		SILLAS			SILLAS	Operativa
126	LAB-201	EQUIPO-LAB	ING. DAHIANA ALVIA	1	PANTALLA/PROYECTOR	SN	GRANDVIEW					EQUIPO/PANTALLA	Operativa
127	LAB-202	PC00	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV55B21	UC CAMBIO DE PC11 a PC01		EQUIPO-PC	Operativa
128	LAB-202	PC01	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV1TB21	UC CAMBIO DE PC01 a PC02		EQUIPO-PC	Operativa
129	LAB-202	PC02	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW0VB21	UC CAMBIO DE PC02 a PC03		EQUIPO-PC	Operativa
130	LAB-202	PC03	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV1TB21	UC CAMBIO DE PC03 a PC04		EQUIPO-PC	Operativa
131	LAB-202	PC04	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW1VB21	UC CAMBIO DE PC04 a PC05		EQUIPO-PC	Operativa
132	LAB-202	PC05	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW0VB21	UC CAMBIO DE PC05 a PC06		EQUIPO-PC	Operativa
133	LAB-202	PC06	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW35B21	UC CAMBIO DE PC06 a PC07		EQUIPO-PC	Operativa
134	LAB-202	PC08	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW5TB21			EQUIPO-PC	Operativa
135	LAB-202	PC09	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV2TB21			EQUIPO-PC	Operativa
136	LAB-202	PC09	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW45B21	UC CAMBIO DE PC09 a PC10		EQUIPO-PC	Operativa
137	LAB-202	PC10	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW0RB21	UC CAMBIO DE PC10 a PC11		EQUIPO-PC	Operativa
138	LAB-202	PC12	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW5VB21			EQUIPO-PC	Operativa
139	LAB-202	PC13	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV5RB21			EQUIPO-PC	Operativa
140	LAB-202	PC14	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW15B21			EQUIPO-PC	Operativa
141	LAB-202	PC15	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV2RB21			EQUIPO-PC	Operativa
142	LAB-202	PC16	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW4VB21			EQUIPO-PC	Operativa
143	LAB-202	PC17	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BV1TB21			EQUIPO-PC	Operativa
144	LAB-202	PC18	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW7RB21			EQUIPO-PC	Operativa
145	LAB-202	PC19	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW6RB21			EQUIPO-PC	Operativa
146	LAB-202	PC20	ING. GILBER LOOR	1	UNIDAD CENTRAL DE PROCESO		DELL	OPTIPLX 9020	BW55B21			EQUIPO-PC	Operativa
147	LAB-202	PC00	ING. GILBER LOOR	1	TECLADO		DELL	MODKB2012B	CN-00639N-71616-319V-019R-A00			PERIFERICO/TECLADO	Operativa
148	LAB-202	PC01	ING. GILBER LOOR	1	TECLADO		DELL	MODKB2012B	CN-00639N-71616-319V-009T-A00			PERIFERICO/TECLADO	Operativa
149	LAB-202	PC02	ING. GILBER LOOR	1	TECLADO		DELL	MODKB2012B	CN-00639N-71616-319V-009P-A00			PERIFERICO/TECLADO	Operativa
150	LAB-202	PC03	ING. GILBER LOOR	1	TECLADO		DELL	MODKB2012B	CN-00639N-71616-319V-009U-A00			PERIFERICO/TECLADO	Operativa
151	LAB-202	PC04	ING. GILBER LOOR	1	TECLADO		KLIP-EXTREME	MOD KKS-050S	KK361614001502750			PERIFERICO/TECLADO	Operativa
152	LAB-202	PC05	ING. GILBER LOOR	1	TECLADO		DELL	MODKB2012B	CN-00639N-71616-319V-017Y-A00			PERIFERICO/TECLADO	Operativa
153	LAB-202	PC06	ING. GILBER LOOR	1	TECLADO		DELL	MODKB2012B	CN-00639N-71616-319V-00F3-A00			PERIFERICO/TECLADO	Operativa

*Ilustración 29: Hoja 4 Activos de la FACCI
Elaboración: Centro Computo de la FACCI*

Ubicación	Nombre-F	Responsable	Cantid	Detalle	Fecha Adquis	Marca	MODELO	SERIE	Observación	No. de Acta de En	Tipo de elemento
SECRETARIA	4	MARTHA	1	MODEM		GRANDSTREAM		21AWKD18301932AB			PERIFERICO/MODEM
SECRETARIA	-		1	AIRE ACONDICIONADO		CONFORTSTART					EQUIPO/ACONDICIONADO
SECRETARIA	VINCULACION	ING. MARIA ELENA GARCIA	1	MOUSE		GENIUS	ISOROLL USB	HS91105401D47	ANTES LAB 203 AHORA SIG. MARIA ELENA GARCIA		PERIFERICO/TECLADO
ADMIN205	ADMIN205	FRANCISCO TOALA	1	UNIDAD CENTRAL DE PROCESO		HP	PAVILION SLIMLINE/5304	20R9240SD0	ANTES LAB 203 AHORA SIG. MARIA ELENA GARCIA		EQUIPO-PC
SECRETARIA SERVIDOR	PC20	LEONOR FUENTES	1	UNIDAD CENTRAL DE PROCESO		LENOVO	THINKCENTRE M93P	HJ01C0DFH	UC EN PC02	04-2015	EQUIPO-PC
SECRETARIA SERVIDOR	PC20	LEONOR FUENTES		MOUSE		LENOVO	USB	HS421HA0V1L9		04-2015	
SECRETARIA SERVIDOR	PC20	LEONOR FUENTES		TECLADO		LENOVO	USB	05928735		04-2015	
LAB REDES		ING. JUAN CARLOS SENDON		MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5242107	ASIGNADO A LAB 203 15 MAYO 2016	04-2016	PERIFERICO/MONITOR
STOK	PC17	CELENIA-FERMIN		MOUSE		LENOVO	USB	HS421HA0PMB	30/11/2015 se proutaron a Vicarrectorado Academico a la rcepano	29-2014	
STOK	PC17	CELENIA-FERMIN		TECLADO		LENOVO	USB	5075107	30/11/2015 se proutaron a Vicarrectorado Academico a la rcepano	29-2014	
VINCULACION CON LA C	PC21	ING. JORGE MOYA		CPU		LENOVO	THINKCENTRE M93P	HJ01C0DE7		23-2014	
VINCULACION CON LA C	PC21	ING. JORGE MOYA		MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5242132		23-2014	
VINCULACION CON LA C	PC21	ING. JORGE MOYA		MOUSE		LENOVO	USB	HS421HA0VJ6		23-2014	
VINCULACION CON LA C	PC21	ING. JORGE MOYA		TECLADO		LENOVO	USB	05875034		23-2014	
VINCULACION CON LA C	PC22	STOCK		MOUSE		LENOVO	USB	HS421HA0YK4		23-2014	
VINCULACION CON LA C	PC22	ING. JORGE MOYA		TECLADO		LENOVO	USB	05875061	nazo encuentra pro quitar inquisiora jorge moya	23-2014	
VINCULACION CON LA C	PC23	ING. JORGE MOYA		CPU		LENOVO	THINKCENTRE M93P	HJ01C0DEJ		23-2014	
VINCULACION CON LA C	PC23	ING. JORGE MOYA		MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5240767		23-2014	
VINCULACION CON LA C	PC23	ING. JORGE MOYA		MOUSE		LENOVO	USB	HS421HA0YJZ	nazo encuentra pro quitar inquisiora jorge moya	23-2014	
VINCULACION CON LA C	PC23	ING. JORGE MOYA		TECLADO		LENOVO	USB	05875096		23-2014	
VINCULACION CON LA C	PC24	ING. JORGE MOYA		CPU		LENOVO	THINKCENTRE M93P	HJ01C0DD2		23-2014	
VINCULACION CON LA C	PC24	ING. JORGE MOYA		MONITOR	41760	LENOVO	THINKVISION 6AB-AHR1-V	SV5242109		23-2014	
VINCULACION CON LA C	PC24	ING. JORGE MOYA		MOUSE		LENOVO	USB	HS421HA0YKM		23-2014	
VINCULACION CON LA C	PC24	ING. JORGE MOYA		TECLADO		LENOVO	USB	05864205		23-2014	

*Ilustración 30: Hoja 5 Activos de la FACCI
Elaboración: Centro Computo de la FACCI*



ANEXO H

Anexo H: Certificado de Capacitación

CERTIFICADO DE CAPACITACIÓN

Manta, 19 de Febrero del 2018

Certifico que:

El día de hoy los estudiantes Acosta Alvarado Nexar Jesús con cédula de identidad No. 1312286972 y Carrillo Morán Fátima Guadalupe con cédula de identidad No. 1309478038, estudiantes de la Facultad de Ciencias Informáticas de la UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, previo a la obtención del título de INGENIERO/A EN SISTEMAS, me han capacitado sobre el funcionamiento del software RISKMANAGEMENT 1.0, el cual es un software de análisis de riesgos informáticos aplicando la metodología MAGERIT y normas ISO/IEC 17799 e ISO/IEC 27001.

Certifico que los peticionarios pueden hacer uso lícito en su beneficio, cualquier enmendadura de la presente certificación invalida el documento.


Encargada de Software de
Análisis de Riesgos de la FACCI
Ing. Martha Ávila Chávez
C.I.: 1305900035



ANEXO I

Anexo I: Certificado de implementación

CERTIFICADO DE IMPLEMENTACIÓN

Manta, 19 de Febrero del 2018

Certifico que:

Los estudiantes Acosta Alvarado Nexar Jesús con cédula de identidad No. 1312286972 y Carrillo Morán Fátima Guadalupe con cédula de identidad No. 1309478038, estudiantes de la Facultad de Ciencias Informáticas de la UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ, previo a la obtención del título de INGENIERO/A EN SISTEMAS, implementaron y está en funcionamiento el **“SOFTWARE DE ANÁLISIS DE RIESGOS INFORMÁTICOS APLICANDO MAGERIT Y NORMAS ISO/IEC 17799 E ISO/IEC 27001”** a los activos de esta facultad.

Certifico que los peticionarios pueden hacer uso lícito en su beneficio, cualquier enmendadura de la presente certificación invalida el documento.


Encargada de Software de
Análisis de Riesgos de la FACCI

Ing. Martha Ávila Chávez

C.I.: 1305900035



MANUAL DE USUARIO

FUNCIONES DE USUARIO TIPO: Administrador

Login, inicio de sesión

Una vez ejecutado el software se muestra la pantalla del login en general, el cual se deben ingresar las credenciales (usuario y contraseña) para acceder al sistema.

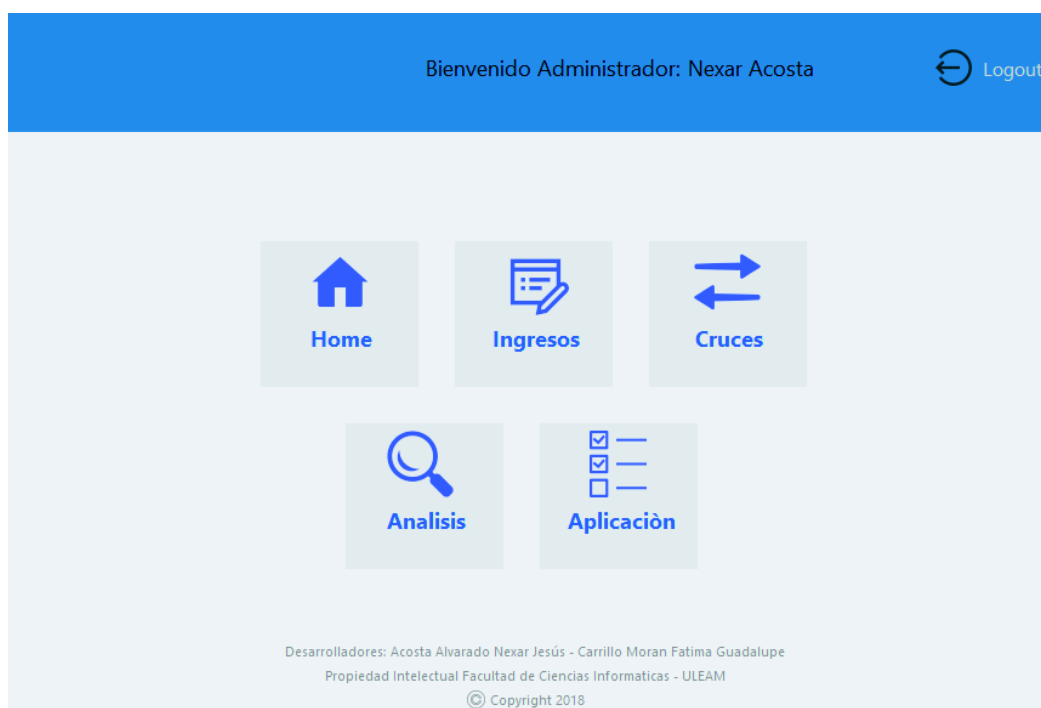


Módulos

Una vez que se loguees con las credenciales correctas la primera pantalla que se nos despliega es la de Módulos y también como se puede observar se

tiene la parte del nombre del usuario que ingresa y también su respectivo botón de << Logout >>; está conformada por los siguientes módulos:

- Modulo -> Home
- Modulo -> Ingresos
- Modulo -> Cruces
- Modulo -> Análisis
- Modulo -> Aplicación



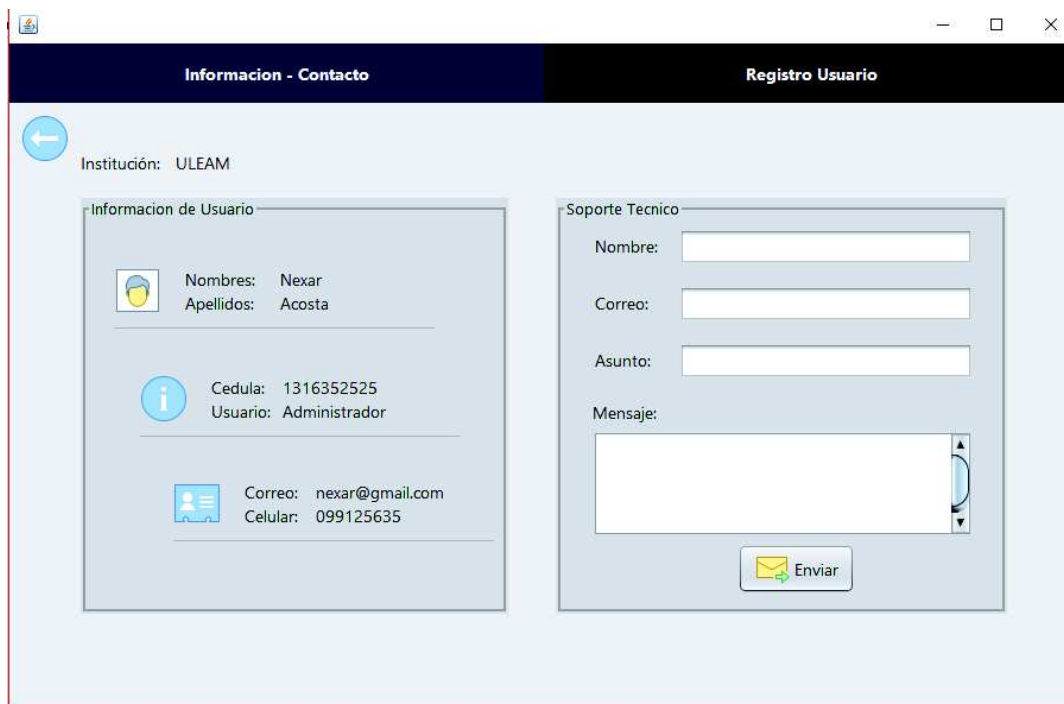
Modulo Home

Información Contacto

En este módulo como se puede observar está dividido en dos secciones como esta en el menú información-contacto y registro de usuarios.

En la primera sección se muestran la información más relevante de los datos del usuario que se logueó y soporte técnico para que se puedan comunicarse con los desarrolladores en tal caso con algún inconveniente.

Módulo de Registro de Usuario Tipo administrador



The screenshot shows a web application window titled 'Registro Usuario'. The window has a dark blue header with 'Informacion - Contacto' on the left and 'Registro Usuario' on the right. Below the header, there is a light blue sidebar with a back arrow icon and the text 'Institución: ULEAM'. The main content area is divided into two panels. The left panel, titled 'Informacion de Usuario', contains a profile icon, a list of user details (Nombres: Nexar, Apellidos: Acosta, Cedula: 1316352525, Usuario: Administrador, Correo: nexar@gmail.com, Celular: 099125635), and a list icon. The right panel, titled 'Soporte Tecnico', contains input fields for 'Nombre', 'Correo', 'Asunto', and 'Mensaje', and an 'Enviar' button with an envelope icon.

En esta sección o ventana como se puede visualizar el administrador tiene todos los privilegios uno de los más importantes es de que puede registrar; administradores y auxiliares a través de una elección, y sus botones de: <<Nuevo>>, <<Guardar>>, <<Modificar>>, <<Eliminar>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de estar ingresando los datos por algún motivo ocurre un error de digitalización se actualizan todos campos y vuelven al estado en blanco.

<<**Guardar**>> una vez llenado el registro se da clic en el botón guardar y se registran los datos y se muestran en la tabla.

<<**Modificar**>> se realiza a dar clic en el registro o fila que se piensa modificar los datos, luego los datos se disparan en los campos y se modifica, posterior a eso se da clic en modificar y los datos automáticamente se muestran en la tabla modificados.

<<**Eliminar**>> Si se quiere eliminar algún registro o fila se selecciona y luego se procede a eliminar que básicamente lo que significa es que se le da de baja a ese usuario tanto administrador como auxiliar.

Información - Contacto
Registro Usuario

Datos de Usuarios

id:

Nombres:

Apellidos:

Institución:

Celular:

Cédula:

Correo:

Datos de Login

Usuario:

Contraseña:

Tipo: Administrador ▼

Nuevo
 Guardar
 Modificar
 Eliminar

Id	Nombres	Apellidos	Correo	Celular	Institucion	Cedula	Usuario	Password	Tipo Usua...
1	Fatima	Carrillo	fattecm@...	0990490186	ULEAM	1309478038	fattecm	12345	Administr...
2	Nexar	Acosta	nexar@g...	099125635	ULEAM	1316352525	nexar	123	Administr...
3	Jesus	Alvarado	jesus@hot...	0981773628	ULEAM	1312286972	chucho	123	Auxiliar

Módulo de Ingresos: Secciones Activos y Amenazas

Activos

En esta sección o ventana se cargan todos los activos que se han registrado como se puede visualizar en la respectiva tabla, el administrador tiene todos los privilegios:

Los cuales son por medio de los botones, <<Nuevo>>, <<Guardar>>, <<Modificar>>, <<Eliminar>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de estar ingresando los datos por algún motivo ocurre un error de digitalización se actualizan todos campos y vuelven al estado en blanco.

<<Guardar>> una vez llenado el registro se da clic en el botón guardar y se registran los datos y se muestran en la tabla.

Al momento de modificar o eliminar algún registro de activos con sus respectivos datos se puede hacer la búsqueda tanto por id, identificador y aplicación.

<<Modificar>> se realiza a dar clic en el registro o fila que se piensa modificar los datos, luego los datos se disparan en los campos y se modifica, posterior a eso se da clic en modificar y los datos automáticamente se muestran en la tabla modificados.

<<Eliminar>> Si se quiere eliminar algún registro o fila se selecciona y luego se procede a dar clic en eliminar.

Activo **Amenaza**

Registro Activo

Area:

Identificador:

Cantidad:

Nombre Activo:

Tipo Activo: Aplicacion:

Buscar Activos

Buscar por:

Tabla de Activos

Area	Identificador	Cantidad	Activo	Tipo Activo	Aplicacion
LAB202	A1	20	CPU DELL	HW	SI
LAB202	A2	20	MONITORES D...	HW	SI
LAB202	A3	20	TECLADOS DELL	HW	SI
LAB203	B1	1	SPLIT LG	AUX	SI
LAB203	B2	20	SO WINDOWS10	SW	NO

Nuevo **Guardar** **Modificar** **Eliminar**

Amenazas

En esta sección o ventana se cargan todas las amenazas que Magerit 3.0 utiliza en su segundo libro de tipo de amenazas, el administrador tiene todos los privilegios:

Los cuales son por medio de los botones, <<Nuevo>>, <<Guardar>>, <<Modificar>>, <<Eliminar>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de estar ingresando la amenaza por algún motivo ocurre un error de digitalización se actualiza el campo y vuelven al estado en blanco.

<<Guardar>> una vez llenado el campo de la amenaza se da clic en el botón guardar seleccionando al tipo de amenaza que le corresponde, y se registran los datos y se muestra en la lista correspondiente.

<<Modificar>> se realiza a dar clic en el registro o fila que se piensa modificar los datos, luego el dato de amenaza se dispara al campo y se modifica, posterior a eso se da clic en modificar y los datos automáticamente se muestran en la lista correspondiente al ser modificada mediante la selección del tipo de amenaza.

<<Eliminar>> Si se quiere eliminar algún registro o fila se selecciona y luego se procede a dar clic en eliminar.

Módulo de Cruces ente Activos y Amenazas

En el módulo de cruces se hace la valoración entre amenazas y activo, cuantas amenazas va a tener dicho activo por medio de un selector entre “SI” y “NO”, el administrador puede realizar por medio de los botones, <<Nuevo>>, <<Guardar>>, <<Exportar>>, <<Reporte>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de haber colocado la aplicación de las amenazas a dicho activos por algún error no se coloca bien se vuelve atrás y los campos vuelven a estar vacíos al momento de darle clic al botón.

<<Guardar>> una vez llenada la tabla con su respectiva aplicación de amenazas que va a tener ese activo se procede a dar clic en guardar.

<<Exportar>> al momento de darle clic al botón se genera una hoja de cálculo “Excel” donde se va a descargar la tabla de cruces y el contenido en ella.

<<Reporte>> al momento de darle clic al botón se genera un reporte donde estarán los datos del administrador y la institución más los datos de dicha tabla con los valores de las amenazas que contienen dichos activos con cuadros estadísticos.



Amenaza/Activo	A1	A2	A3	B1
FUEGO	SI			
DAÑO POR AGUA	SI			
DESASTRES NATURALES	SI			
CORTE SUMISTRO ELECTRICO	SI			
ROBO				
INTERRUPCION DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES		SI		
ERRORES DE LOS USUARIOS		SI		
ERRORES DE ADMINISTRACION		SI		
ERRORES DE CONFIGURACION		SI		
FUGA DE INFORMACION			SI	
INTRODUCCION DE FALSA INFORMACION			SI	
ALTERACION DE LA INFORMACION			SI	
CORRUPCION DE LA INFORMACION				SI
DESTRUCCION DE LA INFORMACION				SI
INTERCEPTACION DE INFORMACION				SI
DIVULGACION DE INFORMACION				SI
ATAQUES DE FUERZA BRUTA		SI		SI
DENEGACION DE SERVICIOS				
VIRUS INFORMATICO O CODIGO MALICIOSO				
DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACION				
DIFUCION DE SOFTWARE DAÑINO				
ERRORES DE MANTENIMIENTO SOFTWARE				
ERRORES DE MANTENIMIENTO HARDWARE				
CAIDA DEL SISTEMA POR SOBRECARGA				SI
PERDIDA DE EQUIPOS				SI

Módulo de Análisis

Como se puede visualizar se tiene los botones, <<Visualizar Análisis>>, <<Guardar>>, <<Exportar>>, <<Reporte>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

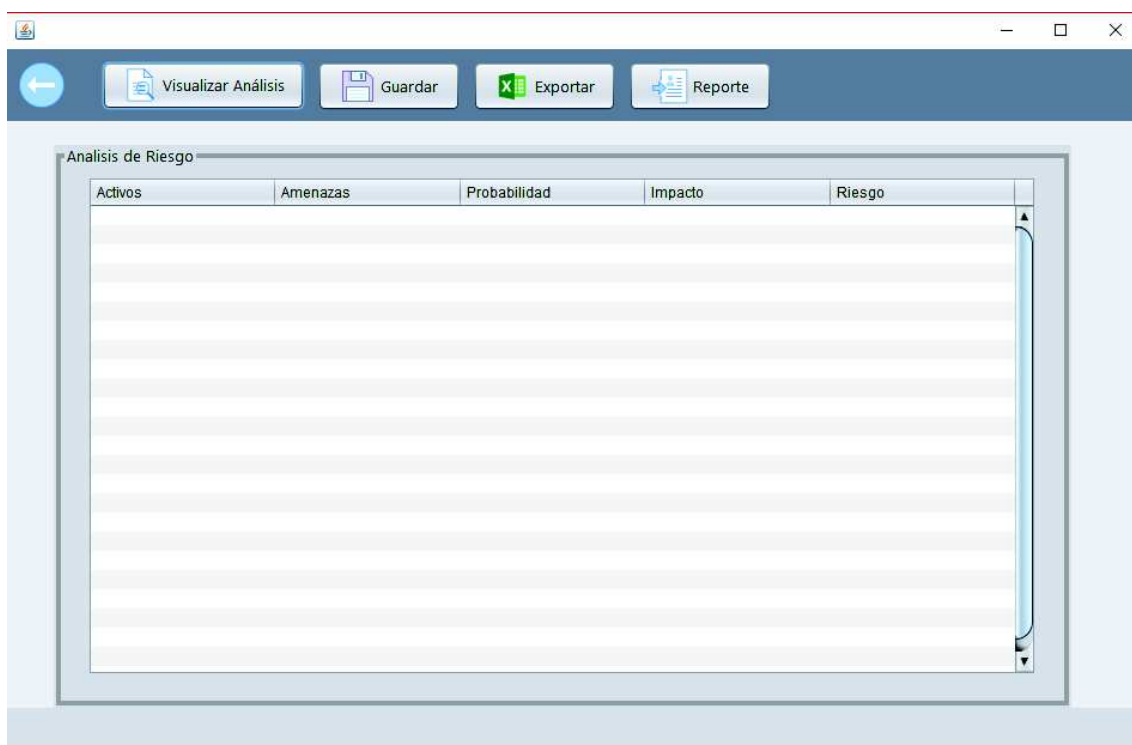
<<Visualizar Análisis>> para obtener o visualizar en la tabla que se observa, todos los activos que contienen esas amenazas se procede a dar clic en el botón y se despliegan dichos datos en la tabla.

Una vez que los datos se visualizan en la tabla se procede a darle la valoración por su probabilidad e impacto que van del uno al tres en un campo de selección y se genera automáticamente su riesgo y el porcentaje que aplica del 1% al 100% según la ponderación.

<<**Guardar**>> una vez llenada la tabla con su respectiva probabilidad e impacto se procede a dar clic en guarda.

<<**Exportar**>> al momento de darle clic al botón se genera una hoja de cálculo “Excel” donde se va a descargar la tabla de análisis y el contenido en ella.

<<**Reporte**>> al momento de darle clic al botón se genera un reporte donde estarán los datos del administrador y la institución más los datos de dicha tabla con los valores de probabilidad e impacto y el riesgo que da como resultados ponderados, con cuadros estadísticos.



Módulo de aplicación de las ISO/IEC 17799 e ISO/IEC 27001

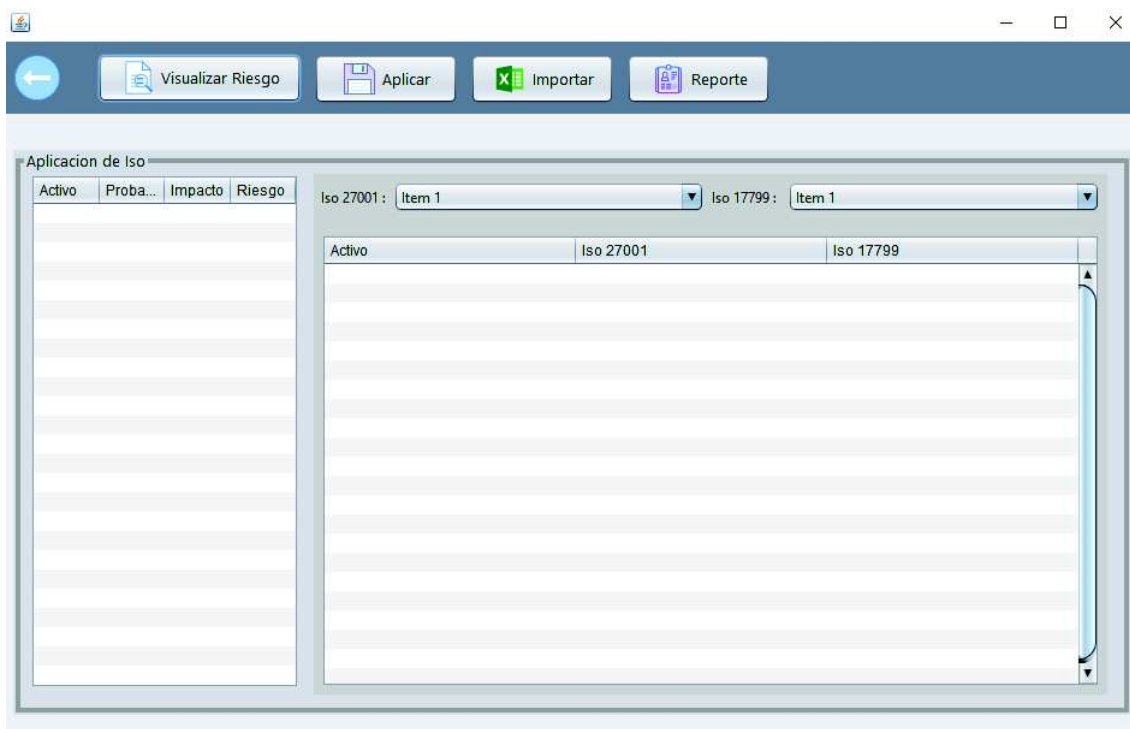
Como se puede visualizar se tiene los botones, <<Visualizar Análisis>>, <<Aplicar>>, <<Exportar>>, <<Reporte>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<**Visualizar Análisis**>> para obtener o visualizar en la tabla que se observa, en la parte izquierda de la tabla donde se quiere visualizar Activo, Probabilidad, Impacto y riesgo se lo realiza haciendo clic en el botón. Luego se le aplica a cada uno de estos registros las ISOS que le corresponda según el riesgo.

<<**Aplicar**>> una vez llenada la tabla con sus respectivas normas isos según el riesgo se procede a dar clic en el botón y posteriormente nos arroja un resultado estadístico en una ventana con sus riesgos y isos aplicadas.

<<**Exportar**>> al momento de darle clic al botón se genera una hoja de cálculo “Excel” donde se va a descargar la tabla de aplicación y el contenido en ella.

<<**Reporte**>> al momento de darle clic al botón se genera un reporte



donde estarán los datos del administrador y la institución más los datos de dicha tabla con el identificador del activo y las isos que son aplicadas, con cuadros estadísticos.

FUNCIONES DE USUARIO TIPO: Auxiliar

Login, inicio de sesión

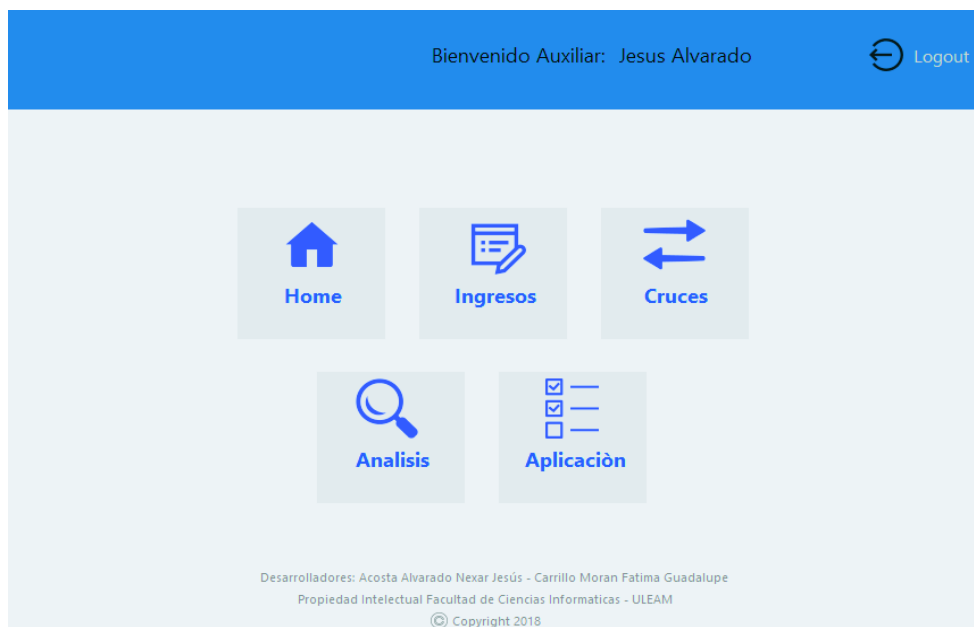
Una vez ejecutado el software se muestra la pantalla del login en general, el cual se deben ingresar las credenciales (usuario y contraseña) para acceder al sistema en este caso del auxiliar.



Módulos

Una vez que se logues con las credenciales correctas la primera pantalla que se nos despliega es la de Módulos, también el auxiliar pierde algunos privilegios por escala de rango de usuarios, y también como se puede observar se tiene la parte del nombre del usuario que ingresa y también su respectivo botón de << Logout >>; está conformada por los siguientes módulos:

- Modulo -> Home
- Modulo -> Ingresos
- Modulo -> Cruces
- Modulo -> Análisis
- Modulo -> Aplicación

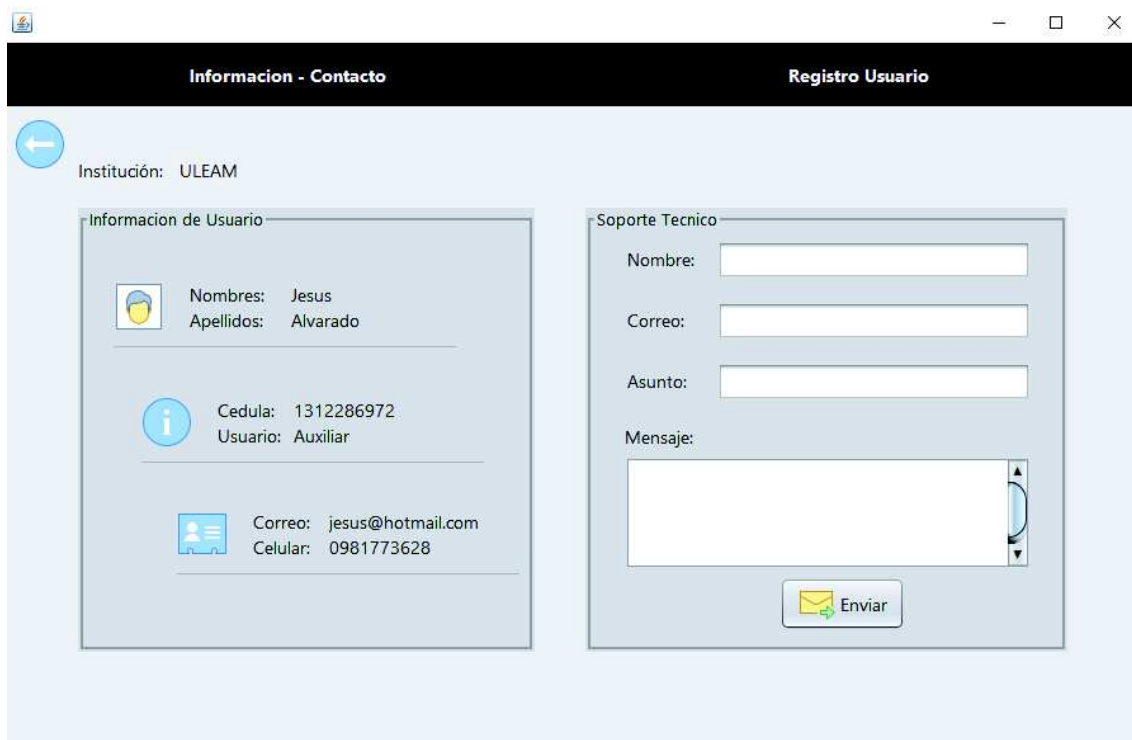


Modulo Home

4.1. Información Contacto

En este módulo como se puede observar está dividido en dos secciones como esta en el menú información-contacto y registro de usuarios.

en la primera sección se muestran la información más relevante de los datos del usuario que se logueó y soporte técnico para que se puedan comunicarse con los desarrolladores en tal caso con algún inconveniente.



The screenshot shows a web application window titled 'Información - Contacto' and 'Registro Usuario'. The interface is divided into two main sections. On the left, under 'Información de Usuario', there is a profile card for 'Jesus Alvarado' with a photo icon, ID number '1312286972', and email 'jesus@hotmail.com'. On the right, under 'Soporte Tecnico', there are input fields for 'Nombre', 'Correo', and 'Asunto', followed by a large text area for 'Mensaje' and an 'Enviar' button.

Información - Contacto		Registro Usuario	
Institución: ULEAM			
Información de Usuario		Soporte Tecnico	
	Nombres: Jesus Apellidos: Alvarado	Nombre:	
	Cedula: 1312286972 Usuario: Auxiliar	Correo:	
	Correo: jesus@hotmail.com Celular: 0981773628	Asunto:	
		Mensaje:	
			

Módulo de Registro de Usuario Tipo administrador

En esta sección o ventana como se puede visualizar el auxiliar solo puede modificar los datos de algún auxiliar, y sus botones de: <<Nuevo>>, <<Modificar>>, Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de estar ingresando los datos por algún motivo ocurre un error de digitalización se actualizan todos campos y vuelven al estado en blanco.

<<Modificar>> se realiza a dar clic en el registro o fila que se piensa modificar los datos, luego los datos se disparan en los campos y se modifica, posterior a eso se da clic en modificar y los datos automáticamente se muestran en la tabla modificados.

Datos de Usuarios

id:

Nombres:

Apellidos:

Institución:

Celular:

Cédula:

Correo:

Datos de Login

Usuario:

Contraseña:

Tipo:

Buttons: Nuevo, Guardar, Modificar, Eliminar

Id	Nombres	Apellidos	Correo	Celular	Institucion	Cedula	Usuario	Password	Tipo Usua...
3	Jesus	Alvarado	jesus@hot...	0981773628	ULEAM	1312286972	chucho	123	Auxiliar

Módulo de Ingresos: Secciones Activos y Amenazas

Activos

En esta sección o ventana se cargan todos los activos que se han registrado como se puede visualizar en la respectiva tabla.

Los cuales son por medio de los botones, <<Nuevo>>, <<Guardar>>, <<Modificar>>, Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de estar ingresando los datos por algún motivo ocurre un error de digitalización se actualizan todos campos y vuelven al estado en blanco.

<<Guardar>> una vez llenado el registro se da clic en el botón guardar y se registran los datos y se muestran en la tabla.

Al momento de modificar o eliminar algún registro de activos con sus respectivos datos se puede hacer la búsqueda tanto por id, identificador y aplicación.

<<Modificar>> se realiza a dar clic en el registro o fila que se piensa modificar los datos, luego los datos se disparan en los campos y se modifica, posterior a eso se da clic en modificar y los datos automáticamente se muestran en la tabla modificados.

Activo **Amenaza**

Registro Activo

Area:

Identificador:

Cantidad:

Nombre Activo:

Tipo Activo: Aplicacion:

Buscar Activos

Buscar por:

Tabla de Activos

Area	Identificador	Cantidad	Activo	Tipo Activo	Aplicacion
LAB202	A1	20	CPU DELL	HW	SI
LAB202	A2	20	MONITORES D...	HW	SI
LAB202	A3	20	TECLADOS DELL	HW	SI
LAB203	B1	1	SPLIT LG	AUX	SI
LAB203	B2	20	SO WINDOWS10	SW	NO

Amenazas

En esta sección o ventana se cargan todas las amenazas que magerit 3.0 utiliza en su segundo libro de tipo de amenazas:

Por medio de los botones, <<Nuevo>>, <<Guardar>>, <<Modificar>>.

Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Nuevo>> que sirve; si al momento de estar ingresando la amenaza por algún motivo ocurre un error de digitalización se actualiza el campo y vuelven al estado en blanco.

<<Guardar>> una vez llenado el campo de la amenaza se da clic en el botón guardar seleccionando al tipo de amenaza que le corresponde, y se registran los datos y se muestra en la lista correspondiente.

<<**Modificar**>> se realiza a dar clic en el registro o fila que se piensa modificar los datos, luego el dato de amenaza se dispara al campo y se modifica, posterior a eso se da clic en modificar y los datos automáticamente se muestran en la lista correspondiente al ser modificada mediante la selección del tipo de amenaza.

Registrar Amenaza

Amenaza: Tipo Amenaza: AM1

A1	A2	A3
FUEGO	CORTE SUMISTRO ELECTRICO	ERRORES DE LOS USUARIOS
DAÑO POR AGUA	INTERRUPCION DE OTROS SERVICIOS Y S	ERRORES DE ADMINISTRACION
DESASTRES NATURALES	Condiciones inadecuadas de temperatura	ERRORES DE CONFIGURACION
	Fallo de servicios de comunicaciones	
	Dependencias industriales	
A4	A5	A6
FUGA DE INFORMACION	DEGRADACION DE LOS SOPORTES DE ALI	ROBO
INTRODUCCION DE FALSA INFORMACION	DIFUSION DE SOFTWARE DAÑINO	DENEGACION DE SERVICIOS
ALTERACION DE LA INFORMACION	ERRORES DE MANTENIMIENTO SOFTWARE	INDISPONIBILIDAD DEL PERSONAL
CORRUPCION DE LA INFORMACION	ERRORES DE MANTENIMIENTO HARDWARE	EXTORSION
DESTRUCCION DE LA INFORMACION	CAIDA DEL SISTEMA POR SOBRECARGA	INGENIERIA SOCIAL

Módulo de Cruces ente Activos y Amenazas

El auxiliar solo puede realizar la visualización de la tabla y también por medio de los botones, <<Exportar>>, <<Reporte>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<**Exportar**>> al momento de darle clic al botón se genera una hoja de cálculo “Excel” donde se va a descargar la tabla de cruces y el contenido en ella.

<<Reporte>> al momento de darle clic al botón se genera un reporte donde estarán los datos del administrador y la institución más los datos de dicha tabla con los valores de las amenazas que contienen dichos activos con cuadros estadísticos.



The screenshot shows a software window titled "Cruce entre Amenaza y Activo". It features a toolbar with buttons for "Nuevo", "Guardar", "Exportar", and "Reporte". Below the toolbar is a table with the following data:

Amenaza/Activo	A1	A2	A3	B1
FUEGO	SI			
DAÑO POR AGUA	SI			
DESASTRES NATURALES	SI			
CORTE SUMISTRO ELECTRICO	SI			
ROBO				
INTERRUPCION DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES		SI		
ERRORES DE LOS USUARIOS		SI		
ERRORES DE ADMINISTRACION		SI		
ERRORES DE CONFIGURACION		SI		
FUGA DE INFORMACION			SI	
INTRODUCCION DE FALSA INFORMACION				
ALTERACION DE LA INFORMACION			SI	
CORRUPCION DE LA INFORMACION			SI	
DESTRUCCION DE LA INFORMACION				
INTERCEPCION DE INFORMACION				
DIVULGACION DE INFORMACION				
ATAQUES DE FUERZA BRUTA				
DENEGACION DE SERVICIOS			SI	
VIRUS INFORMATICO O CODIGO MALICIOSO				
DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACION				
DIFUCION DE SOFTWARE DAÑINO				SI
ERRORES DE MANTENIMIENTO SOFTWARE				SI
ERRORES DE MANTENIMIENTO HARDWARE				
CAIDA DEL SISTEMA POR SOBRECARGA				
PERDIDA DE EQUIPOS				

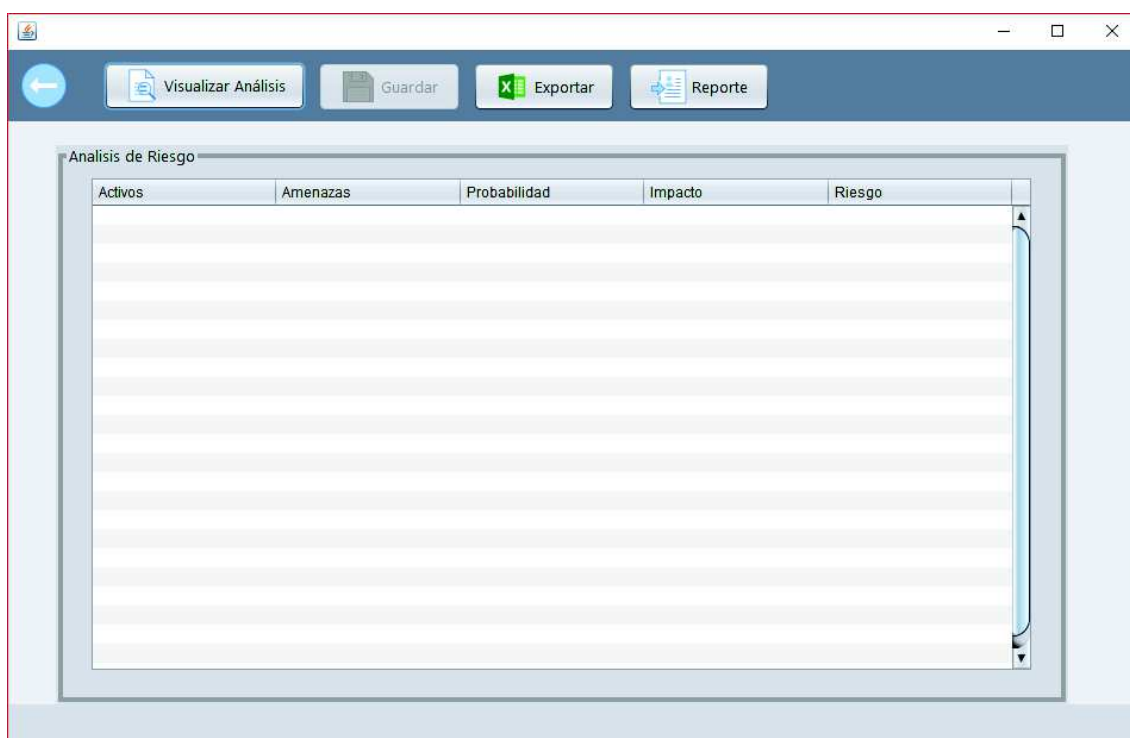
Módulo de Análisis

Como se puede visualizar se tiene los botones, <<Visualizar Análisis>>, <<Exportar>>, <<Reporte>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<Visualizar Análisis>> para obtener o visualizar en la tabla que se observa, todos los activos que contienen esas amenazas se procede a dar clic en el botón y se despliegan dichos datos en la tabla con su probabilidad e impacto y el riesgo.

<<**Exportar**>> al momento de darle clic al botón se genera una hoja de cálculo “Excel” donde se va a descargar la tabla de análisis y el contenido en ella.

<<**Reporte**>> al momento de darle clic al botón se genera un reporte donde estarán los datos del administrador y la institución más los datos de dicha tabla con los valores de probabilidad e impacto y el riesgo que da como resultados ponderados, con cuadros estadísticos.



Módulo de aplicación de las ISO/IEC 17799 y ISO/IEC 27001

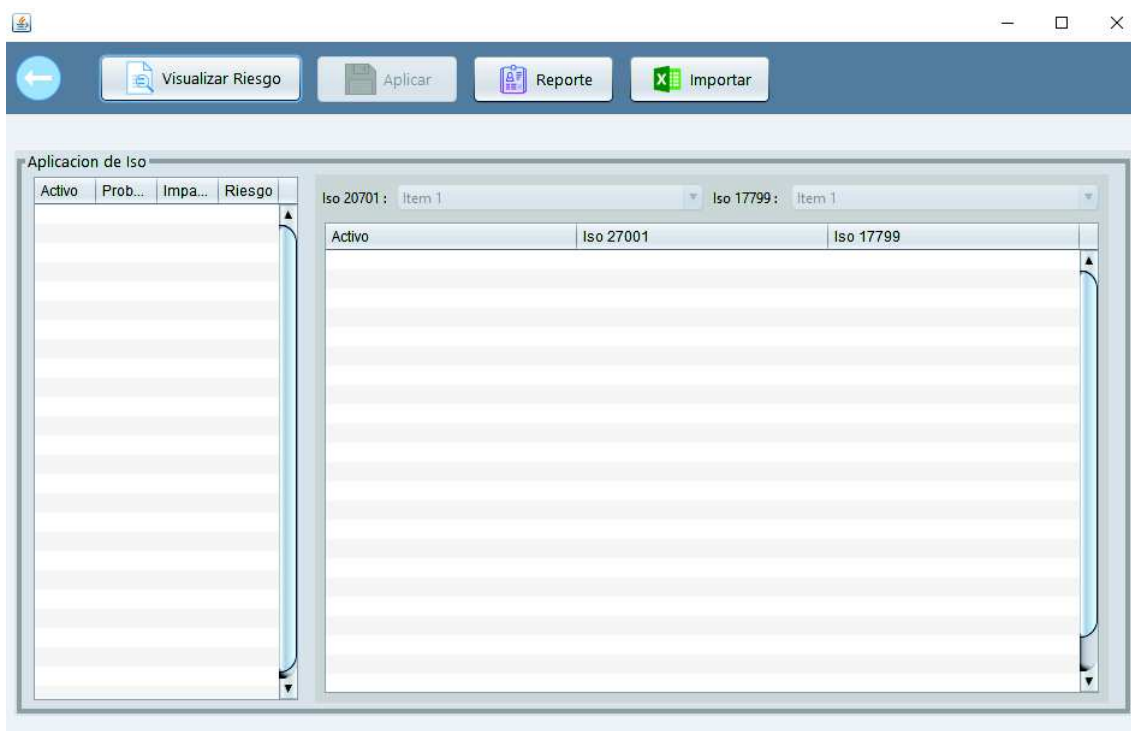
Como se puede visualizar se tiene los botones, <<Visualizar Análisis>>, <<Exportar>>, <<Reporte>>. Cada uno de los botones que se nombró tiene su acción, por ejemplo:

<<**Visualizar Análisis**>> para obtener o visualizar en las tablas que se observan, en la parte izquierda y derecho donde se quiere visualizar Activo,

Probabilidad, Impacto, riesgo y su aplicación de ISOS se lo realiza haciendo clic en el botón.

<<**Exportar**>> al momento de darle clic al botón se genera una hoja de cálculo “Excel” donde se va a descargar la tabla de aplicación y el contenido en ella.

<<**Reporte**>> al momento de darle clic al botón se genera un reporte donde estarán los datos del administrador y la institución más los datos de dicha tabla con el identificador del activo y las ISOS que son aplicadas, con cuadros estadísticos.



Glosario

Activo: Conjunto de bienes con valor, pueden pertenecer a una empresa, institución o individuo.

Ataque: Amenaza de origen intencionado.

Impacto: Resultado sobre un activo ante la materialización de una amenaza

Incidente: Cualquier evento no esperado o no deseado que pueda comprometer la seguridad del sistema.

ISO: Organización Internacional de Estandarización

IEC: Comisión Electrotécnica Internacional

Vulnerabilidad: Fragilidad o debilidad en la operación de un sistema.

Valor: Estimación de la unidad de un determinado activo de información para la organización teniendo en cuenta los diferentes requerimientos.