UNIVERSIDAD NACIONAL JOSÉ MARIÁ ARGUEDAS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

SISTEMA WEB DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ASISTIDA POR COMPUTADORA BASADA EN EL ESTÁNDAR ISO 27001 EN LA UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

Presentado por

ANDREA MARGOT OCHOA TAPIA

TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

ANDAHUAYLAS – APURÍMAC – PERÚ
2017

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Presentado por:

Bach. ANDREA MARGOT OCHOA TAPIA

SISTEMA WEB DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ASISTIDA POR COMPUTADORA BASADA EN EL ESTÁNDAR ISO 27001 EN LA UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

Asesor:
Dr. ANGEL FERNANDO NAVARRO RAYMUNDO

ANDAHUAYLAS – APURÍMAC – PERÚ
2017

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño a mi madre, Elsa Alicia Tapia Ledesma por su sacrificio y esfuerzo, por darme una carrera para mi futuro por creer en mi capacidad, a pesar de los tiempos difíciles, siempre ha estado brindándome su comprensión, cariño y amor.

A mi padre Encarnación Ochoa cruz, por su apoyo, y sus palabras de aliento que no me dejaban decaer para que siguiera adelante y siempre sea perseverante y cumpla con mis ideales.

A mis compañeros y amigos presentes y pasados, quienes sin esperar nada a cambio compartieron su conocimiento, alegrías y tristezas y a todas aquellas personas que durante estos cinco años estuvieron a mi lado apoyándome y lograron que este sueño se haga realidad.

AGRADECIMIENTO

En primer lugar, agradezco a la Universidad Nacional José María Arguedas, por hacerme parte de ella y abrirme sus puertas de su seno científico, para poder estudiar mi carrera, del mismo modo agradezco a mis docentes que me brindaron sus conocimientos y su apoyo para seguir adelante día a día.

Agradezco también a mi asesor de tesis el Dr. Angel Fernando Navarro Raymundo, por brindarme la oportunidad de recurrir a su capacidad y conocimiento, así como también haberme tenido toda la paciencia del mundo para guiarme durante todo el desarrollo de la tesis.

RECONOCIMIENTO

A mi madre y padre por su apoyo incondicional, a mis hermanos por su gran apoyo y cariño.

A mis amigos más cercanos quienes estuvieron presentes en todo mi recorrido para realizarme profesional y también dieron su pequeño granito de arena.

A mis compañeros de clase que durante toda mi carrera fueron un pilar en mi crecimiento profesional.

A mi asesor, por todo el apoyo constante, y brindarme sus conocimientos.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La información es un activo valioso para las empresas, instituciones, organizaciones, etc. tanto en el sector público como privado, por lo que buscan diferentes formas de protegerla de los riesgos internos como externos.

Debido a la importancia que tiene este activo, la Organización Internacional de Normalización crea una norma específica para la seguridad de la Información, la cual es denominada como un Sistema de Gestión de la Seguridad de la Información (SGSI).

A consecuencia de la importancia que le brindan a la información la presente tesis ha realizado una investigación de las normas, estándares y buenas prácticas reconocidos mundialmente para poder desarrollas cada una de las etapas del diseño del Sistema de Gestión de Seguridad de la Información (SGSI), tomando los aspectos más importantes de la norma ISO/IEC 27001:2013, a partir de los cuales se buscará poder desarrollas cada una de las etapas del diseño de un sistema de gestión de seguridad de la información que pueda ser empleado en la Universidad Nacional José María Arguedas, lo cual permitirá que ésta cumpla con las normas de regulación vigente en lo respecta a seguridad de la información.

Para efectos del análisis de riesgo para esta tesis, se decidió trabajar con los activos de la institución. El mismo que mide el nivel de importancia según de cada activo que está categorizado en: servicios, información, hardware, software, soporte, instalaciones, personal y comunicaciones.

Para la evaluación de los riesgos, se utiliza los 14 dominios, 35 objetivos y 114 controles de la ISO/IEC 27001:2013, lo que nos permitirá medir el nivel de madurez de cada control, en donde es necesario poseer un grado máximo al nivel anterior.

El sistema también nos permitirá realizar copias de seguridad de toda la base de datos ingresadas al sistema, el mismo que se guardará con fecha y hora.

Palabras claves:

Sistema web, activos, copias de seguridad, evaluación de riesgo, nivel de madurez, disponibilidad, integridad, confidencialidad.

Abstract

information is a valuable asset in order to the companies, institutions, organizations, etc. so I have a meal in the public sector prevailed, for what they look for different you form of to preserve her from the internal risks as day boys.

He creates a specific norm in order to the Information's certainty Due to the importance that this asset has Normalización's Organization Internacional due to, her as she is named as a System of Gestión of the Information's Certainty (SGSI).

In consequence of the importance that one offer in consequence of to the information show it(subj) thesis has accomplished an investigation of the standards, standards and good recognized practices worldwide to be able to be able to you develop each of the stages of the design of the steps system of certainty of the information (SGSI), taking the norm's more important aspects as one will look for ISO/IEC 27001:2013, starting from them could have been able to develop each of the stages of the design of a steps system of certainty of the information that I may be employed(subj) in the University Nacional José María Arguedas, it as he will permit that this one comply with (subj) the regulation standardsIn use in it relates to it to the information's certainty.

In order to properties of the risk analysis in order to this thesis, he decided being worked up with the institution's the assets. The same one that measures the of importance level according to out of every asset that he is categorized in: Services, information, hardware, software, bear, facilities, personnel and comunicacione.

In order to the risks's evaluation, utilizes him the 14 dominions, 35 objectives and her 114 controls ISO/IEC 27001:2013, what will permit us measuring the maturity level out of every control, where possessing a maximum grade to the level previous is necessary.

The system also he will permit selling off the system, the same one that he will keep with date and hour certainty copies of all the data base entered.

Key words:

System Web, assets, you cheat of certainty, risk, level evaluation of maturity, availability, integrity, confidentiality.

INTRODUCCIÓN

Un sistema de Gestión de la Seguridad de la Información podríamos definirlos como una herramienta de gestión que nos permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en la Organización.

La gestión de los riesgos a través de un sistema de gestión de la seguridad de la información nos va a permitir preservar la confidencialidad, la integridad y la disponibilidad de la misma, por lo que en la presente tesis se desarrolló un Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas, con el objetivo de hacer más fácil la tarea de la evaluación de riesgo, la verificación de los mismos y el nivel de importancia de los activos, a través del nivel de madurez, para ello se desarrollo 5 módulos que nos permitirá cumplir con los objetivos plantados, dichos módulos son:

- Módulo activos
- Módulo evaluación de riesgo
- Módulo verificación
- Módulo reportes
- Módulo copia de seguridad

Los módulos mencionados estan basados en 14 dominios, 35 objetivos y 114 controles de seguridad de la información normado en la ISO 27001.

Para entender la funcionalidad del Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas, la tesis se dividió en 5 capítulos que a continuación se mencionan:

1. **Datos generales:** En donde se encuentra los datos generales del proyecto como título del proyecto, autor, asesor, líneas de investigación, etc.

2. **Planteamiento del problema**: en el planteamiento del problema se menciona la realidad problemática, que la que nos lleva a desarrollar una solución ante el problema percibido, el cual nos permite formular el problema, plantear nuestros objetivos y justificación y buscar la viabilidad posible para la ejecución del mismo.

3. **Marco teórico:** en el marco teórico encontraremos todos los conceptos relacionados con el Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad

4. Nacional José María Arguedas, así como los antecedentes, que nos ayudaran a entender los diferentes términos utilizados en la presente tesis.

5. **Propuesta de solución:** En la propuesta de Solución se detalla de manera clara el desarrollo y diseño del Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas.

6. **Evaluación de la solución:** En la evaluación de la solución se analiza analizar el funcionamiento correcto del Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas.

La presente tesis desarrollada también cuenta con conclusiones que dan respuesta a nuestros objetivos planteados, así como las recomendaciones que nos ayudan en un futuro a mejorar el trabajo realizado.

1. CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. REALIDAD PROBLEMÁTICA

A diario las empresas, instituciones, organizaciones, etc. Están siendo amenazados por riesgos que ponen en peligro la integridad de su activo más valioso, la información, riesgos que pueden provenir del interior como del exterior del mismo, por lo que las organizaciones buscan la manera de asegurar la información, a través de diferentes sistemas y planes de gestión que les permita conocer, gestionar y minimizar los riesgos.

(Martinez, 2005) Licenciado de sistemas de información administrativa en el artículo **"importancia de los sistemas de información para las pequeñas empresas"** indica que "La información es un recurso vital para toda organización, y el buen manejo de esta puede significar la diferencia entre el éxito o el fracaso para todos los proyectos que se emprendan dentro de un organismo que busca el crecimiento y el éxito".

(Fonseca, 2012) en el artículo **La información el activo más importante de cualquier organización**, indica que Como primero se debe tener en cuenta el valor del activo más importante en la empresa u organización "La Información", se debe tener conciencia de la importancia que tiene la información en una empresa, muchas veces esta puede ser medida imaginariamente, suponiendo el impacto que tendría esta, si llegara a desaparecer o lo que es peor, que llegara a caer en manos de la competencia o personas malintencionadas.
En sentido general, la información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

(Información, 2012) En México en la 13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México, las organizaciones están empleando una estrategia que proteja la información más importante y que responda rápidamente cuando ocurra una violación.
Según los encuestados, los tres controles principales que las organizaciones están implementando son: ajustes a políticas (39%), más actividades de concientización de la seguridad (38%) y técnicas de encriptación (29%).

Figura 1: Implementación de controles en las organizaciones

Fuente: 13a Encuesta Global de Seguridad de la Información (EGSI) y comparativo México.

(Información, 2012) En México en la Encuesta de Agenda de Riesgo de TI (IT Risk Agenda Survey) se investigó el grado de adopción de la ITRM (Information Technology Risk Management) y se descubrió que más de una tercera parte de las empresas tenía un programa (proyecto) bien establecido y que casi una cuarta parte había implementado un programa de ITRM recientemente. El 30% de los encuestados se encontraba implementando o estaba considerando implementar un programa. Así mismo, un análisis más profundo de estos resultados arrojó que también existe una correlación entre el tamaño de las empresas y el porcentaje de adopción. Es decir, es mucho más probable que las grandes empresas (700 o más empleados) hayan implementado un programa establecido de ITRM que las compañías con menos empleados.

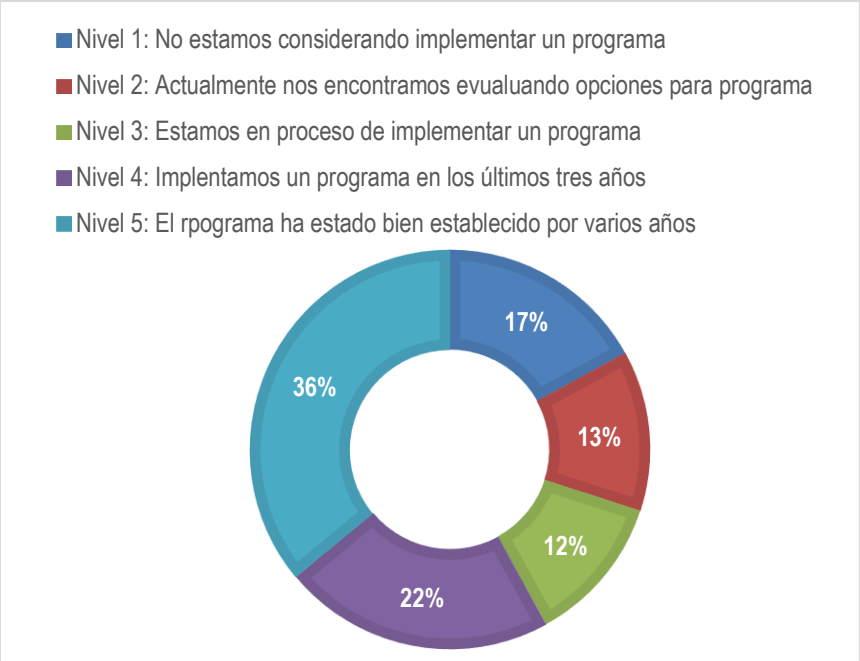


Figura 2: La aceptación de la ITRM
Fuente: Encuesta de Agenda de Riesgo de TI

En España existe la Ley Orgánica de Protección de Datos, que, desde su punto de vista, las medidas de seguridad van destinadas a todas las Organizaciones, empresas e instituciones que almacenan y tratan datos de carácter personal en sus sistemas de información, siendo su finalidad principal proteger los datos de carácter personal tratados de posibles incidencias que puedan provocar su perdida, alteración u acceso no autorizado (tanto interno como externo).

Por ello, la adopción de medidas técnicas y organizativas tendentes a garantizar la seguridad de los datos de carácter personal es una obligación básica que debe ser cumplida por todas las empresas que traten, almacenen y accedan a datos de carácter personal; medidas que deberán adoptarse en función del nivel de los datos almacenados/tratados, de la estructura y organización de la Empresa y del estado de la tecnología.

En Perú, según el padrón Registro Único de Contribuyente (RUC) de la Superintendencia Nacional de Administración Tributaria (SUNAT), en el 2012 se han identificado 1 345 390 micro, pequeñas y medianas empresas (MIPYMES) formales. Por distribución geográfica, el 72,4% de las MIPYMES se ubica en las regiones de la costa (el 52,0%se localiza en Lima y el callao).

La sierra concentra el 21,4% de las MIPYMES y solo el 6,2% se ubica en las regiones de la selva.

Para estimar el porcentaje de la informalidad en empresas de dos a cien trabajadores, nos basamos en dos fuentes de información: la Encuesta Nacional de Hogares (Enaho) y la SUNAT con el Registro Único del Contribuyente (RUC).

Según lo descrito, en el 2012, el número total de empresas fue de 3 218 709, monto superior en 1,5% al registrado en el periodo anterior como se muestra en la tabla 2.

Tabla 1: Perú: Estimación del total de empresas formales y no formales de 2 a 100 trabajadores

TAMAÑO	2010	2011	2012
De 2 a 10 trabajadores	3 162 344	3 127 128	3 173 065
De 11 a 100 trabajadores	41 593	42 682	45 644
TOTAL DE EMPRESAS	3 203 937	3 169 810	3 218 709

Fuente: ENAHO, Encuestas Nacional de Hogares 2012

Por otra parte, la SUNAT a través del RUC contiene el número total de empresas formales, las cuales fueron agrupadas según el rango de trabajadores. Esos resultados se presentan en la tabla 3.

Tabla 2: Perú: Empresas formales, según rango de trabajadores 2010-2012

TAMAÑO	2010	2011	2012
De 2 a10 trabajadores	1 111 427	1 179 275	1 321 992
De 11 a100 trabajadores	20 072	22 047	23 398
TOTAL DE EMPRESAS	1 199 347	1 289 107	1 345 390

Fuente: SUNAT, Registro único del contribuyente 2012

De la diferencia de la tabla 1 y 2 se estima los porcentajes de la informalidad en el Perú. Así en el 2012, el 58,2% (1 873 318) de empresas que emplean de dos a cien trabajadores son informales, es decir de cada 100, 58 de ellas se encuentran en situación de informalidad. Como se muestra en la tabla 4.

Tabla 3: Perú: Estimación de la informalidad en empresas de 2 a 100 trabajadores 2010-2012

AÑO	Nº DE EMPRESAS DE 2 A 100 TRABAJADORES			EN PORCENTAJES		
	Total	Formales	Informales	Formales	Informales	Total
2010	3 203 937	1 199 347	2 004 590	37,3	62,6	100
2011	3 169 810	1 289 107	1 880 703	40,7	59,3	100
2012	3 218 709	1 345 390	1 873 318	41,8	58,2	100

Fuente: SUNAT – ENAHO

En la región Apurímac, de acuerdo a la data de la Superintendencia de Administración Tributaria (SUNAT), existen un total de 57 141 contribuyentes con RUC; de los cuales 39 122 (68.5%) tienen la condición de activos, mientras que 18 019 (31.5%) de contribuyentes tienen la condición de no activos.

La Superintendencia de Banca, Seguros y la Administradora de Fondos y Pensiones (AFP) (2013), señalan que la región de Apurímac cuenta con 41 números de oficinas del sector financiero de los cuales 4 son Banca múltiple y 37 instituciones no bancarias que comprende de cajas municipales, cajas rurales, edpymes y empresas financieras como se puede Observar en la figura 4.

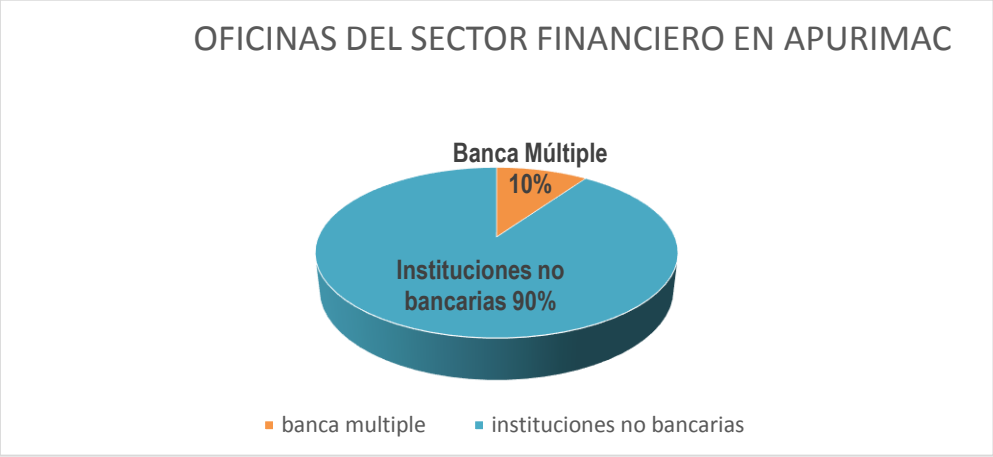


Figura 3: Número de Oficinas del Sector Financiero en la Región de Apurímac
Fuente: Súper intendencia de Banca, Seguros y la Administración de Fondos y Pensiones

En el grafico se puede observar que el 90% del sector financiero lo ocupan las instituciones no bancarias las cuales esta conformadas por 10 Cajas Rurales de Ahorro y Crédito (CRAC), 12 Cajas Municipales de Ahorro y Crédito (CMAC), 10 Entidades de Desarrollo de la Pequeña y Microempresa (EDPYME) y 5 financieras especializadas como se puede observar en la figura 5.

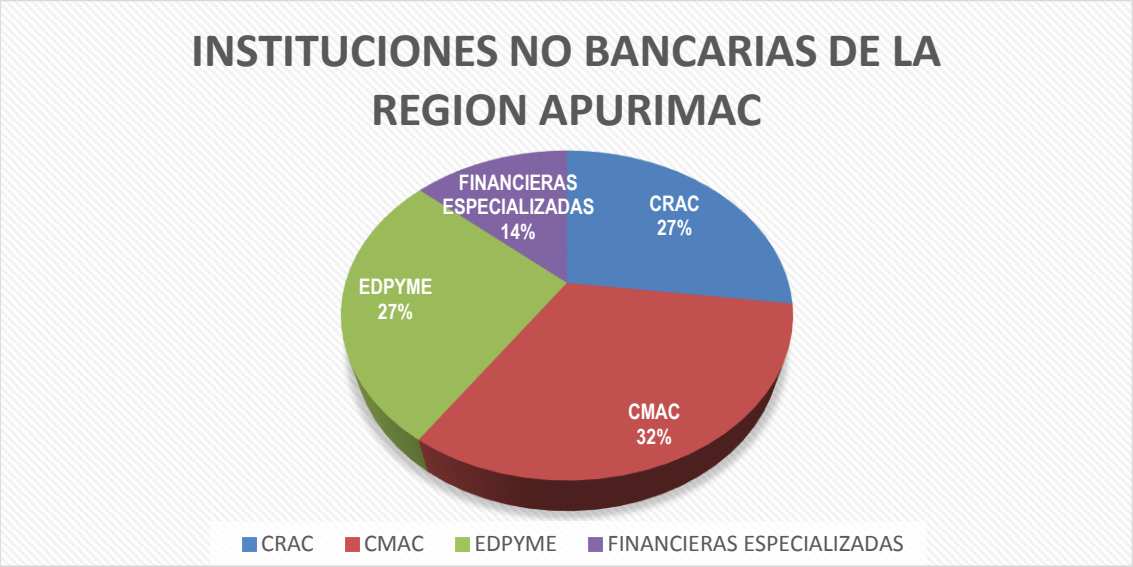


Figura 4: Número de financieras no bancarias de la Región de Apurímac
Fuente: Súper intendencia de Banca, Seguros y la Administración de Fondos y Pensiones

De los gráficos observados podemos concluir que en la región de Apurímac solo el 10% de las instituciones financieras le toma importancia a la seguridad de la información.

(Valle, 2012) docente de la Universidad Nacional José María Arguedas en el Proyecto “Censo empresarial de la provincia de Andahuaylas año 2012” señala que en la ciudad de Andahuaylas de las MYPES que existen, el 0,05% son formales y el 99.95% informales, Se puede observar que el 99.95% de las empresas de Andahuaylas no cumplen con las normas ni políticas establecidas, Por lo que no le dan interés a la seguridad informática y carece de un análisis técnico profesional de seguridad a los sistemas de información lo cual genera información poco fiable e inconsistente a la hora de tomar decisiones.

La universidad Nacional José María Arguedas es una institución que requiere información oportuna y confiable, para tomar decisiones, para ello cuenta con la Oficina de Sistemas de Información que vela por el mantenimiento y adecuado funcionamiento de los sistemas informáticos con los que cuenta la universidad, Pero al igual que en otras instituciones públicas no le dan un interés al tema de seguridad informática.

A continuación, se nombra algunas deficiencias en la Universidad Nacional José María Arguedas:

- Ausencia de una política de seguridad de la Información.
- Ausencia de un plan de Gestión de Riesgo.
- Inadecuado plan de la seguridad de la información.
- Inapropiada administración de recursos informáticos.
- Inadecuada seguridad de los recursos humanos.
- Ausencia de la seguridad física y del entorno.
- Inadecuada administración de las comunicaciones y operaciones.
- Inadecuado control de acceso a la Información.
- Inadecuada adquisición de sistemas de información, desarrollo y mantenimiento.
- Inadecuada administración de los incidentes de seguridad de la Información.
- Inadecuado cumplimiento (legal, de estándares, técnico y auditorias).

1.2. FORMULACIÓN DEL PROBLEMA

Deficiencia en la gestión de la seguridad de la Información en la Universidad Nacional José María Arguedas.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Desarrollar un Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad Nacional José María Arguedas.

1.3.2. OBJETIVOS ESPECÍFICOS

- Analizar y diseñar los procesos y controles de gestión de la seguridad de la información de la Universidad Nacional José María Arguedas.

- Construir y probar eficientemente las medidas y controles de gestión de la seguridad de la información en la Universidad Nacional José María Arguedas.
- Implementar y desplegar los controles del sistema de gestión de seguridad de la información en la Universidad Nacional José María Arguedas.

1.4. JUSTIFICACIÓN

La información es un activo valioso para la organización, mantener su integridad, confidencialidad y disponibilidad es especial para alcanzar los objetivos de toda organización.

En la actualidad, el desarrollo de las nuevas tecnologías ha dado un giro radical a la forma de hacer negocios, a la vez que va aumentado los riesgos para las empresas que se exponen a nuevas amenazas.

Desafortunadamente hoy en día personas no autorizadas tienen fácil acceso a las herramientas de nuestra información protegida, sin hacer mucho esfuerzo y teniendo poco conocimiento, esto causa perjuicios a nuestra organización, información que en mayor parte reside en equipos informáticos, soportes de almacenamiento y redes de datos englobados dentro de lo que se conoce como sistemas de información.

La Universidad Nacional José María Arguedas al igual que muchas organizaciones cuenta con información muy valiosa para la institución, por lo que se debe garantizar la confidencialidad, integridad y disponibilidad de la misma, para ello existe la Organización Internacional de Normalización la que crea una norma específica para la seguridad de la Información, la cual es denominada como un Sistema de Gestión de la Seguridad de la Información (SGSI), la que está establecida a través de la ISO 27001 que cuenta con 14 dominios, 35 objetivos y 114 controles.

El proyecto incluirá el desarrollo de un Sistema web de Gestión de Seguridad de la Información que beneficiara a las áreas académicas y administrativas de la Universidad Nacional José María Arguedas garantizando la

confidencialidad, integridad y disponibilidad de la información que es el activo más valioso de la organización.

1.5. VIABILIDAD DE LA INVESTIGACIÓN

1.5.1. VIABILIDAD TÉCNICA

La viabilidad técnica del presente proyecto radica en el sistema informático de gestión de la seguridad de la información que está orientado y basado en las políticas y medidas de control del estándar ISO 27001 que brindara confidencialidad integridad y disponibilidad de la información en cada uno de los procesos de la Universidad Nacional José María Arguedas.

1.5.2. VIABILIDAD ECONÓMICA

Generalmente, se considera a la seguridad de la información como un costo sin una ganancia financiera evidente. Sin embargo, hay una ganancia financiera si se disminuye los gastos ocasionados por incidentes. Probablemente sí se produce interrupciones de servicio o esporádicos filtrados de datos, o tengan empleados descontentos. O ex empleados descontentos.

La verdad es que aún no existe una metodología ni tecnología que pueda calcular cuánto dinero se puede ahorrar si evita ese tipo de incidentes. Pero siempre es oportuno alertar a la dirección sobre estos casos.

Mejora la eficiencia y eficacia en la gestión, reduciendo costes, permite la organización y gestión de toda la documentación de la empresa, reduciendo riesgos y evitando multas y sanciones.
Finalmente se evaluará la Tasa Interna de Retorno (TIR), que determinaran la viabilidad del sistema.

Tabla 4: Análisis de costo de Inversión

ITEM	DESCRIPCION	Cantidad	UNID. MEDIDA	PRECIO UNITARIO	PRECIO PARCIAL
1.00.00	BIENES				**4655.50**
1.01.00	Materiales de escritorio				**4000.00**
1.01.01	Laptop	1	Unid	3.000,00	3000.00
1.01.02	Disco Duro Externo de 1 TB	1	Unid	300,00	300.00

1.01.03	Impresora EpsonL355 Multifuncional	1	Unid	700,00	700.00
1.02.00	Materiales Consumibles				655.50
1.02.01	Papel Bond A4	8	Millar	25.00	200.00
1.02.02	tinta Epson L355	8		45.00	360.00
1.02.03	lápices	1	caja	10.00	10.00
1.02.04	lapiceros	1	caja	45.00	45.00
1.02.05	Borradores	1	caja	10.00	10.00
1.02.06	Correctores	3	Unid	7.00	21.00
1.02.07	Tajador	2	Unid	1.00	2.00
1.02.08	resaltador	3	Unid	2.50	7.50
2.00.00	SERVICOS				4,240.00
2.01.00	Servicios comunicación				440.00
2.01.01	Internet	4	Mes	60.00	240.00
2.01.02	teléfono	4	Mes	50.00	200.00
2.02.00	servicios de movilidad				600.00
2.02.03	Pasajes	4	mes	150.00	600.00
2.03.00	servicios de Alimentación				2,000.00
2.03.01	desayuno	4	Mes	150.00	600.00
2.03.02	Almuerzo	4	Mes	200.00	800.00
2.03.03	Cena	4	Mes	150.00	600.00
2.04.00	servicios de impresión				1,200.00
2.04.01	fotocopias	4	Mes	100.00	400.00
2.04.02	impresiones	4	Mes	200.00	800.00
3.00.00	Software				1000
3.01.00	Desarrollo del sistema				0.00
3.01.01	Lenguaje de programación (Software libre)	1	Unid	-	-
3.02.00	Desarrollo del proyecto				1,000.00
3.02.01	licencia de antivirus	1	Unid	200.00	200.00
3.02.02	Microsoft office	1	Unid	500.00	500.00
3.02.03	Project profesional	1	Unid	300.00	300.00
4.00.00	RECURSOS HUMANOS				13,000.00
4.01.00	Asesores	1	persona	4,000.00	4,000.00
4.02.00	Desarrollo del sistema				9,000.00
4.02.01	Analista	1	persona	1,000.00	1,000.00
4.02.02	Diseñador	1	persona	1,000.00	1,000.00
4.02.03	Programador	1	persona	3,000.00	3,000.00
4.02.04	Prueba e implementación	1	persona	2,000.00	2,000.00
4.02.05	Capacitación	1	persona	2,000.00	2,000.00
5.00.00	GASTOS GENERALES				2089.55
	Imprevistos				
	Imprevistos 10% del costo total	1	Unid	2089.55	2089.55
	COSTO TOTAL DE LA TESIS				**25,185.05**

Fuente: Elaboración propia

Tabla 5: Flujo de costo sin proyecto

AÑO	0	1	2	3	4	5
Inversión	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00
Operación y mantenimiento	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00
Flujo	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00	S/. 0.00

Fuente: Elaboración propia

Tabla 6: Flujo de costo con proyecto

AÑO	0	1	2	3	4	5
Inversión (S/.)	25,185.05	0.00	0.00	0.00	0.00	0.00
Operación y mantenimiento (S/.)	0.00	0.00	2,000.00	2,000.00	2,000.00	2,000.00
Flujo	25,185.05	0.00	2,000.00	2,000.00	2,000.00	2,000.00

Fuente: Elaboración propia

Tabla 7: Gastos generados sin un sistema

BENEFICIO	TOTAL
Papel	S/. 3,000.00
Personal capacitado en seguridad de la información	S/. 3,500.00
Total	S/. 6,500.00

Fuente: Elaboración propia

Tabla 8: Flujo de costo y beneficio

AÑO	0	1	2	3	4	5
Flujo de costo y beneficio	25,185.05	0.00	2,000.00	2,000.00	2,000.00	2,000.00
Beneficio incremental	6,500.00	6,500.00	6,500.00	6,500.00	6,500.00	6,500.00
Flujo de caja	-18,685.00	6,500.00	4,500.00	4,500.00	4,500.00	4,500.00
TIR	10%					

Fuente: Elaboración propia

1.5.3. VIABILIDAD OPERATIVA

Los beneficiarios encontraran en los sistemas de gestión de la seguridad de la información un software ágil ya que se podrá disponer de una metodología dedicada a la seguridad de la información reconocida internacionalmente; se contará con un proceso definido para Evaluar, Implementar, Mantener y Administrar la seguridad de la información; se disminuirá en costo e inversiones; se formalizará las responsabilidades operativas y legales de los usuarios internos y externos de la información se cumplirá con disposiciones legales y se dispondrá de una metodología para poder administrar los riesgos.

1.5.4. VIABILIDAD LEGAL

Para el desarrollo del sistema se hará uso de XAMPP versión 5.6.23, XAMPP es un servidor independiente de plataforma (software libre), dispone de un sistema de gestión de bases de datos MySQL, servidor web Apache y intérpretes para lenguajes de script (PHP y Perl).

XAMPP está liberado bajo la licencia GNU y por lo tanto es un servidor web libre, con respecto a los dreamweaver cs6, erwin data modeler, programas de oficina, entre otros se adquirirán sus respectivas licencias.

1.6. LIMITACIÓN DEL ESTUDIO

El presente trabajo de investigación está limitado, al alcance que tiene el sistema en el área de usuarios, debido a que está dirigido directamente a usuarios del área de Sistemas de Información de la Universidad Nacional José María Arguedas, además para la gestión de la seguridad de la información se basará únicamente en las políticas y medidas de control del estándar ISO 27001, también se tiene una limitación tecnológica por el hosting de pago anual.

2. CAPÍTULO II: MARCO TEÓRICO

2.1. ANTECEDENTES

En un mundo actual de constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel se convierte en un problema grave cuando no se le brinda el control y tratamiento apropiado. Una efectiva administración sobre este tema es un aspecto de negocio y regulación, no sólo de tecnología.

A esto se suman las nuevas leyes y/o normas que van surgiendo (Basilea II1, Sarbanes Oxley2), las cuales, en un futuro cercano, impartirán lineamientos obligatorios sobre cómo las instituciones financieras del Perú deberán manejar su información, los controles internos que deberán asignarse e implementarse y el presupuesto que deberán destinar a la administración de los riesgos.

La gestión de la seguridad de información deberá lidiar con estos aspectos de una manera proactiva y oportuna, para así poder ser considerada como efectiva, estando siempre alienada a los objetivos y estrategias de negocio de la organización. Por el momento la SBS viene exigiendo anualmente a las instituciones financieras, en oficios múltiples, información de gestión de sus seguros, alineados con los eventos establecidos por Basilea II.

Tesis para optar el título de ingeniero de sistemas de la Pontificia Universidad Católica del Perú de Moisés Antonio Villena Aguilar intitulado: “SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA UNA INSTITUCION FINANCIERA”, en la tesis realiza una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Se rescató los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, lo cual permite que ésta cumpla con las normas de regulación vigentes en lo relacionado a la Seguridad de Información.

La Universidad Nacional de Ciencia y Tecnología de Taiwán, NTUST por sus siglas en inglés, se creó el primero de agosto en 1974 como el primer instituto educativo del tipo tecnológico dentro de Taiwán. Actualmente

cuentan con 4953 alumnos, 48337 graduados y 336 profesores a tiempo completos.
Al alcanzar el estado de “Universidad” en 1997, la escuela se reorganizo en 5 facultades: ingeniería, ingeniería eléctrica y de sistemas, gestión, diseño y arte y ciencias sociales. Entre los departamentos se incluyen los programas de ingeniería mecánica, ingeniería civil, ingeniería química, ingeniería informática, etc.

En abril del 2011, el SGS (Société Générale de Surveillance) en Taiwán, una compañía certificadora reconocida a nivel mundial, le entrego la certificación de la ISO 27001 a la universidad NTUST, mencionando que la calidad de la gestión de la seguridad de información de la NTUST alcanza los más altos estándares de calidad e integridad hoy en día a nivel mundial.

La certificación mencionada cubre los procesos de mantenimiento y operación del centro de cómputo de NTUST y el desarrollo, operación y mantenimiento de todos los sistemas de información de los alumnos. Las compañías de certificación visitaban el campus de vez en cuando para una serie de inspecciones de documentación e in-situ. Asimismo, condujeron una serie de entrevistas con los administradores de los sistemas para verificar si cada módulo de los sistemas de información está asegurado adecuadamente. Finalmente, luego de 10 meses de las fases de planeamiento e implementación que el estándar ISO 27001 demanda que se realice, en conjunto con las inspecciones de la entidad certificadora, la NTUST logro dicha certificación.

La Universidad Libre de Bozen/Bolzano es fundada el 31 de octubre de 1997 en Italia como una institución educativa orientada a la internalización y pluralidad de lenguas. Dicha universidad, promueve el libre intercambio de ideas y conocimiento científico, vinculándose con la tradición europea de humanidades y el respeto por los principios democráticos.
Actualmente cuenta con 5 facultades: la facultad de ciencias de la computación, la escuela de administración y economía, la facultad de educación, la facultad de diseño y de arte y finalmente, la facultad de ciencias y tecnología.

El 12 de enero del 2007 la universidad libre de Bozen/Bolzano recibió la certificación ISO 27001. Esta universidad es la primera organización científica a nivel mundial en obtener en la certificación en el ISO 27001.

Por una semana, dicha universidad estuvo auditada por dos entidades certificadoras: OQS (Austrian Association forcertification of quality and management systems) y CIS (Certification & Information Security Services). Ellas estuvieron auditando y verificando que todo el proceso de transferencia del conocimiento de la información (desde la infraestructura de bases de datos hasta el código de conducta dentro de la universidad) en la institución estuviera lo suficientemente segura, como lo exige la norma que se maneje.

En conjunto con dicha certificación, el departamento de informática y comunicaciones, encargada de gestionar la red informática de la universidad y el desarrollo del software interno educativo, obtuvo también la certificación ISO 9001:2000 por la calidad de sus sistemas de gestión, siendo el primer y único departamento en la Universidad Libre de Bozen/Bolzano que maneja dichas Certificaciones.

La universidad Kyushu es una universidad ubicada en Japón la cual se fundó en 903 con solo dos carreras universitarias: medicina e ingeniería. Desde ese entonces, varias reformas se han hecho para alcanzar un mejor sistema educacional en Japón como la introducción de nuevos formatos educativos después de la segunda guerra mundial y la reorganización de las universidades de Japón en el 2004.

El total de estudiantes de esta universidad es de 18765 aproximadamente, mientras que los miembros de la facultad son de 2186. Asimismo, los programas de intercambio son alentados ya que aceptan a varios estudiantes de intercambio cada año. En la actualidad hay más de 1700 estudiantes de aproximadamente 8 países estudiando dentro de la universidad Kyushu.

El 3 de abril del presente año, esta universidad recibió la certificación ISO/IEC27001 a través del vicepresidente de TI Hiroto Yusuura por parte del BSI (British Standards Institution).

2.2. BASES TEÓRICAS

2.2.1. SISTEMA DE GESTIÓN

A. Sistema

(Alegsa, 2014) Define a un sistema como un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

B. Sistema de información

(andreu, ricart y valor, 1996) definen los sistemas de información "como el conjunto formal de procesos que operando con un conjunto estructurado de datos estructurada de acuerdo con las necesidades de una empresa recopila, elabora y distribuye (Parte de) la información necesaria para la operación dicha empresa y para las actividades de dirección de control correspondientes, apoyando al menos en parte, la toma de decisiones necesaria para desempeñar las funciones y procesos de negocio de la empresa de acuerdo con su estrategia."

(Alarcón, 2006) Define los sistemas de información como un conjunto de componentes que interaccionan entre sí para lograr un objetivo común. Aunque existen una gran variedad de sistemas, la mayoría de ellos pueden representarse a través de un modelo formado por cinco bloques básicos: elementos de entrada de, elementos de salida, sección de transformación, mecanismos de control y objetivos. Tal y como se muestra en la figura 1, los recursos acceden al sistema a través de elementos de entrada para ser modificados en la sección de transformación.

Este proceso es controlado por el mecanismo de control con el fin de lograr el objetivo marcado. Una vez se ha llevado a cabo la transformación, el resultado sale del sistema a través de los elementos de salida.

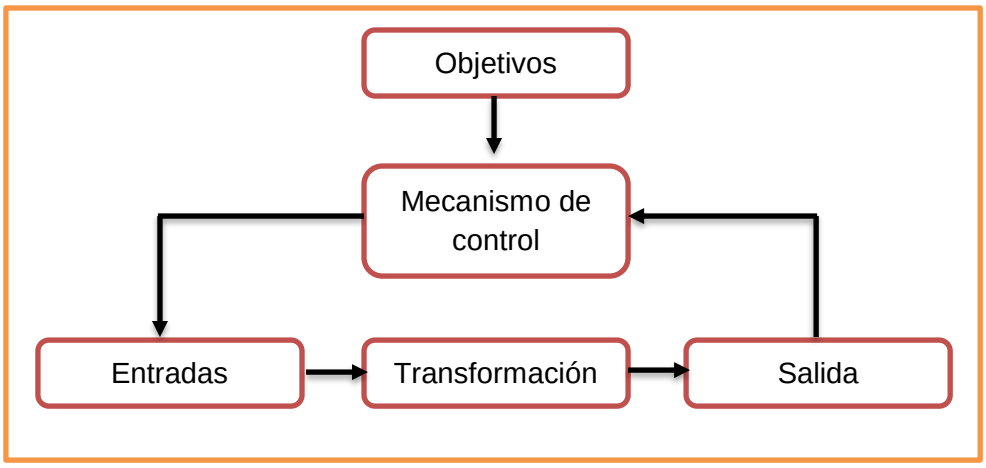


Figura 5: Modelo general de un sistema
Fuente: Alarcón, 2006

2.2.2. SEGURIDAD DE LA INFORMACIÓN

(Project Management Consultores de Proyectos, 2006) Es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Se logra implementando un adecuado conjunto de controles incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

A. Evento de seguridad de información

Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

B. Incidente de seguridad de información

Es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

2.2.3. ISO 27001

(GESCONSULTOR, 2015) La Información es un activo fundamental para el desarrollo, operativa, control y gestión del Modelo de Negocio / Servicio de cualquier Organización.

A través de sus Sistemas de Información se canalizan la práctica totalidad de las actividades corporativas, desde sus aspectos operativos hasta las decisiones gerenciales, siendo estos sistemas elementos clave en el gobierno corporativo de dichas Organizaciones, sea cual sea su tamaño y sector.

La Seguridad de la Información, extendida a todas las infraestructuras físicas, lógicas y organizativas donde se gestiona, se ha convertido en una prioridad al máximo nivel. En los entornos globalizados actuales, donde las transacciones de negocio (Empresas) y servicio (Administraciones Públicas) llevan en su praxis el sufijo “electrónico”, esta prioridad se maximiza ante las especiales características del medio en que se desarrollan y sus riesgos asociados.

Estas cuestiones derivan en la existencia de una serie de Normas estándares, aceptadas como acreditaciones de la Seguridad de la Información universalmente, y cuya implementación aporta a la Organización no solo una certificación reconocida sino, como punto fundamental, una cultura y práctica de la Seguridad que le aporta valores al negocio / servicio en muy diferentes aspectos.

- Mejora de la competitividad
- Mejora de la imagen corporativa
- Protección y continuidad del negocio
- Cumplimiento legal y reglamentario
- Optimización de recursos e inversión en tecnología
- Reducción de costes

La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Entre las actividades propias a desarrollar al abordar una implantación a ISO27001 se encuentran:

- Definición del alcance del SGSI
- Definición de una Política de Seguridad

- Definición de una metodología y criterios para el Análisis y Gestión del Riesgo.
- Identificación de riesgos
- Evaluación de los posibles tratamientos del riesgo
- Elaboración de un Declaración de Aplicabilidad de controles y requisitos
- Desarrollo de un Plan de Tratamiento de Riesgos
- Definición de métricas e indicadores de la eficiencia de los controles
- Desarrollo de programas de formación y concienciación en seguridad de la información
- Gestión de recursos y operaciones
- Gestión de incidencias
- Elaboración de procedimientos y documentación asociada

Como otras Normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta Norma aplican a todo tipo de Organizaciones, independientemente de su tipo, tamaño o área de actividad. Asimismo, está basada en un enfoque por procesos y en la mejora continua, por lo tanto, es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la Organización.

(poveda, 2011) La Norma fue publicada en el año 2007, pero tiene una larga historia antes de llegar a este punto.
En el año de 1995 el British Standard Institute (BSI) publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.

En vista de la gran aceptación de esta Norma, en 1998, el BSI pública la norma BS7799-2, Especificaciones para los sistemas de gestión de la seguridad de la información. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en el año 2002 y denominada ISO/IEC 17799 en el año 2005.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27001 y en octubre del 2007 la norma ISO 27001 se adopta también por IEC. Con

la publicación de la ISO/IEC 27001, dejó de estar vigente la UNE 71502 y las empresas nacionales se certifican ahora únicamente con esta nueva norma (UNE-ISO/IEC 27001).

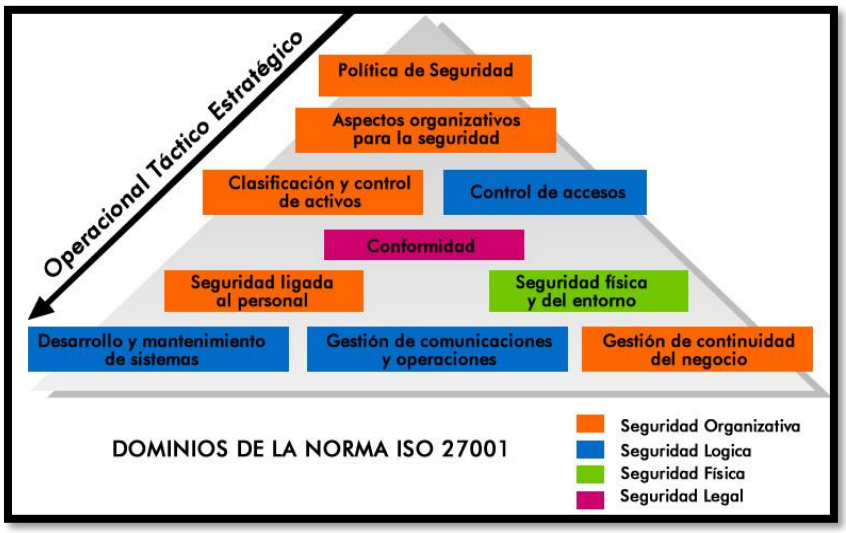


Figura 6: Contenido de la norma ISO 27001

Fuente: UNE-ISO/IEC 27001

La norma ISO/IEC 27001 da a conocer las pautas para elaborar una metodología para un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro del contexto de los riesgos identificados por la Organización.

Los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

La Norma ISO 27001 permite la elaboración de una metodología para:

- Los componentes del SGSI, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.
- Cómo se debe implantar el SGSI.
- Define los controles que deberán ser adaptados a la realidad de una organización para proceder a la implantación de la metodología que se estime conveniente.
- La ISO 27001 permite elaborar una metodología que adopte un proceso estructurado para implementar un SGSI.

2.2.4. GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

El termino gestión según la definición de la Real Academia de la Lengua Española es la Acción y efecto de gestionar (Hacer diligencias conducentes al logro de un negocio o de un deseo cualquiera).

La Gestión de la Tecnología de la Información es un conjunto de disciplinas de gestión que permite a las organizaciones crear ventajas competitivas a partir de fundamentos tecnológicos.
En cuanto a las disciplinas de Gestión, Según Información Technology Infraestructure Library (ITIL) las áreas de gestión son: Gestión de Servicios, Gestión de Infraestructura, Gestión de las Aplicaciones y Gestión de la seguridad.

Según SICELCA IT SYSTEMS la Gestión de Tecnología de Información es una disciplina de gestión basada en procesos horizontales diseñados para facilitar una metodología orientada al cliente, mejorando considerablemente la alineación entre la organización de TI (Proveedora de Servicios de TI) y los clientes (usuarios responsables del uso de estos servicios para el cumplimiento de los objetivos del negocio) poniendo énfasis en los beneficios que puede percibir el cliente final.

Según Herrán, J (2001) define a la Gestión de Tecnología de Información como un conjunto de capacidades organizacionales especializadas para proveer valor a los clientes en forma de servicios.

Dichas capacidades organizacionales incluyen: Procesos, Métodos, Funciones, Roles, Actividades. A cargo de los directores de Tecnología de Información, responsables técnicos de lograr las metas.
Meta: Tener capacidad y recursos disponibles en los servicios para que estos sean útiles y aceptables por el cliente considerando la calidad, costos y riesgos respectivos.

Un proveedor debe ofrecer servicios que otorguen valor a sus clientes y debe desarrollar un sistema de administración de servicios dinámico.
Según ISACA que considera que, en la mayoría de las empresas, el gobierno de Tecnología de Información es responsabilidad del consejo de administración bajo la dirección de su presidente.

Definiendo a la Gestión de tecnología de Información como: La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

2.2.5. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

La ISO 27000 en su página web www.iso27000.es define al SGSI de la siguiente forma:

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

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

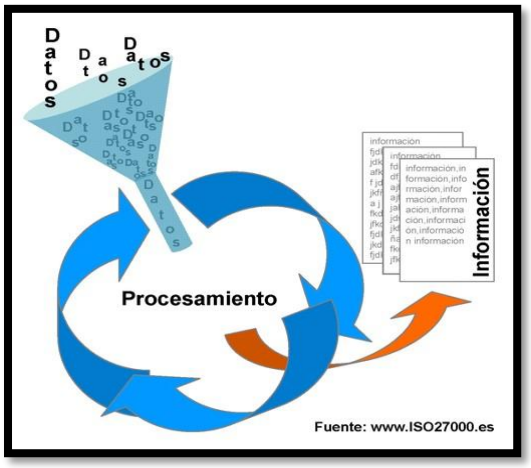


Figura 7: Sistema de gestión de la seguridad de la información
fuente: www.iso .es

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así

pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

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

A. PARA QUE SIRVE UN SGSI

La ISO 27000 en su página web www.iso27000.es define al SGSI de la siguiente forma:

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos

provocados accidentalmente por catástrofes naturales y fallos técnicos.

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

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

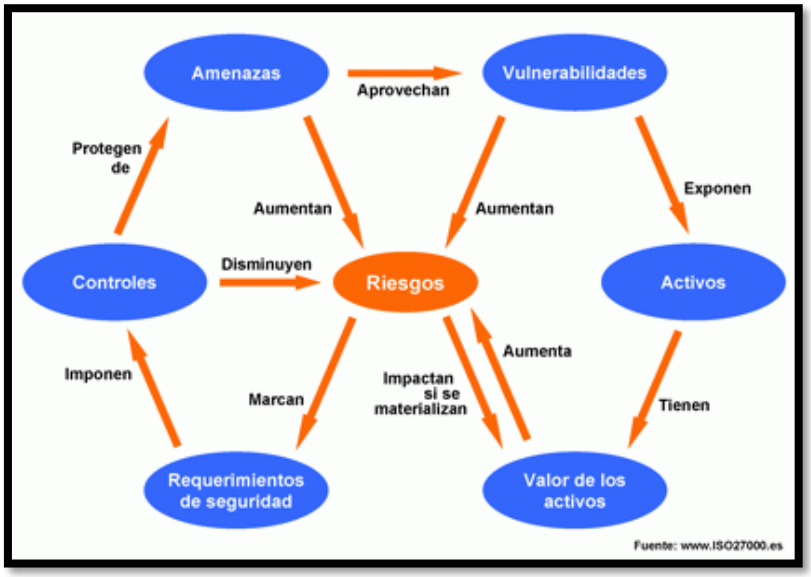


Figura 8: Modelo de gestión de seguridad
Fuente: www.iso27000.es

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un

nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

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

B. QUE INCLUYE UN SGSI

La ISO 27000 en su página web www.iso27000.es define al SGSI de la siguiente forma:

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

Figura 9: Pirámide del SGSI basado en ISO 27001

Fuente: www.iso27000.es

Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y

determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

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

Documentos de Nivel 3

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

Documentos de Nivel 4

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

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

- Alcance del SGSI: ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).
- Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Procedimientos y mecanismos de control que soportan al SGSI: aquellos procedimientos que regulan el propio funcionamiento del SGSI.

- Enfoque de evaluación de riesgos: descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- Procedimientos documentados: todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- Registros: documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- Declaración de aplicabilidad: (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

CONTROL DE LA DOCUMENTACIÓN

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

- Aprobar documentos apropiados antes de su emisión.

- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

3. CAPÍTULO III: PROPUESTA DE SOLUCIÓN

3.1. MODELO CONCEPTUAL

Para el desarrollo del presente proyecto se toma como modelo la ISO 27001 que permite una adecuada gestión de la seguridad de la información, que se basa en políticas y medidas de control. Se observa que la ISO 27001 se centra en garantizar la confidencialidad, integridad y disponibilidad de la información.

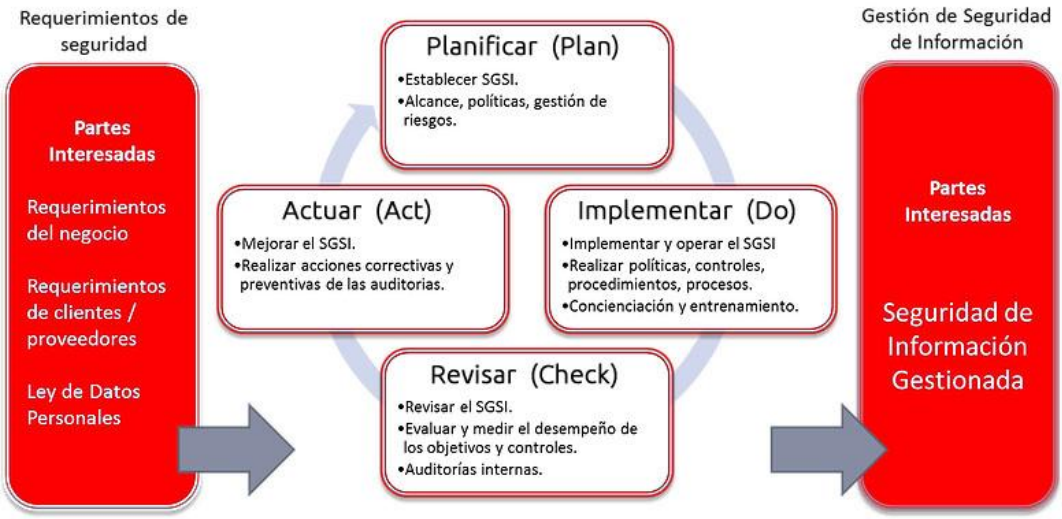


Figura 10: Modelo conceptual del SGSI

Fuente: *www.iso27000.es*

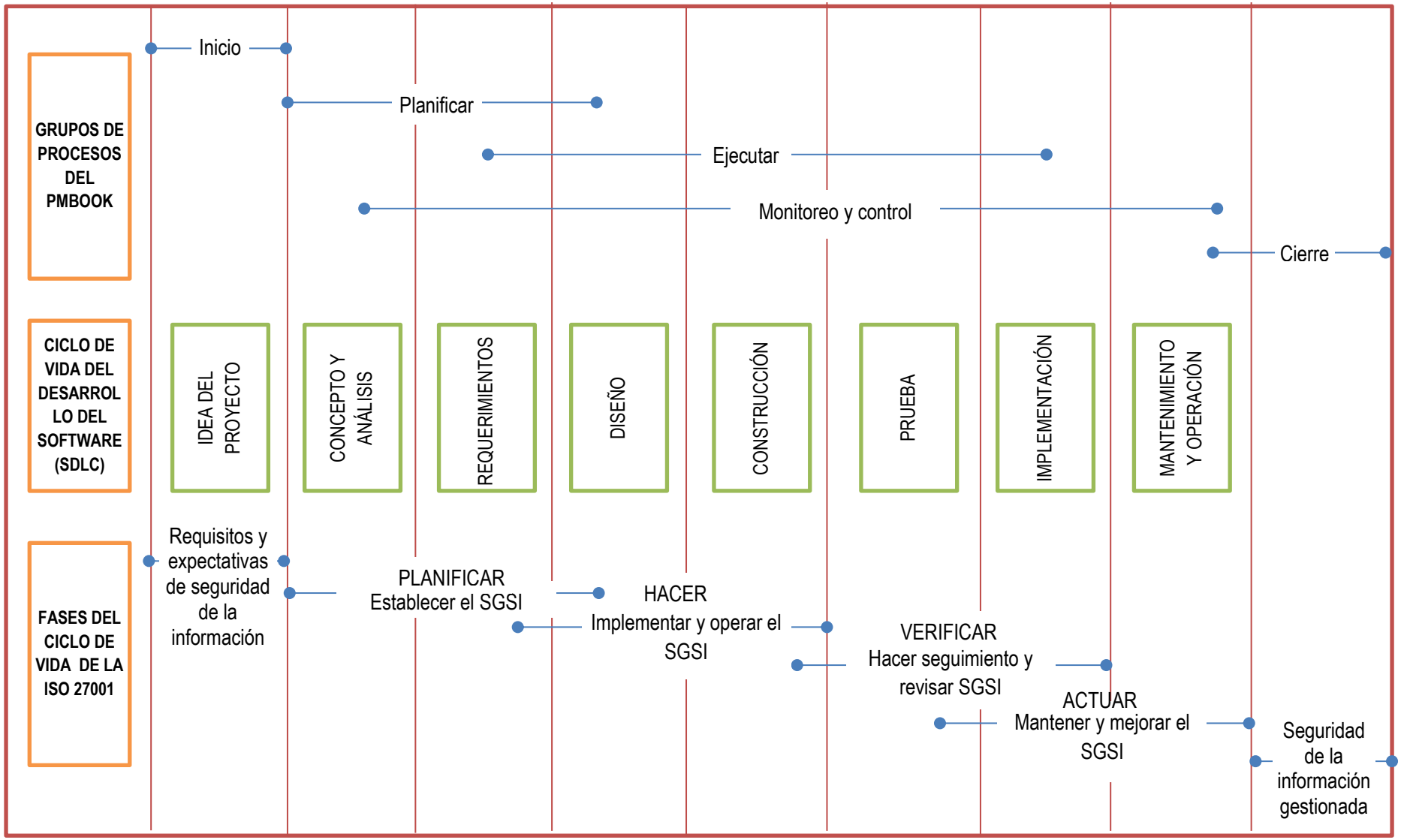


Figura 11: Modelo conceptual del proyecto
Fuente: Elaboración propia

3.2. GESTIÓN DEL PROYECTO

Para la elaboración del plan del proyecto de tesis se ha tomado como referencia los conocimientos, técnicas y prácticas vigentes, para la gestión exitosa de proyectos reunidas por el PMI (Project Management Institute) en el documento llamado PMBOK (Project Management Body of Knowledge) quinta edición.

A continuación, se muestra las áreas de conocimiento y los procesos que se tomaran en cuenta para el presente proyecto de tesis:

3.2.1. PROCESOS DE LA DIRECCIÓN DEL PROYECTO

Se agrupan en 5 procesos los cuales son:

- **El grupo de procesos de iniciación**: Aquí se encuentran los procesos que definen el proyecto de investigación en el área de Sistemas de información de la UNAJMA.
- **El grupo de procesos de planificación:** En este grupo de procesos se definen los procesos que establecen el alcance del proyecto, definir objetivos y acciones a tomar para alcanzar los objetivos.
- **El grupo de procesos de ejecución:** en este grupo se encuentran los procesos que se realizarán para completar el proyecto.
- **El grupo de procesos de seguimiento y control:** en este grupo se encuentran los procesos que se usaran para dar seguimiento, analizar y regular el progreso y el desempeño del proyecto, además que permitirá identificar áreas en las que el proyecto requiere cambios.
- **El grupo de procesos de cierre:** En este grupo están los procesos que permitirán finalizar todas las actividades a fin de cerrar formalmente el proyecto de investigación en el área de tecnologías de información de la UNAJMA**.**

3.2.2. ÁREAS DE CONOCIMIENTO

En la versión actual de PMBOK (5ta. Edición), cuenta con 10 áreas de conocimiento, con las cuales se desarrolla el presente proyecto:

A. Gestión de la Integración del Proyecto: El proyecto está basado en las políticas y medidas de control de la ISO 27001; dedicada a la parte del modelo conceptual.

La gestión del proyecto está dada por la integración de los conocimientos, técnicas y prácticas vigentes en el PMBook.

Tabla 9: Gestión de Integración del Proyecto

Proyecto	**Sistema web de Gestión de Seguridad de la Información Asistida por Computadora basada en el estándar ISO 27001 en la Universidad Nacional José María Arguedas.**		
Patrocinador	**Jefe de proyecto:** Andrea Margot Ochoa Tapia		
Preparado por	**Jefe de Proyecto:** Andrea Margot Ochoa Tapia	**Fecha**	10/11/2016
Revisado por	**Jefe de Proyecto:** Andrea Margot Ochoa Tapia	**Fecha**	10/11/2016
Aprobado por	**Jefe de Proyecto:** Andrea Margot Ochoa Tapia	**Fecha**	15/11/2016
REVISIÓN	**DESCRIPCIÓN**		**FECHA**
1	Preparación de acta de constitución (Andrea Margot Ochoa Tapia)		15/11/2016
BREVE DESCRIPCIÓN DE LA APLICACIÓN WEB DEL PROYECTO			
El proyecto incluirá el desarrollo de un Sistema Web de Gestión de la Seguridad de la Información que beneficiara a las áreas académicas y administrativas de la Universidad Nacional José María Arguedas garantizando la confidencialidad, integridad y disponibilidad de la información que es el activo más valioso de la organización			
ALINEAMIENTO DEL PROYECTO			
OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN	**PROPÓSITO DEL PROYECTO**		
Desarrollar talleres de capacitación en el uso del sistema web al personal de la oficina de sistemas de información de la UNAJMA.	Promover el funcionamiento y la utilización de la aplicación.		
OBJETIVOS DEL PROYECTO			
1. Analizar y diseñar los procesos y controles de gestión de la seguridad de la información de la Universidad Nacional José María Arguedas.			
2. Construir y probar eficientemente las medidas y controles de gestión de la seguridad de la información en la Universidad Nacional José María Arguedas.			
3. Implementar y desplegar los controles del sistema de gestión de seguridad de la información en la Universidad Nacional José María Arguedas.			
FACTORES CRÍTICOS DE ÉXITO DEL PROYECTO			
4. Disposición de las herramientas para el desarrollo de la aplicación web dentro de los plazos establecidos.			
5. Diseño de la aplicación web acorde a los requerimientos de los interesados			
REQUERIMIENTO DE ALTO NIVEL			
1. La aplicación debe ser desarrollada exactamente de acuerdo a los requerimientos funcionales planteados.			
EXTENSIÓN Y ALCANCE DEL PROYECTO			
FASES DEL PROYECTO	**PRINCIPALES ACTIVIDADES**		
FASE I: ANÁLISIS	Acta de constitución del proyecto		
	Análisis de la información recolectada		
	Análisis de los requerimientos funcionales		
	Análisis de los requerimientos no funcionales		
	Diagrama de caso de usos		

	Diagrama de secuencias
FASE II: DISEÑO	Diseño de la base de datos
	Diseño de navegación
FASE III: CODIFICACIÓN	Adquisición de la laptop
	Adquisición de las herramientas de desarrollo
	Codificación
FASE IV: PRUEBAS	Pruebas durante el desarrollo
	Pruebas unitarias
	Pruebas integradas
INTERESADOS CON EL PROYECTO	
1. Personal Administrativo de la Oficina de Sistemas de Información de la UNAJMA	
2. Programador o desarrollador	
RIESGOS	
1. Demora en la adquisición de la laptop y las herramientas de desarrollo.	
2. Poca información brindada y tiempo disponible por los interesados.	
3. Retraso en la programación	
HITOS PRINCIPALES DEL PROYECTO	
1. Aprobación del acta de constitución del proyecto.	
2. Alcanzar todos los objetivos trazados.	
3. Pruebas y correcciones de la aplicación.	
PRESUPUESTO DEL PROYECTO	
El costo del proyecto que haciende a la suma total de veinticinco mil cientos ochenta y cinco con 5/100 soles S/ 25 185.05, el cual es asumido en su totalidad por el jefe del proyecto.	

Fuente: Elaboración propia

B. Gestión del Alcance del Proyecto: El alcance del proyecto que tiene el Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas, está dirigido directamente al personal de la Oficina de Sistemas de Información, además para la gestión de la seguridad de la información se basará únicamente en las políticas y medidas de control del estándar ISO 27001, reduciendo los riesgos e incrementando las medidas de control para dar mayor seguridad a los activos más valiosos de la UNAJMA, para lo cual se utiliza la Estructura de Descomposición de Trabajo (EDT).

La Estructura de Descomposición de Trabajo Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas, está compuesta por cuatro (04) fases, en las cuales se describe cada una de las actividades realizadas, tal como se muestra en la figura 12.

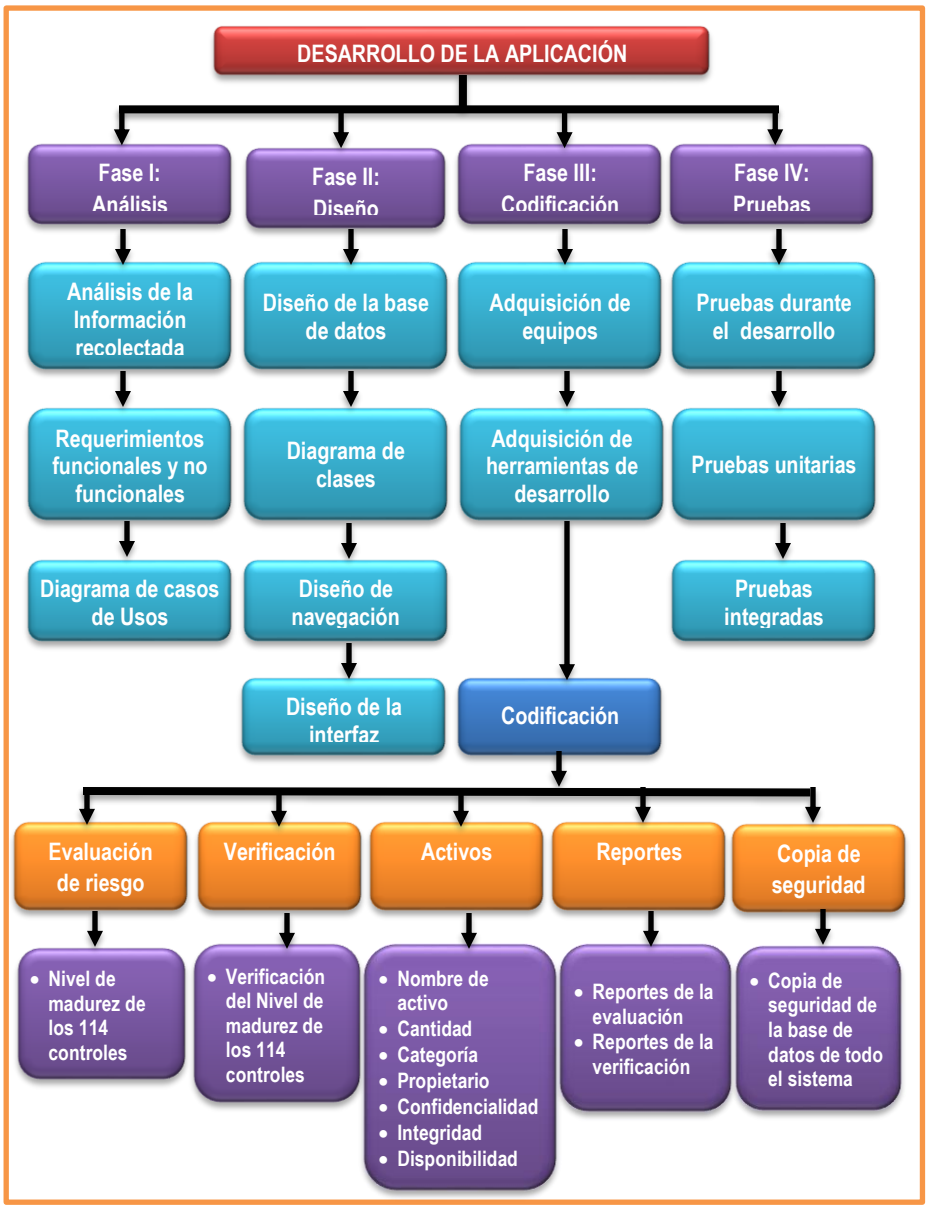


Figura 12: Estructura de Descomposición de Trabajo (EDT)
Fuente: Elaboración Propia

C. Gestión del Tiempo del Proyecto: la gestión de tiempo del proyecto se llevó a cabo a través de un diagrama GANT teniendo una ruta crítica de 6 actividades que a continuación se detalla:

- **ELABORACIÓN DEL PROYECTO DE INVESTIGACIÓN:** La elaboración del proyecto de investigación, tiene un tiempo de duración de 70 días dando inicio el lunes 18 de julio del

2016 hasta el día viernes 21 de octubre del 2016 sin tomar en cuenta los días sábados y domingos.

- **SOLICITUD DE JURADOS Y APROBACIÓN DE PROYECTO DE INVESTIGACIÓN:** La solicitud de jurados y la aprobación del proyecto de investigación, tiene un tiempo de duración de 17 días dando inicio el día lunes 24 de octubre hasta el martes 15 de noviembre de 2016.

- **ELABORACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS:** La elaboración de instrumentos de recolección de datos, tiene una duración de 30 días, dando inicio el día lunes 21 de noviembre hasta el día viernes 30 de diciembre del 2016.

- **DESARROLLO DEL SGSI:** El desarrollo del SGSI, tiene un tiempo de duración de 190 días iniciando el día lunes 06 de febrero de 2016 hasta el día viernes 27 de octubre de 2017 y se divide en 5 faces que se menciona a continuación.

    - Análisis de SGSI: tiene un tiempo de duración de 30 días iniciando el día lunes 06 de febrero y culmina el día viernes 17 de marzo de 2017.

    - Diseño de SGSI: tiene un tiempo de duración de 50 días iniciando el día lunes 20 de marzo y culmina el día viernes 26 de mayo de 2017.

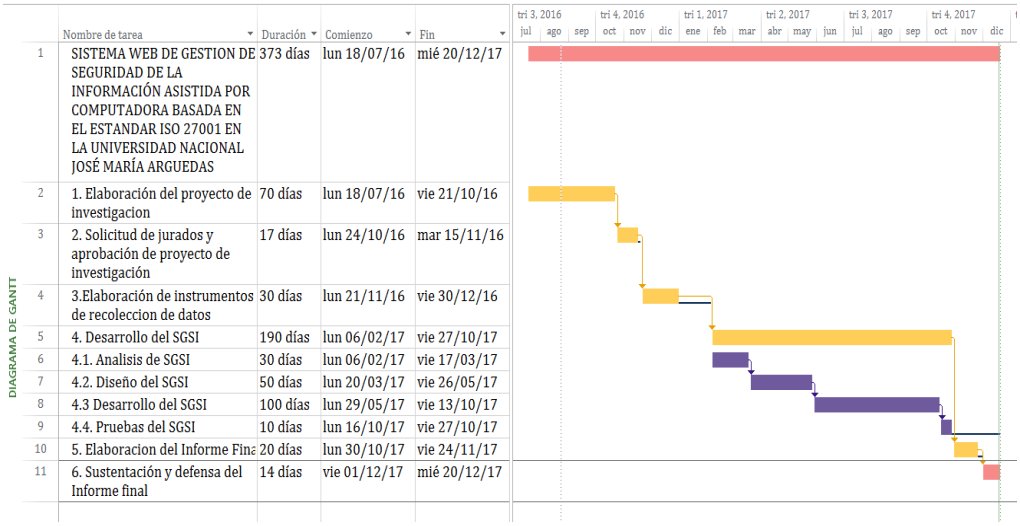
    - Desarrollo del SGSI: tiene un tiempo de duración de 100 días iniciando el día lunes 29 de mayo y culmina el día viernes 13 de octubre 2017.

- Pruebas de SGSI: tiene un tiempo de duración de 10 días iniciando el día lunes 16 de octubre y culmina el día viernes 27 de octubre de 2017.

- **ELABORACIÓN DEL INFORME FINAL:** La Elaboración del Informe Final de tesis, tiene un tiempo de duración de 20 días, iniciando el día lunes 30 de octubre hasta el viernes 24 de noviembre de 2017.

- **SUSTENTACIÓN Y DEFENSA DEL INFORME FINAL:** La Sustentación y defensa de la tesis, tiene un tiempo de duración de 14 días dando inicio el día viernes 01 de diciembre hasta el miércoles 20 de diciembre de 2017.

El proyecto está estimado en un tiempo de duración de 373 días, dando inicio el día lunes 18 de julio del 2016 con la recopilación de información y se sustentará el Informe Final de tesis final el día miércoles 20 de diciembre del 2017, el mismo que se realizó en un diagrama de Gantt, tal como se muestra en figura 13.



	Nombre de tarea	Duración	Comienzo	Fin
1	SISTEMA WEB DE GESTION DE SEGURIDAD DE LA INFORMACIÓN ASISTIDA POR COMPUTADORA BASADA EN EL ESTANDAR ISO 27001 EN LA UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS	373 días	lun 18/07/16	mié 20/12/17
2	1. Elaboración del proyecto de investigacion	70 días	lun 18/07/16	vie 21/10/16
3	2. Solicitud de jurados y aprobación de proyecto de investigación	17 días	lun 24/10/16	mar 15/11/16
4	3.Elaboración de instrumentos de recoleccion de datos	30 días	lun 21/11/16	vie 30/12/16
5	4. Desarrollo del SGSI	190 días	lun 06/02/17	vie 27/10/17
6	4.1. Analisis de SGSI	30 días	lun 06/02/17	vie 17/03/17
7	4.2. Diseño del SGSI	50 días	lun 20/03/17	vie 26/05/17
8	4.3 Desarrollo del SGSI	100 días	lun 29/05/17	vie 13/10/17
9	4.4. Pruebas del SGSI	10 días	lun 16/10/17	vie 27/10/17
10	5. Elaboracion del Informe Fina	20 días	lun 30/10/17	vie 24/11/17
11	6. Sustentación y defensa del Informe final	14 días	vie 01/12/17	mié 20/12/17

Figura 13: Cronograma de Actividades

Fuente: Elaboración Propia

D. **Gestión de los costos del proyecto:** la gestión de costos del proyecto se basará el 5 Ítems que se mencionado en la tabla 10 Presupuesto, que se detalla a continuación.

Ítem 1: bienes, dividido en Materiales de Escritorios y Materiales Consumibles que haciende a la suma de S/ 4000.00 y S/ 655.50 respectivamente haciendo un total de S/ 4655.50 soles.

Ítem 2: Servicios, dividido en Servicios de Comunicación, Servicios de Movilidad, Servicios de Alimentación y Servicios de Impresión que haciende a la suma de S/ 440.00, S/ 600.00, S/ 2 000.00 y S/ 1 200.00 respectivamente haciendo un total de S/. 4 240.00 soles.

Ítem 3: Software, dividido en Desarrollo del sistema y Desarrollo del proyecto, para el desarrollo del sistema se usará software libre por lo que no genera gasto alguno, y se invertirá S/1,000.00 soles para el desarrollo del proyecto.

Ítem 4: Recursos Humanos, dividido en Asesores y Desarrollo del sistema, que hacienden a la suma de S/4000.00 y S/ 9 000.00 respectivamente haciendo un total de S/ 13 000.00 soles.

Ítem 5: Gastos Generales, En este Ítem se consideran los gastos imprevistos que es el 10% de la suma total del proyecto haciendo un total de S/ 2 089.55 soles.

El costo de proyecto en los 5 ítems antes mencionados haciende a un total de S/ 25 185.05 soles.

Tabla 10: Gestión de Integración del Proyecto

ITEM	DESCRIPCION	Cant.	UNID. MEDIDA	PRECIO UNITARIO	PRECIO PARCIAL
1.00.00	BIENES				**4655.50**
1.01.00	Materiales de escritorio				**4000.00**
1.01.01	Laptop	1	Unid	3.000,00	3000.00
1.01.02	Disco Duro Externo de 1 TB	1	Unid	300,00	300.00
1.01.03	Impresora EpsonL355 Multifuncional	1	Unid	700,00	700.00
1.02.00	Materiales Consumibles				**655.50**
1.02.01	Papel Bond A4	8	Millar	25.00	200.00
1.02.02	tinta Epson L355	8		45.00	360.00
1.02.03	lápices	1	caja	10.00	10.00
1.02.04	lapiceros	1	caja	45.00	45.00
1.02.05	Borradores	1	caja	10.00	10.00
1.02.06	Correctores	3	Unid	7.00	21.00
1.02.07	Tajador	2	Unid	1.00	2.00
1.02.08	resaltador	3	Unid	2.50	7.50
2.00.00	SERVICOS				**4,240.00**
2.01.00	Servicios comunicación				**440.00**
2.01.01	Internet	4	Mes	60.00	240.00
2.01.02	teléfono	4	Mes	50.00	200.00
2.02.00	servicios de movilidad				**600.00**
2.02.03	Pasajes	4	mes	150.00	600.00
2.03.00	servicios de Alimentación				**2,000.00**
2.03.01	desayuno	4	Mes	150.00	600.00
2.03.02	Almuerzo	4	Mes	200.00	800.00
2.03.03	Cena	4	Mes	150.00	600.00
2.04.00	servicios de impresión				**1,200.00**
2.04.01	fotocopias	4	Mes	100.00	400.00
2.04.02	impresiones	4	Mes	200.00	800.00
3.00.00	Software				**1000**
3.01.00	Desarrollo del sistema				**0.00**
3.01.01	Lenguaje de programación (Software libre)	1	Unid	-	-
3.02.00	Desarrollo del proyecto				**1,000.00**
3.02.01	licencia de antivirus	1	Unid	200.00	200.00
3.02.02	Microsoft office	1	Unid	500.00	500.00
3.02.03	Project profesional	1	Unid	300.00	300.00
4.00.00	RECURSOS HUMANOS				**13,000.00**
4.01.00	Asesores	1	persona	4,000.00	**4,000.00**
4.02.00	Desarrollo del sistema				**9,000.00**
4.02.01	Analista	1	persona	1,000.00	1,000.00
4.02.02	Diseñador	1	persona	1,000.00	1,000.00
4.02.03	Programador	1	persona	3,000.00	3,000.00
4.02.04	Prueba e implementación	1	persona	2,000.00	2,000.00
4.02.05	Capacitación	1	persona	2,000.00	2,000.00
5.00.00	GASTOS GENERALES				**2089.55**
	Imprevistos				
	Imprevistos 10% del costo total	1	Unid	2089.55	2089.55
	COSTO TOTAL DE LA TESIS				**25,185.05**

Fuente: Elaboración Propia

E. Gestión de la Calidad del Proyecto: la gestión de la calidad del proyecto se desarrollará de acuerdo a los siguientes ítems:

ASEGURAR LA CALIDAD

El proceso para asegurar la calidad de la aplicación web se realizó mediante la ISO/IEC 9126 (parte 1,2 y 3) tanto en la parte interna como externa de la aplicación.

- Se empleó en la aplicación web aun no ejecutable.
- Se empleó durante las etapas de desarrollo.
- Permitió entregar entregables intermedios de calidad.
- Permitió realizar acciones correctivas tempranas en el ciclo de su desarrollo.
- Permitió el resultado final de aplicación web de calidad.

Tabla 11: Modelo utilizado en la medición de Calidad

	FASE	ENTREGABLES CLAVES	MÉTRICAS UTILIZADAS
Actividad 1	Análisis	Análisis de la información recolectada Análisis de los requerimientos no funcionales Diagrama de casos de uso Diagrama de secuencias	Internas
Actividad 2	Diseño	Diseño de la base de datos Diseño de clases Diseño de navegación Definición de las interfaces abstractas.	Internas
Actividad 3	Codificación		Internas y externas
Actividad 4	Pruebas	Resultados de prueba durante el desarrollo Resultados de pruebas unitarias Resultados de pruebas integradas.	Internas y externas

Fuente: Elaboración Propia

Tabla 12: Requisitos de calidad Identificados

CARACTERÍSTICAS	SUB CARACTERÍSTICAS
Usabilidad	Entendible Atractivo
Funcionalidad	Exactitud Seguridad
Portabilidad	Instalación Compatibilidad

Fuente: Elaboración Propia

Tabla 13: Evaluación en los Requisitos de Calidad

CARACT.	SUB CARACT.	ENTREGABLES EVALUADAS	MÉTRICAS INTERNAS APLICADAS	MÉTRICAS EXTERNAS APLICADA
Usabilidad	Entendible	1. Interfaz de ingreso de activos 2. Interfaz evaluación de riesgo. 3. Interfaz de la verificación. 4. Interfaz de los reportes de evaluación, verificación y activos.	1. Cruce de las relaciones de BD 2. Líneas de códigos. 3. Funciones 4. Procedimientos 5. Atributos enteros 6. Atributos de cadena de caracteres.	1. Tiempo que toma en cargar las interfaces 2. Tiempo de navegación en las interfaces
	Atractivo		Tipografías clara	Tiempo en que toma en cargar las interfaces
Funcionalidad	Exactitud	1. Evaluación de riesgo basada en la ISO 270001 2. Verificación de riesgos. del riesgo 3. Reportes de la evaluación. 4. Reportes de la verificación 5. Ingreso de los activos de la institución.	1. Conexión entidad /relación 2. Atributos enteros 3. Atributos de cadena de característica 4. Funciones 5. Procedimientos 6. Líneas de códigos	1. Tiempo que toma en la evaluación de los controles de seguridad. 2. Tiempo que toma en ingresar los activos de la institución
	Seguridad	1. Logueo (user y password) 2. Copias de seguridad		1. Tiempo de autenticación 2. Tiempo que toma en hacer una copia de seguridad
Portabilidad	Instalación	Ingreso de URL de la página web	Conexión a internet	Tiempo de carga de la página web
	Compatibilidad			

Fuente: Elaboración propia

Tabla 14: Resultado de la evaluación de los requisitos de calidad

CARACT.	SUB CARACT.	MÉTRICA	NIVEL REQUERIDO	NIVEL OBTENIDO
Usabilidad	Entendible	Interna y externa	100%	100%
	Atractivo	Interna y externa	100%	98%
Funcionalidad	Exactitud	Interna y externa	100%	100%
	Seguridad	Interna y externa	100%	100%
Portabilidad	Instalación	Interna y externa	100%	100%
	Compatibilidad	Interna y externa	100%	100%

Fuente: Elaboración propia

CONTROL DE CALIDAD

El control de calidad se realizó con éxito utilizando las técnicas y actividades de la ISO/IEC 9126 (parte 1,2 y 3)

Calidad de funcionalidad, usabilidad y portabilidad con el usuario

Se realizó pruebas de funcionamiento para corroborar que se cumpla los requisitos planteados en los casos de usos, así mismo se realizó las pruebas de usabilidad para verificar que el sistema sea entendible al usuario y por último se realizó la prueba en diferentes dispositivos electrónicos que son capaces de conectarse a internet, y puedan acceder desde cualquier parte del país.

F. Gestión de los Recursos Humanos del Proyecto: La gestión de Recursos Humanos se desarrolló de acuerdo al planificador organizacional del personal involucrado en el proyecto tal como se muestra en la figura 14.

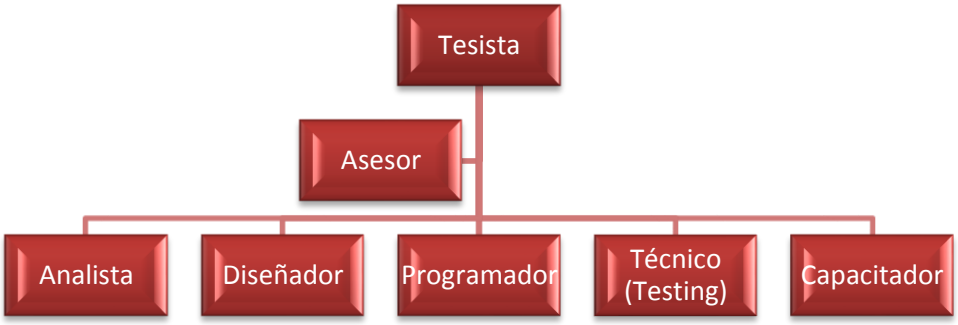


Figura 14: Organigrama del personal involucrado
Fuente: Elaboración propia

Tabla 15: Perfil de Recursos Humanos del Proyecto

PERSONAL	PERFIL
Tesista	Bachiller en Ingeniería de Sistemas.
Asesor	Doctor en Ingeniería de sistemas. Magister en Administración de negocios. Ingeniero de sistemas y computación.
Analista	• Conocimiento en ingeniería del software y ciclo de vida del software en cascada. • Modelado funcional: Diagrama de flujo de datos, diagrama de estado. • Modelado de datos y sus técnicas: Diagrama entidad-relación, modelo relacional. • Conocimiento de la tecnología: arquitectura de software, bases de datos.
Diseñador	***Dominio*** de ***HTML***, ***CSS***, Conocimientos de Javascript y ***JQuery***. Conocimientos de CMS Wordpress.
Programador	• Entre sus conocimientos destacan lenguajes del lado del servidor como Java, .NET, PHP y gestor de base de datos MySql.
Técnico (testing)	• Capacidad para detectar las disconformidades y los errores. • mantenimiento: la corrección de los errores después de la salida del programa informático, y la mejora para hacer evolucionar el producto.
Capacitador	El objetivo general del capacitador es lograr la adaptación de personal para el ejercicio y dominio del software.

Fuente: Elaboración propia

Tabla 16: Asignación de responsabilidad al personal

ÍTEM	ROL	PERFIL	FUNCIONES	RESULTADOS
1	Asesor	Asesoría	Asesorar	Cumplido
			Revisar	Cumplido
2	Programador	PHP	Analizar	Cumplido
			Diseñar	Cumplido
			Implementar	Cumplido
			Realizar pruebas	Cumplido

Fuente: Elaboración propia

G. Gestión de las Comunicaciones del Proyecto: la Gestión de comunicación del proyecto se realizó mediante reuniones programadas con el asesor durante el desarrollo del proyecto e informe final de acuerdo a la siguiente manera:

Tabla 17: Reunión con el asesor

REUNIÓN CON EL ASESOR DE TESIS	
Frecuencia	Una vez a la semana
Día de la semana	Los días viernes
Duración	3 horas
Agenda	Revisión del avance del informe Observaciones del informe Correcciones del informe

Fuente: Elaboración propia

H. Gestión de los riesgos del proyecto: La Gestión de riesgos de proyecto se identificó de acuerdo a las categorías de riesgo de la ISO 31000 tal como se muestra en la figura 15.

Figura 15: Categorías de riesgo
Fuente: www.iso31000.com

Prestamos: será considerado medio por la necesidad de ellos y un eventual recorte de estos en el futuro podría representar un riesgo para el proyecto.

Mal especificados: será considerado bajo por que los profesionales que ejecutan el proyecto tienen un amplio conocimiento.

Daños de Equipos: será considerado bajo ya que se cuenta con garantía de los equipos por su reciente adquisición.

Cambio de Leyes: Podrían ser más exigentes y por ende involucrar mayor inversión en un determinado momento, en tanto es considerado medio.

Trabajos defectuosos: es considerado bajo ya que se trabaja con una adecuad planificación y diseño.

Obsolescencia: Los quipos e instalaciones serán nuevas con un mínimo de 3 años de vida útil siendo el horizonte del proyecto de 1.5 años, en tanto se considera bajo.

Tabla 18: Probabilidad de riesgo

	PROBABILIDAD DE QUE SUCEDA	IMPACTO	RIESGO
Préstamo	2	3	5
Mal especificado	1	3	4
Daño de equipos	1	3	4
Cambios de leyes	2	3	5
Trabajos defectuosos	1	3	4
Obsolescencia	1	3	4

Fuente: Elaboración propia

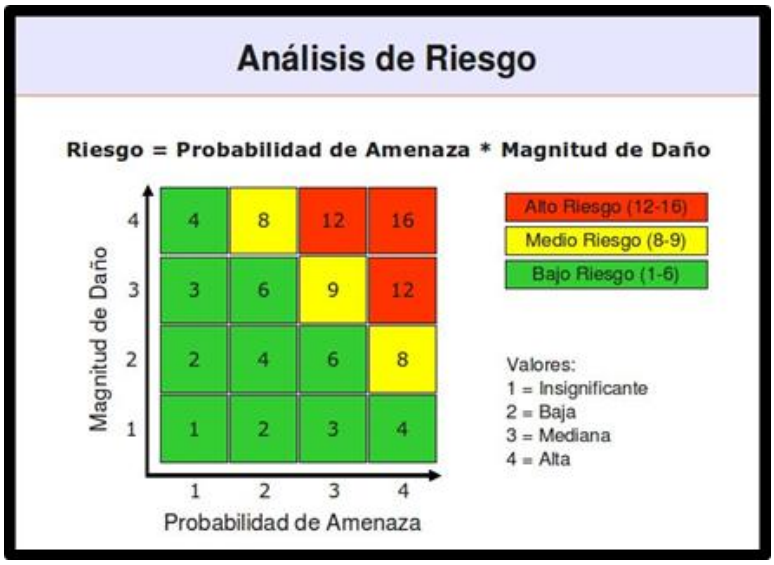


Figura 16: Análisis de riesgo
Fuente: Elaboración propia

El proyecto alcanza valores de 5, 4, 4, 5, 4 y 4 considerando como de Bajo riesgo.

I. **Gestión de las Adquisiciones del Proyecto:** La gestión de las adquisiciones del proyecto se desarrollará de la siguiente manera:

Tabla 19: Gestión de las adquisiciones del proyecto

ESCRIPCIÓN	CANT	PRECIO UNITARIO (S/)	PRECIO PARCIAL (S/)	FORMA DE ADQUISICIÓN	MESES				
					2015				
					JULIO	AGOSTO	SETIEMBRE	OCTUBRE	NOVIEMBRE
BIENES			**4.655,50**						
Materiales de escritorio		**4.000,00**	**4.000,00**						
Laptop	1	3.000,00	3.000,00	compra	3.000,00				
Disco Duro Externo de 1 TB	1	300,00	300,00	compra	3.000,00				
Impresora EpsonL355 Multifuncional	1	700,00	700,00	compra	700,00				
Materiales Consumibles			**655,50**						
Papel Bond A4	8	25,00	200,00	compra		200,00			
tinta Epson L355	8	45,00	360,00	compra		360,00			

Lápices	1	10,00	10,00	compra		10,00			
Lapiceros	1	45,00	45,00	compra		45,00			
Borradores	1	10,00	10,00	compra		10,00			
Correctores	3	7,00	21,00	compra		21,00			
Tajador	2	10,00	2,00	compra		2,00			
Resaltador	3	2,50	7,50	compra		7,50			
SERVICOS			**4.240,00**						
Servicios comunicación		**110,00**	**440,00**						
Internet	4	60,00	240,00	Alquiler	60,00	60,00	60,00	60,00	
Teléfono	4	50,00	200,00	Alquiler	50,00	50,00	50,00	50,00	
Servicios de movilidad		**150,00**	**600,00**						
Pasajes	4	150,00	600,00	compra	150,00	150,00	150,00	150,00	
Servicios de Alimentación		**500,00**	**2.000,00**						
Desayuno	4	150,00	600,00	compra	150,00	150,00	150,00	150,00	
Almuerzo	4	200,00	800,00	compra	200,00	200,00	200,00	200,00	
Cena	4	150,00	600,00	compra	150,00	150,00	150,00	150,00	
Servicios de impresión		**300,00**	**1.200,00**						
Fotocopias	4	100,00	400,00	compra		100,00	100,00	100,00	100,00
Impresiones	4	200,00	800,00	compra		200,00	200,00	200,00	200,00
SOFTWARE			**1.000,00**						
Desarrollo del proyecto		**300,00**	**1.000,00**						
Licencia de antivirus	1	200,00	200,00	compra	200,00				
Microsoft office	1	500,00	500,00	compra	500,00				
Project profesional	1	300,00	300,00	compra	300,00				
RECURSOS HUMANOS			**13.000,00**						
Asesores	**1**	**4.000,00**	**4.000,00**		1.000,00	1.000,00	1.000,00	1.000,00	
Desarrollo del sistema			**9.000,00**						
Analista	1	1.000,00	1.000,00	Contrato		500,00	500,00		
Diseñador	1	1.000,00	1.000,00	Contrato		1.000,00			
Programador	1	3.000,00	3.000,00	Contrato		1.000,00	1.000,00	1.000,00	
Prueba e implementación	1	2.000,00	2.000,00	Contrato			500,00	500,00	1.000,00
Capacitación	1	2.000,00	2.000,00	Contrato					2.000,00
Imprevisto 10%	1	2.289,55	2.289,55		457,91	457,91	457,91	457,91	457,91
FLUJO DE CAJA		**∑**	**25.185,05**		**9.917,91**	**5.673,41**	**4.517,91**	**4.017,91**	**3.757,91**

Fuente: Elaboración Propia

3.3. DESARROLLO DE APLICACIÓN WEB

El desarrollo de la aplicación web, se basó en cuatro fases de la metodología XP (Programación Extrema), debido a que permite gestiona de manera ágil y flexible el proyecto.

3.3.1. FASE 1: ANÁLISIS

A. Análisis de la información recolectada

Análisis de los participantes: los participantes de la investigación se detallan en la figura 17 que se muestra a continuación:

Figura 17: Análisis de riesgo
Fuente: Elaboración propia

Esquema para el detalle de los controles: Se establece caminos para proteger dichos los 114 controles.

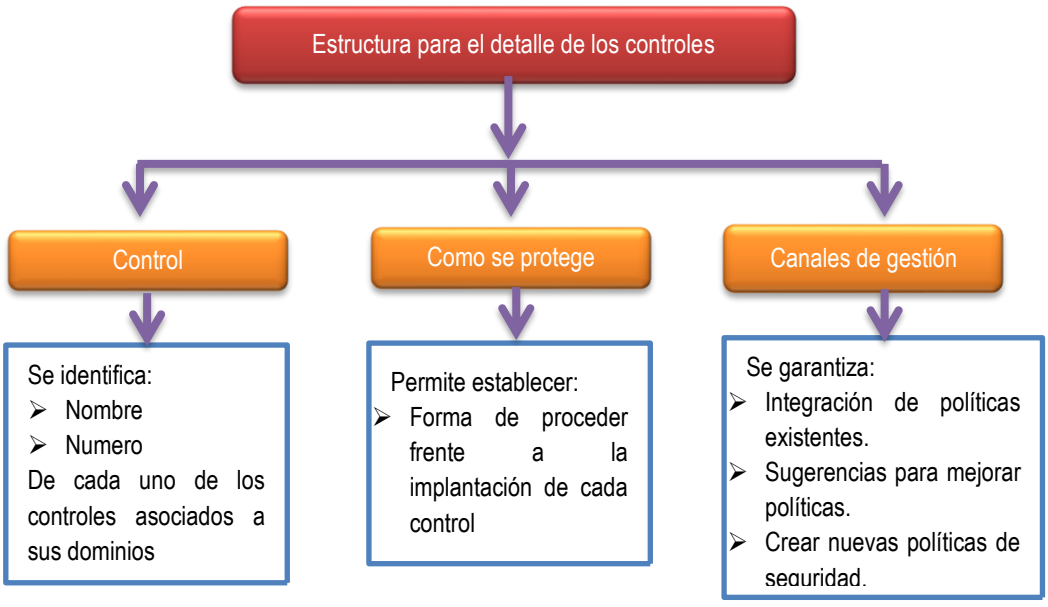


Figura 18: Esquema para el detalle de los controles
Fuente: Elaboración propia

Tabla 20: Desarrollo de los controles de seguridad de la información

N°	control	¿Cómo se Protege?	Canales de ejecución y comunicación Garantías de cumplimiento
POLÍTICAS DE SEGURIDAD			
Directrices de la Dirección en seguridad de la Información			
01	CONJUNTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.	La Dirección debería definir y gestionar su aprobación para publicar un documento de la política de seguridad de la información a todos los empleados y las partes externas relevantes.	Dar a conocer a todos los integrantes del departamento la política de seguridad aprobada y vigente que se va emplear en la seguridad de la Información. **Posibles Documentos a elaborarse:** Política de Seguridad de la Información. Formato de Procedimiento de comunicación de políticas de seguridad.
02	REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios funcionales o de gestión de la seguridad de la información significativos en el departamento) para garantizar que la seguridad es adecuada, eficaz y suficiente.	Ajustarse a los intervalos de tiempo planificados para la revisión o cambios que afectaron a la base de la evaluación inicial de riesgos, tales como los incidentes de seguridad, nuevas vulnerabilidades o cambios en la infraestructura organizativa y técnica. El proceso de revisión y evaluación consta de dos pasos distintos: **Planificación.** El coordinador del grupo de gestión de lanzamientos organiza el proceso de revisión. Esta persona se encarga de la programación de la revisión, la definición del papel de cada participante y determinar cómo los errores se pueden clasificar. **Examen preliminar de la reunión (opcional)** Esta reunión sirve para familiarizar a todos los miembros del departamento, con la revisión de la política de seguridad de la información y que se trate de reducir al mínimo el tiempo de Preparación. **Posibles Documentos a elaborarse:** Manual de planificación de revisión de la política de seguridad de la información con fechas de revisión adaptadas a las necesidades.
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
ORGANIZACIÓN INTERNA			
03	ASIGNACIÓN DE R ESPONSABILIDADES RELATIVAS A LA SEGURIDAD.	Definir y distribuir claramente todas las responsabilidades a los empleados (personal de apoyo y técnicos) del departamento para la seguridad de la información.	Emitir documentos formales que detallen el ámbito y nivel de responsabilidad sobre una tarea específica, un proceso o una actividad en la cual se utilice los activos físicos y lógicos del departamento. **Posibles Documentos a elaborarse:** Formato de Asignación de Responsabilidades y todo lo que ello implique.
04	SEGREGACIÓN DE TAREAS.	Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización.	Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación, autorización, y concienciación a los usuarios respecto de su responsabilidad. **Posibles Documentos a elaborarse:** Políticas de Segregación de tareas

05	CONTACTO CON LAS AUTORIDADES.	Se deberían mantener los contactos apropiados con las autoridades pertinentes.	Mantener registros de documentos físicos y/o digitales formales sobre la gestión de seguridad del departamento que ha sido informada a las autoridades. **Posibles Documentos a elaborarse:** Registro o Bitácora de Documentos formales de contacto con las autoridades
06	CONTACTO CON GRUPOS DE ESPECIAL INTERÉS.	Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.	El personal debe estar en constante preparación académica sobre la seguridad de la información, para obtener información actualizada y muy completa sobre aquellas amenazas publicadas a Través Internet que están activas, y explica cómo evitarlas. **Posibles Documentos a elaborarse:** Política de identificación de grupos especiales de interés.
07	SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	Se debería proteger la documentación de los sistemas contra accesos no autorizados.	En base a la política de seguridad de la información debe mantenerse la Seguridad de la documentación del sistema. **Posibles documentos a elaborarse:** Política de Seguridad de la documentación del sistema Manual de procedimiento de acceso a terceros a la documentación del sistema. Formato de ACTAS ENTREGA – RECEPCION.
DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO			
08	POLÍTICAS DE USO DE DISPOSITIVOS PARA MOVILIDAD	Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.	La protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones debe ser documentada por la dirección. **Posibles Documentos a elaborarse:** Política de acceso a ordenadores portátiles y acceso a sus comunicaciones móviles.
09	TELETRABAJO	Se debería desarrollar e implantar una política, planes operacionales y procedimientos para las actividades de teletrabajo.	En el caso de existir con un plan operacional de teletrabajo. Ej. Turnos de Monitorización del Data Center y las aplicaciones fuera de horario de trabajo y fuera de la institución. **Posibles Documentos a elaborarse:** Política de Control de Acceso de Teletrabajo.
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
ANTES DE LA CONTRATACIÓN			
10	INVESTIGACIÓN DE ANTECEDENTES	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener	Comprobación de referencias puede ser el método de detección más eficaz en un proceso de selección de personal. Verificación de referencias confirma la experiencia y la competencia de los candidatos, y proporciona una opinión de terceros sobre las aptitudes y actitudes de los solicitantes. **Posibles Documentos a elaborarse:** Manual de selección de personal. Manual de comprobación de referencias. ALTERNATIVA: Manual de Inserción y Ambientación de sus funciones.

		acceso y los riesgos percibidos.	
11	TÉRMINOS Y CONDICIONES DE CONTRATACIÓN	Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	La elección del acuerdo depende de las necesidades de las partes interesadas y sobre la relación de poder que existe entre ellos. **Posibles Documentos a elaborarse:** Manual de contratación de personal
DURANTE LA CONTRATACIÓN			
12	RESPONSABILIDADES DE GESTIÓN	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización	Son responsabilidades ya definidas en base a las políticas de la seguridad de la información. **Posibles Documentos a elaborarse:** Informes por periodos académicos respecto a la concordancia de personal vs responsabilidades departamentales. Guiarse en las políticas de la seguridad de la información definida con la dirección.
13	CONCIENCIACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	La capacitación debe ser constante de esto depende la proyección de mejora de la organización. **Posibles Documentos a elaborarse:** Cronograma de capacitación a los empleados a intervalos de tiempo que se consideren necesarios sobre la seguridad de la información en base a sus responsabilidades.
14	PROCESO DISCIPLINARIO	Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.	Las sanciones correctoras deben existir caso contrario no habrá una mejora continua. **Posibles Documentos a elaborarse:** Manual de sanciones a empleados que produzcan brechas en la seguridad.
CESE O CAMBIO DE PUESTO DE TRABAJO			
15	CESE O CAMBIO DE PUESTO DE TRABAJO	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas.	Este aspecto debe formar parte del acuerdo de trabajo pues claramente nos damos cuenta de la ventaja o desventaja que puede ocasionar un cambio en una responsabilidad determinada. **Posibles Documentos a elaborarse:** Manual de cese o cambio de las responsabilidades del personal.
GESTIÓN DE ACTIVOS			
RESPONSABILIDAD SOBRE LOS ACTIVOS			
16	INVENTARIO DE ACTIVOS	Todos los activos deberían estar claramente Identificados, confeccionando y manteniendo un	No descartar ningún activo y lo más efectivo es revisar en varias ocasiones todos los activos existentes y comprobar su existencia. **Posibles Documentos a elaborarse:**

		inventario con los más importantes.	Política de revisión de inventarios. Formatos de Actas de entrega recepción.
17	PROPIEDAD DE LOS ACTIVOS	Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la organización.	El director del departamento puede tomar todas las decisiones necesarias relativas a la información bajo su control a fin de mantener su integridad y su confidencialidad, por lo tanto: Entiende los principales riesgos involucrados en todos los usos internos de un tipo específico de información. Especifica los métodos de control adicionales necesarias para proteger esta información. Aprueba las solicitudes usuarias para acceder a la información. Revisa la lista de control de acceso de los usuarios para determinar si los privilegios deben ser retirados. **Posibles Documentos a elaborarse:** Manual de procedimiento para entrega de responsabilidades de activos. Actas de Entrega recepción de activos y responsabilidades.
18	USO ACEPTABLE DE LOS ACTIVOS	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.	El uso de un activo debe ser estrictamente lo necesario. **Posibles Documentos a elaborarse:** Manual de uso de activos.
19	DEVOLUCIÓN DE ACTIVOS	Todos los empleados, contratistas y terceros deberían devolver todos los activos de la organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo.	Por eso es importante el acuerdo de uso de los activos para que en la culminación de un empleo no existan inconvenientes que afecten a la organización. **Posibles Documentos a elaborarse:** Formato de ACTAS ENTREGA RECEPCION.
CLASIFICACIÓN DE LA INFORMACIÓN			
20	DIRECTRICES DE CLASIFICACIÓN	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la organización.	Clasificación de la información de acuerdo a la importancia para el departamento. **Posibles Documentos a elaborarse:** Política de Clasificación de la información Parámetros de Clasificación de la información.
21	ETIQUETADO Y MANIPULACIÓN DE LA INFORMACIÓN	Se debería desarrollar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización.	La información es vulnerable cuando su protección no es adecuada y esto se mejora con la clara identificación de la misma. **Posibles Documentos a elaborarse:** Manual de etiquetado de la información
22	MANIPULACIÓN DE ACTIVOS	Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o	La organización debe cuidar su información contra divulgaciones o usos no autorizados o inadecuados. **Posibles documentos a elaborarse:** Políticas de Manipulación de la información.

		usos no autorizados o inadecuados.	Manual de Procedimiento para la entrega de información confidencial a terceros.
MANEJO DE LOS SOPORTES DE ALMACENAMIENTO			
23	GESTIÓN DE SOPORTE EXTRAÍBLES	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.	En la medida más adecuada no deben utilizarse unidades de almacenamiento provenientes del exterior del departamento. **Posibles Documentos a elaborarse:** Políticas de uso de soportes extraíbles. Manual de procedimiento para el uso de soportes extraíbles.
24	ELIMINACIÓN DE SOPORTES	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.	Registrar el soporte, su origen y la forma de retirarla. **Posibles documentos a elaborarse:** Manual de procedimientos de retirada de soportes. Formato de Informe de Retiro de Soportes
25	SOPORTES FÍSICOS EN TRANSITO	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	Evitar el cambio constante de medios que contengan información importante. **Posibles documentos a elaborarse:** Política de transporte de la información fuera de los límites físicos de la organización. Manual de Procedimiento de soportes físicos en tránsito. Formato de Salida y Entrada de soportes físicos en tránsito.
CONTROL DE ACCESO			
REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO			
26	POLÍTICA DE CONTROL DE ACCESO	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Es recomendable que el acceso sea restringido al personal autorizado, contándose con registro de entradas y salidas de los visitantes **Posibles documentos a elaborarse:** Política de Control de Acceso a todas las dependencias del Departamento.
27	CONTROL DE ACCESO A LAS REDES Y SERVICIOS ASOCIADOS	En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio.	El control de conexiones se debe realizar en base a la política de control de accesos y necesidad de conexión a la red **Posibles documentos a elaborarse:** Política de Control de conexión a la red. Formato de Informe de conexión inadecuada a la red.
GESTIÓN DE ACCESO DE USUARIO			
28	GESTIÓN DE ALTAS/BAJAS EN EL REGISTRO DE USUARIOS	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.	Impedir el acceso no autorizado a los sistemas de información del departamento. **Posibles documentos a elaborarse:** **REF:** PUERTAS DE ACCESO AUTOMATICAS, cámara de seguridad (REGISTRO EN VIDEO).
29	GESTIÓN DE LOS DERECHOS DE ACCESO		

	ASIGNADOS A USUARIOS		
30	GESTIÓN DE LOS DERECHOS DE ACCESO CON PRIVILEGIOS ESPECIALES	Se debería restringir y controlar la asignación y uso de los privilegios.	Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso, deberán ser notificados al administrador con el visto bueno del Director. **Posibles documentos a elaborarse:** Política de Gestión de Privilegios. Manual de procedimiento para asignación, eliminación y cambio de privilegios.
31	GESTIÓN DE INFORMACIÓN CONFIDENCIAL DE AUTENTICACIÓN DE USUARIOS	Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal.	La asignación de pastor debe ser realizada de forma individual, por lo que el uso de password compartidos debe ser notificado formalmente. **Posibles documentos a elaborarse:** Política de gestión de contraseñas de usuario. Manual de procedimiento para asignación de contraseñas (para responsables y backups) y uso de las mismas.
32	REVISIÓN DE LOS DERECHOS DE ACCESO DE LOS USUARIOS	El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Se debe documentar con regularidad los derechos de acceso de los usuarios. **Posibles documentos a elaborarse:** Política de revisión de derechos de acceso de usuario.
33	RETIRADA O ADAPTACIÓN DE LOS DERECHOS DE ACCESO	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio.	Ningún empleado podrá acceder a la organización y su conjunto luego de haber terminado su función (Esto debe contar en la firma del contrato). **Posibles Documentos a elaborarse:** Formato de Retirada de acceso a activos (hardware o software).
RESPONSABILIDADES DEL USUARIO			
34	USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	Se debe asignar prioridades de acceso a la información en base a la política de control de accesos definida.
USO DE INFORMACIÓN CONFIDENCIAL PARA LA AUTENTICACIÓN			
35	RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN	Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.	Se debe evitar que las contraseñas se encuentren de forma legible en cualquier medio impreso o dejarlos en un lugar donde personas no autorizada puedan descubrirlos. **Posibles Documentos a elaborarse:** Política de Identificación y Autenticación de usuario al SO.
36	PROCEDIMIENTOS SEGUROS DE INICIO DE	Debería controlarse el acceso al sistema operativo mediante	Se debe incorporar controles de acceso autorizados. Posibles documentos a elaborarse:

	SESIÓN	procedimientos seguros de conexión.	Política de procedimientos seguros de conexión al SO.
37	GESTIÓN DE CONTRASEÑAS DE USUARIO	Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas.	Las formas de gestionar la creación de contraseñas dependen de la organización pero deben enmarcarse en estándares de seguridad como: Combinaciones de letras y números, longitud de la contraseña, etc. **Posibles Documentos a elaborarse:** Política de Gestión de Contraseñas al Sistema Operativo.
38	USO DE HERRAMIENTAS DE ADMINISTRACIÓN DE SISTEMAS	Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones.	La garantía de seguridad depende de los controles del sistema y de sus aplicaciones mediante la restricción de programas que no son de utilidad. **Posibles Documentos a elaborarse:** Formato de Inventario de los recursos su funcionalidad, sus configuraciones y otros.
39	CONTROL DE ACCESO AL CÓDIGO FUENTE DE LOS PROGRAMAS	Se debería restringir el acceso al código fuente de los programas.	El control de acceso al código fuente debe ser en base a la importancia, privacidad y autenticidad del código. **Posibles Documentos a elaborarse:** Política de Control de acceso al código fuente de los programas.
CRIPTOGRAFÍA (ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO EN SISTEMAS DE INFORMACIÓN)			
CONTROLES CRIPTOGRÁFICOS			
40	POLÍTICA DE USO DE LOS CONTROLES CRIPTOGRÁFICOS	Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	De acuerdo a la necesidad se podría contar con controles criptográficos para el tratamiento de la información. **Posibles Documentos a elaborarse.** Política de uso de los controles criptográficos.
41	GESTIÓN DE CLAVES	Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la organización.	La asignación de claves debe realizarse es base a la complejidad de técnicas criptográficas. **Posibles Documentos a Generar**. Política de Gestión de claves para controles criptográficos. Manual de Procedimiento para gestión de claves de controles criptográficos.
SEGURIDAD FÍSICA Y AMBIENTAL			
ÁREAS SEGURAS			
42	PERÍMETRO DE SEGURIDAD FÍSICA	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.	El acceso al departamento debe contar con la seguridad física necesaria en base a políticas establecidas y a la importancia de la información. **Posibles Documentos a elaborarse:** Manual de controles de entrada a áreas restringidas.
43	CONTROLES FÍSICOS DE ENTRADA	Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.	Las entradas pueden convertirse en escapes, es necesario garantizar el acceso únicamente al personal autorizado. **Posibles Documentos a elaborarse:** Manual de controles de entrada a áreas restringidas.
44	SEGURIDAD DE OFICINAS DESPACHOS Y	Se debería asignar y aplicar la seguridad física para oficinas,	La seguridad debe ser asignada de acuerdo a la estructura física del departamento.

	RECURSOS	despachos y recursos.	**Posibles Documentos a elaborarse:** Manual de controles de entrada a oficinas, despachos e instalaciones.
45	PROTECCIÓN CONTRA LAS AMENAZAS EXTERNAS Y DE ORIGEN AMBIENTAL	Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	La ubicación de la información debe estar respaldada con varios escudos de protección para garantizar su seguridad. **Posibles Documentos a elaborarse:** Manual contra las amenazas externas y de origen ambiental.
46	TRABAJO EN ÁREAS SEGURAS	Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras.	Un área segura de trabajo cuenta con controles de acceso a la misma.
47	ÁREAS DE ACCESO PÚBLICO, CARGA Y DESCARGA	Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.	El aislamiento de la información para el público en general debe ser estricto.
SEGURIDAD DE LOS EQUIPOS			
48	EMPLAZAMIENTO Y PROTECCIÓN DE EQUIPOS	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.	Se debe evitar el acceso no autorizado tomando las debidas precauciones en base a la ubicación de los equipos. **Posibles Documentos a elaborarse:** Manual de acceso no autorizado.
49	INSTALACIONES DE SUMINISTRO	Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.	Previo a la instalación de equipos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.
50	SEGURIDAD DEL CABLEADO	Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.	Se debe etiquetar el cableado, las extensiones y los tableros de distribución eléctrica. Evitar los cableados sueltos o dispersos, estos deberán entubarse.
51	MANTENIMIENTO DE LOS EQUIPOS	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Es necesario establecer puntos centrales de corte de fluido eléctrico, a nivel de los pisos de las sedes de la UNAJMA. **Posibles Documentos a elaborarse:** Políticas de Mantenimiento de Recursos Hardware y Software. Manual de Procedimiento para mantenimiento de Hardware y Software.
52	SALIDA DE ACTIVOS FUERA DE LAS DEPENDENCIAS DE LA EMPRESA	No deberían sacarse equipos, información o software fuera del local sin una autorización. Posibles documentos a elaborarse manual de registro de movimientos de materiales fuera de la empresa. Formato Actas entrega – recepción.	Controlar los accesos a los activos a través de un registro de movimientos con periodos de tiempo.

53	SEGURIDAD DE LOS EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.	Se debe aplicar seguridad de acuerdo a la importancia de los equipos. **Posibles Documentos a elaborarse:** Políticas de Seguridad para equipos fuera de las instalaciones.
54	REUTILIZACIÓN O RETIRADA SEGURA DISPOSITIVOS DE ALMACENAMIENTO	Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.	Se debe considerar aspectos importantes en la eliminación de la información como: pérdidas irreparables, daños, etc. **Posibles Documentos a elaborarse:** Políticas de reutilización o retirada segura de equipos. Manual de Procedimiento para la reutilización o retirada segura de equipos.
55	EQUIPO INFORMÁTICO DE USUARIO DESATENDIDO	Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.	En este control se consideran desatendidos a los equipos que no son controlados frecuentemente, pero poseen información relevante de la organización, por lo cual se debe tener garantías de seguridad para el acceso no autorizado.
56	POLÍTICA DE PUESTO DE TRABAJO DESPEJADO Y BLOQUE DE PANTALLA	Políticas para escritorios y monitores limpios de información.	Todos los usuarios deberán cumplir con la política de puesto de trabajo despejado y pantalla limpia.
SEGURIDAD EN LAS OPERACIONES			
RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN			
57	DOCUMENTACIÓN DE LOS PROCEDIMIENTOS DE OPERACIÓN	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.	Es necesario mantener informado a todo el personal de la documentación existente para mejorar el desempeño de la organización. **Posibles Documentos a elaborarse:** Política de comunicación de procedimientos de operación. Manual de procedimiento de comunicación de procedimientos de operación.
58	GESTIÓN DE CAMBIO	Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.	Los cambios deben ser solo los necesarios acoplados a la política vigente. **Posibles Documentos a elaborarse:** Política de Gestión de cambios Manual de procedimiento de gestión de Cambios. Formatos para la gestión de cambios.
59	GESTIÓN DE CAPACIDADES	Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.	La dirección debe monitorizar el uso y capacidades de los recursos así como la eficiencia en la utilización del personal. **Posibles Documentos a elaborarse:** Política: Generación de Informes semestrales de gestión de capacidades.
60	SEPARACIÓN DE LOS RECURSOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN	La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.	Los recursos deben ser asignados en base a la operación a realizarse Posibles Documentos a elaborarse: Políticas de Separación de los recursos de desarrollo, prueba y operación. Manual de Procedimiento para separación de recursos de desarrollo, prueba y operación (producción) de sistemas.

PROTECCIÓN CONTRA CÓDIGO MALICIOSO			
61	CONTROLES CONTRA EL CÓDIGO MALICIOSO	Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.	El personal que tiene acceso a los servidores en forma mono usuaria, deberá encargarse de detectar y eliminar en los medios magnéticos u ópticos, la infección o contagio de código malicioso. **Posibles Documentos a elaborarse:** Políticas de controles de detección, prevención y recuperación
COPIA DE SEGURIDAD			
62	COPIAS DE SEGURIDAD DE LA INFORMACIÓN	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.	Se deben hacer copias permanentes de seguridad con periodos de tiempo establecidas por la dirección dependiendo de la criticidad de la información. **Posibles documentos a elaborarse:** Políticas de copias de seguridad de la información. Manual de controles de copias de seguridad.
REGISTRO DE ACTIVIDAD Y SUPERVISIÓN			
63	REGISTRO Y GESTIÓN DE EVENTOS DE ACTIVIDAD	Se deberían registrar, analizar y tomar acciones apropiadas de las averías.	Frente a la presencia de fallos es necesario un registro adecuado para evitar inconvenientes futuros. **Posibles documentos a elaborarse:** Política de Registro de Fallos Manual de procedimiento para fallos Formato de Informe de Fallos.
64	PROTECCIÓN DE LOS REGISTROS DE INFORMACIÓN	Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.	La protección de la información debe ser en base a las normas establecidas. **Posibles documentos a elaborarse:** Política de protección de la información de los registros.
65	REGISTROS DE ACTIVIDAD DEL ADMINISTRADOR Y OPERADOR DEL SISTEMA	Se deberían registrar las actividades del administrador y de los operadores del sistema.	Se deben contar con registros periódicos dependiendo de la criticidad o de eventualidades para comprobar el desempeño de las partes involucradas. **Posibles documentos a elaborarse:** Políticas de registros de administración y operación Formato de Registro de administración y operación
66	SINCRONIZACIÓN DE RELOJES	Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.	El tiempo debe ser coordinado y cronometrado. **Posibles documentos a elaborarse:** Política de sincronización de relojes en los sistemas. Manual de Procedimiento de sincronización de relojes de los sistemas.
CONTROL DEL SOFTWARE EN EXPLOTACIÓN			
67	INSTALACIÓN DEL SOFTWARE EN SISTEMAS EN PRODUCCIÓN	Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos	Los sistemas que estén operando deben cumplir con controles de software para su correcta manipulación. Posibles Documentos a Generar: Política de Control de software en explotación Manual de Procedimiento para el control de software en explotación Formatos de Informes de Control del Software en Explotación

GESTIÓN DE LA VULNERABILIDAD TÉCNICA			
68	GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las adecuadas para hacer frente a los riesgos asociados. Medidas	Se debe realizar una capacitación de todo el personal oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando y evitar daños futuros. **Posibles Documentos a elaborarse:** Política de Control de Vulnerabilidades. Manual de Procedimiento para el control de vulnerabilidades técnicas. Manual de Procedimiento para el tratamiento de vulnerabilidades identificadas.
69	RESTRICCIONES EN LA INSTALACIÓN DE SOFTWARE	Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.	Los cambios en los paquetes de software se deben evitar en lo posible, pues en su creación se establecen requerimiento con su tiempo de duración. **Posibles Documentos a elaborarse:** Política de Restricciones a los cambios de paquetes de software Manual de Procedimiento de restricciones de los cambios de paquetes de software
CONSIDERACIONES DE LAS AUDITORIAS DE LOS SISTEMAS DE INFORMACIÓN			
70	CONTROLES DE AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN	Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio.	Una vez iniciado el proceso de elaboración de un SGSI se debe gestionar controles de auditoria para garantizar el análisis del desarrollo. **Posibles Documentos a elaborarse:** Plan de Auditorias que deben constar en el Plan Estratégico del departamento
SEGURIDAD DE LAS TELECOMUNICACIONES			
GESTIÓN DE LA SEGURIDAD DE LAS REDES			
71	CONTROLES DE RED	Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.	Se debe evitar el acceso de usuarios de la intranet a redes externas sin el justificativo correspondiente (Ej. Red del Banco Pacifico – Sistema de Cobros en Línea), cualquier excepción deberá ser documentada y contar con el visto bueno de la dirección. **Posibles documentos a elaborarse:** Política de acceso a redes externas. Formato de Justificación al acceso a redes externas.
72	MECANISMOS DE SEGURIDAD ASOCIADOS A SERVICIOS EN RED	Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.	Para la utilización de los servicios en red, se debe contar con las garantías de accesos a los mismos, considerando jerarquías de autorización de acceso. **Posibles Documentos a elaborarse:** Política de uso de los servicios de Red Formato de Autorización de Acceso a los servicios de red.
73	SEGURIDAD DE LOS SERVICIOS DE RED	Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de	Acuerdos Internos: los podemos definir la asignación de responsabilidades de implementación de un servicio de red, que deberá ser plasmado con un informe técnico que describa todos los indicadores de funcionamiento del

		seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.	servicio de red implementado. Acuerdo Externos: proveedores externos de servicios de red, en los que los indicadores de funcionamiento estarán plasmados en los contratos. Seguimiento y Monitoreo de los indicadores de servicio definidos en el acuerdo. Identificar claramente el acuerdo sobre los servicios de red. **Posibles documentos a elaborarse:** Políticas de Seguridad de servicios de red. Manual de procedimiento para la implementación de servicios de red.
INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS			
74	POLÍTICAS Y PROCEDIMIENTOS DE INTERCAMBIO DE INFORMACIÓN	Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.	La información debe ser manejada cuidadosamente el intercambio de la misma debe ser analizado y autorizado. **Posibles documentos a elaborarse:** Política de intercambio de la información.
75	ACUERDOS DE INTERCAMBIO	Se deberían establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.	La información debe ser manejada cuidadosamente el intercambio de la misma debe ser analizada y autorizada y documentada. **Posibles documentos a elaborarse:** Formato de acuerdos para el intercambio de información y software entre la
76	MENSAJERÍA ELECTRÓNICA	Se debería proteger adecuadamente la información contenida en la mensajería electrónica.	La mensajería electrónica en caso de existir no debe ser autorizada en los equipos donde consta la información relevante de la organización. **Posibles documentos a elaborarse:** Políticas de Seguridad de Mensajería electrónica.
77	ACUERDOS DE CONFIDENCIALIDAD Y SECRETO	Se deberían identificar y revisar regularmente en los acuerdos de confidencialidad aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización.	Determinar claramente los acuerdos de confidencialidad al que están sometidos al pertenecer a una entidad que necesita la protección de su información. **Posibles Documentos a elaborarse:** Formato de actas de confidencialidad
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN			
REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN			
78	ANÁLISIS Y ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD	Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad.	Se debería especificar conjuntamente entre los jefes y técnicos tanto de las dependencias requirentes como del DESITEL, los requerimientos de seguridad necesarios, y se deberán verificar y validar (SRS)los mismos por parte de los jefes de los departamentos a través de la firma de documentos en los cuales se detallen fechas, involucrados, responsabilidades y requerimientos, tanto para las demandas de nuevos sistemas de información o mejoras de los sistemas ya existentes y garantizar

			que no se pierden recursos. **Posibles Documentos a elaborarse:** Actas de Reuniones para Análisis y especificación de los requisitos de seguridad.
79	SEGURIDAD DE LAS COMUNICACIONES EN SERVICIOS ACCESIBLES POR REDES PÚBLICAS	Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.	Se debe proteger los puertos de diagnóstico y configuración remotos con un control de acceso a los mismos. **Posibles documentos a elaborarse:** Política de protección de puertos de diagnóstico y configuración remotos.
80	PROTECCIÓN DE LAS TRANSACCIONES POR REDES TELEMÁTICAS	Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.	De acuerdo a las políticas de la organización se debe contar con métodos de autenticación de acceso remoto de conexiones externas. **Posibles documentos a elaborarse:** Política de autenticación para conexiones externas.
SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE			
81	POLÍTICA DE DESARROLLO SEGURO DE SOFTWARE	Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen de negocio. la política de control de accesos a las aplicaciones	Verificar la política de control de acceso de las conexiones de los ordenadores a través de un registro permanente de rating. Posibles **Documentos a elaborarse:** Informe de Control de encaminamiento (routing) de red.
82	PROCEDIMIENTOS DE CONTROL DE CAMBIO EN LOS SISTEMAS	Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	El PCC generado para un cambio debe estar con firma de responsabilidad de los jefes de los departamentos o dependencias involucradas, en este caso el Director del OSI – UNAJMA y el jefe del departamento requirente, estas autoridades a su vez controlaran las responsabilidades operativas de los técnicos operativos.
83	REVISIÓN TÉCNICA DE LAS APLICACIONES TRAS EFECTUAR CAMBIO EN EL SISTEMA OPERATIVO	Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización	Debido a los cambios que se generen en la revisión técnica de las aplicaciones, es crucial garantizar su eficiencia. **Posibles Documentos a elaborarse:** Política de revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo Manual de Procedimiento para efectuar cambios en el sistema operativo.
84	RESTRICCIONES A LOS CAMBIOS EN LOS PAQUETES DE SOFTWARE	Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados.	Establecer grupos o personal, métodos y técnicas de validación de datos de entrada **Posibles Documentos a elaborarse:** Política de validación de datos de ingreso. Manual de Procedimiento de validación de datos de entrada Formato de Informe de Validación de datos de entrada.
85	USO DE PRINCIPIOS DE INGENIERÍA EN PROTECCIÓN DE	Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible	Establecer grupos o personal, métodos y técnicas para el control de procesamiento interno. **Posibles Documentos a elaborarse:**

	SISTEMAS	corrupción en la información debida a errores de procesamiento o de acciones deliberadas.	Política de validación control del procesamiento interno (SRS) Manual de Procedimiento de Control del procesamiento interno. Formato de Informes de Control del procesamiento interno.
86	SEGURIDAD EN ENTORNOS DE DESARROLLO	Se deberían identificar los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, e identificar e implantar los controles apropiados.	Se deben identificar los requisitos para asegurar la autenticidad y protección de la integridad de los mensajes. Establecer grupos o personal, métodos y técnicas para el control de procesamiento interno. **Posibles Documentos a elaborarse:** Política de validación Integridad de los mensajes. (SRS) Manual de Procedimiento de integridad de los mensajes.
87	EXTERNALIZACIÓN DEL DESARROLLO DE SOFTWARE	Se debería supervisar y monitorizar el desarrollo del software subcontratado por la organización.	El director del Departamento debe ser el encargado de supervisar el desarrollo del software generado fuera de la organización. **Posibles Documentos a elaborarse:** Política de Externalización del desarrollo de software. Manual de Procedimiento para recepción de software desarrollado externamente.
88	PRUEBAS DE FUNCIONALIDAD DURANTE EL DESARROLLO DE LOS SISTEMAS	Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo.	Revisar regularmente los resultados de las actividades de monitoreo, para el efectivo cumplimiento. **Posibles documentos a elaborarse:** Política de Supervisión del uso del sistema. Manual de procedimiento para supervisión del uso del sistema. Formato de Informe de Supervisión del uso del sistema.
89	PRUEBAS DE ACEPTACIÓN	Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.	Definir los requerimientos mínimos acordes con la política de seguridad que garantice su aceptación y buen funcionamiento. **Posibles Documentos a elaborarse:** Políticas de Establecimiento de criterios de aceptación para nuevos sistemas, actualizaciones y nuevas versiones. Políticas de pruebas durante desarrollo y previo la aceptación. Manual de Procedimiento de Aceptación de nuevos sistemas. (ESTUDIO DE FACTIBILIDAD, Análisis Costo Beneficio Análisis de Riegos, Planificación Temporal) Formato de Solicitud de Implementación de Nuevos Sistemas. Formatos de Seguimiento y Aceptación de Nuevos Sistemas. Formato de actualización de Nuevos Sistemas Formato de producción de Nuevos
DATOS DE PRUEBA			
90	PROTECCIÓN DE LOS DATOS UTILIZADOS EN PRUEBAS	Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.	Se debe contar con un equipo especial para la prueba del sistema. **Posibles Documentos a elaborarse:** Política de protección de los datos de prueba del sistema Manual de Procedimiento de Protección de los datos de prueba de sistemas. Formatos de Confidencialidad de datos de prueba del sistema

RELACIÓN CON SUMINISTRADORES			
SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON SUMINISTRADORES			
91	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA SUMINISTRADORES	Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.	Identificar las partes terceras que no intervienen significativamente en el desarrollo del proyecto. **Posibles Documentos a elaborarse:** Política de Identificación de terceros en el ámbito lógica como físico. Nivel de acceso que se le puede conceder. Formato de riesgos derivados de la utilización de terceros.
92	TRATAMIENTO DEL RIESGO DENTRO DE ACUERDOS DE SUMINISTRADORES	Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.	Es necesario identificar las partes relevantes frente a la seguridad de la información, el momento de contratos con terceros. **Posibles Documentos a elaborarse:** Política de tratamiento de la seguridad en contratos con terceros. Control y cumplimiento de Contratos con terceros.
93	CADENA DE SUMINISTRO E TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	Se deberían anexar todos los requisitos Identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.	Un cliente consume no genera por lo tanto solo debe enmarcarse en la forma de consumir no en su origen. **Posibles Documentos a elaborarse:** Política de tratamiento de la seguridad en la relación con los clientes Identificar clientes de acuerdo a los servicios prestados.
GESTIÓN DE LA PRESENTACIÓN DEL SERVICIO POR SUMINISTRADORES			
94	SUPERVISIÓN Y REVISIÓN DE LOS SERVICIOS PRESTADOS POR TERCEROS	Los servicios, informes y registros suministrados por terceros deberían ser monitoreados y revisados regularmente, y las auditorías se deberían realizar a intervalos regulares.	Se debe garantizar la prestación segura de los servicios de terceros con una clara identificación de su participación. **Posibles Documentos a elaborarse:** Política de Generación de Reportes por unidad de tiempo (definirla de acuerdo a la criticidad del servicio) sobre la provisión de servicios.
95	GESTIÓN DE CAMBIOS EN LOS SERVICIOS PRESTADOS POR TERCEROS	Se deberían gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existente, en los procedimientos y los controles teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	Los cambios se deben aceptar luego de una reevaluación de los riesgos. **Posibles Documentos a elaborarse:** Política de Gestión de Cambios prestados por terceros Manual de procedimiento de Gestión de cambios prestados por terceros. Formatos para la gestión de cambios prestados por terceros.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORA			
96	RESPONSABILIDADES Y PROCEDIMIENTOS	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.	La respuesta frente a un incidente en la seguridad de la información, se la debe realizar en base a un procedimiento involucrado donde se definan responsables y formas de enfrentar el problema. **Documentos Posibles a elaborarse.** Política de Responsabilidad y Procedimientos en la gestión de incidentes. Manual de Responsabilidades y procedimiento de la gestión de incidentes.
97	NOTIFICACIÓN DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados.	La comunicación de un fallo de seguridad debe ser realizada lo más rápido posible a las instancias pertinentes y de acuerdo a la complejidad de la información para canalizar soluciones óptimas. **Documentos Posibles a elaborarse:** Política de Notificación de los eventos de fallo en la seguridad de la información. Manual de Procedimiento de notificación de los eventos de fallo en la seguridad de la información. Formato de Notificación.
98	NOTIFICACIÓN DE PUNTOS DÉBILES DE LA SEGURIDAD	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Cuando se encuentren puntos débiles en la seguridad de la información, a través de un informe adecuado se debe notificar para garantizar la integridad del funcionamiento del sistema y de la información del mismo. **Documentos Posibles a elaborarse:** Política de Notificación de puntos débiles de seguridad Manual Procedimiento de Notificación de puntos débiles de seguridad. Formato de Notificación
99	VALORACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y TOMA DE DECISIONES	Se deberían producir y mantener durante un periodo establecido los registros de auditoría con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.	Los registros de auditoría deben ser documentados con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información. **Posibles documentos a elaborarse:** Política de Mantenimiento de Registros
100	RESPUESTA A LOS INCIDENTES DE SEGURIDAD	Se debería disuadir a los usuarios del uso de los recursos dedicados al tratamiento de la información para propósitos no autorizados.	Los recursos de tratamiento de la información deben ser de uso estricto y mantener un control del uso de los activos según su importancia. **Posibles Documentos a elaborarse:** Política de Prevención del uso indebido de recursos de tratamiento de la información. Manual de procedimiento de notificación del uso indebido de recursos de tratamiento de la información.
101	APRENDIZAJE DE LOS INCIDENTES DE	Debería existir un mecanismo que permitan cuantificar y	Los incidentes de seguridad de la información, deben ser almacenados mediante un informe para en tiempos posteriores analizar su evolución.

	SEGURIDAD DE LA INFORMACIÓN	monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información.	**Documentos Posibles a elaborarse.** Formato de Informes de Incidentes de seguridad de la información. Bitácora de Incidentes y Soluciones. (Aplicar algún tipo de Codificación).
102	RECOPILACIÓN DE EVIDENCIAS	Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada conforme a las reglas para la evidencia establecidas en la jurisdicción relevante.	En base a la política de sanciones determinada por el departamento después de un incidente en la seguridad de información la evidencia debe ser guardada, para proceder de acuerdo a las políticas vigentes. **Posibles Documentos a elaborarse:** Procedimiento Técnico: Análisis Forense. Procedimiento Legal: Departamento de RRHH, y Unidad de Procuraduría
LOS ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIOS			
CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN			
103	PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio.	El plan de continuidad deberá incluir el análisis de los procesos que componen la organización, qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas. **Posibles Documentos a elaborarse:** Guía de desarrollo del plan de continuidad. Plan de Continuidad para aseguramiento de la información.
104	IMPLANTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Se debería desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la	La continuidad del negocio no es más que el **cumplimiento de las políticas de seguridad vigente** y por lo tanto se debe sugerir mejoras en el desarrollo de la política de seguridad de la
105	VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	Se deberían dar el seguimiento adecuado para CONTROLAR, VALIDAR VERIFICAR Y REEVALUAR los planes de continuidad regularmente para garantizar su consistencia.	Los planes de continuidad deben ser analizados luego de un periodo considerable de tiempo para garantizar la sostenibilidad de la metodología y políticas establecidas en la organización. Posibles Documentos a elaborarse: Formato para la reevaluación del plan de continuidad.
REDUNDANCIAS			
106	DISPONIBILIDAD DE INSTALACIONES PARA EL PROCEDIMIENTO DE LA INFORMACIÓN	Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información.	De acuerdo a la magnitud de la información y el valor de los activos se debe realizar el tratamiento de la información con herramientas adecuadas en base a un informe técnico detallado del personal que lo requiera. **Posibles Documentos a elaborarse:**

			Manual de procesos de Autorización de recursos. Formato de autorización de recursos.
CUMPLIMIENTO			
CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES			
107	IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE	Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Organización para cumplir con estos requisitos, deberían ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización	De acuerdo a la política establecida se debe gestionar el cumplimiento de las reglas establecidas para garantizar que no existan demoras en el desarrollo de la seguridad de la información. **Posibles Documentos a elaborarse:** Política de Cumplimiento de reglas. Manual de Procedimiento de sanción por incumplimiento de reglas
108	DERECHOS DE PROPIEDAD INTELECTUAL (DPI)	Se deberían implantar procedimientos adecuados que garanticen el cumplimento de la legislación, regulaciones y requisitos contractuales para el uso de material con posibles derechos de propiedad intelectual asociados y para el uso de productos software propietario.	Los derechos de propiedad intelectual deben ser respetados en base a la ley vigente. Art 55 CP. Patentar software institucional. Mantener Actualizado el Inventario de Software utilizado y licenciado por la UNAJMA (CONTRATO DE LCAMPUS AGREEMENT) **Posibles Documentos a elaborarse:** Política de Patente y Licenciamiento del uso de Software en la UNAJMA. Manual de Procedimiento de Patente y Licenciamiento de Software Propietario. Formato de Inventario del uso Software Formato de Solicitud de Patente de Software Institucional.
109	PROTECCIÓN DE LOS REGISTROS DE LA ORGANIZACIÓN	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio.	El activo más importante de la organización es la información por lo tanto la protección de los documentos relacionados a esta se la debe realizar en base a políticas definidas. **Posibles Documentos a elaborarse:** Política de protección de los documentos de la organización. Manual de Procedimiento por pérdida, destrucción o falsificación de documentos. Formato de Notificación de Perdida, Destrucción o Falsificación de Documentos
110	PROTECCIÓN DE DATOS Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL	Se debería garantizar la protección y privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales.	Si la organización no requiere información relevante de carácter personal, no es necesario acceder a ella. **Posibles Documentos a elaborarse:** Política protección de datos y privacidad de la información de carácter personal.
111	REGULACIÓN DE LOS CONTROLES CRIPTOGRÁFICOS	Se deberían utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes.	Se deben implantar los algoritmos criptográficos en base a las consideraciones del OSI – UNAJMA.

CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO			
112	REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	Se deberían revisar las prácticas de la organización para la gestión de la seguridad de la información y su implantación (por ej. objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.	No descuidar por periodos largos de tiempo la estructuración de la seguridad de la información y el cumplimiento de la misma, de esta manera se evita retrasos en el cumplimiento de la planificación establecida y fundamentalmente definir ámbitos de independencia en la seguridad de la información. **Posibles Documentos a elaborarse:** Políticas de revisión independiente de la seguridad de información Manual de procedimientos de revisión independiente de la seguridad de la información, en la cual se defina la autorización, responsabilidades, tiempos de cumplimiento y métodos de revisión con el único objetivo de asegurar la independencia de la revisión. Formato Final del Informe de la revisión independiente realizada.
113	CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS DE SEGURIDAD	Los directivos se deberían asegurar que todos procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad.	Los documentos elaborados (políticas y de seguridad) deben cumplirse por lo cual la dirección debe proporcionar garantías de cumplimiento a través de políticas de sanciones establecidas si fuera necesario a quienes incumplan con el proceso y se observe demoras en las respuestas. **Posibles Documentos a elaborarse:** Generación de Informes de Seguimiento del cumplimiento de las políticas y nomás de seguridad
114	COMPROBACIÓN DEL CUMPLIMIENTO	Se debería comprobar regularmente la conformidad de los sistemas de información con los estándares de implantación de la seguridad.	La gerencia debe asumir el proceso de desarrollo de seguridad de la información con responsabilidad ya que de esto depende el progreso del personal involucrado. **Posibles Documentos a elaborarse:** Registro de Documentos sobre Reuniones, Autorizaciones, Seguimiento de las responsabilidades adquiridas

B. REQUERIMIENTO DEL USUARIO

Los requerimientos tomados son: requerimientos funcionales y requerimientos no funcionales.

Requerimientos funcionales

Tabla 21: *Base de Datos*

REFERENCIA	REQUERIMIENTOS
R1	Se debe crear una base de datos
R2	La BD debe permitir almacenar el nivel de madures de los 114 controles de la ISO 27001
R3	La BD debe permitir almacenar el nivel de importancia de cada activo de la institución
R4	La BD debe permitir almacenar la copia de seguridad del sistema web

Fuente: Elaboración propia

Tabla 22: *Ingreso al sistema*

REFERENCIA	REQUERIMIENTOS
R1	El ingreso al sistema debe ser mediante autenticación (user y pasword)
R2	Sólo será utilizados por el personal de la Oficina de Sistemas de información de la UNAJMA

Fuente: Elaboración propia

Requerimientos no funcionales

Tabla 23: *Requerimientos no funcionales*

REFERENCIA	REQUERIMIENTOS
R1	La aplicación se utilizará en cualquier computador con acceso a internet

Fuente: Elaboración propia

C. DIAGRAMA DE CASOS DE USO

Los casos de uso de la aplicación, son los que definen los requerimientos de los usuarios y representan justamente la funcionalidad de la aplicación cuando el actor lleva un proceso o una actividad.

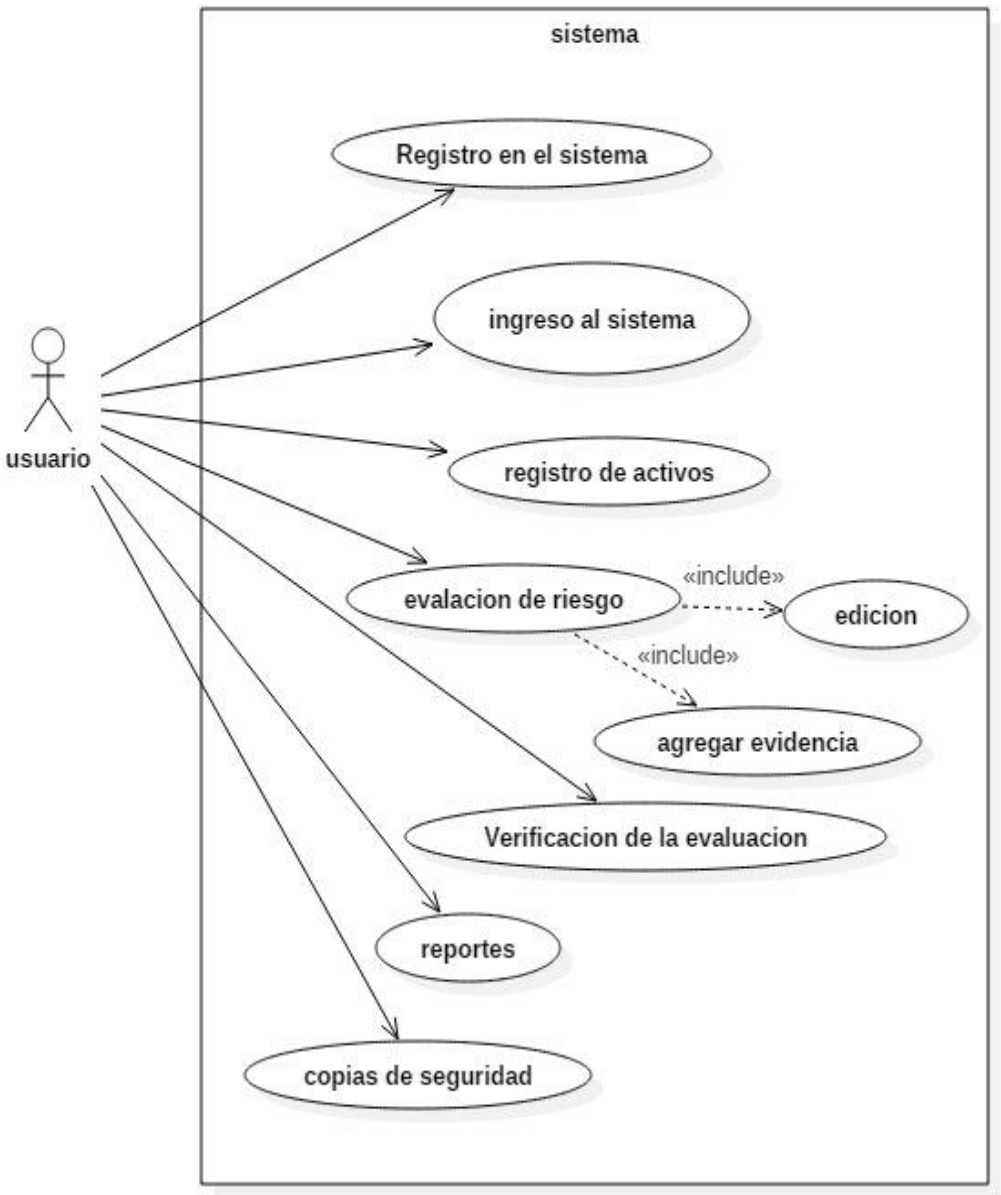


Figura 19: Diagrama de caso de Usos
Fuente: Elaboración propia

D. ESPECIFICACIÓN DE CASOS DE USOS

La especificación de caso de uso es la descripción de las partes definidas con el fin de detallar la información completa. La especificación se realizó bajo un cuadro que muestra las partes y las indicaciones básicas para que sea más sencilla y fácil de escribir y leer.

Tabla 24: *Especificación de Casos de usos*

CASO DE USO	REGISTRAR NOTAS
Tipo	Primario
Propósito	Evalúa los riesgos
Precondiciones	Agrega evidencias
Final exitoso	La evaluación de los riesgo es guardada
Final Fallido	La evaluación de los riesgo no es guardada
Actores	Usuario
Evento de inicio	el usuario ingresa al sistema
Flujo Principal	El usuario ingresa al sistema
	El usuario registra los activos
	El usuario evalúa los riesgos
	El usuario verifica la evaluación
	El usuario hace reportes
	El usuario realiza copia de seguridad

Fuente: Elaboración Propia

E. DIAGRAMAS DE SECUENCIAS

El diagrama de secuencia de la aplicación muestra los pasos generales que la aplicación toma cuando se llama una acción.

En la figura 20 podemos apreciar el diagrama de secuencia “Registro en el sistema”, donde el usuario ingresa y guarda los datos.

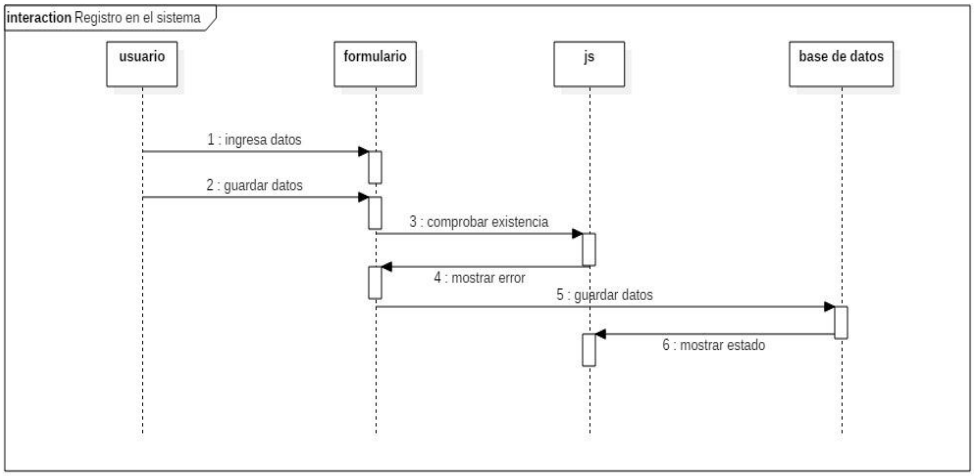


Figura 20: Diagrama de secuencia: Registro en el sistema

Fuente: Elaboración propia

La figura 21 podemos apreciar el diagrama de secuencia “Ingreso al Sistema”, en donde el usuario se registra para poder ingresar al sistema ingresando su usuario y contraseña.

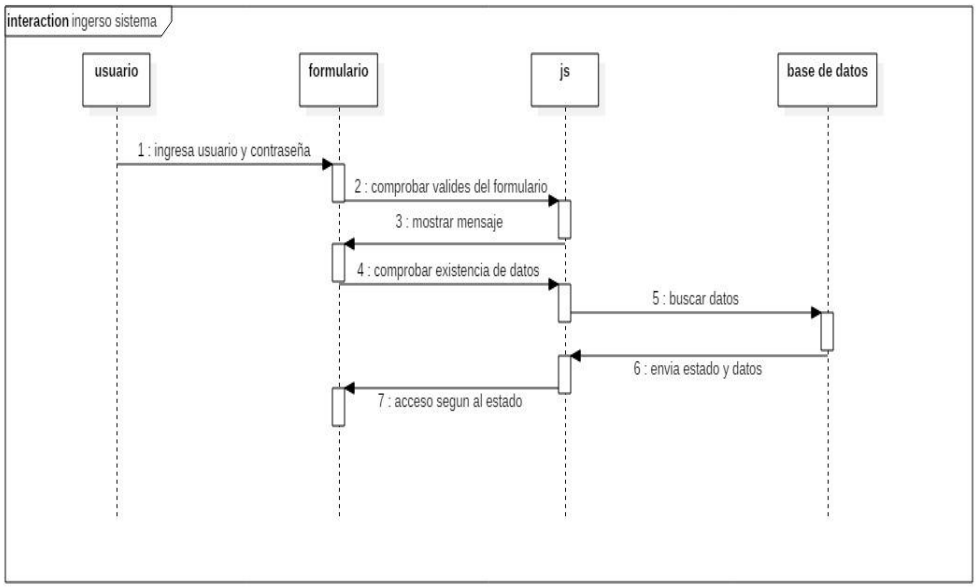


Figura 21: Diagrama de secuencia: Ingreso al Sistema
Fuente: Elaboración propia

En la figura 22 podemos apreciar el diagrama de secuencia “Evaluacion de riesgo”, donde se realiza y guarda la evaluacion de riesgo

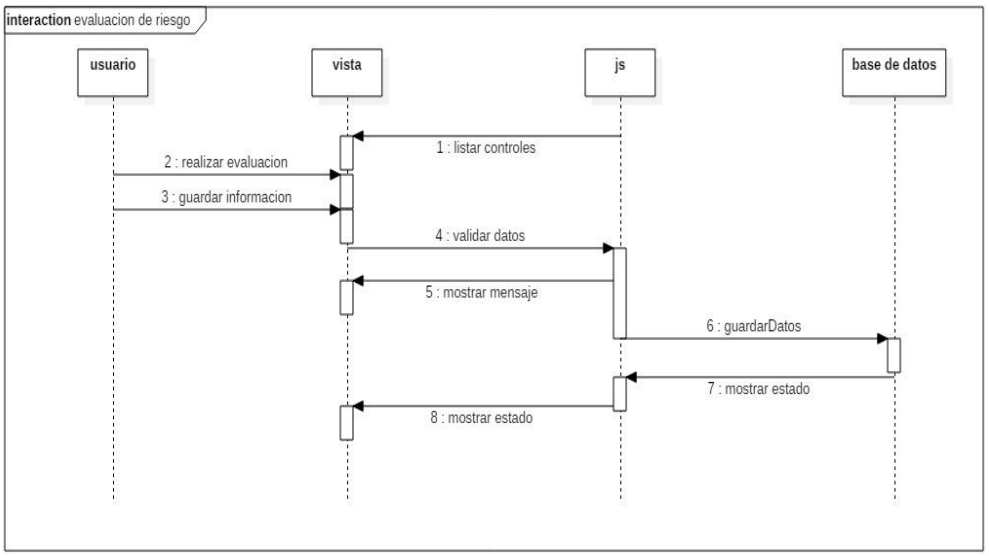


Figura 22: *Diagrama de secuencia: Evaluación de riesgo*
Fuente: Elaboración propia

En la figura 23 podemos apreciar el diagrama de secuencia “Agregar evidencia”, donde se muestra el formulario, se ingresa y guarda los datos.

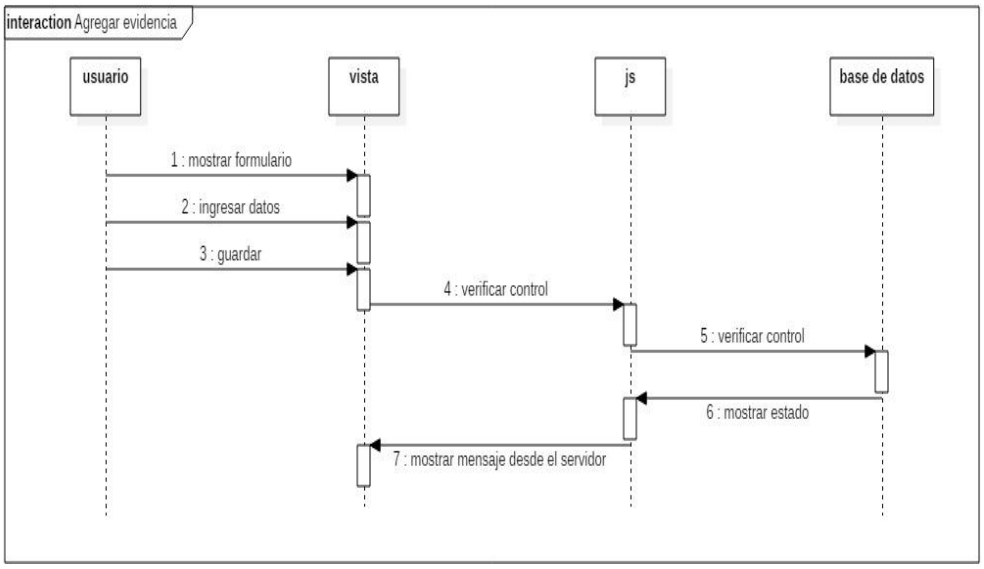


Figura 23: *Diagrama de secuencia: Agregar evidencia*

Fuente: Elaboración propia

En la figura 24 podemos apreciar el diagrama de secuencia “Edicion de Evaluación”, donde se ingresa y gurada datos.

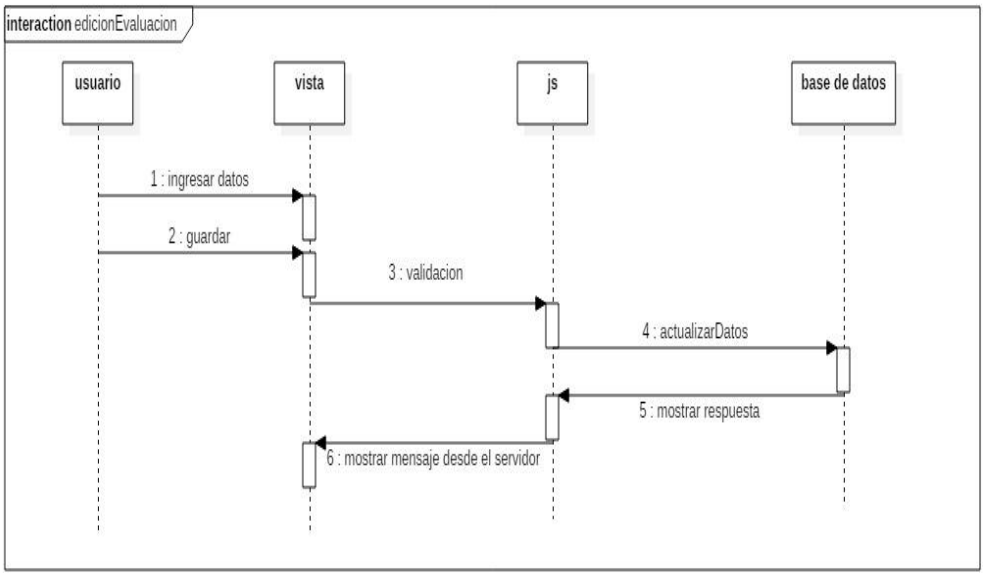


Figura 24: *Diagrama de secuencia: Edición de la Evaluación*

Fuente: Elaboración propia

En la figura 25 podemos apreciar el diagrama de secuencia “verificacion de la evaluación”, donde se selecciona el control evaluado, se verifica la evaluación, se selecciona y guardar las opciones de estado.

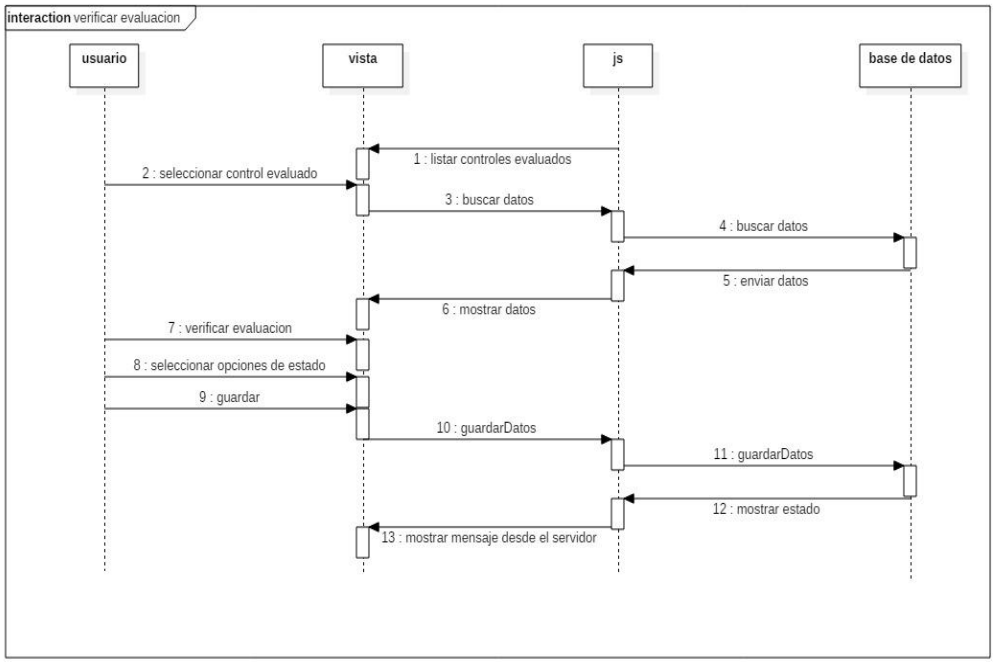


Figura 25: *Diagrama de secuencia: Verificación de la Evaluación*

Fuente: Elaboración propia

En la figura 26 podemos apreciar el diagrama de secuencia “registro de activos”, donde se ingresan y guardan los datos

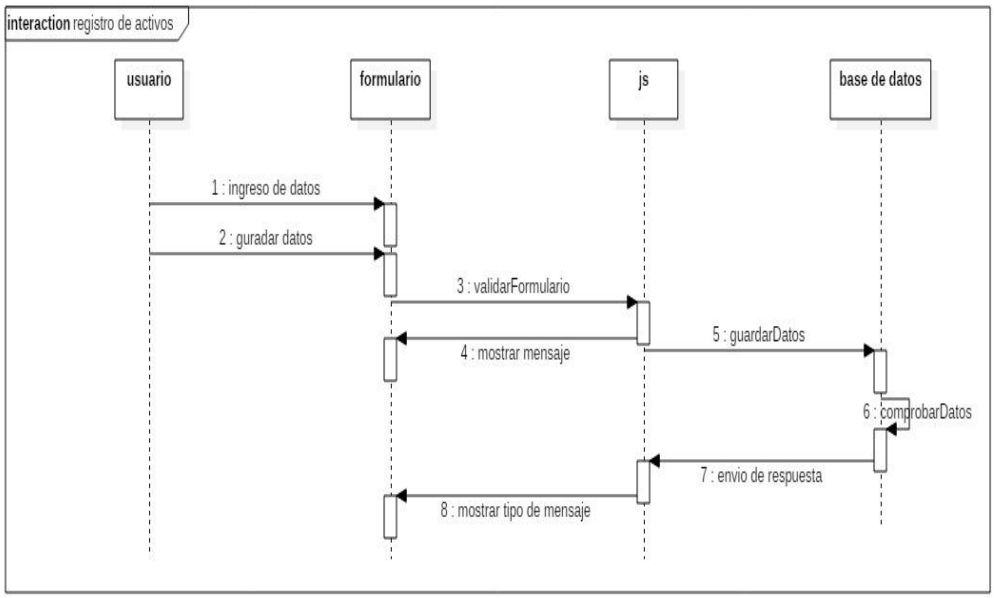


Figura 26: *Diagrama de secuencia: Registro de Activos*

Fuente: Elaboración propia

En la figura 27 se aprecia el diagrama de secuencia “reportes”, donde se puede seleccionar las opciones del reporte.

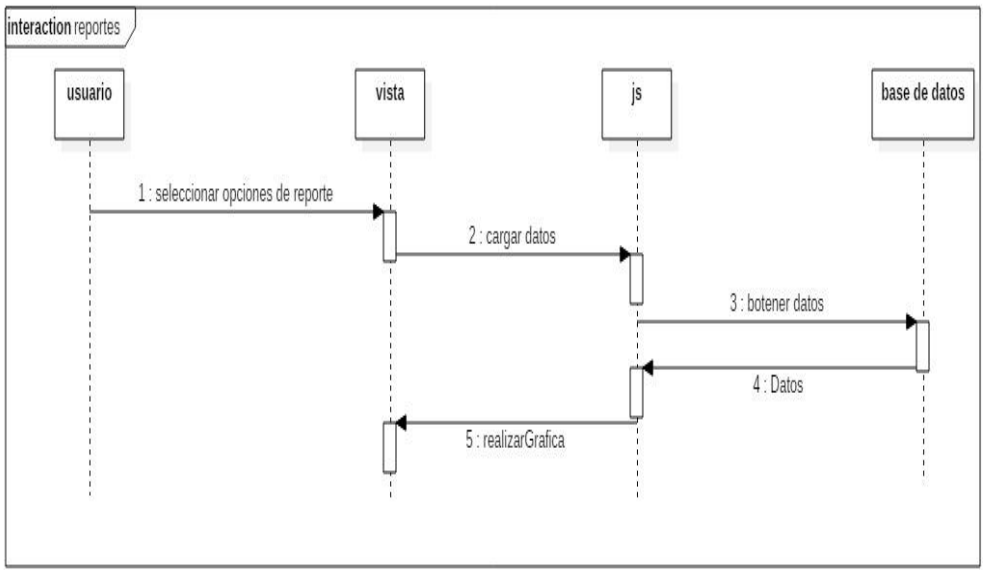


Figura 27: *Diagrama de secuencia: Reportes*

Fuente: Elaboración propia

En la figura 28 se aprecia el diagrama de secuencia “Copia de Seguridad”, donde se realiza la copia de seguridad y se descarga la copia.

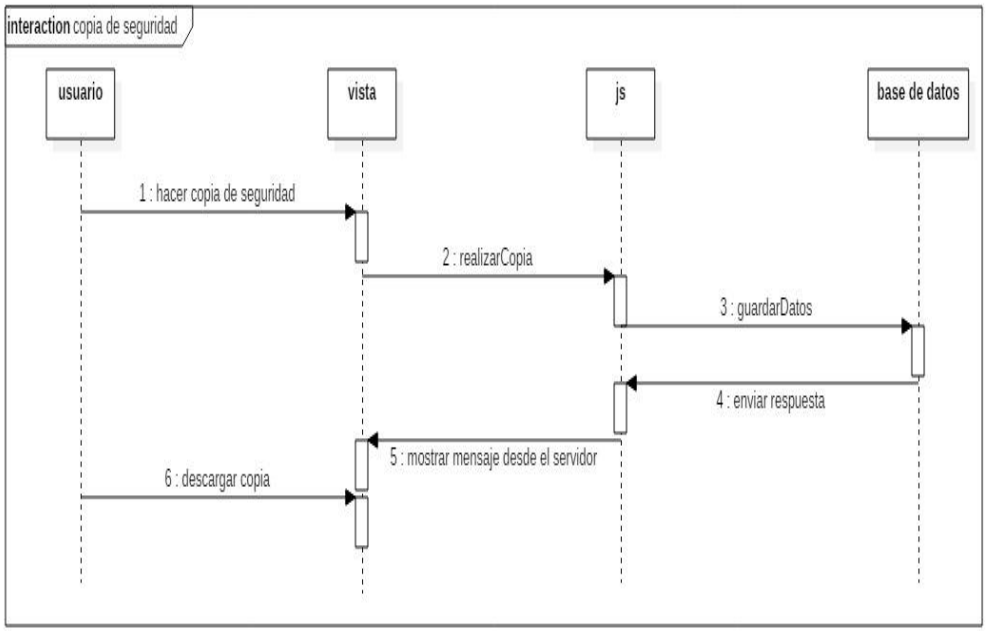


Figura 28: *Diagrama de secuencia: Copia de seguridad*

Fuente: Elaboración propia

3.3.2. FASE 2: DISEÑO

El diseño de la aplicación web para Universidad Nacional José María Arguedas se diseñó de la siguiente manera:

A. Diseño Entidad/Relación

El diseño de Sistema Web de Gestión de Seguridad de la Información Asistida por Computadora basada en el Estándar ISO 27001 en la Universidad Nacional José María Arguedas se diseñó de acuerdo a la entidad relación tal como se muestra la figura 18.

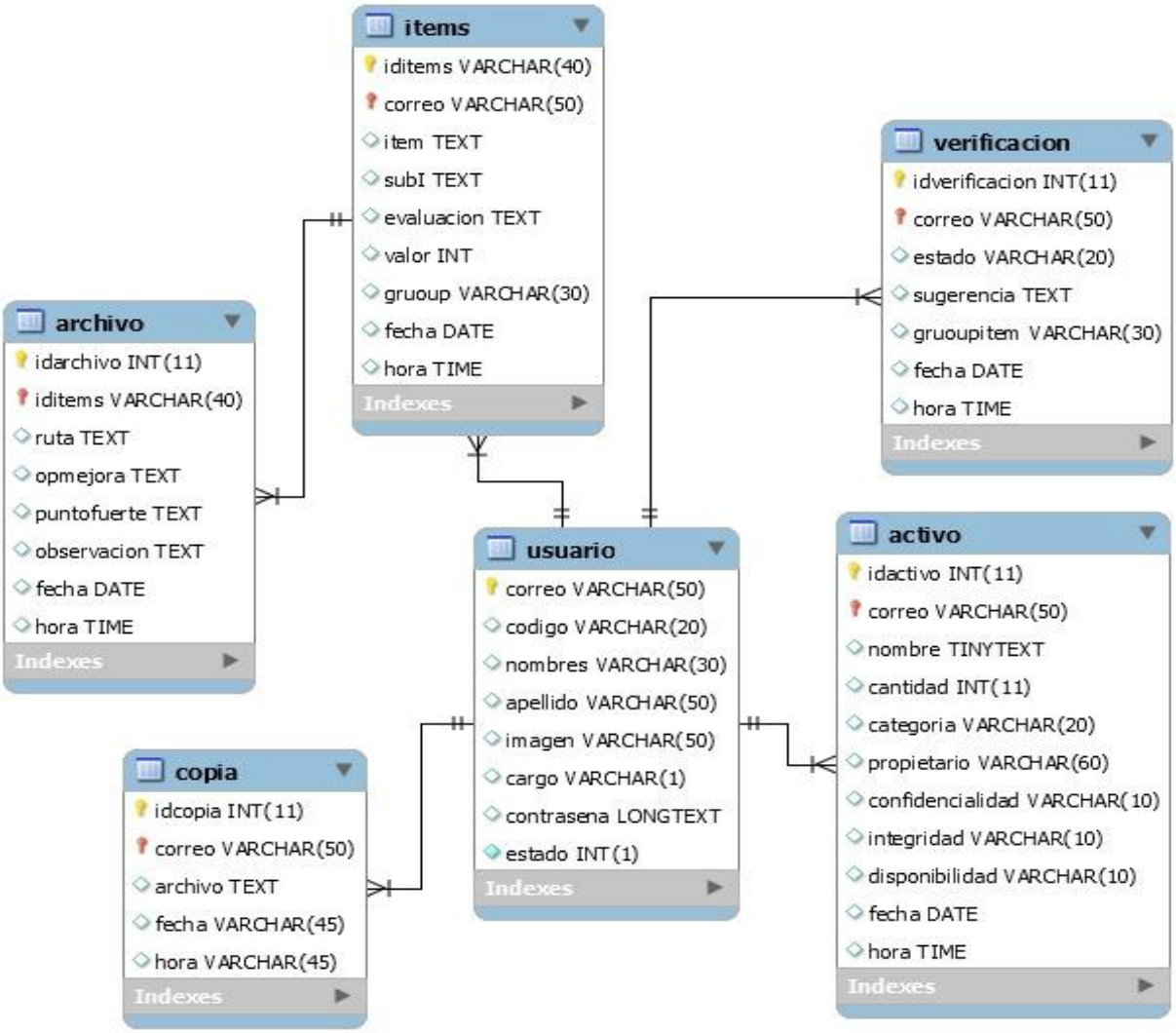


Figura 29: Base de datos: modelo entidad/relación
Fuente: Elaboración propia

B. Diseño de la navegación

El diseño de la navegación muestra que el usuario seguirá para utilizar la aplicación. Ésta se representa de manera jerárquica, donde el número de niveles representa el número de clic que debe realizar el usuario para obtener lo deseado.

Tabla 25: Identificación de los módulos

ÍTEM	DESCRIPCIÓN
1	Módulo activos
2	Módulo Evaluación de riesgo
3	Módulo Verificación
4	Módulo Reportes
5	Módulo Copia de Seguridad

Fuente: Elaboración propia

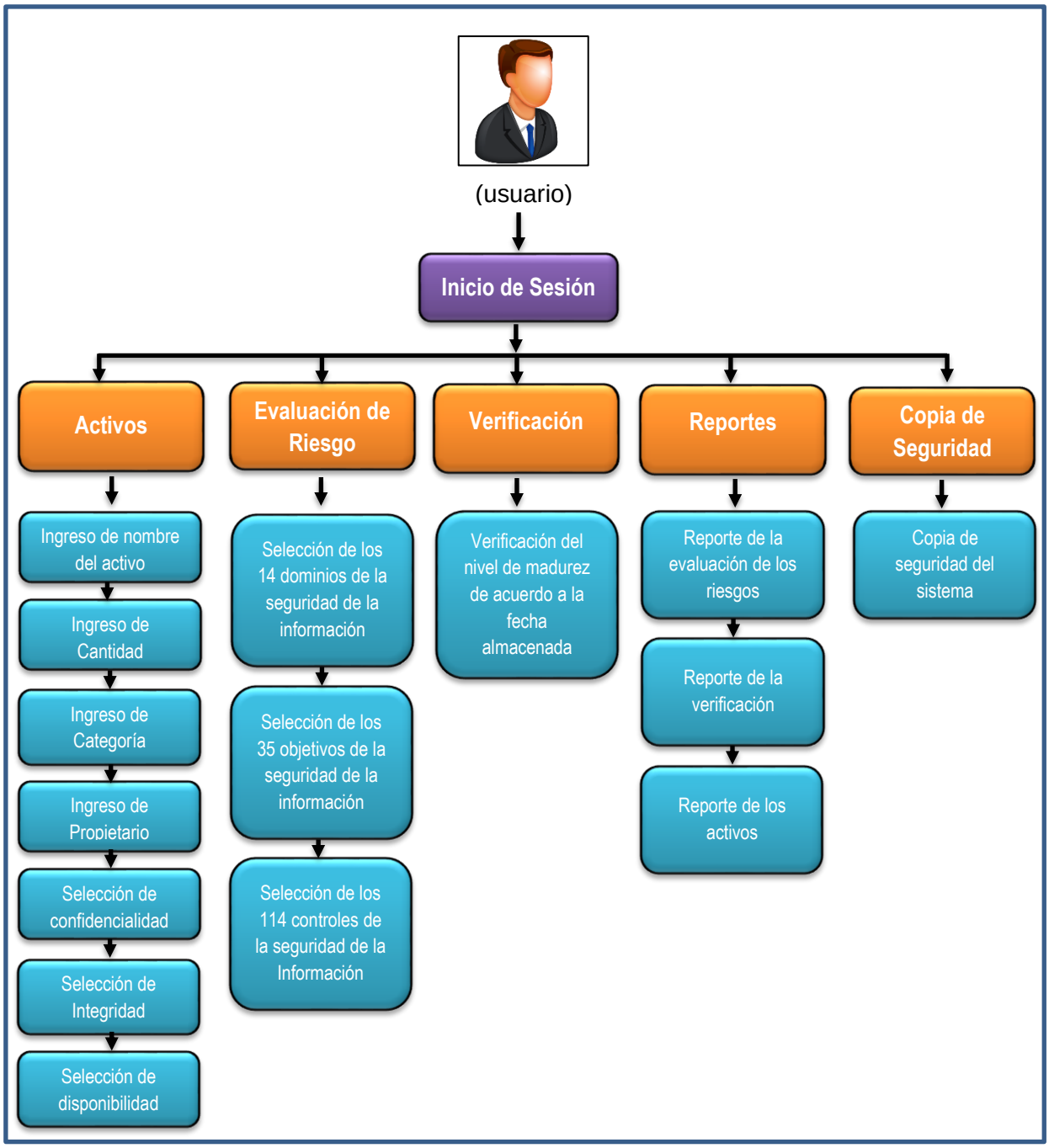


Figura 30: Diseño de navegación
Fuente: Elaboración propia

3.3.3. FASE 3: CODIFICACIÓN

A. Tecnologías utilizadas

En la codificación del desarrollo de la aplicación se utilizaron las siguientes herramientas:

- Lenguaje de programación
  - ❖ Php

- Base de datos
  - ❖ MySql
- Programa de diseño
  - ❖ HTML5
  - ❖ Boostrap
  - ❖ StarUML
  - ❖ Erwin

B. Codificación

Se ha codificado cada una de las funcionalidades de los siguientes módulos de la aplicación:

- ❖ Módulo de activo
- ❖ Módulo de Evaluación de riesgo
- ❖ Módulo de Verificación
- ❖ Módulo de reportes
- ❖ Módulo de Copia de Seguridad

Dejando en correcto funcionamiento.

3.3.4. FASE 4: PRUEBAS

Las pruebas que se realizaron a la aplicación fue un proceso constante e iterativo y se realizaron durante el desarrollo de la misma. Durante la fase de diseño e implementación se realizaron pruebas a cada uno de los módulos de la aplicación con el fin de encontrar errores y corregirlos a tiempo.

A. pruebas durante el desarrollo

La metodología de desarrollo de software XP (Programación Extrema) requiere que se realicen pruebas durante el desarrollo para verificar el correcto funcionamiento del código programado. Por lo que las pruebas se hicieron en el localhost.

B. pruebas unitarias

Las pruebas unitarias se aplicaron en cada uno de la programación de la funcionalidad de la aplicación y los errores encontradas se corrigieron dejando en correcto funcionamiento

C. pruebas integradas

Las pruebas integradas se llevaron a un conjunto de funcionalidades ya que el funcionamiento de un caso requería de otro caso, los errores encontradas se corrigieron en el momento dejando en correcto funcionamiento en forma conjunta toda la aplicación.

4. CAPÍTULO IV: EVALUACIÓN DE LA SOLUCIÓN

En el desarrollo del sistema web, se ha aplicado una serie de pruebas que verifican el correcto funcionamiento de cada uno de las funcionalidades y los módulos. Las pruebas de navegación en los diferentes menús de la aplicación y pruebas de persistencia de la base de datos a la hora de registrar los 114 controles de la seguridad de la información e ingreso de los activos.

4.1. PRUEBAS DE NAVEGACIÓN

La interfaz de la navegación se puede realizar desde cualquier computador con acceso a internet, para ello el usuario debe autenticarse de manera correcta y así poder ingresar al menú que se muestra en la figura 20.

Figura 31: Prueba de navegación de la Interfaz principal del sistema web
Fuente: Elaboración propia

Como se puede apreciar en el menú de la Figura 17 aparecen 6 opciones: activos, evaluación de riesgo, verificación, reportes, copia de seguridad y usuario.

- **Activos:** el módulo activo es donde se ingresan los activos de la institución, cada uno de ellos cuenta con las siguientes características:
  - ❖ Nombre del activo

- ❖ Cantidad
- ❖ Categoría
- ❖ Propietario
- ❖ Confidencialidad
- ❖ Integridad
- ❖ Disponibilidad.

En la que se mide a través de una tabla de colores (rojo, amarillo y verde) el nivel de importancia de la confidencialidad, integridad y disponibilidad de cada activo, en donde rojo es de mayor importancia y verde el de menor importancia.

- **Evaluación de Riesgo:** En la evaluación de riesgo, el sistema nos permite evaluar a la institución de acuerdo ISO 27001: 2013 el cual cuenta con 14 dominios, 35 objetivos y 114 controles a los que se mide el nivel de madurez, de acuerdo a la figura 18.

Figura 32: Medición del nivel de madurez
Fuente: Elaboración propia

Figura 33: Medición del nivel de madurez por cada control de seguridad de la información
Fuente: Elaboración propia

- **Verificación**: En el módulo verificación de puede visualizar el nivel de madures de cada control evaluado, con su respectiva fecha.

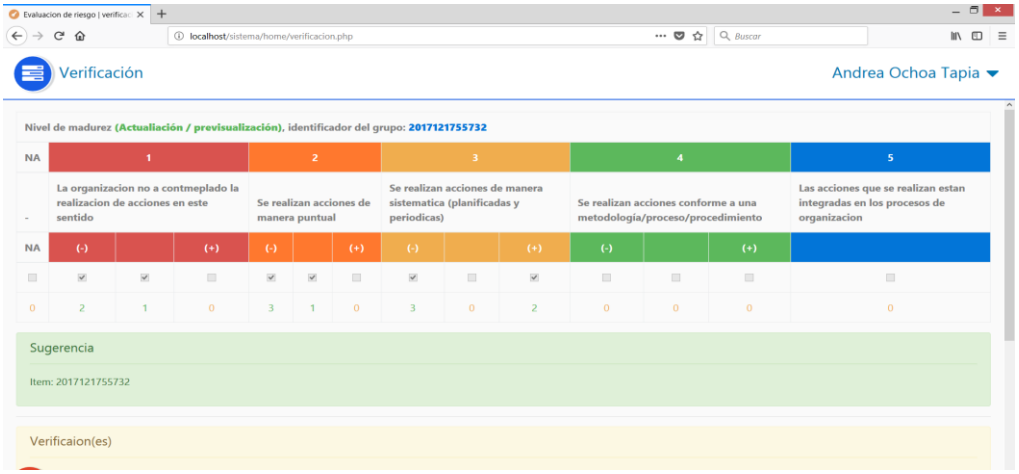


Figura 34: Verificación del nivel de madurez
Fuente: Elaboración propia

- **Reportes:** En el módulo reportes se aprecia el reporte de la evaluación de riesgo.

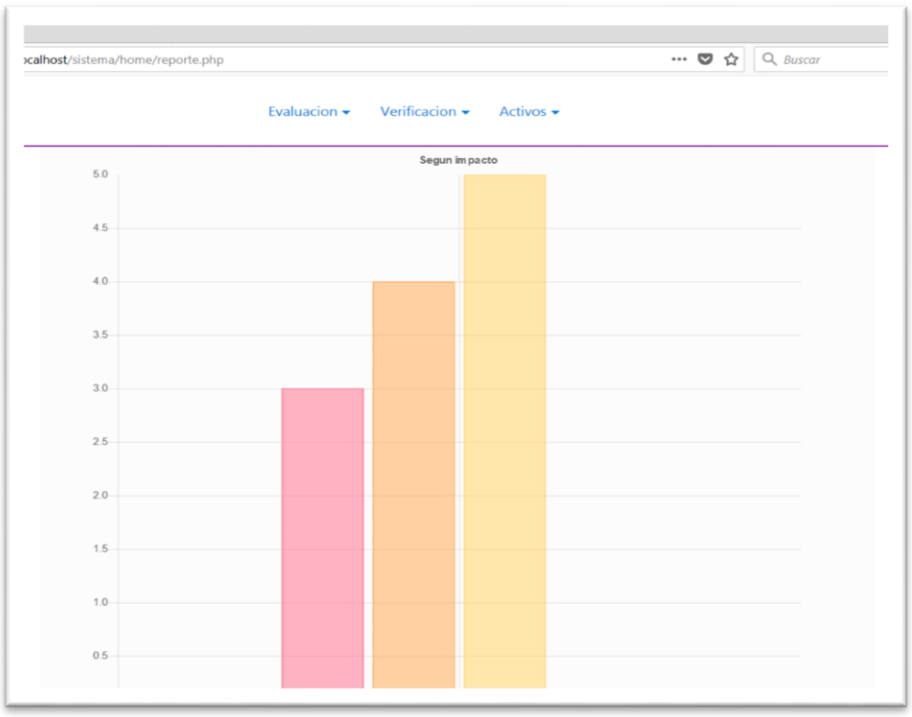


Figura 35: Reporte de la evaluación de riesgo
Fuente: Elaboración propia

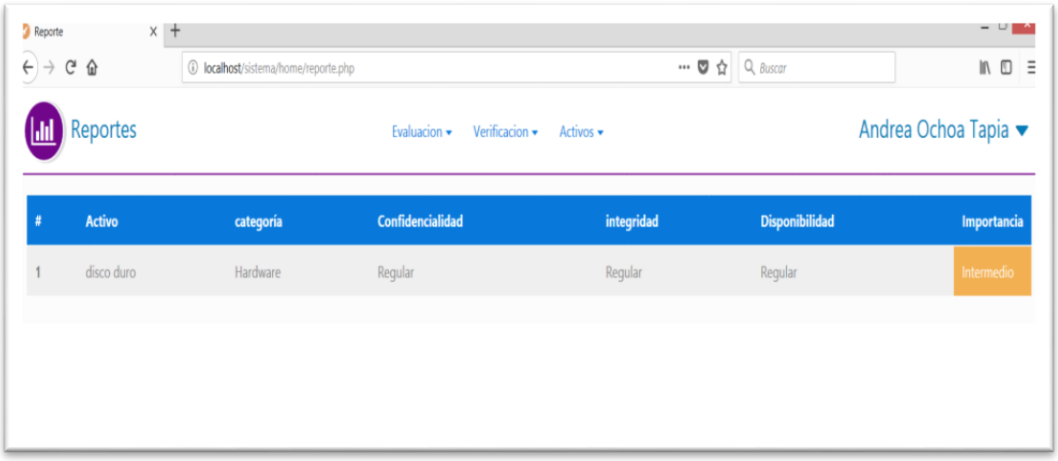


Figura 36: Reporte de los activos
Fuente: Elaboración propia

- **Copia de seguridad:** Este módulo se encarga de hacer una copia de seguridad de toda la base de datos del sistema.

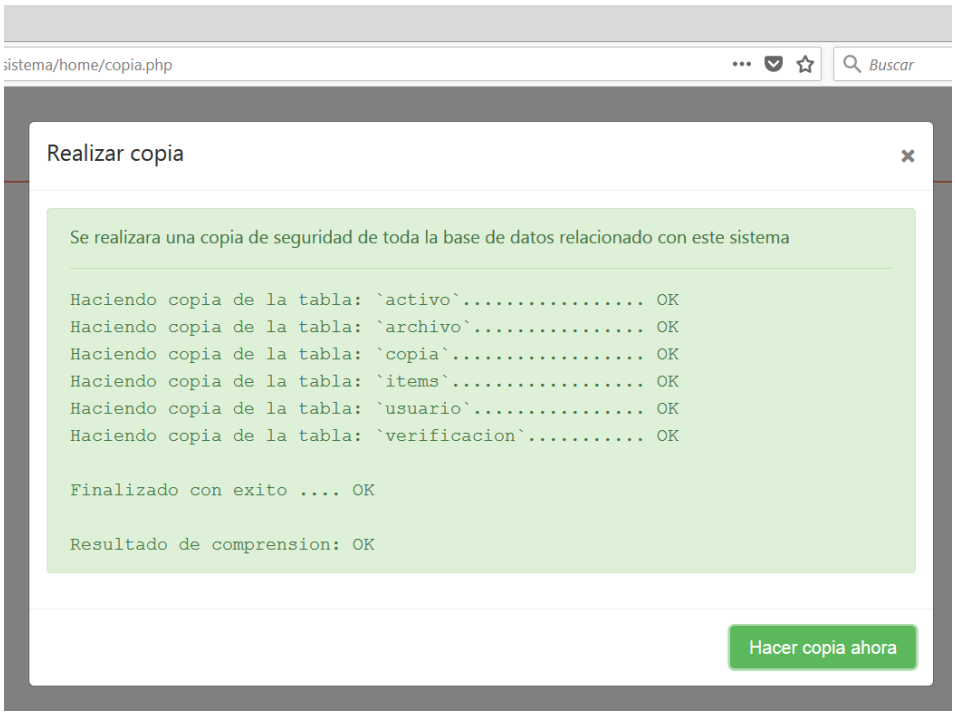


Figura 37:Copia de seguridad
Fuente: Elaboración propia

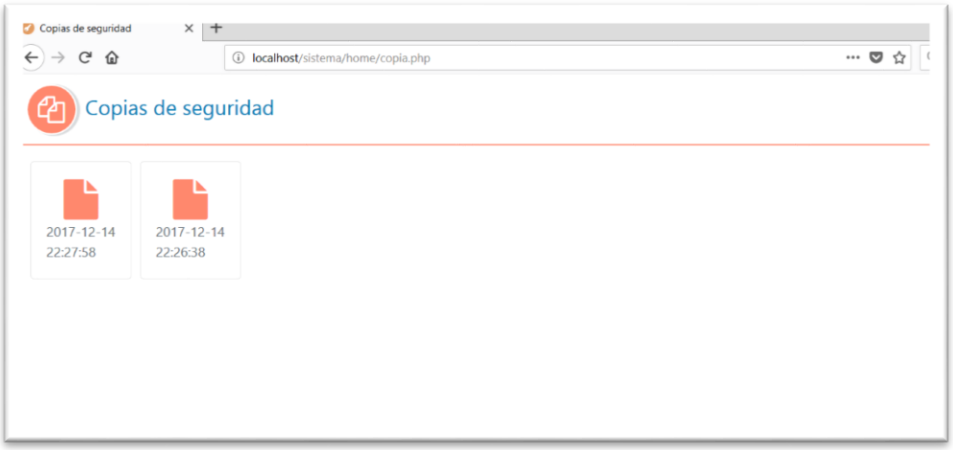


Figura 38:Copias de seguridad guardadas
Fuente: Elaboración propia

4.2. PRUEBAS DE USABILIDAD:

La prueba de usabilidad permite conocer si la interfaz de usuario es amigable, intuitiva y si funciona correctamente. Para esta prueba se mostró y se pidió a los trabajadores de la Oficina de Sistemas de Información de la Universidad Nacional José María Arguedas y se analizó lo siguiente:

- Número total de actividades realizadas exitosamente.
- El tiempo empleado en realizar una actividad.

Para analizar las pruebas se indicó al usuario que inicie sesión y realizar las actividades en la aplicación.

Al finalizar las pruebas se aplicó una encuesta (Anexo: Formato de usabilidad) obteniendo que el 100% de los trabajadores realizó las actividades exitosamente.

El tiempo empleado para realizar una actividad fue óptimo para el 100% de los trabajadores.

4.3. PRUEBAS DE FUNCIONALIDAD

La prueba funcional se aplica para validar si el comportamiento de la aplicación cumple con las especificaciones. Esta prueba se realizó teniendo en cuenta los casos de uso definidos en la fase de análisis y diseño. Los resultados en todos los casos fueron favorables para los trabajadores de la Oficina de Sistemas de información de la Universidad Nacional José María Arguedas. La aplicación funciona correctamente de acuerdo a lo especificado.

4.4. PRUEBAS DE PORTABILIDAD

La prueba de portabilidad permite verificar la funcionalidad de la aplicación en diferentes tipos de computador con acceso a internet. Para ello se utilizó los equipos de cómputo de la Oficina de Sistemas de Información de la Universidad Nacional José María Arguedas obteniendo resultados satisfactorios, ya que se proporciona los procesos de forma fácil y rápida.

5. CAPÍTULO V: CONCLUSIONES

CONCLUSIÓN GENERAL

Se desarrolló un Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad Nacional José María Arguedas.

CONCLUSIONES ESPECÍFICOS

- Se analizó y diseñó los procesos y controles de gestión de la seguridad de la información de la Universidad Nacional José María Arguedas.
- Se construyó y probó eficientemente las medidas y controles de gestión de la seguridad de la información en la Universidad Nacional José María Arguedas.
- Se implementó y desplegó los controles del sistema de gestión de seguridad de la información en la Universidad Nacional José María Arguedas.

6. CAPÍTULO VI: RECOMENDACIONES

PRIMERO: Se recomienda en un futuro analizar y diseñar los procesos y controles de gestión de la seguridad de la información de la Universidad Nacional José María Arguedas incluyendo la ISO 31000 para la gestión de riesgo.

SEGUNDO: Realizar capacitaciones para la prueba de las medidas y controles de la gestión de la seguridad de la información en la Universidad Nacional José María Arguedas.

TERCERO: Realizar capacitaciones para el uso e Implementación de los controles del sistema de gestión de la seguridad de la Información en todas las áreas de la Universidad Nacional José María Arguedas.

7. REFERENCIAS BIBLIOGRÁFICAS

Alarcón, V. F. (2006). *Desarrollo de sistemas de información: una metodología basada en el modelado.* catalunya: edicions UPC.

Alegsa, L. (05 de 03 de 2014). *alegsa*. Obtenido de http://www.alegsa.com.ar

andreu, ricart y valor. (1996). sistemas de información. En V. F. Alarcón, *Desarrollo de sistemas de información: una metodología basada en el modelado* (pág. 14). españa: edicions upc.

C. (s.f.).

Fonseca. (2012). La información el activo más importante de cualquier organizacion.

GESCONSULTOR. (2015). ISO 27001 – Sistema de Gestión de la Seguridad de la Información. *GESCONSULTOR*, 1.

Información, E. G. (2012). *Encuesta de Agenda de Riesgo de Tecnologias de la Información*. Mexico.

Juan, P. (2007). *Flexibilidad con Scrum, principios de diseño e implantación en campos Scrum.*

Martinez. (2005). Importancia de los sistemas de información para las pequeñas empresas.

poveda, j. M. (2011). Estándares de gestión de la seguridad de la información . *auditoria informatica*, 4.

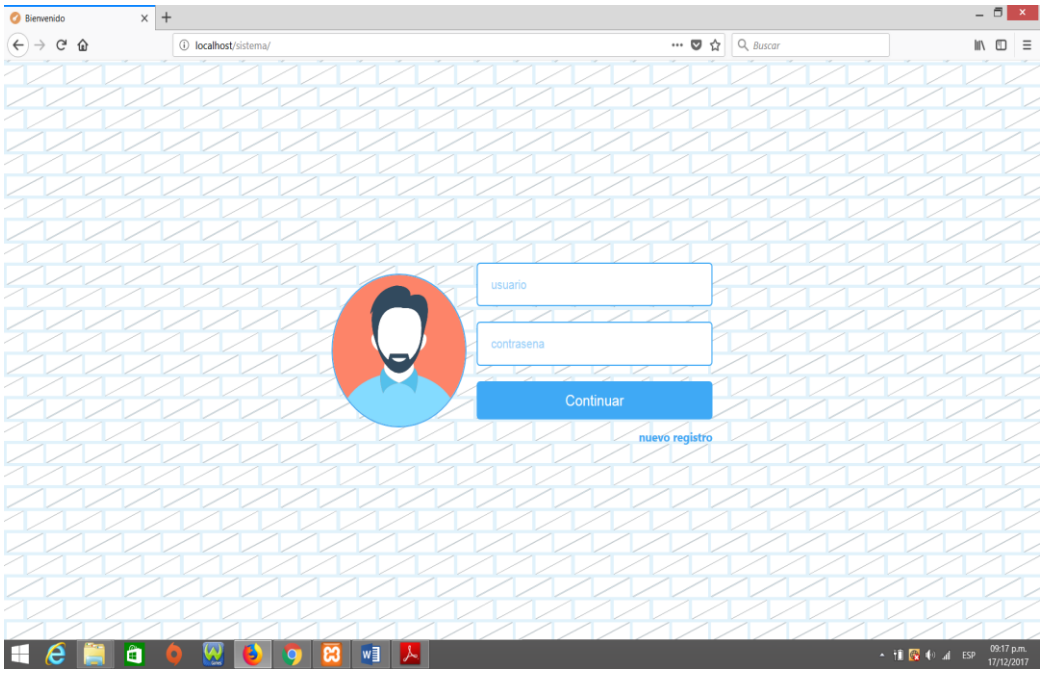
Project Management Consultores de Proyectos, S. (2006). Sistemas de Gestión de la Seguridad de la Informacion: ISO 27001. *Project Management Consultores de Proyectos, S.A.*, 1-2.

Valle, F. R. (2012). *Censo empresarial de la provincia de Andahuaylas*. Andahuaylas, Apurimac.

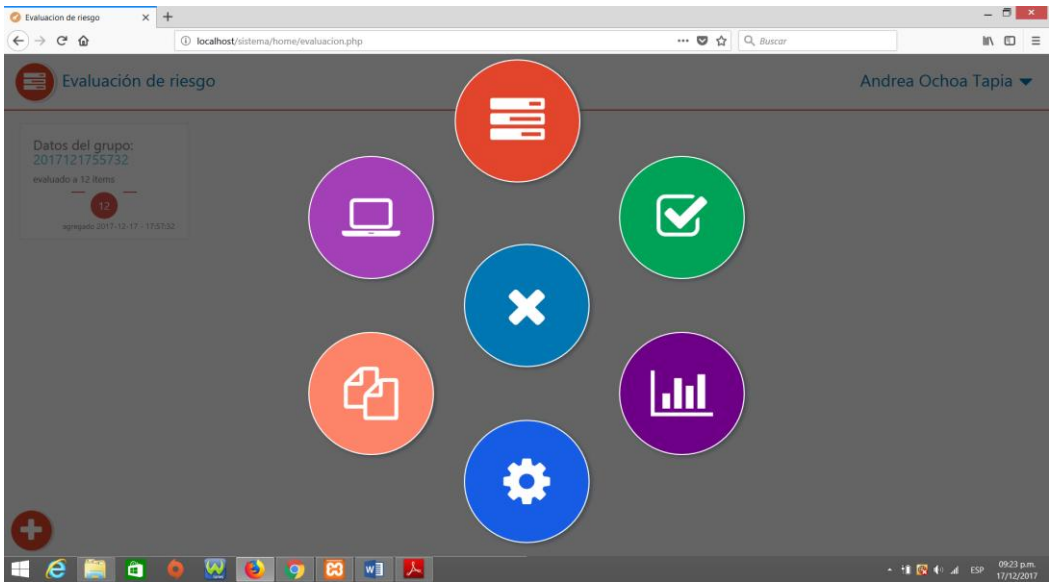
8. ANEXOS

8.1. MANUAL DE USUARIO

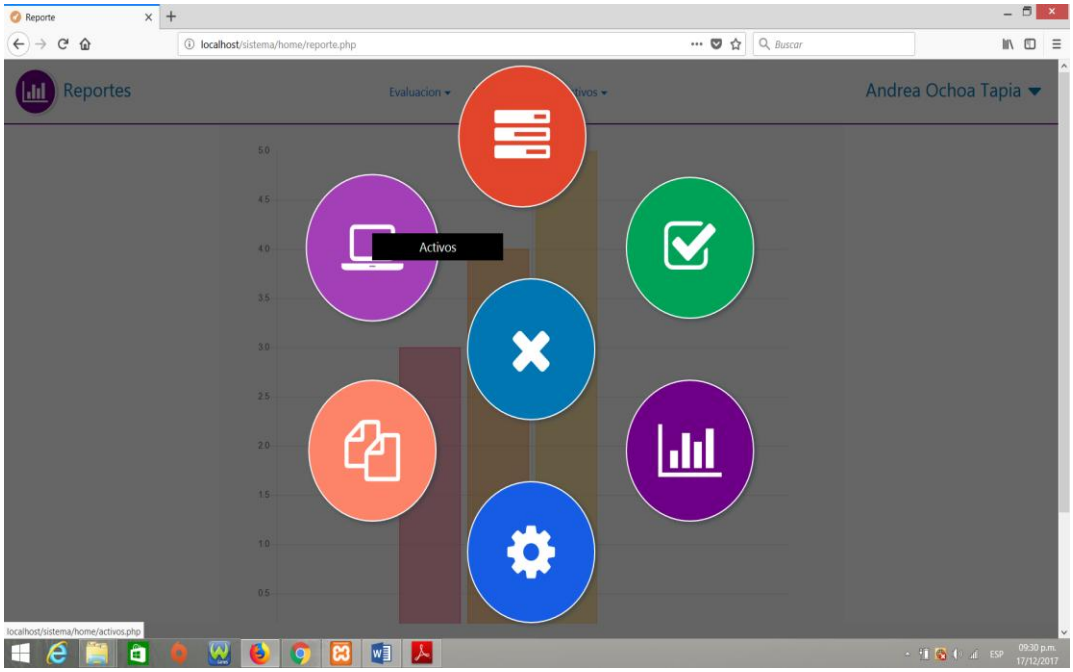
A. Inicio de sesión en el sistema: El usuario inicia sesión con usuario y una contraseña establecida.

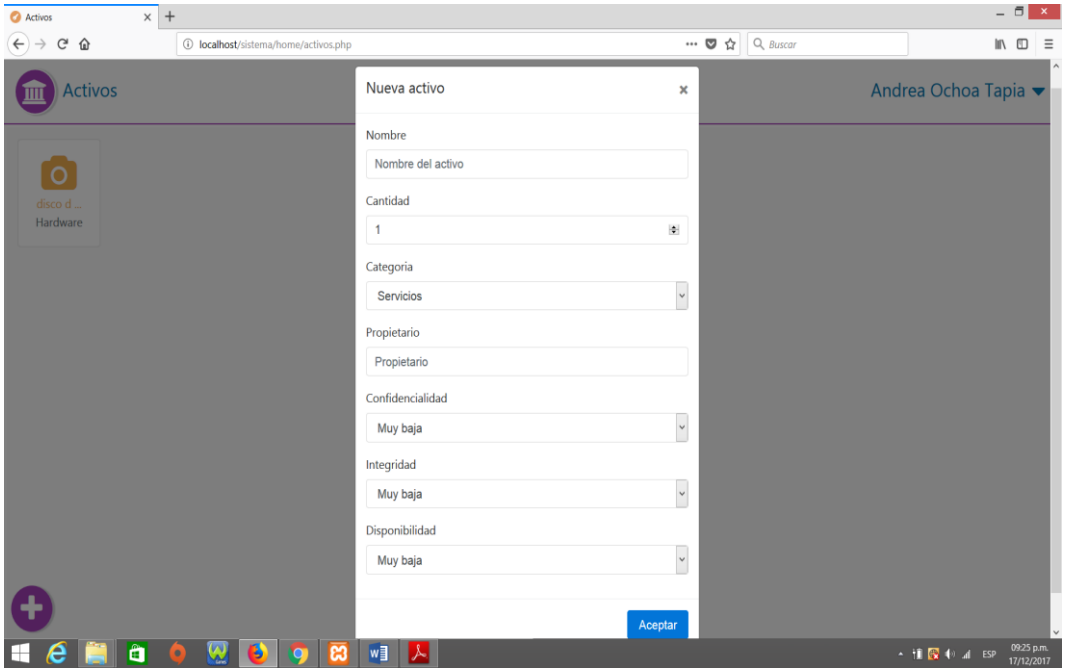


B. Ingreso al menú: Se muestra el siguiente menú el cual contiene 6 módulos.

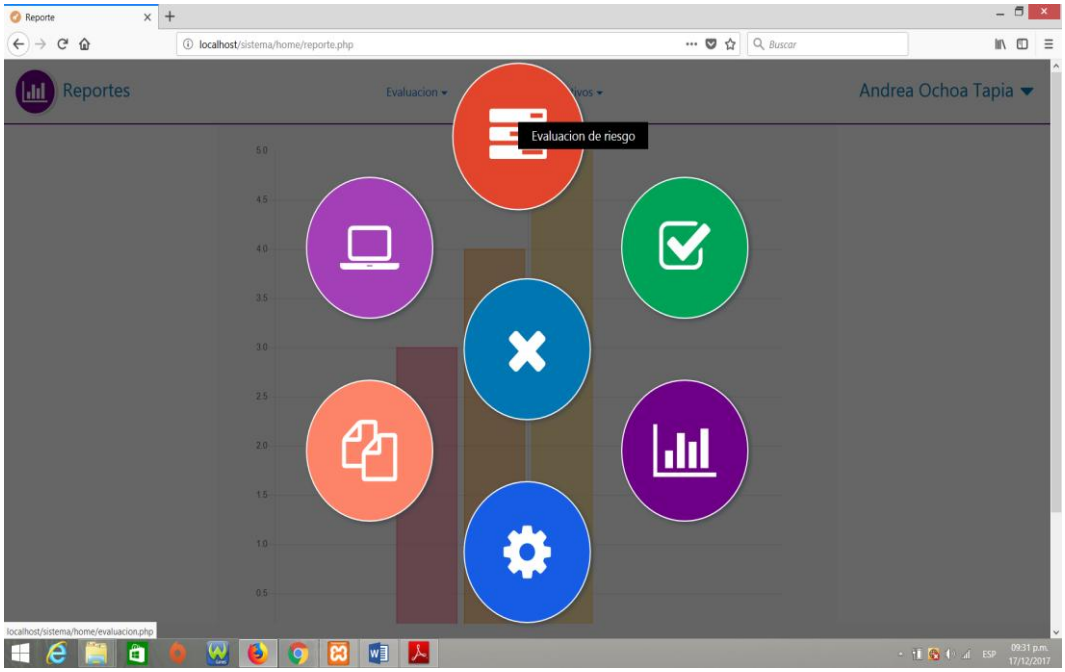


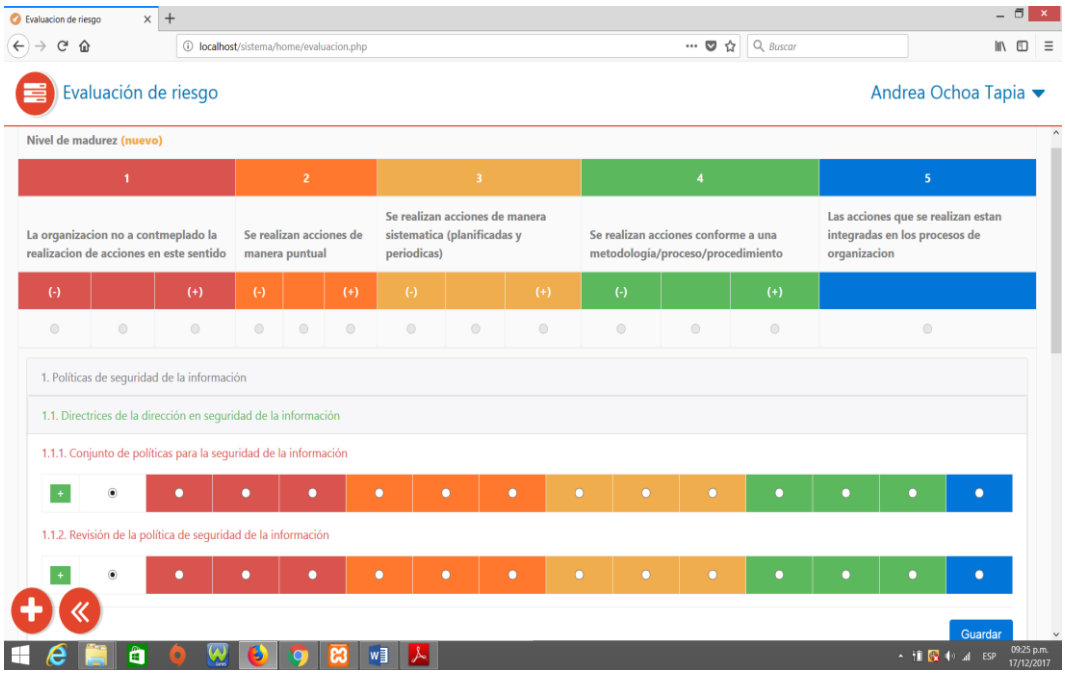
C. Módulo 1 - Activos: El usuario puede ingresar los activos de la institución, en el cual se le dará el nivel de importancia del activo.



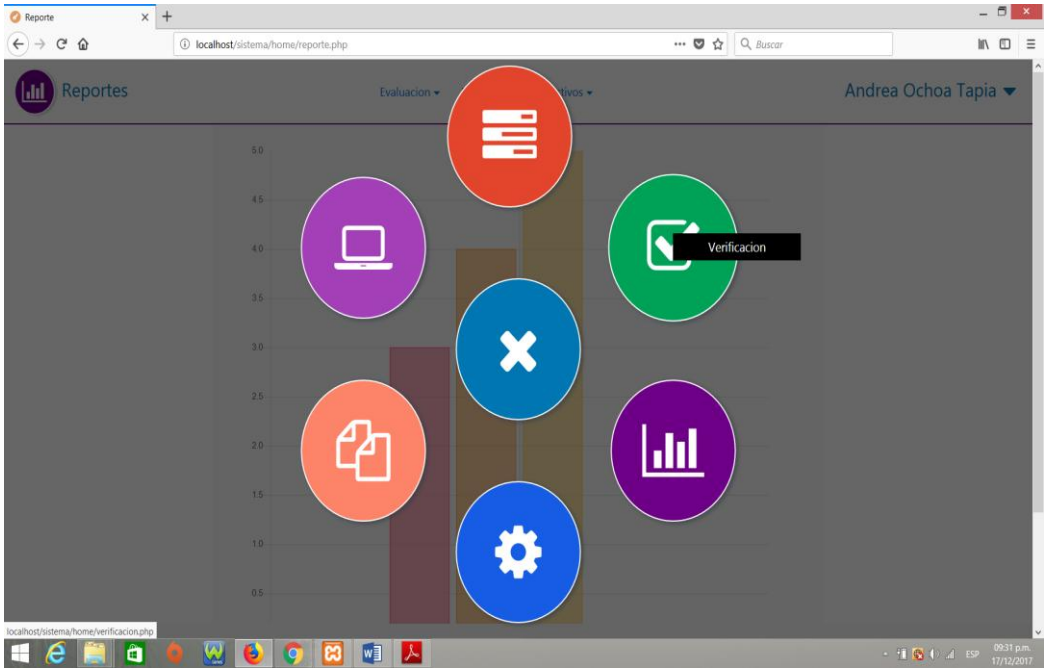


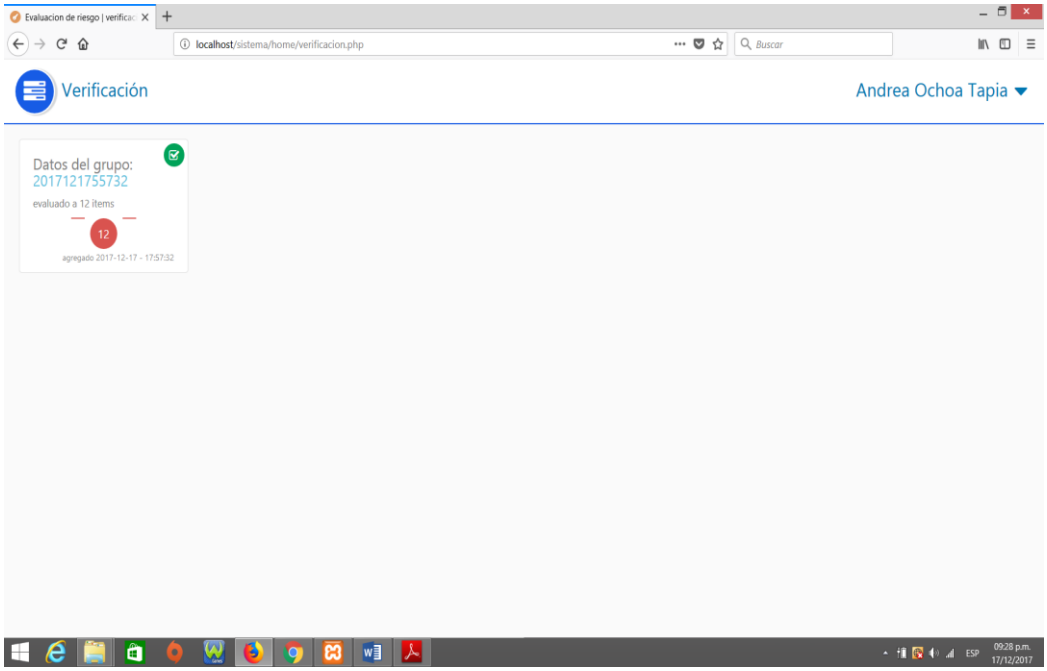
D. Módulo 2 - Evaluación de riesgo: El usuario evaluará los 14 dominios que contienen 35 objetivos y 114 controles de la seguridad de la información basada en la ISO 27001

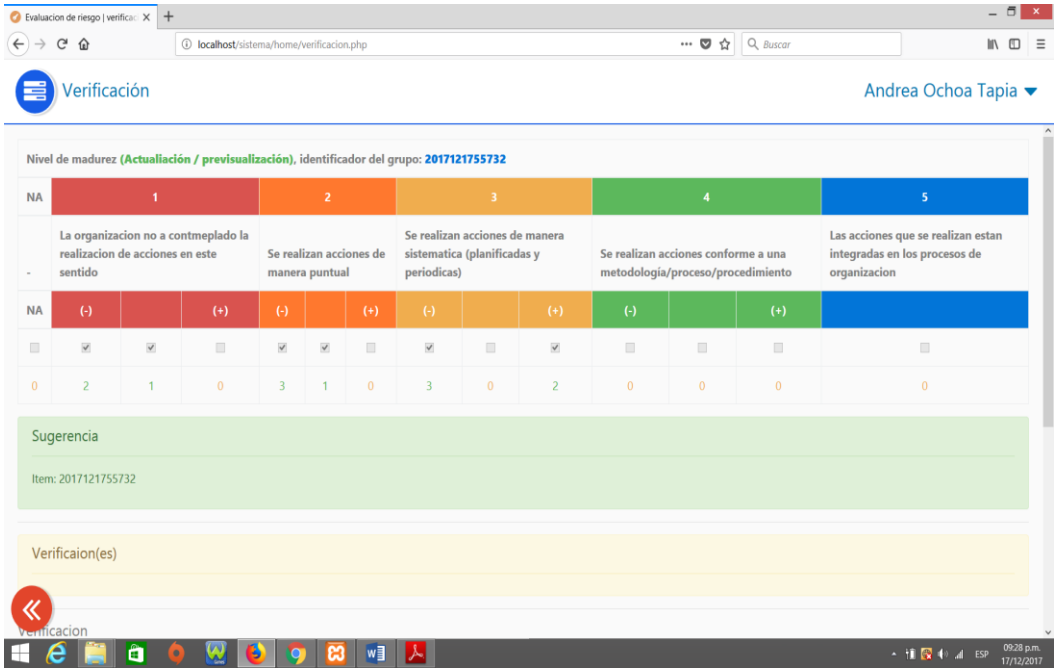




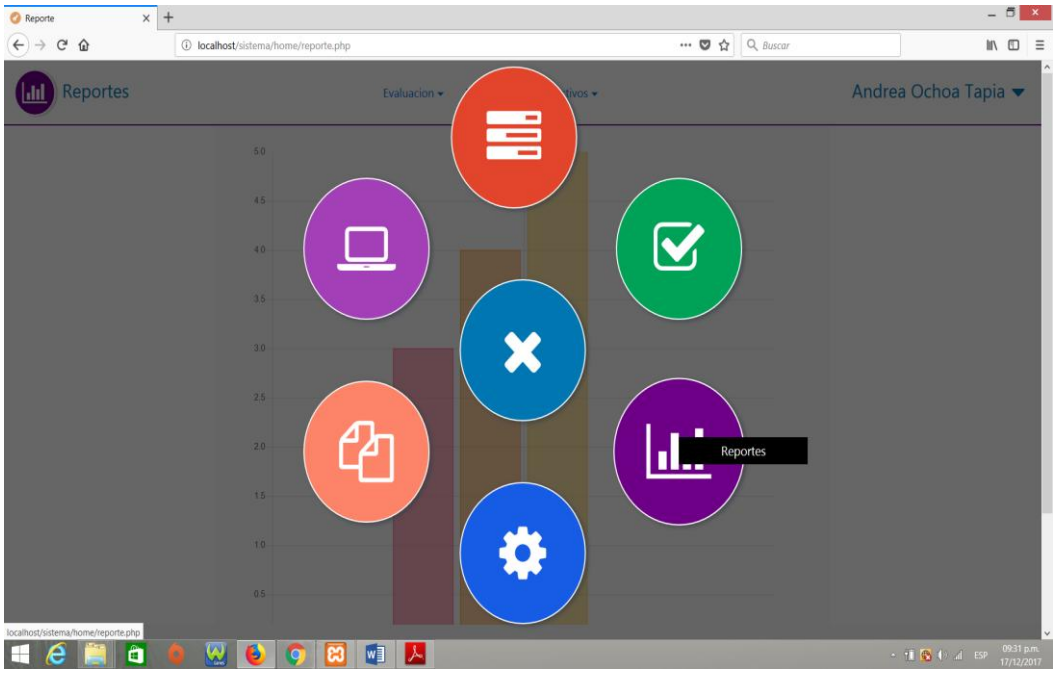
E. Módulo 3 - Verificación: En este módulo el usuario puede verificar el nivel de madurez de los controles de seguridad evaluados:


Reporte
localhost/sistema/home/reporte.php
Buscar
Reportes
Evaluacion
Andrea Ochoa Tapia
Verificacion
localhost/sistema/home/verificacion.php
ESP
09:31 p.m.
17/12/2017

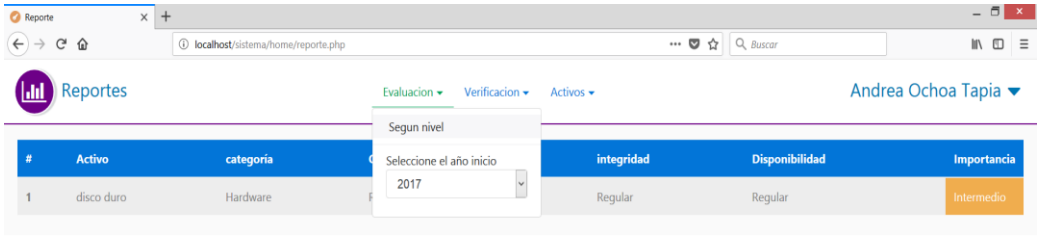

Evaluacion de riesgo | verificac
localhost/sistema/home/verificacion.php
Buscar
Verificación
Andrea Ochoa Tapia
Datos del grupo:
201712175732
evaluado a 12 items
12
agregado 2017-12-17 - 17:57:32
ESP
09:28 p.m.
17/12/2017

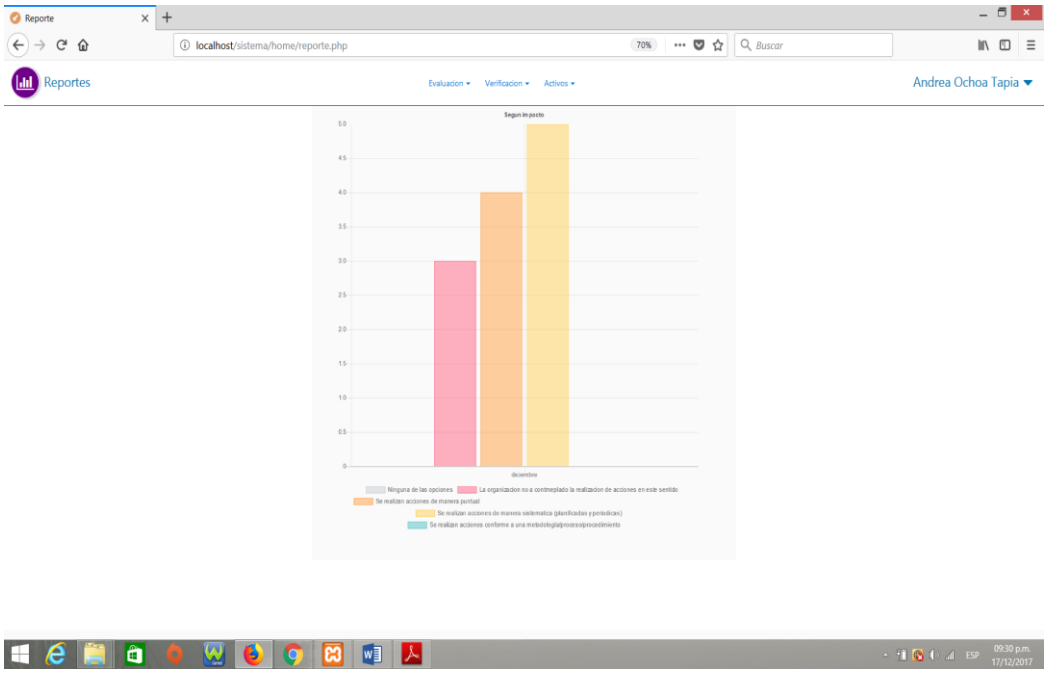


F. Módulo 4 - Reportes: En este módulo el usuario puede verificar los reportes según evaluación, verificación y según activos

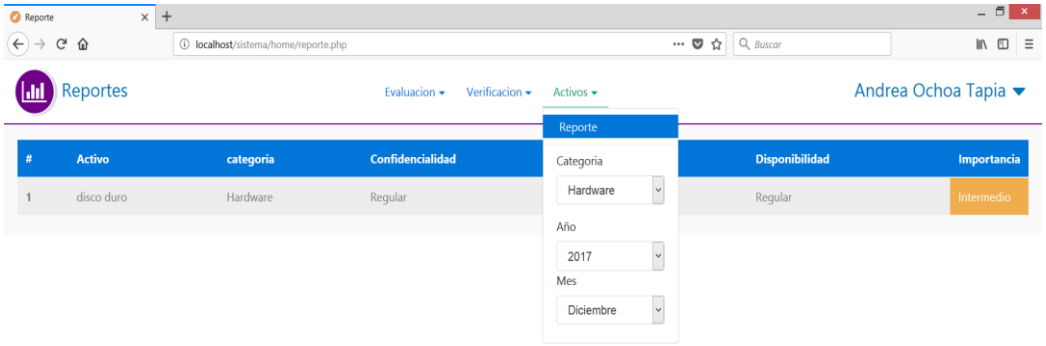


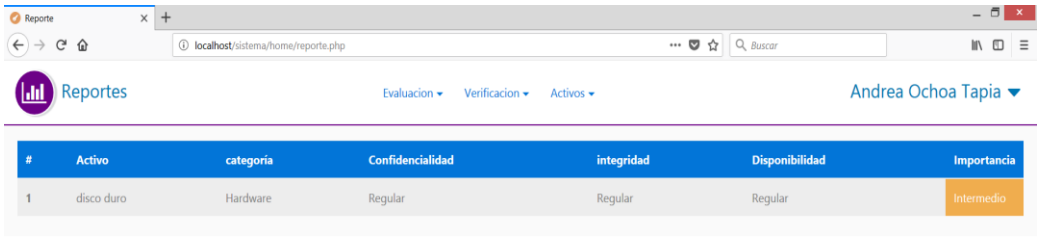
Reporte de la evaluación



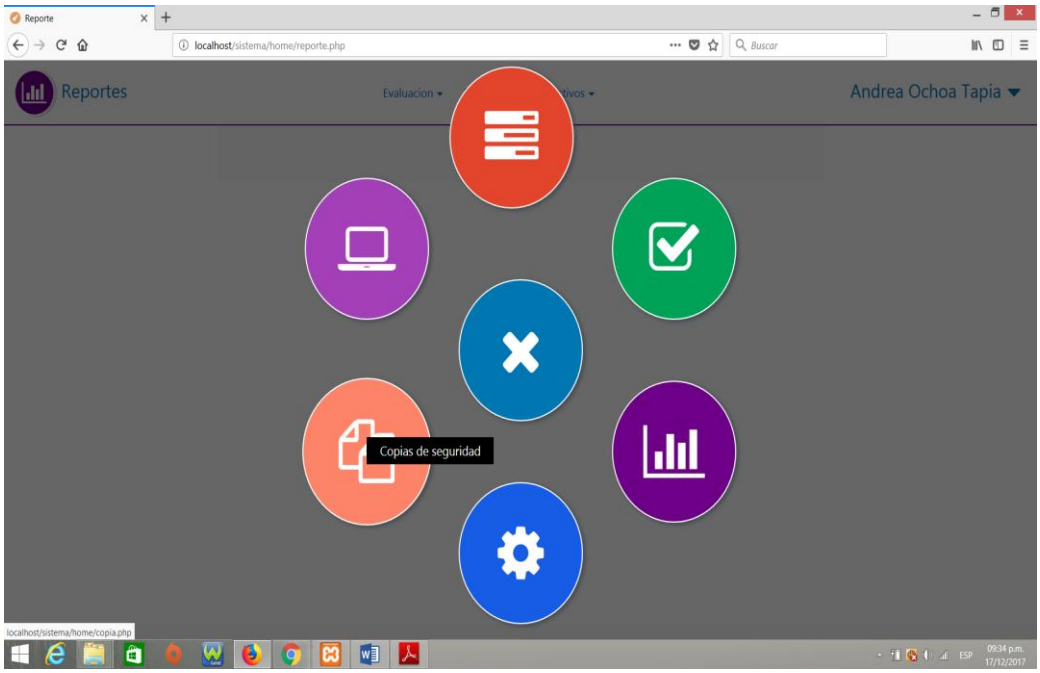


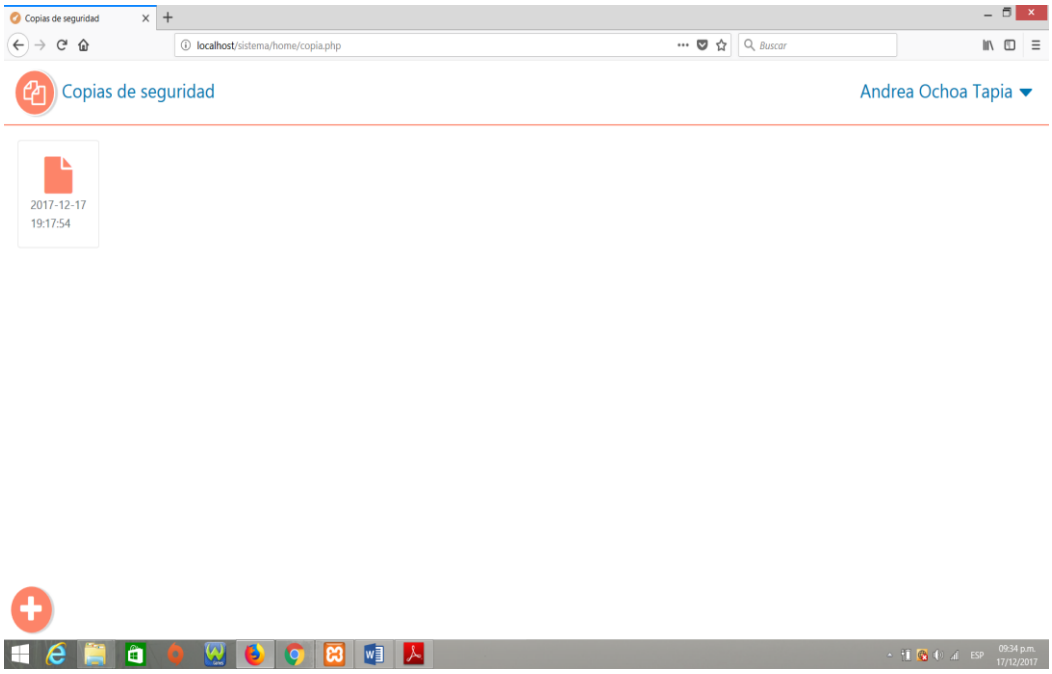
Reporte de los activos

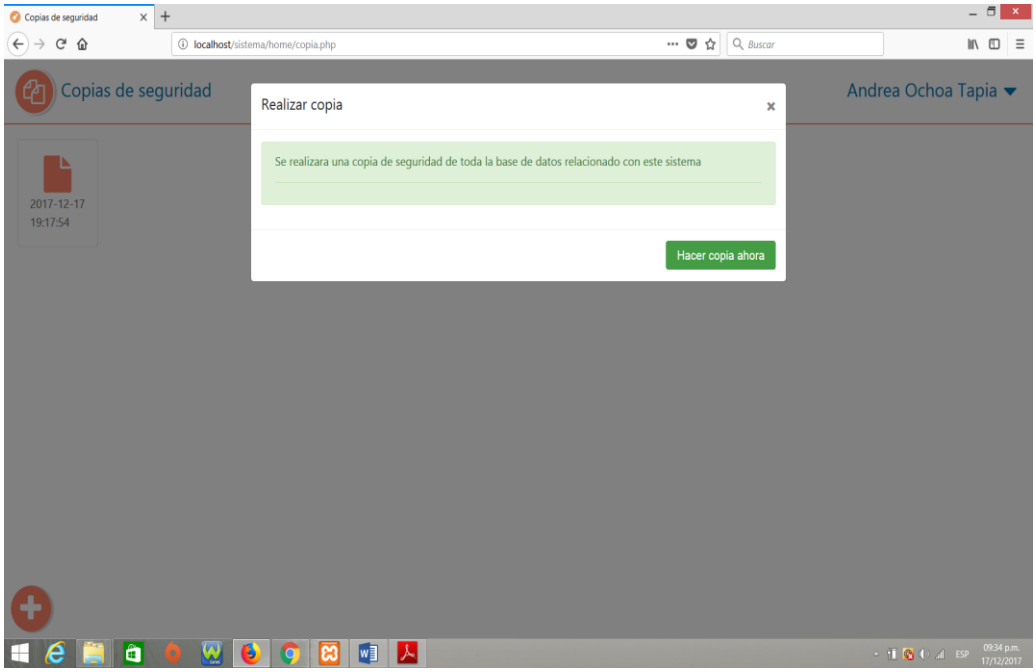


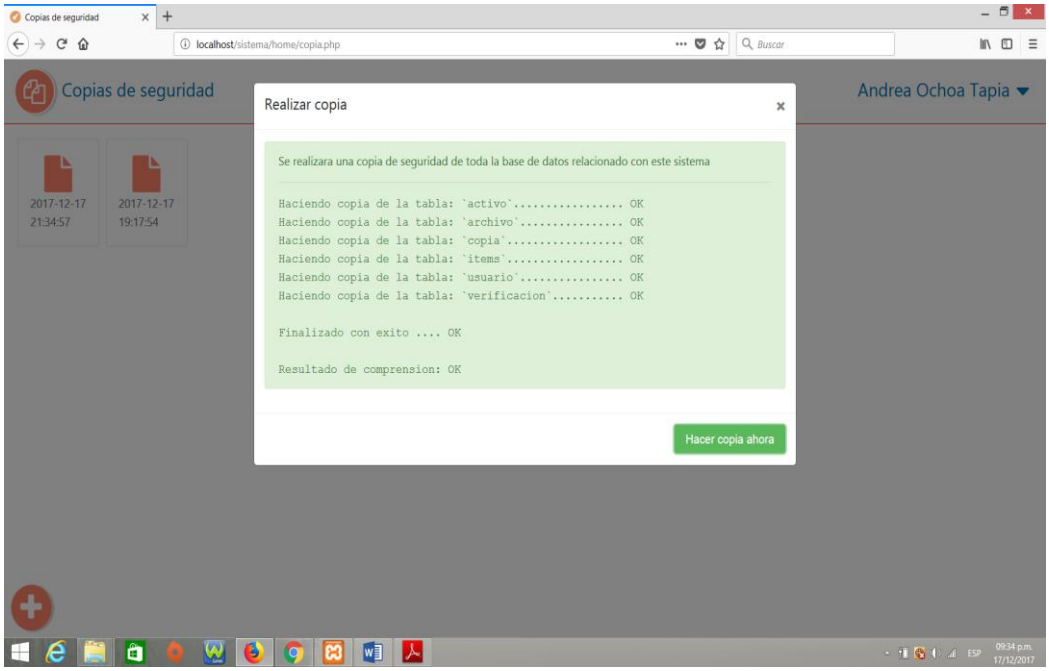


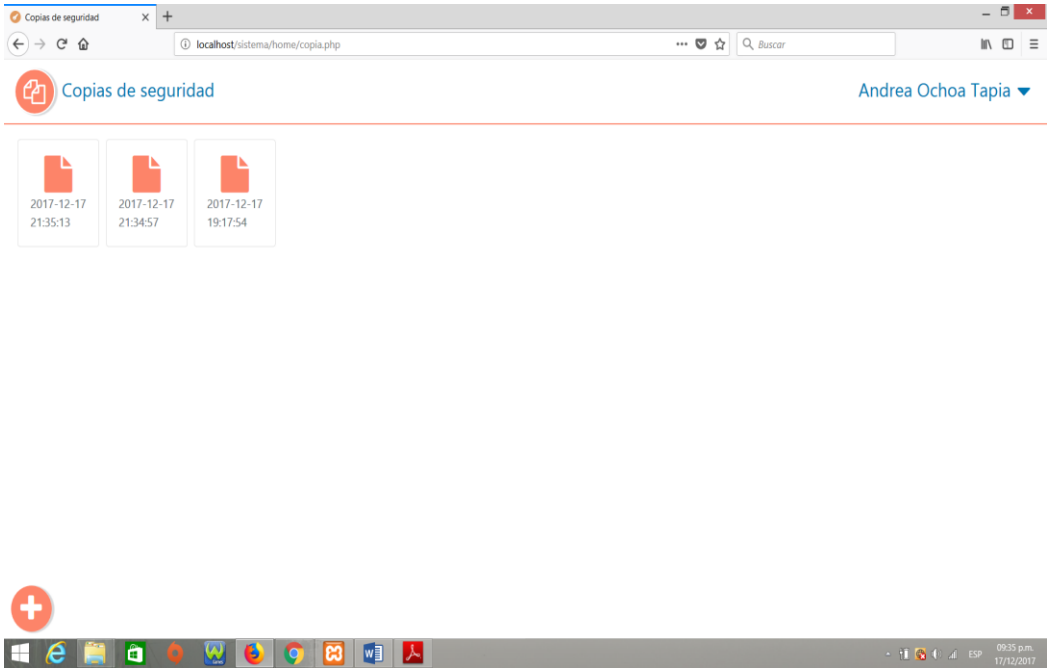
G. Módulo 5 - Copia de seguridad



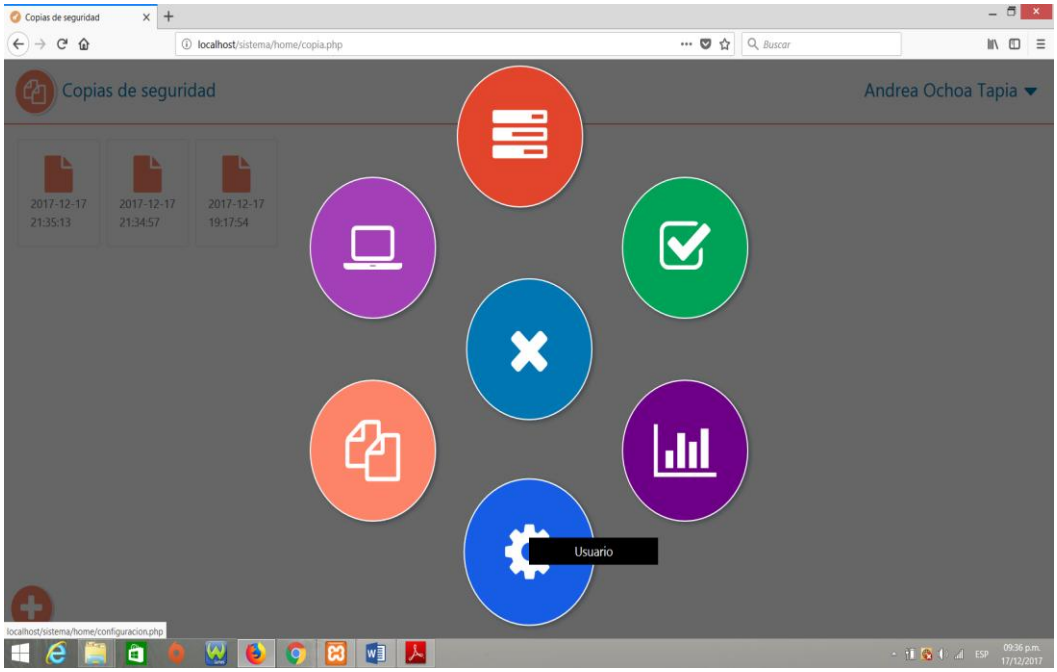


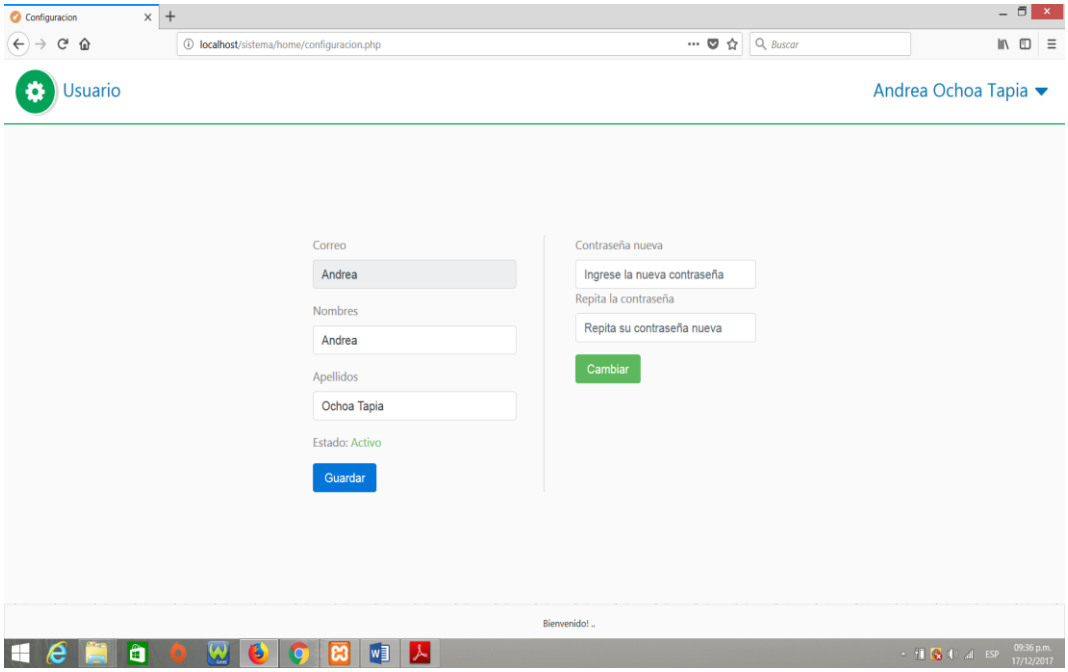

Copias de seguridad
Andrea Ochoa Tapia
Realizar copia
Se realizara una copia de seguridad de toda la base de datos relacionado con este sistema
Hacer copia ahora
2017-12-17
19:17:54


Copias de seguridad
Andrea Ochoa Tapia
Realizar copia
Se realizara una copia de seguridad de toda la base de datos relacionado con este sistema
Haciendo copia de la tabla: `activo`..... OK
Haciendo copia de la tabla: `archivo`..... OK
Haciendo copia de la tabla: `copia`..... OK
Haciendo copia de la tabla: `items`..... OK
Haciendo copia de la tabla: `usuario`..... OK
Haciendo copia de la tabla: `verificacion`..... OK
Finalizado con exito .... OK
Resultado de comprension: OK
Hacer copia ahora
2017-12-17
21:34:57
2017-12-17
19:17:54



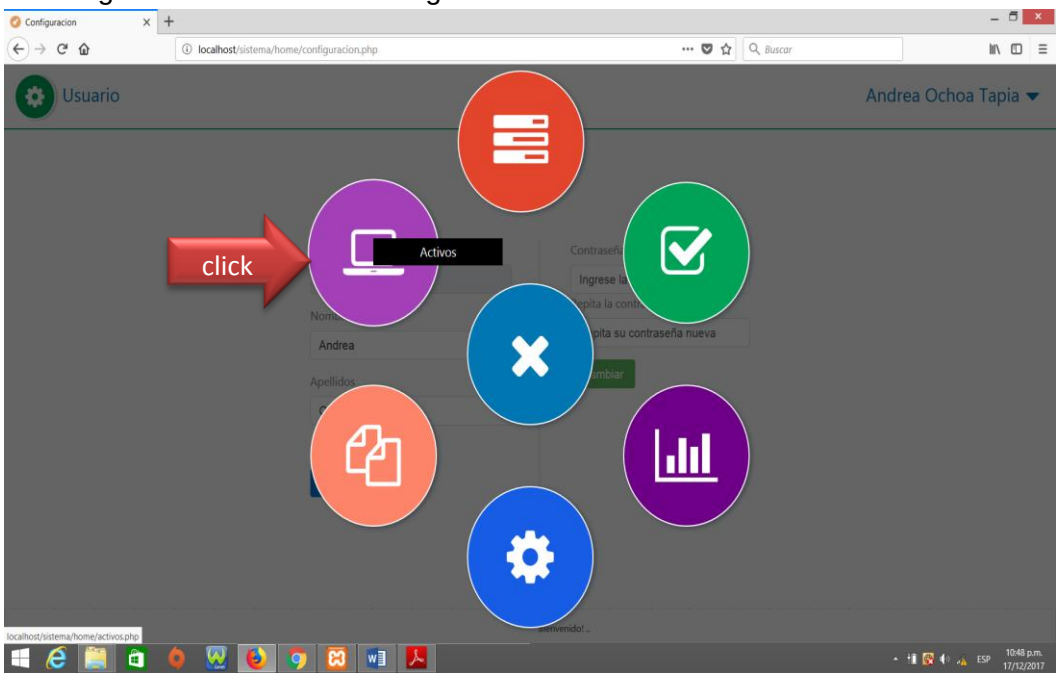
H. Módulo 6 - Usuario: En este módulo, se puede cambiar la configuración del usuario.



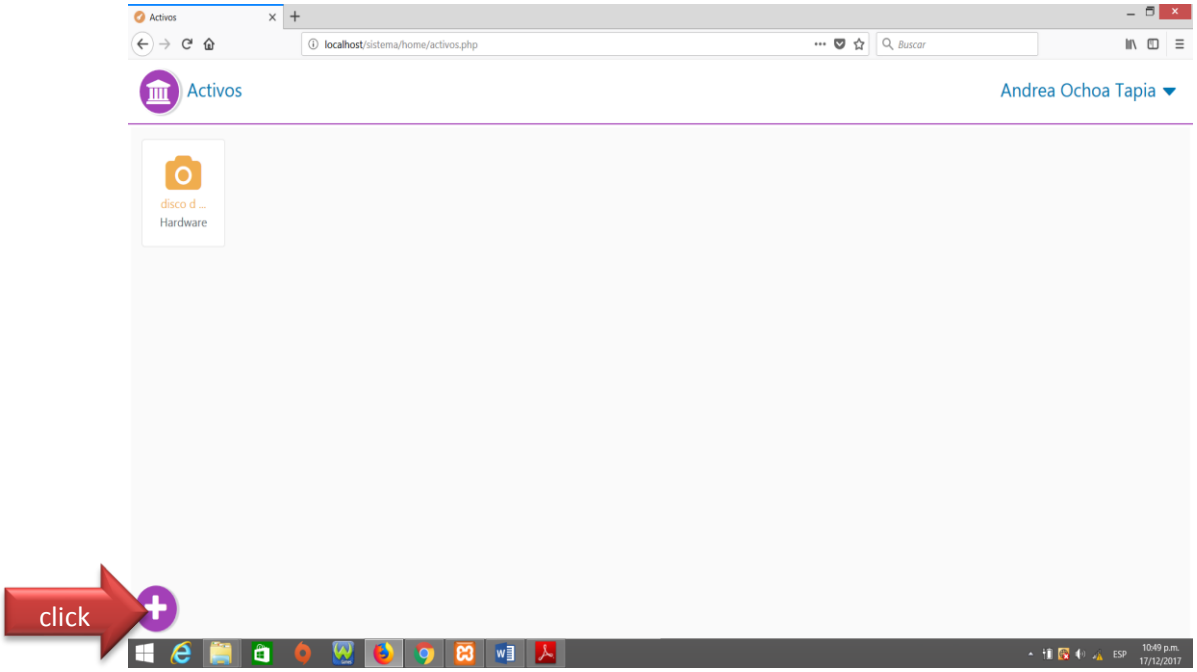


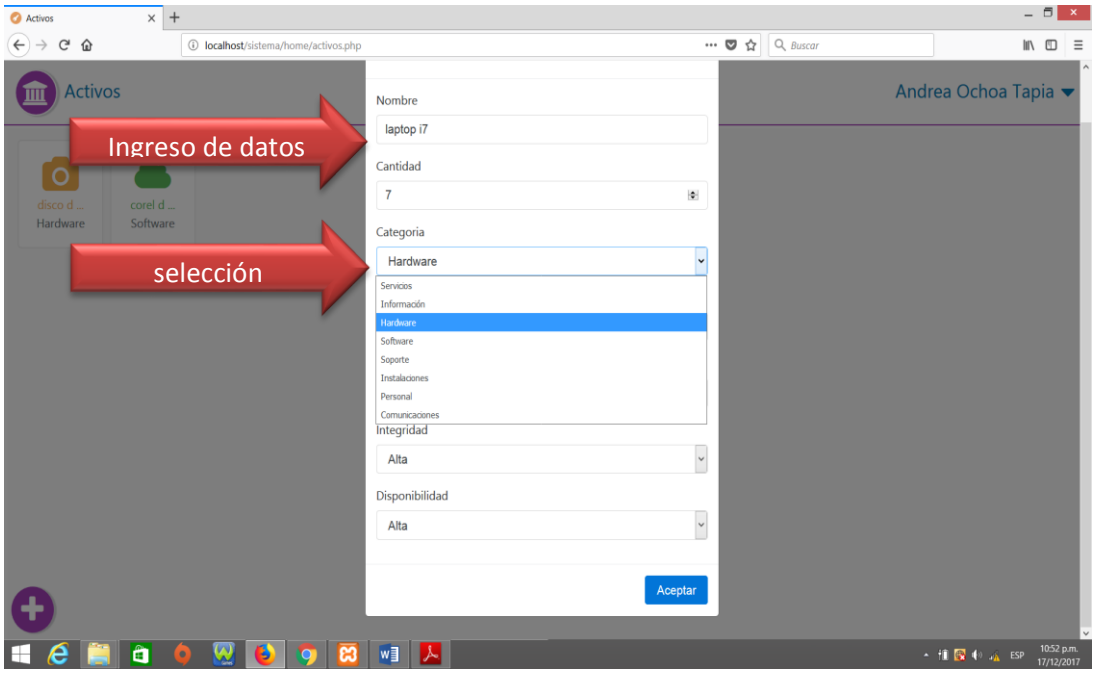
I. Ingresar un nuevo activo

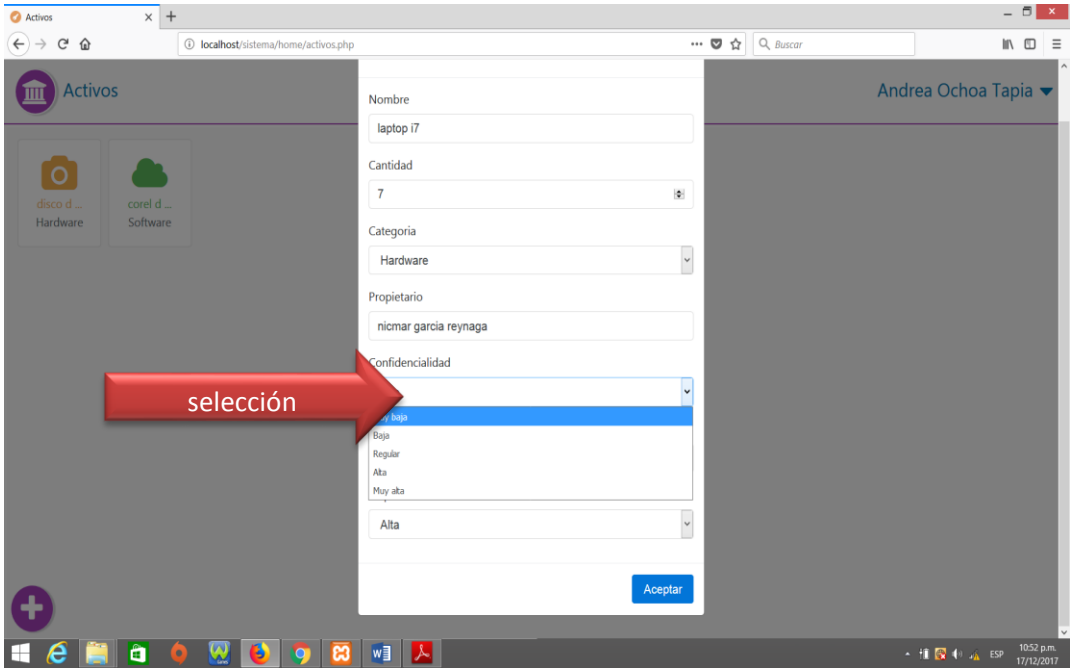
Para ingresar un nuevo activo ingresamos al módulo ACTIVO

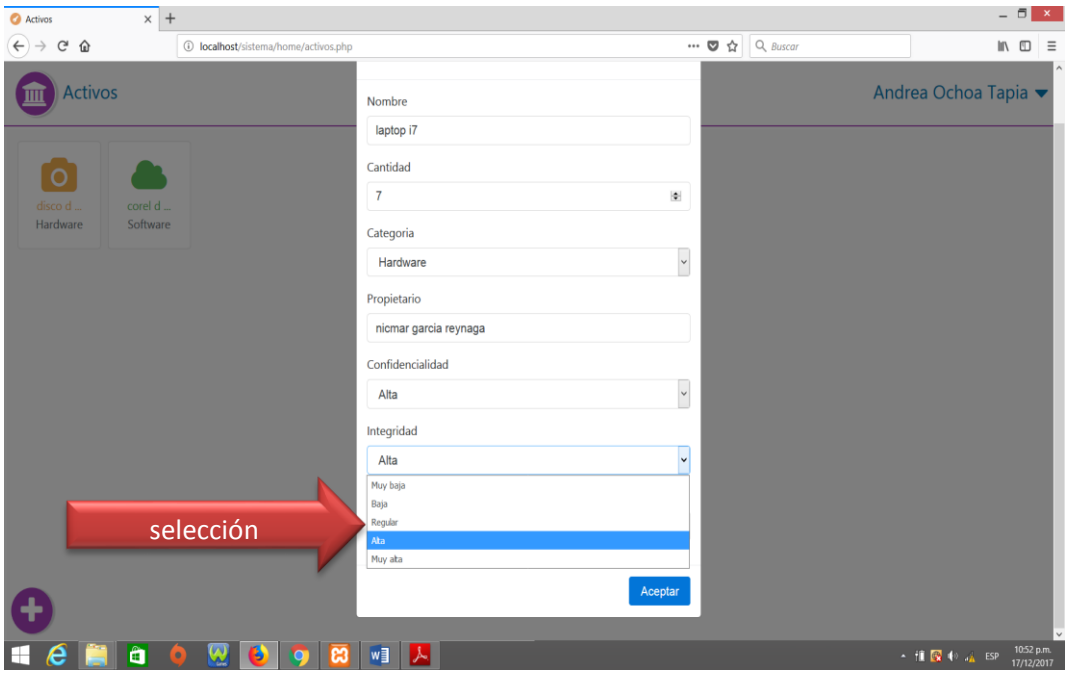


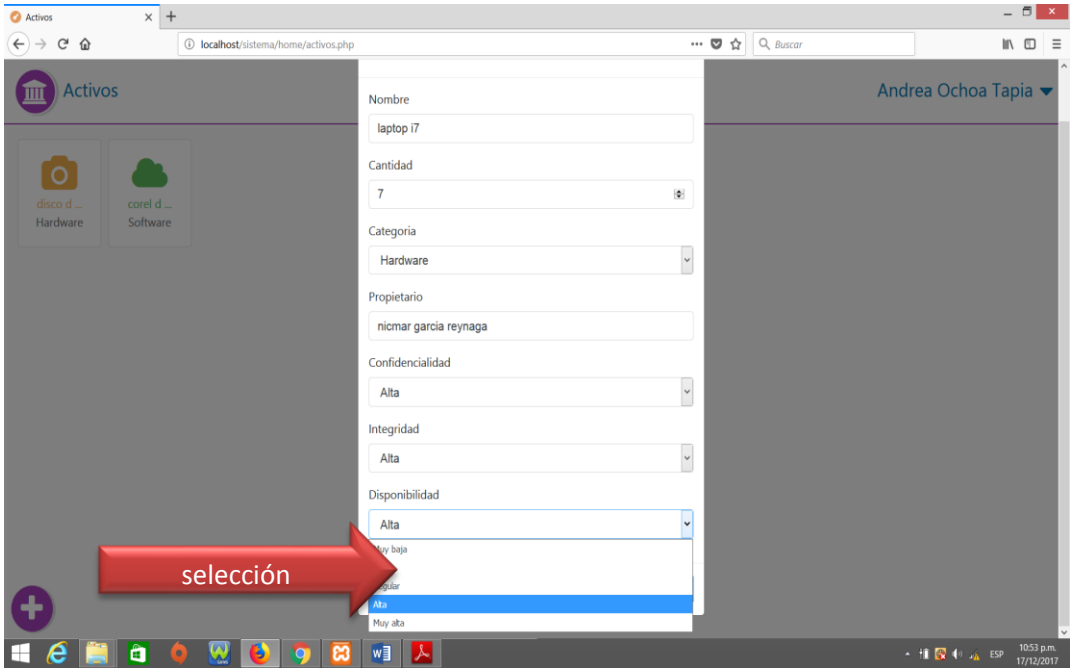
Clic en el signo “más” para agregar un nuevo activo

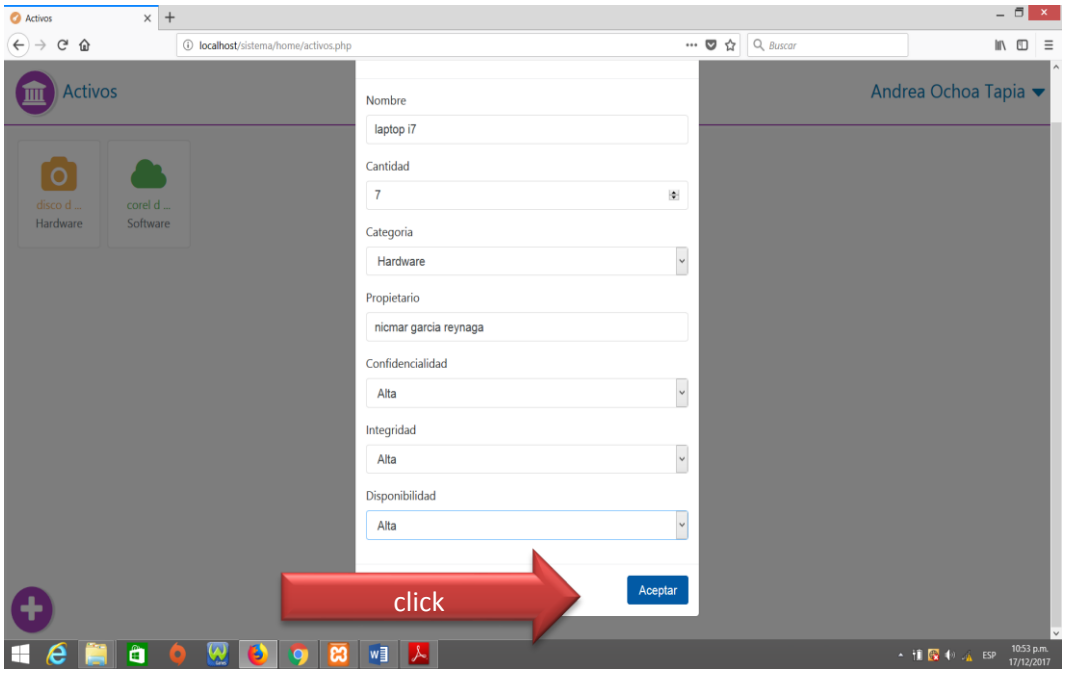


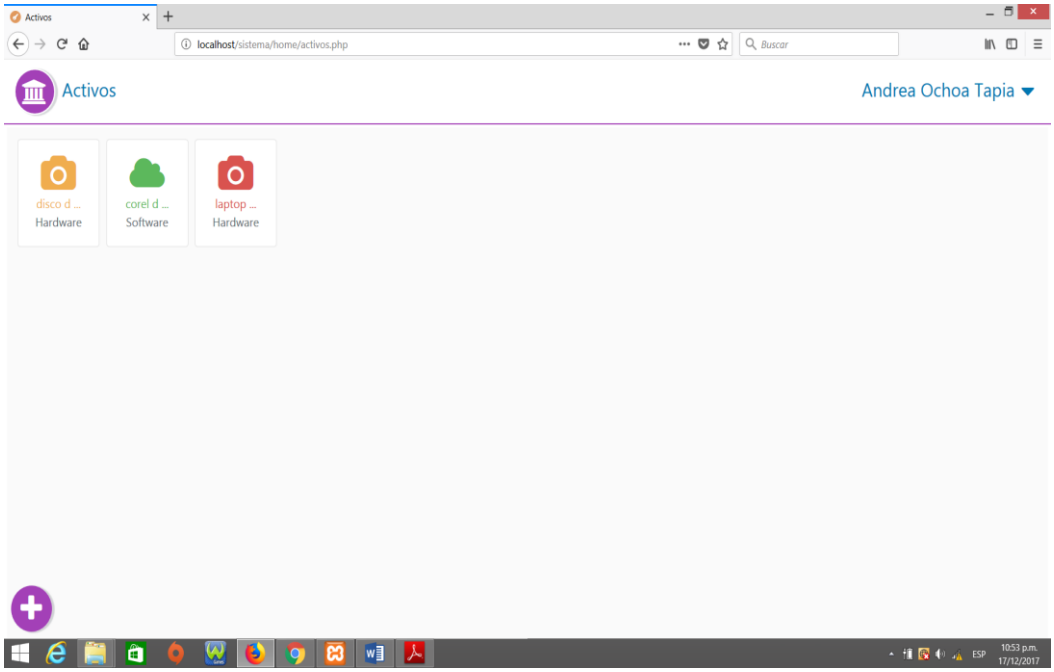



Activos
localhost/sistema/home/activos.php
Buscar
Activos
Andrea Ochoa Tapia
disco d ...
Hardware
corel d ...
Software
Nombre
laptop i7
Cantidad
7
Categoria
Hardware
Propietario
nicmar garcia reynaga
Confidencialidad
selección
Muy baja
Baja
Regular
Alta
Muy alta
Alta
Aceptar
ESP
10:52 p.m.
17/12/2017

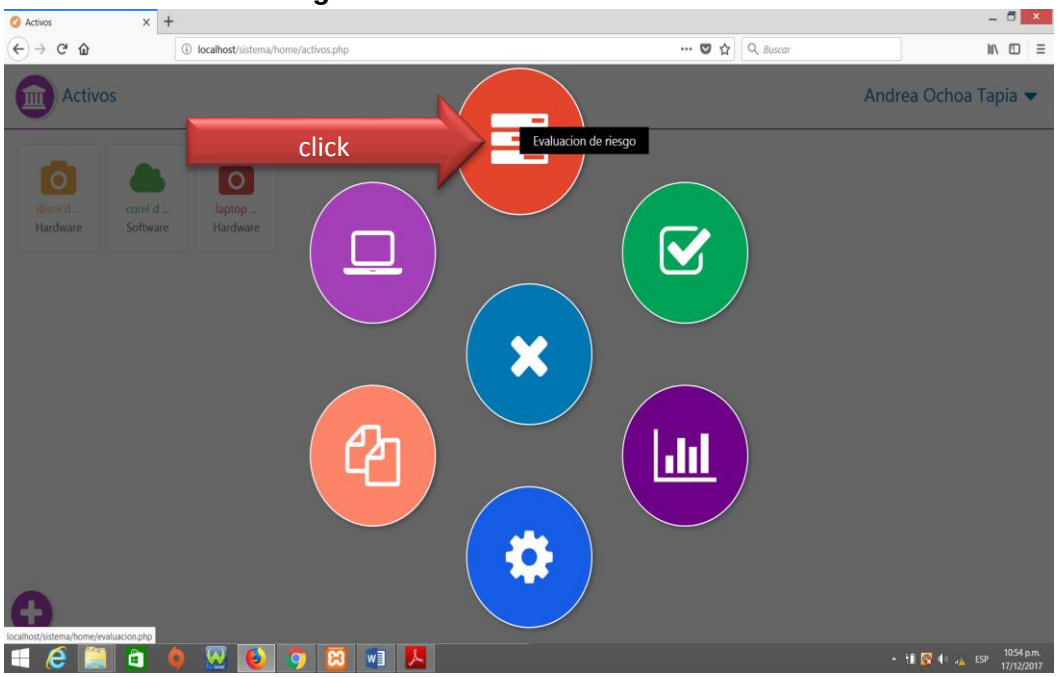

Activos
localhost/sistema/home/activos.php
Buscar
Activos
Andrea Ochoa Tapia
disco d ...
Hardware
corel d ...
Software
Nombre
laptop i7
Cantidad
7
Categoria
Hardware
Propietario
nicmar garcia reynaga
Confidencialidad
Alta
Integridad
Alta
selección
Muy baja
Baja
Regular
Alta
Muy alta
Aceptar
ESP
10:52 p.m.
17/12/2017


Activos
localhost/sistema/home/activos.php
Buscar
Activos
Andrea Ochoa Tapia
disco d ...
Hardware
corel d ...
Software
Nombre
laptop i7
Cantidad
7
Categoria
Hardware
Propietario
nicmar garcia reynaga
Confidencialidad
Alta
Integridad
Alta
Disponibilidad
Alta
Muy baja
Alta
Muy alta
selección
ESP
10:53 p.m.
17/12/2017

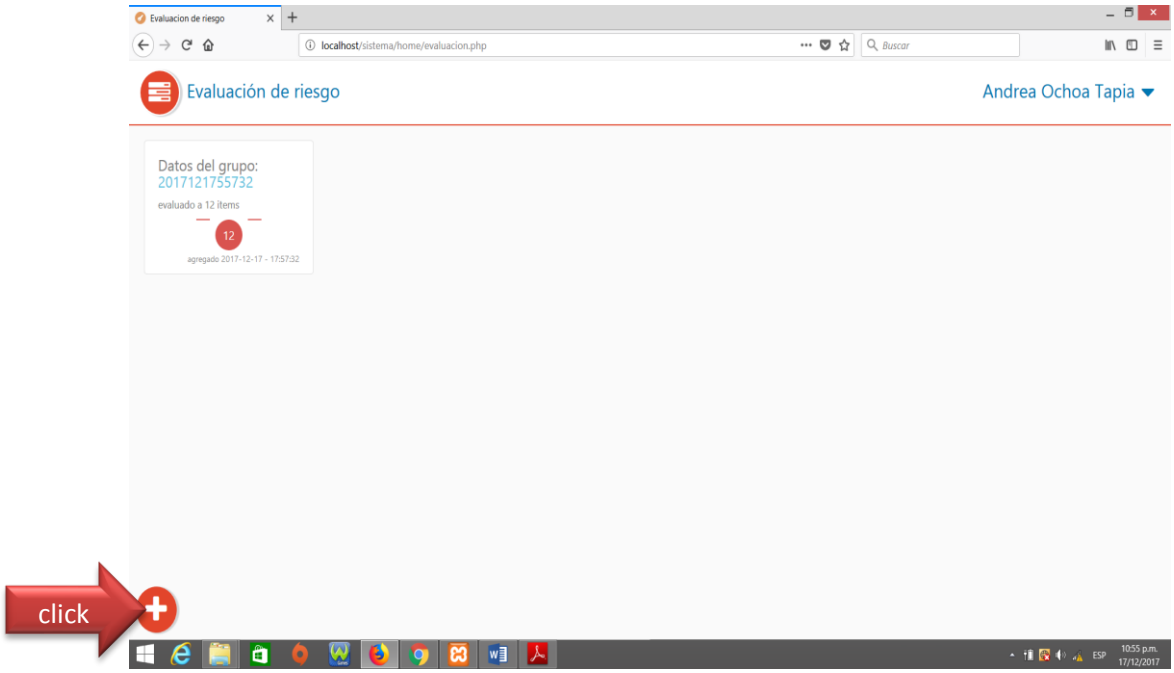

Activos
localhost/sistema/home/activos.php
Buscar
Activos
Andrea Ochoa Tapia
disco d ...
Hardware
corel d ...
Software
Nombre
laptop i7
Cantidad
7
Categoria
Hardware
Propietario
nicmar garcia reynaga
Confidencialidad
Alta
Integridad
Alta
Disponibilidad
Alta
Aceptar
click
ESP
10:53 p.m.
17/12/2017



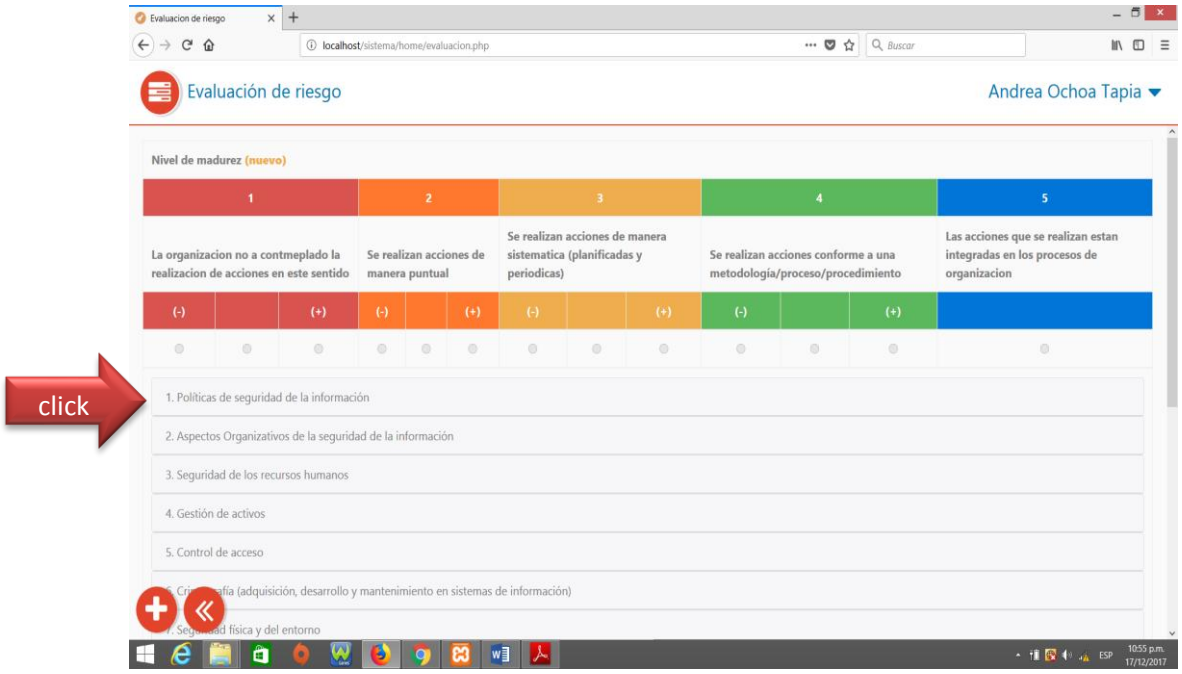
J. Evaluación de los riesgos

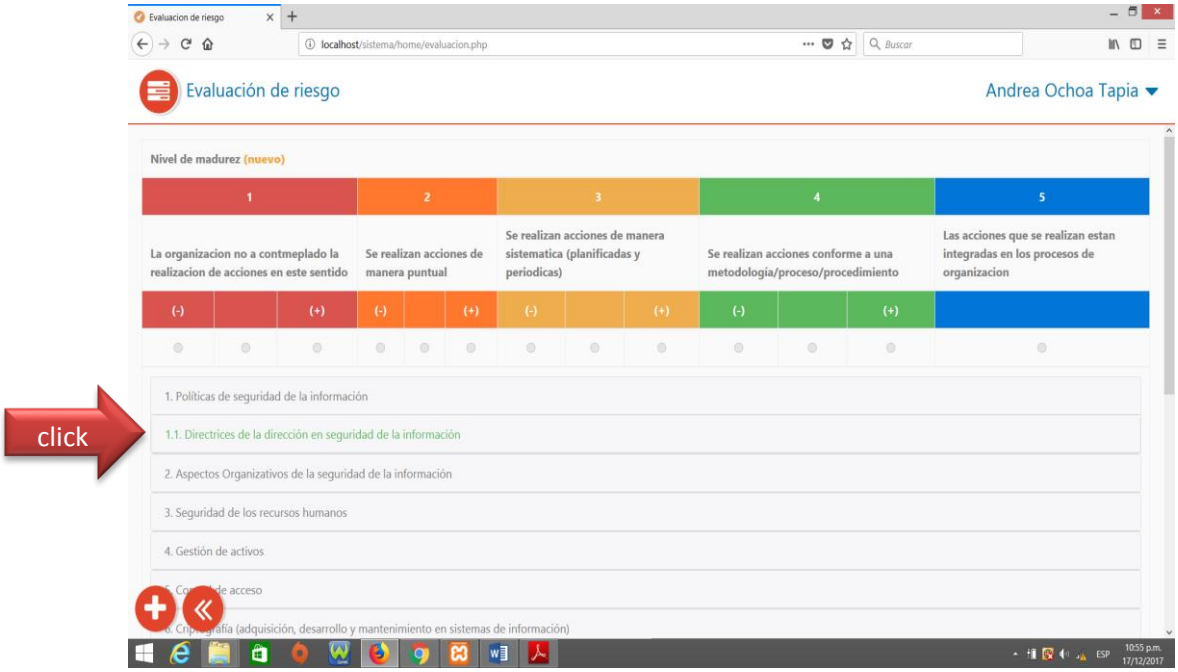


Para realizar una evaluación nueva se hace click en el botón “+”

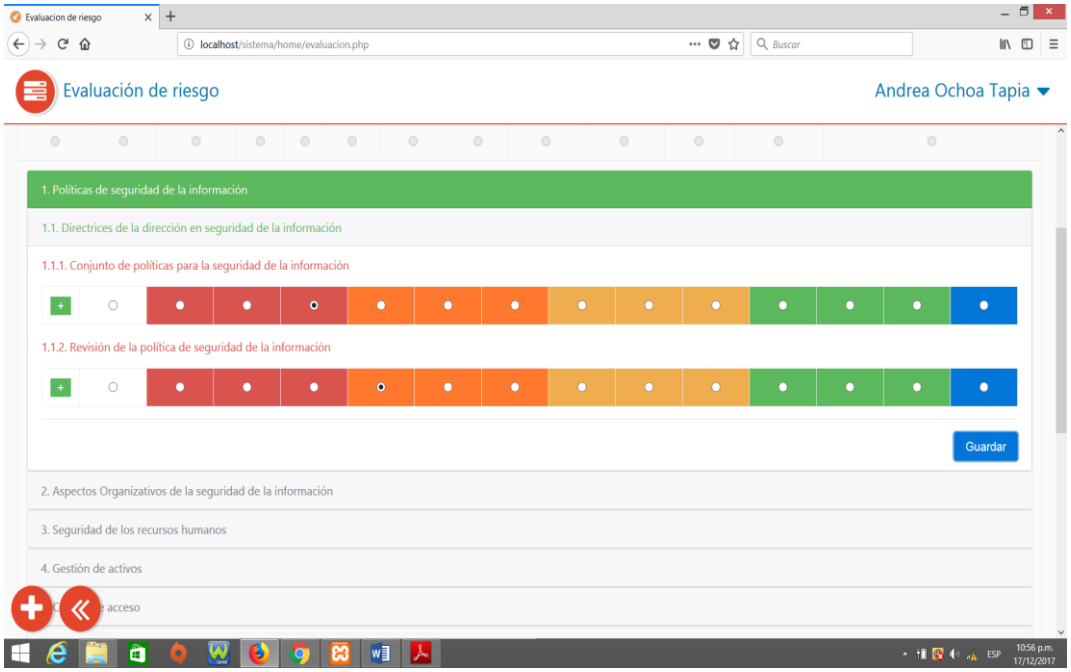


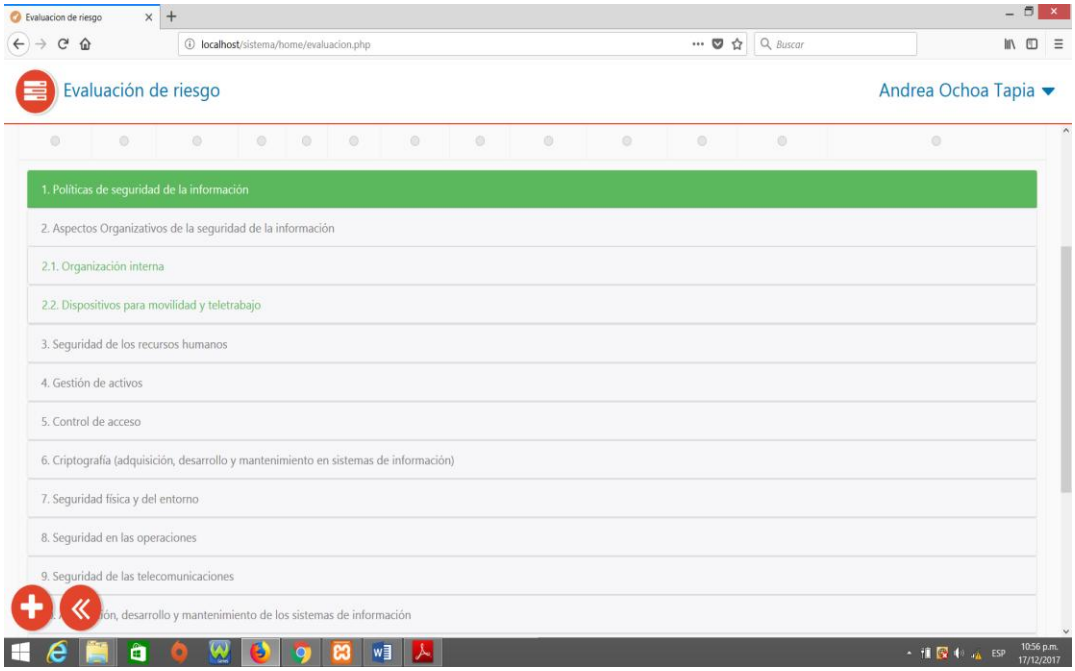
En donde nos mostrará la siguiente pantalla la cual muestra los 14 dominios con sus 35 objetivos y 114 controles.

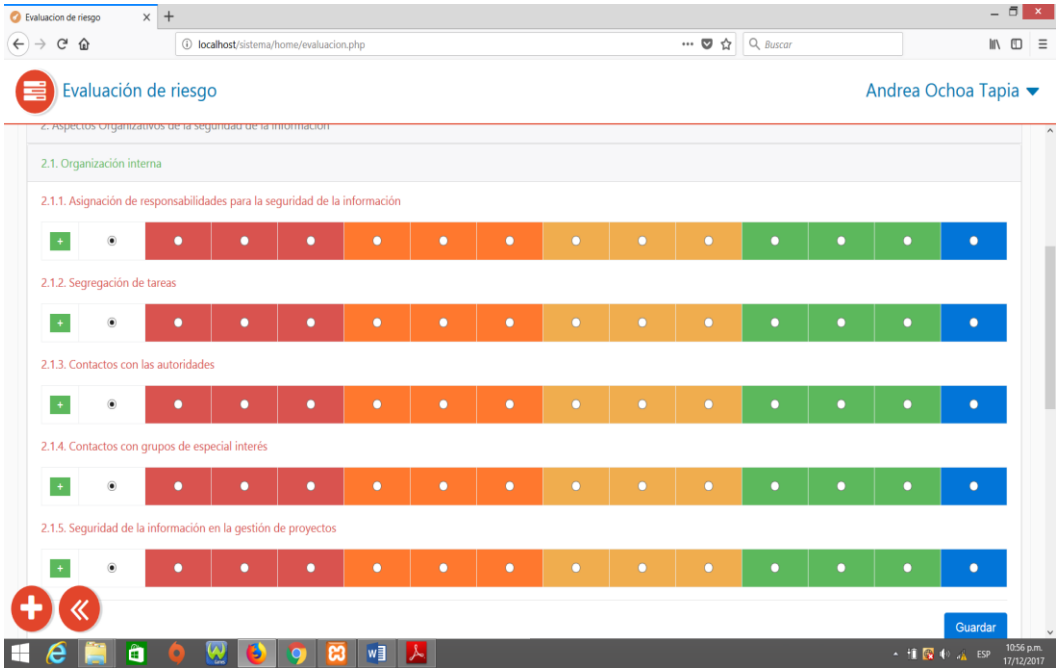




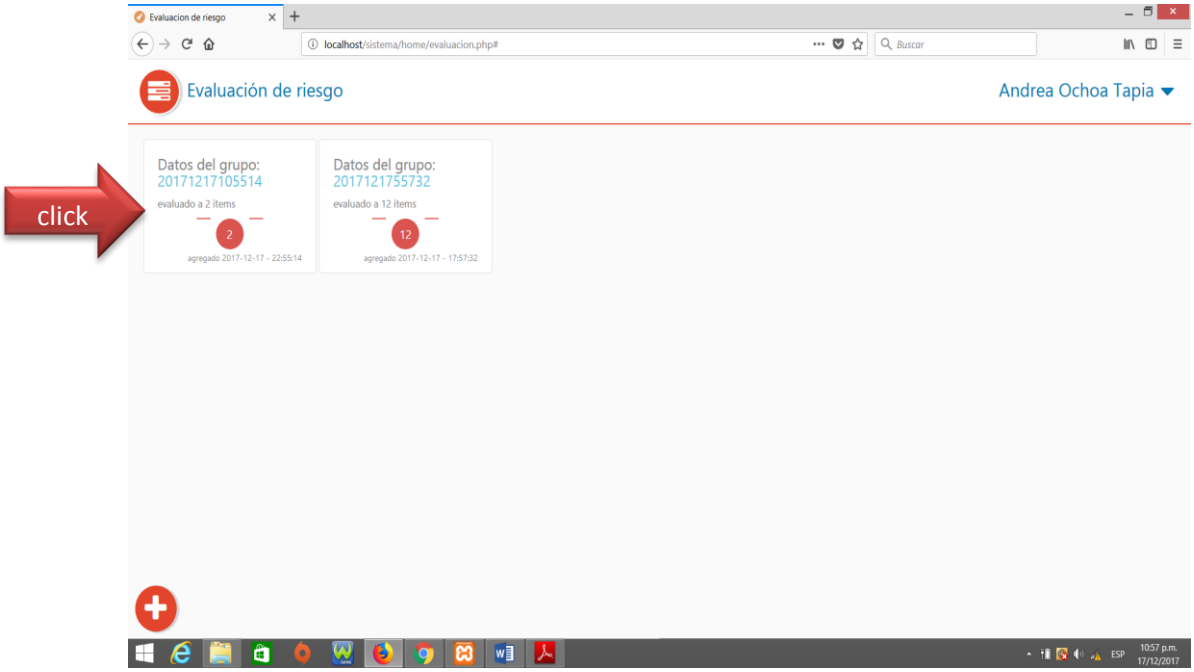
Después de seleccionar los objetivos podemos empezar a evaluar los controles en una escala de muy baja a alta.

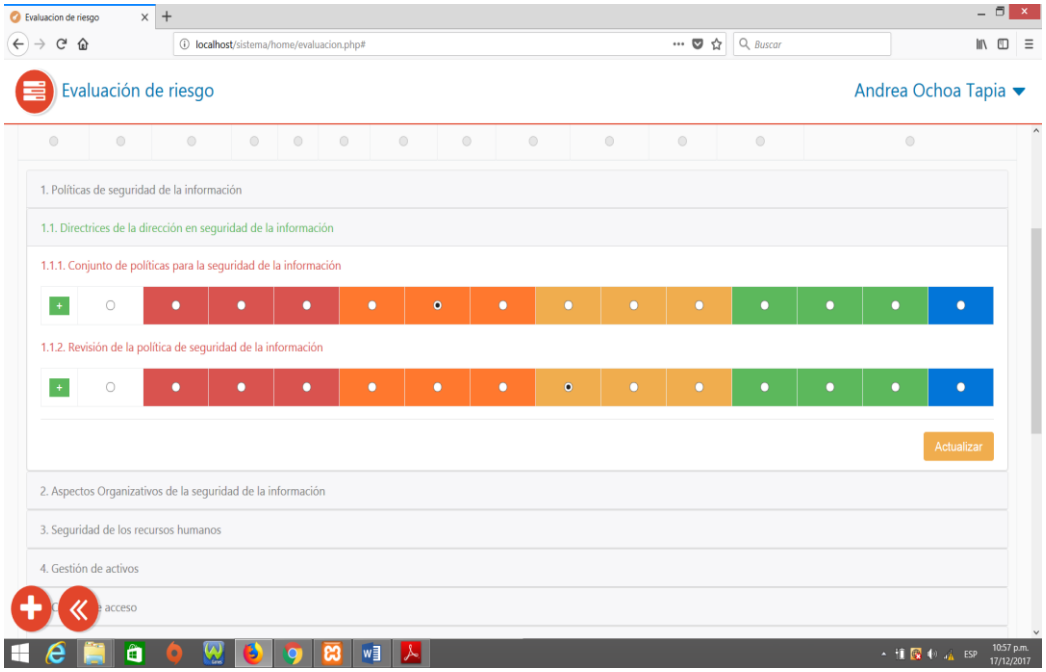

Evaluacion de riesgo
localhost/sistema/home/evaluacion.php
Buscar
Evaluación de riesgo
Andrea Ochoa Tapia
1. Políticas de seguridad de la información
1.1. Directrices de la dirección en seguridad de la información
1.1.1. Conjunto de políticas para la seguridad de la información
1.1.2. Revisión de la política de seguridad de la información
Guardar
2. Aspectos Organizativos de la seguridad de la información
3. Seguridad de los recursos humanos
4. Gestión de activos
acceso
ESP
10:56 p.m.
17/12/2017

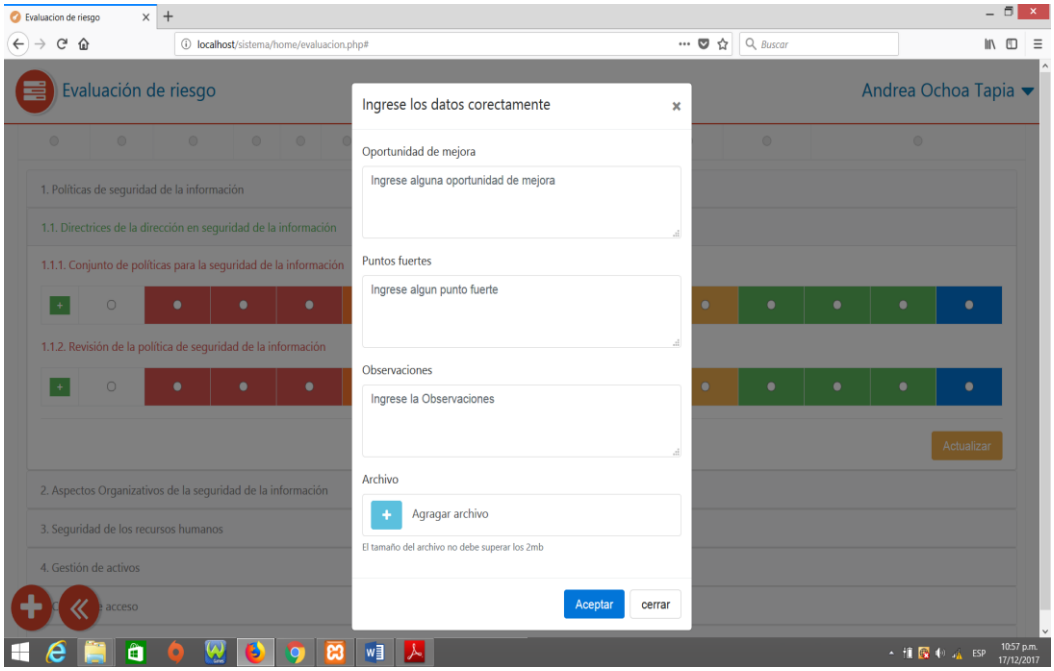

Evaluacion de riesgo
localhost/sistema/home/evaluacion.php
Buscar
Evaluación de riesgo
Andrea Ochoa Tapia
1. Políticas de seguridad de la información
2. Aspectos Organizativos de la seguridad de la información
2.1. Organización interna
2.2. Dispositivos para movilidad y teletrabajo
3. Seguridad de los recursos humanos
4. Gestión de activos
5. Control de acceso
6. Criptografía (adquisición, desarrollo y mantenimiento en sistemas de información)
7. Seguridad física y del entorno
8. Seguridad en las operaciones
9. Seguridad de las telecomunicaciones
ión, desarrollo y mantenimiento de los sistemas de información
ESP
10:56 p.m.
17/12/2017



Luego de evaluar cada control y guarda en el menú principal de la evaluación de riesgo, no aparecerá, cada evaluación que se va realizando por fecha e indicando la cantidad de controles evaluados, el mismo que nos permite modificar si fuera de necesidad.

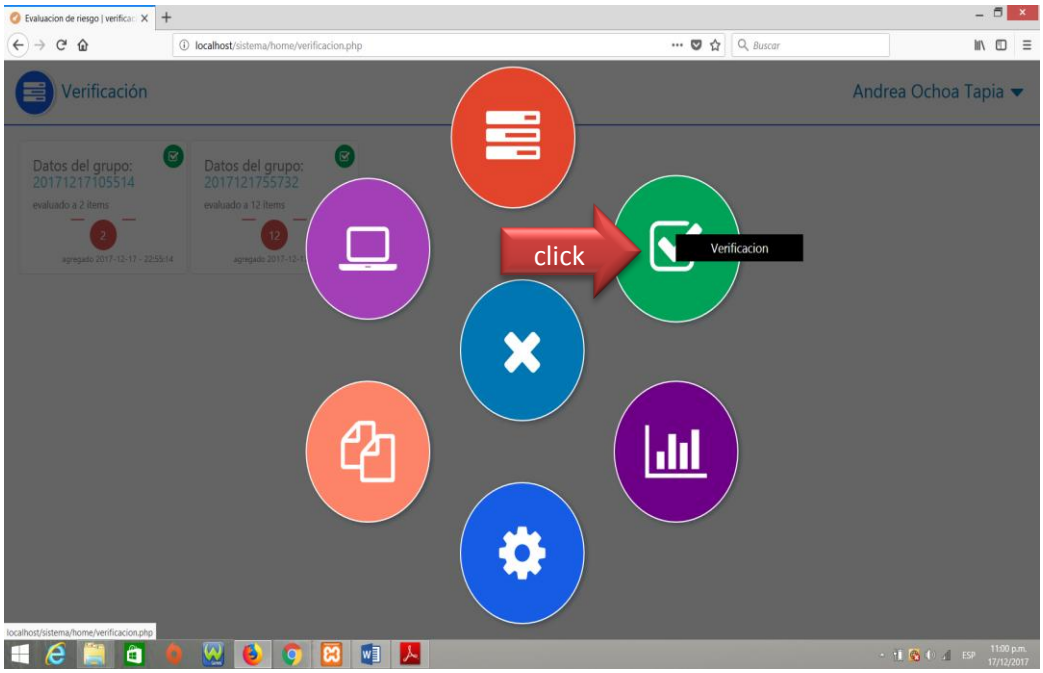



Evaluacion de riesgo
localhost/sistema/home/evaluacion.php#
Buscar
Evaluación de riesgo
Andrea Ochoa Tapia
1. Políticas de seguridad de la información
1.1. Directrices de la dirección en seguridad de la información
1.1.1. Conjunto de políticas para la seguridad de la información
1.1.2. Revisión de la política de seguridad de la información
Actualizar
2. Aspectos Organizativos de la seguridad de la información
3. Seguridad de los recursos humanos
4. Gestión de activos
ESP
10:57 p.m.
17/12/2017

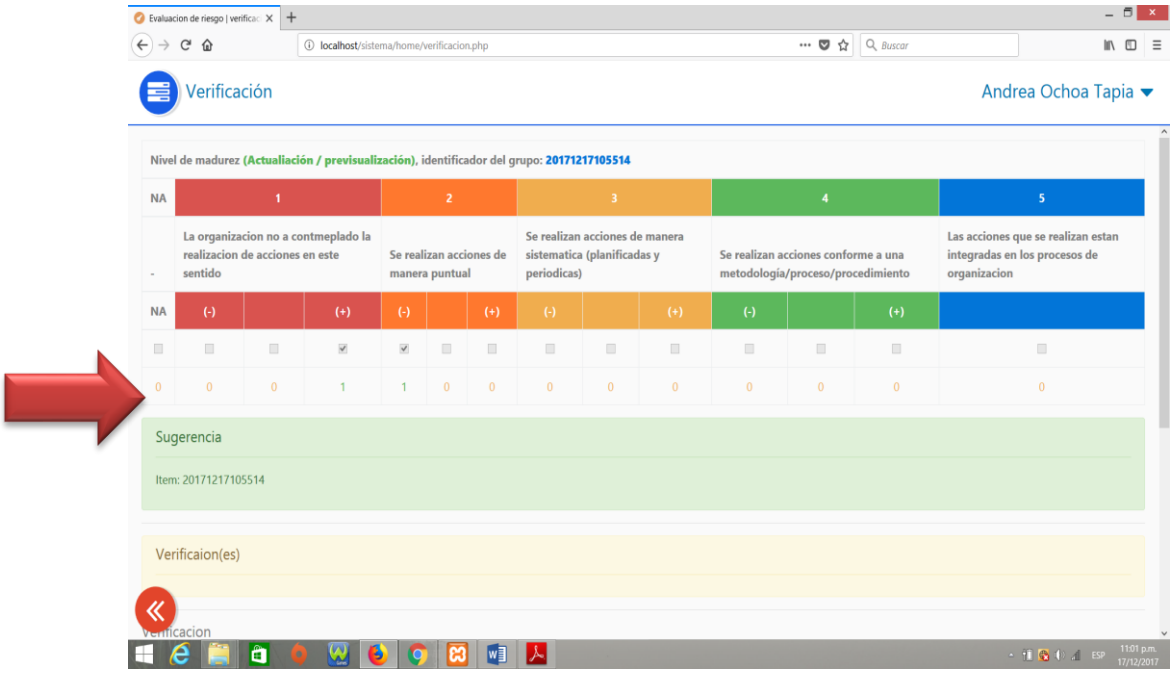

Evaluacion de riesgo
localhost/sistema/home/evaluacion.php#
Buscar
Evaluación de riesgo
Andrea Ochoa Tapia
Ingrese los datos corectamente
Oportunidad de mejora
Ingrese alguna oportunidad de mejora
Puntos fuertes
Ingrese algun punto fuerte
Observaciones
Ingrese la Observaciones
Archivo
Agragar archivo
El tamaño del archivo no debe superar los 2mb
Aceptar
cerrar
1. Políticas de seguridad de la información
1.1. Directrices de la dirección en seguridad de la información
1.1.1. Conjunto de políticas para la seguridad de la información
1.1.2. Revisión de la política de seguridad de la información
Actualizar
2. Aspectos Organizativos de la seguridad de la información
3. Seguridad de los recursos humanos
4. Gestión de activos
ESP
10:57 p.m.
17/12/2017

K. Verificación

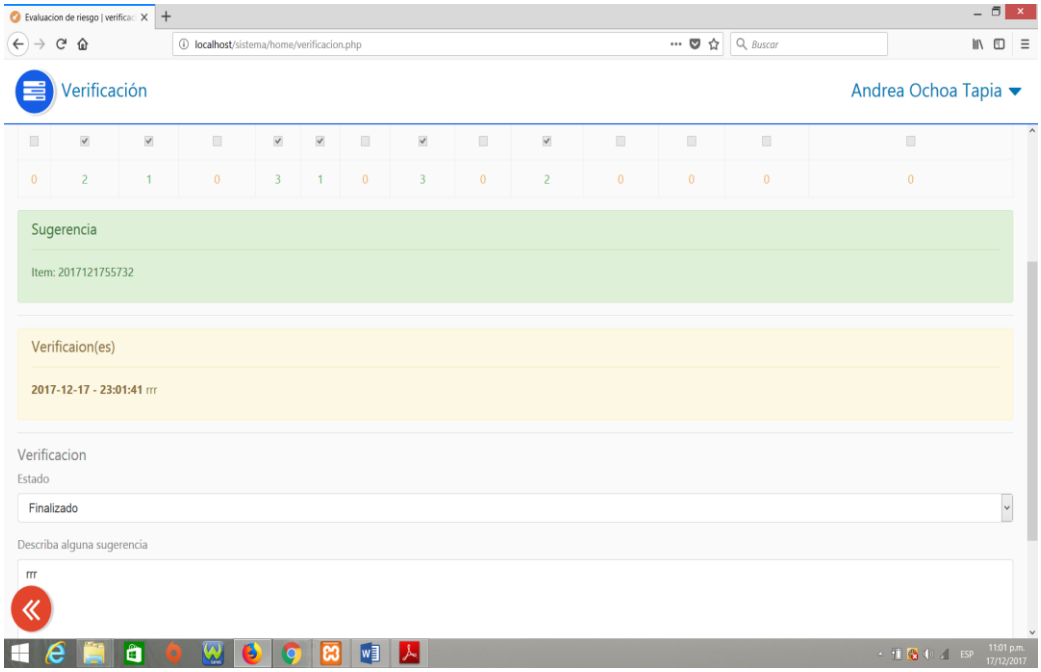
para la verificación se debe hacer clic en icono indicado en la siguiente imagen.



El cual nos mostrará la siguiente ventana, en donde nos indica la cantidad de controles evaluados en cada nivel.

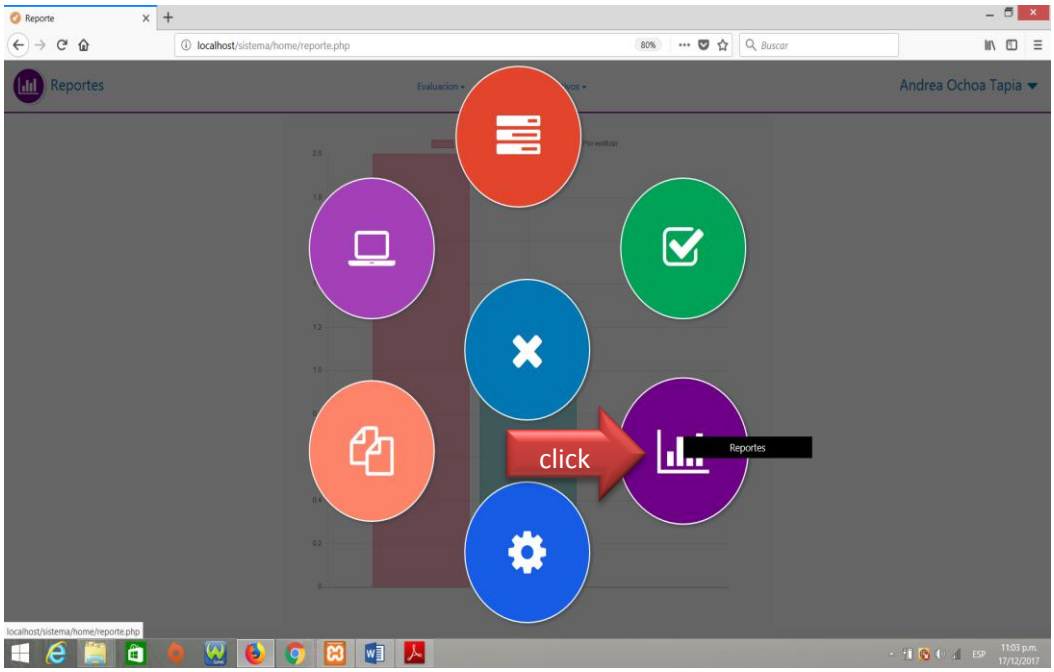


También nos permite introducir una sugerencia, la misma que se guarda por fecha

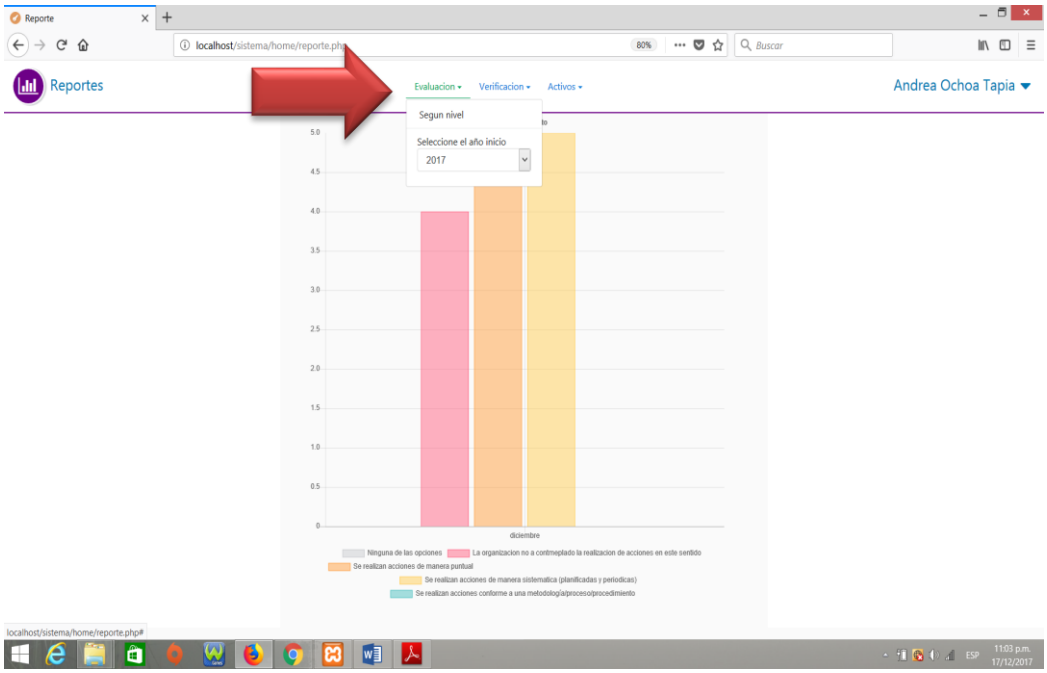


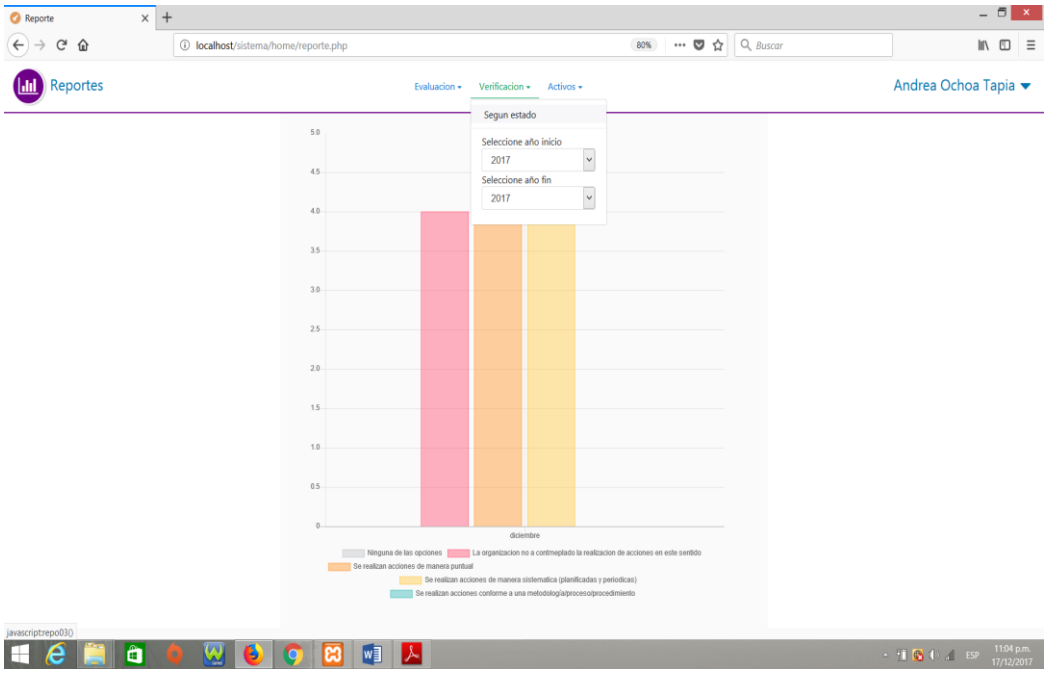
L. Reportes

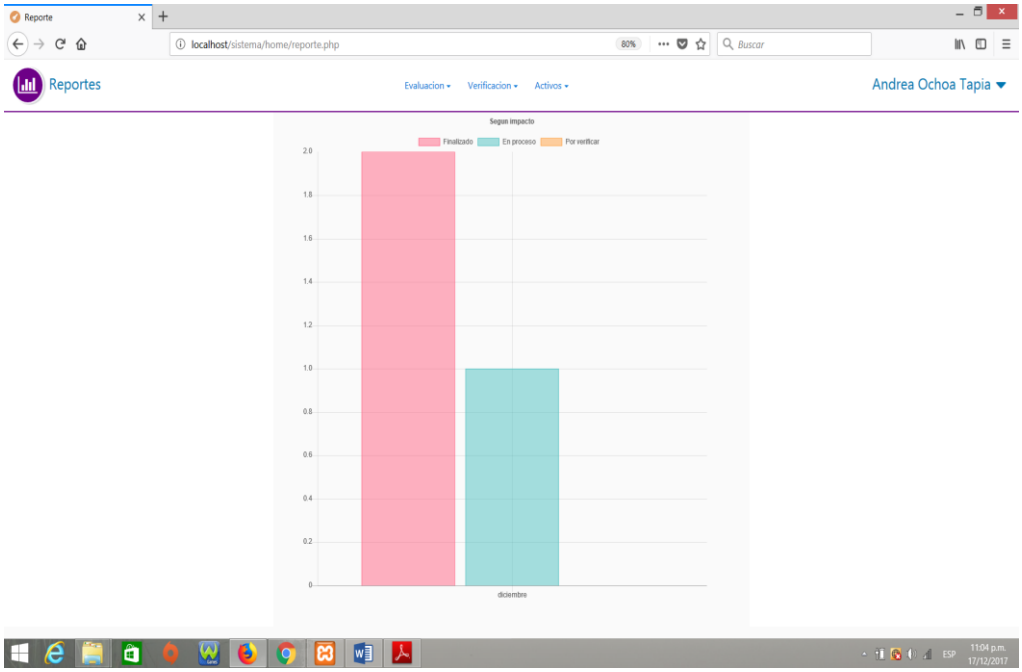
Para los reportes se debe hacer clic en el icono que se muestra a continuación.

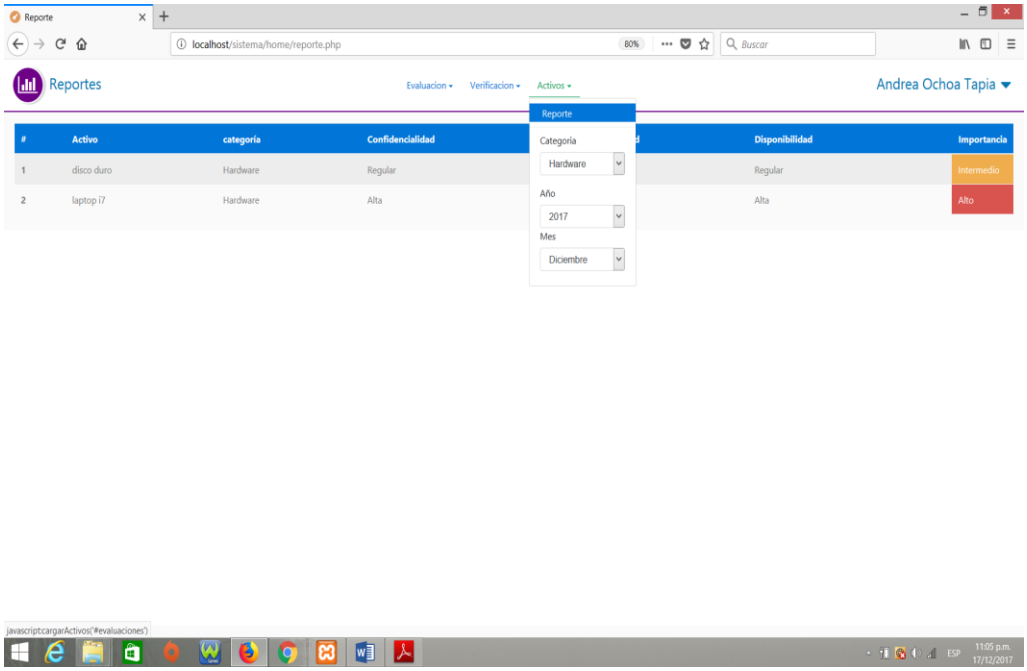


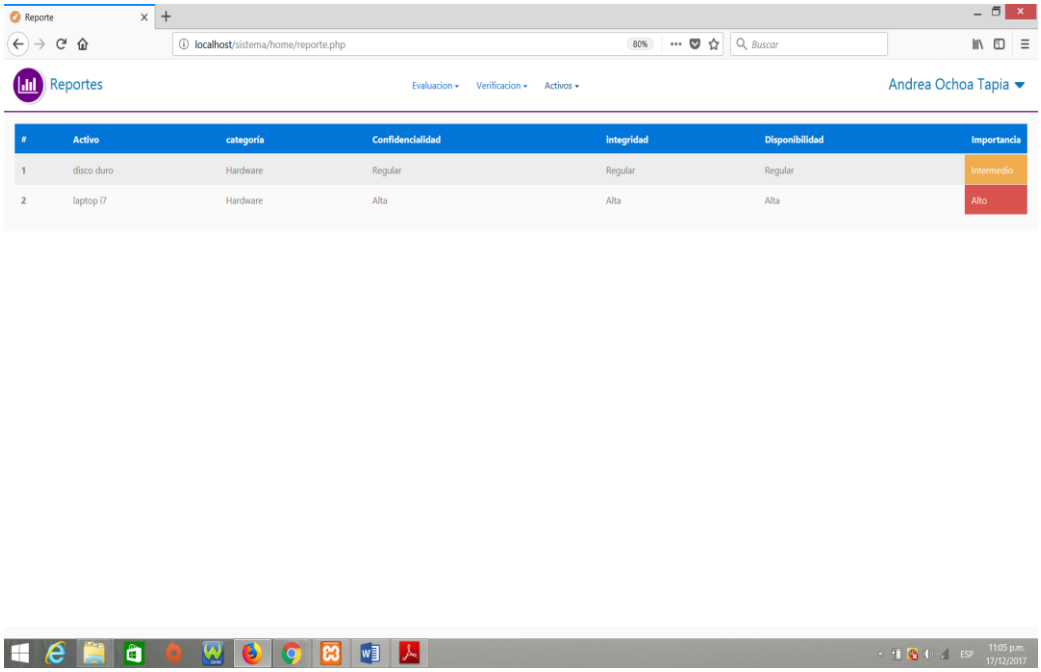
El cual nos mostrará la siguiente ventana, donde se puede ver un reporte según evaluación de riesgo, verificación, y activos






Reporte
localhost/sistema/home/reporte.php
Buscar
Reportes
Evaluacion
Verificacion
Activos
Andrea Ochoa Tapia
Segun impacto
Finalizado
En proceso
Por verificar
2.0
1.8
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0
diciembre
ESP
11:04 p.m.
17/12/2017


Reporte
localhost/sistema/home/reporte.php
Buscar
Reportes
Evaluacion
Verificacion
Activos
Andrea Ochoa Tapia
Reporte
Categoría
Hardware
Año
2017
Mes
Diciembre
Activo categoría Confidencialidad Disponibilidad Importancia
1 disco duro Hardware Regular Regular Intermedio
2 laptop i7 Hardware Alta Alta Alto
javascript:cargarActivos('#evaluaciones')
ESP
11:05 p.m.
17/12/2017



8.2. CÓDIGO FUENTE

8.2.1. CÓDIGO FUENTE PARA LA INTERACCIÓN CON LA BASE DE DATOS

A. PARA ADMINISTRAR LA BASE DE DATOS

```
<?php
        require_once("openServer.php");
        class ManagerDb{
                public $rs = array();
                public $queryG;
                //limites
                public $lim_min = 0;
                public $lim_max = 15;

                function __construct(){
                        $this->lim_min = 0;
                        $this->lim_max = 0;
                        $this->queryG = "";
                }
                function obtenerDatosW($query, $options){
                        $openServer = new OpenServ();
                        if(is_array($options)){
                                //$options = ["min"=>0, "max"=>15];
                                $this->lim_min = $options["min"];
                                $this->lim_max = $options["max"];
                                $openServer->cnS = $query." LIMIT ".$this-
>lim_min.", ".$this->lim_max;
                        }elseif($this->lim_max != 0) $openServer->cnS =
$query." LIMIT ".$this->lim_min.", ".$this->lim_max;
                        else $openServer->cnS = $query;

                        $this->rs = $openServer->ejecutarConsultaR();
                        //$this->rs["g"] = $this->reunirEnGrupos();
```

```
                return($this->rs);
        }
        function obtenerDatos($query, $options){
                $openServer = new OpenServ();
                if(is_array($options)){
                        //$options = ["min"=>0, "max"=>15];
                        $this->lim_min = $options["min"];
                        $this->lim_max = $options["max"];
                        $openServer->cnS = $query." LIMIT ".$this-
>lim_min.", ".$this->lim_max;
                }else $openServer->cnS = $query;

                $this->rs = $openServer->ejecutarConsultaR();
                return($this->rs);
        }
        function reunirEnGrupos(){
                $openServer = new OpenServ();
                $openServer->cnS = $this->queryG;
                $rs = $openServer->ejecutarConsultaR();
                $grupo = array();
                $grupo["agrupado"] = $this->lim_max;

                if($rs["response"] == "Exito"){
                        $rs = $rs["datos"];

                        //operaciones de agrupacion
                        $grupo["cantidad"] = $rs[0]["reunir"] * 1;
                        $gr = $rs[0]["reunir"] % $this->lim_max;
                        $ge = floor($rs[0]["reunir"] / $this->lim_max);
                        $agr = array();
                        $anterior = 0;

                        if($this->lim_max   >=   $grupo["cantidad"])
array_push($agr, array($anterior, $grupo["cantidad"]));
                        else{
                                $sig = $this->lim_max;

                                for ($i=1; $i <= $ge; $i++) {
                                        $sig = $i * $this->lim_max;
                                        $agr[$i - 1] = array($anterior,
$sig);
                                        $anterior = $sig + 1;
                                }
                                if($gr>0)               array_push($agr,
array($anterior, $sig + $gr));
                        }
                        $grupo["grupo"] = $agr;
                }
                else $grupo["response"] = "error";

                return $grupo;
        }
        function tipoAdmin($a){
                //1: administrador
                //2: usuario comun
```

```
		//3: bloquedo
		$a = $a * 1;
		if(is_integer($a)){
			switch($a){
				case 1: return("Administrador");
				case 2: return("Usuario comun");
				case 3: return("Bloqueado");
				default: return("Sin acceso");
			}
		}else return("Sin acceso");
	}
	function estadoUsuario($a){
		//1: administrador
		//2: usuario comun
		//3: bloquedo
		$a = $a * 1;
		if(is_integer($a)){
			switch($a){
				case 0: return("Bloqueado");
				case 1: return("Activo");
				default: return("Sin acceso");
			}
		}else return("Sin acceso");
	}
	function fechaWinthNumber($n){
		switch($n){
			case 1: return("enero");
			case 2: return("febrero");
			case 3: return("marzo");
			case 4: return("abril");
			case 5: return("mayo");
			case 6: return("junio");
			case 7: return("julio");
			case 8: return("agosto");
			case 9: return("setiembre");
			case 10: return("octubre");
			case 11: return("noviembre");
			case 12: return("diciembre");
		}
	}
	function fechaToLetter($fecha){
		//2017-07-15
		if($fecha != ""){
			list($y, $m, $d) = split("-", $fecha);
			$m = $this->fechaWinthNumber($m);
			return($d." de ".$m." de ".$y);
		}else return("");
	}
	function tipoIn($num){
		$num = $num * 1;
		switch ($num) {
			case 0: return("Muy baja");
			case 2.5: return("Baja");
			case 5: return("Regular");
			case 7.5: return("Alta");
```

```
                                case 10: return("Muy alta");
                                default: return("Muy alta");
                        }
                }
        }
        class All{
        function searchTipoContent($text){
                        $img = array("png", "jpg", "jpeg", "gif", "tif");
                        $clip = array("mp4", "avi", "mov", "3gp", "3gpp", "tif",
"wmv");
                        $audio = array("mp3", "ogg", "wav", "midi", "mpeg");
                        $documento = array("pdf", "txt", "doc", "docx", "ppt",
"pptx", "xls", "xlsx");
                        $comprimido = array("rar", "zip", "tar");
                        $tipo = "";
                        if (in_array($text, $img)) $tipo = "imagen";
                        elseif (in_array($text, $clip)) $tipo = "video";
                        elseif (in_array($text, $audio)) $tipo = "audio";
                        elseif (in_array($text, $documento)) $tipo = "doc";
                        elseif (in_array($text, $comprimido)) $tipo =
"comprimido";
                        else $tipo = "unknow";

                        return $tipo;
                }
                function estadoUsuario($estado){
                        $s = array();
                        if($estado == 0){
                                $sms_p = "Desactivado";
                                $text_class = "text-danger";
                        }else if($estado == 1){
                                $sms_p = "Activo";
                                $text_class = "text-success";
                        }else{
                                $sms_p = "Suspendido";
                                $text_class = "text-info";
                        }

                        $s["sms"] = $sms_p;
                        $s["class_t"] = $text_class;
                        $s["estado"] = $estado;

                        return $s;
                }

                function prioridad($n){
                        $s = array();
                        if($n == 0){
                                $sms_p = "Primera plana";
                                $text_class = "text-danger";
                        }else if($n == 1){
                                $sms_p = "Urgente";
                                $text_class = "text-success";
                        }else{
                                $sms_p = "No urgente";
```

```
                $text_class = "text-info";
            }

            $s["sms"] = $sms_p;
            $s["class_t"] = $text_class;
            $s["send_i"] = $n;

            return $s;
        }
        function tipoAdmin($a){
            //1: administrador
            //2: usuario comun
            //3: bloquedo
            $a = $a * 1;
            if(is_integer($a)){
                switch($a){
                    case 1: return("Administrador");
                    case 2: return("Usuario comun");
                    case 3: return("Bloqueado");
                    default: return("Sin acceso");
                }
            }else return("Sin acceso");
        }    }?>
```

B. PARA LA EJECUCIÓN DE LAS CONSULTAS

```
<?php
    //headers
    //header("Access-Control-Allow-Origin: *");
    //header("Access-Control-Allow-Methods: GET");
    header("Content-Type: application/json");
    //calls class's
    require_once("../actions/openServer.php");
    require_once("../actions/usuario.php");
    require_once("../actions/carpeta.php");
    //require_once("../actions/contactos.php");
    //require_once("../actions/mensajes.php");
    require_once("../actions/archivo.php");
    require_once("../actions/cryptography.php");

    //datos require
    $rs = array();
    $data = array();
    $type = "";//add, del, upd
    $tabl = "";
    $os = new OpenServ();

    if(isset($_GET["data"]) && isset($_GET["type"]) &&
isset($_GET["tb"])){
        $data = $_GET["data"];
        $type = $_GET["type"];
        $tabl = $_GET["tb"];
    }elseif(isset($_POST["data"]) && isset($_POST["type"]) &&
isset($_POST["tb"])){
```

```
		$data = $_POST["data"];
		$type = $_POST["type"];
		$tabl = $_POST["tb"];
	}else{
		$rs["r"] = "Error: datos no encontrados";
		$data = "";
		$type = "";
		$tabl = "";
	}
	//comprobaciones
	if($data == "" && $type == "" && $tabl == ""){
		$rs["r"] = "Error: datos no encontrados";
		print_r(json_encode($rs));
		return;
	}
	//llamada global
	$cry = new Criptografia();
	$hashing = new HashD();
	//usuarios
	$usu = new Usuario();
	$arch = new Archivo();
	if($tabl=="usu"){
		switch($type){
			case "add":
				$usu->correo = $data["usuari"];
				$usu->codigo = "";
				$usu->nombres = $data["nombre"];
				$usu->apellido = $data["apelli"];
				$usu->imagen = $data["imgsrc"];
				$usu->cargo = "2";

				$hashing->setPass($data["contra"]);
				$usu->contrasena = $hashing->hashR();
				print_r(json_encode($usu-
>agregarUsuario()));

				$carpeta = new Carpeta();
				$carpeta->nombre = "root_snd_private";
				$carpeta->correo = $usu->correo;
				$carpeta->permiso = "rwx";

				$carpeta->agregarFolder();
				break;
			case "login":
				$usu->correo = $data["usu"];

				$hashing->setPass($data["pass"]);
				$usu->contrasena = $hashing->hashR();

				print_r(json_encode($usu->login()));
				break;
			case "loginA":
				$usu->correo = $data["correo"];
				//$usu->contrasena = $data["contrasena"];
```

```
                $usu->contrasena = $data["contrasena"];

                print_r(json_encode($usu->login()));
                break;
            case "update":
                $res = array();
                $val =
"`nombres`='".$data["nombre_user"]."',  `apellido`='".$data["ape_user"]."'
WHERE `correo`='".$data["Correo_user_ed"]."'";
                $table = "`usuario`";

                $os->cnS = "UPDATE ".$table." SET ".$val;
                $res = $os->ejecutarConsultaD();

                /*************************/
                if($res["r"] == "Exito"){
                    $res["data"] = $data;
                }else $res["data"] = "";
                /*************************/
                //$res["data"] = $data;
                print_r(json_encode($res));
                break;
            case "updatePass":
                $res = array();
                if($data["passAn_user"] ==
$data["passNu_user"]){

                    $hashing-
>setPass($data["passAn_user"]);
                    $pass = $hashing->hashR();

                    $val = "`contrasena`='".$pass."'
WHERE `correo`='".$data["Correo_user_edp"]."'";
                    $table = "`usuario`";

                    $os->cnS = "UPDATE ".$table." SET
".$val;
                    $res = $os->ejecutarConsultaD();

                    /*************************/
                    if($res["r"] == "Exito"){
                        $res["data"] = $data;
                    }else $res["data"] = "";
                    /*************************/
                    //$res["data"] = $data;
                }else $res["r"] = "Error";
                print_r(json_encode($res));
                break;
            case "comprobar":
                session_start();
                $a = array();
                if(isset($_SESSION["S"])) $a["response"] =
"Si";
                else $a["response"] = "No";
                print_r(json_encode($a));
```

```
                                        break;
                                case "datos":
                                        $usu->correo = $data["correo"];
                                        print_r(json_encode($usu-
>obtenerDatosWid()));
                                        break;
                                default:
                                        print_r(json_encode(array("r"=>"sin    datos
:(")));
                                        break;
                        }
                }
elseif($tabl=="institucion"){
                        session_start();
                        switch($type){
                                case "add":
                                        $res = array();
                                        $val    =    "'".$_SESSION["S"]["USER"]."',
'".$data["nombre_act"]."',   '".$data["cant_act"]."',   '".$data["categ_act"]."',
'".$data["propie_act"]."',  '".$data["confid_act"]."',  '".$data["integri_act"]."',
'".$data["dispo_act"]."', CURRENT_DATE, CURRENT_TIME";
                                        $table    =    "`activo`(`correo`,    `nombre`,
`cantidad`,  `categoria`,  `propietario`,  `confidencialidad`,  `integridad`,
`disponibilidad`, fecha, hora)";
                                        $os->cnS    =    "INSERT    INTO    ".$table."
VALUES (".$val.")";
                                        $res = $os->ejecutarConsultaD();
                                        //$res["q"] = $os->cnS;
                                        /*****************************/
                                        if($res["r"] == "Exito"){
                                                $res["data"] = $data;
                                        }else $res["data"] = "";
                                        /*****************************/
                                        //$res["data"] = $data;
                                        print_r(json_encode($res));
                                        break;
$res = array();
                                        $os->cnS    =    "DELETE    FROM    `institucion`
WHERE `idinstitucion`='".$data["_id"]."'";
                                        $res = $os->ejecutarConsultaD();
                                        $res["q"] = $os->cnS;
                                        /*****************************/
                                        if($res["r"] == "Exito"){
                                                $res["data"] = $data;
                                        }
                                        print_r(json_encode($res));
                                        break;
                                default:
                                        print_r(json_encode(array("r"=>"sin    datos
:(")));
                                        break;
                        }
                }
                elseif($tabl=="evaluacion"){
                        session_start();
```

```
switch($type){
	case "add":
		$res = array();
		$os->cnS = "SELECT * FROM `items` WHERE iditems='".$data["idItemAddAdjunt"]."'";
		$resItem = $os->ejecutarConsulta();
		$datosItem = isset($resItem["datos"]) ? $resItem["datos"] : "sinDatos";
		if($datosItem != "sinDatos"){
			$os->cnS = "SELECT MAX(idarchivo) AS nmax FROM archivo";
			$cns = $os->ejecutarConsulta();
			$cantMax = isset($cns["datos"]) ? $cns["datos"]["nmax"] : 0;
			$cantMax = isset($cantMax)?(intval($cantMax)+1):1;
			$idFile = intval($cantMax);

			$val = "'".$idFile."', '".$data["idItemAddAdjunt"]."', '".$data["ruta"]."', '".$data["oportunidad"]."', '".$data["puntos"]."', '".$data["observaciones"]."', CURRENT_DATE, CURRENT_TIME";
			$table = "`archivo`(`idarchivo`, `iditems`, `ruta`, `opmejora`, `puntofuerte`, `observacion`, `fecha`, `hora`)";
			$os->cnS = "INSERT INTO ".$table." VALUES (".$val.")";
			$res = $os->ejecutarConsultaD();

}else $res["r"] = "no";
		print_r(json_encode($res));
		break;
	case "comprobar":
		$res = array();
		$os->cnS = "SELECT * FROM `items` WHERE iditems='".$data["idItemAddAdjunt"]."'";
		$resItem = $os->ejecutarConsulta();
		$datosItem = isset($resItem["datos"]) ? $resItem["datos"] : "sinDatos";
		if($datosItem == "sinDatos") $res["e"] = 0;
		else $res["e"] = 1;

		$os->cnS = "SELECT * FROM `archivo` WHERE iditems='".$data["idItemAddAdjunt"]."'";
		$resItem = $os->ejecutarConsulta();
		$datosItem = isset($resItem["datos"]) ? $resItem["datos"] : "sinDatos";
		if($datosItem == "sinDatos") $res["ee"] = 0;
		else $res["ee"] = 1;
		print_r(json_encode($res));
		break;
	case "addEva":
		$res = array();
```

```
                                $val = "'".$data["idItems"]."',
'".$_SESSION["S"]["USER"]."', '".$data["politica"]."',
'".$data["sugerencia"]."', CURRENT_DATE, CURRENT_TIME";
                                $table = "`evaluacion`(`iditems`, `correo`,
`control`, `sugerencias`, `fecha`, `hora`)";
                                $os->cnS = "INSERT INTO ".$table."
VALUES (".$val.")";
                                $res = $os->ejecutarConsultaD();
                                $res["q"] = $os->cnS;
                                /***************************/
                                if($res["r"] == "Exito"){
                                        $res["data"] = $data;

                                }else $res["data"] = "";
                                /***************************/
                                print_r(json_encode($res));
                                break;
                        case "addEvaItems":
                                $itmLen = count($data["ti"]);
                                $res = array();
                                $val = "";
                                if(!is_array($data["ti"])){
                                        $idI = $data["idC"]."".$data["cnI"]."1";
                                        $valu = $data[$data["cnI"]."1"];
                                        $val = "('".$idI."',
'".$_SESSION["S"]["USER"]."', '".$data["to"]."', '".$data["ts"]."',
'".$data["ti"]."', '".$valu."', '".$data["idC"]."', '".$data["idFecha"]."',
'".$data["idHora"]."')";
                                        //CURRENT_DATE,
CURRENT_TIME)";
                                }else{
                                        $val = array();
                                        for($i=0;$i<$itmLen;$i++){
                                                $idI =
$data["idC"]."".$data["cnI"].($i + 1);
                                                $valu = $data[$data["cnI"].($i
+ 1)];
                                                $ti = $data["ti"][$i];
                                                $q = "('".$idI."',
'".$_SESSION["S"]["USER"]."', '".$data["to"]."', '".$data["ts"]."', '".$ti."',
'".$valu."', '".$data["idC"]."', '".$data["idFecha"]."', '".$data["idHora"]."')";
                                                //CURRENT_DATE,
CURRENT_TIME)";

                                                array_push($val, $q);
                                        }
                                }
                                $val = is_array($val) ? join(",", $val) : $val;

                                $table = "`items`(`iditems`, `correo`, `item`,
`subI`, `evaluacion`, `valor`, `gruoup`, `fecha`, `hora`)";
                                $os->cnS = "INSERT INTO ".$table."
VALUES ".$val;
                                $res = $os->ejecutarConsultaD();
                                //**************************
```

```
                                if($res["r"] == "Exito"){
                                        $res["data"] = $data;
                                }else $res["data"] = "";
                                //**************************
//                              $data["ids"] = $idI;
//                              $data["cns"] = $os->cnS;
//                              $data["ca"] = $itmLen;
                                print_r(json_encode($res));
                                break;
                        case "upEvaItems":
                                $res = array();
                                $cant = count($data["idItem"]);
                                $iA = 0;
                                if(is_array($data["idItem"])){
                                        $fR = count($data["idItem"]);
                                        for($i=0;$i<$fR;$i++){
                                                $valu = $data[$data["cnI"].($i
+ 1)];
                                                $val    =    "`valor`='".$valu."'
WHERE `iditems`='".$data["idItem"][$i]."'";
                                                $table = "`items`";
                                                $os->cnS      =      "UPDATE
".$table." SET ".$val;
                                                $rU             =             $os-
>ejecutarConsultaD();

                                                if($rU["r"] == "Exito") $iA++;
                                        }
                                }else{
                                        $valu = $data[$data["cnI"]."1"];
                                        $val  =  "`valor`='".$valu."'  WHERE
`iditems`='".$data["idItem"]."'";
                                        $table = "`items`";
                                        $os->cnS = "UPDATE ".$table." SET
".$val;
                                        $rU = $os->ejecutarConsultaD();

                                        if($rU["r"] == "Exito") $iA++;
                                }
                                if($cant == $iA) $res["r"] = "Exito";
                                else $res["r"] = "Error";

                                print_r(json_encode($res));
                                break;
                        case "addVer":
                                $res = array();
                                $val            =            "'".$data["correo"]."',
'".$data["estadoVer"]."',    '".$data["sugerencia"]."',    '".$data["idItems"]."',
CURRENT_DATE, CURRENT_TIME";
                                $table  =  "`verificacion`(`correo`,  `estado`,
`sugerencia`, `gruoupitem`, `fecha`, `hora`)";
                                $os->cnS  =  "INSERT  INTO  ".$table."
VALUES (".$val.")";
                                $res = $os->ejecutarConsultaD();
                                $res["q"] = $os->cnS;
```

```
                                        /*****************************/
                                        if($res["r"] == "Exito"){
                                                $res["data"] = $data;

                                        }else $res["data"] = "";
                                        /*****************************/
                                        print_r(json_encode($res));
                                        break;
                                case "addCopy":
                                        $res = array();
                                        $val     =     """.$_SESSION["S"]["USER"].'",
'".$data["fileS"].'", CURRENT_DATE, CURRENT_TIME";
                                        $table = "`copia`(`correo`, `archivo`, `fecha`,
`hora`)";
                                        $os->cnS    =    "INSERT    INTO    ".$table."
VALUES (".$val.")";
                                        $res = $os->ejecutarConsultaD();
                                        $res["q"] = $os->cnS;
                                        /*****************************/
                                        if($res["r"] == "Exito"){
                                                $res["data"] = $data;

                                        }else $res["data"] = "";
                                        /*****************************/
                                        print_r(json_encode($res));
                                        break;
                                case "actualizar":
                                        //data[idItems]5
                                        $res = array();
                                        $val                                                =
"`control`='".$data["politica"]."',`sugerencias`='".$data["sugerencia"]."'
WHERE `idevaluacion`='".$data["idEvaluacion"]."'";
                                        $table = "`evaluacion`";

                                        $os->cnS = "UPDATE ".$table." SET ".$val;
                                        $res = $os->ejecutarConsultaD();
                                        $res["q"] = $os->cnS;
                                        /*****************************/
                                        if($res["r"] == "Exito"){
                                                $res["data"] = $data;
                                        }else $res["data"] = "";
                                        /*****************************/
                                        //$res["data"] = $data;
                                        print_r(json_encode($res));
                                        break;
                                default:
                                        print_r(json_encode(array("r"=>"sin     datos
:(")));
                                        break;
                        }
                }
                elseif($tabl==""){
                        switch($type){
                                case "":
                                        break;
```

```
                default:
                        print_r(json_encode(array("r"=>"sin datos
:(")));
                        break;
                }
        }
        else{
                print_r(json_encode(array("r"=>"sin datos :(")));
        }
?>
```

C. PARA ENCRIPTAR LA CONTRASEÑA DEL INICIO DE SESIÓN DEL SISTEMA

```
<?php
        class Criptografia{
                private $keyA;
                private $encryption;
                private $mode;
                private $iv;
                private $cryptM;

                public $number;
                public $message;
                public $encript;

                function __construct(){
                        $this->encryption =
MCRYPT_RIJNDAEL_128;//MCRYPT_RIJNDAEL_128;
                        $this->keyA = ""; //16, 24, 32
                        $this->mode = MCRYPT_MODE_CBC;
                        $this->number = 5;
                }
                function encriptar(){
                        //$this->iv =
mcrypt_create_iv(mcrypt_get_iv_size($this->encryption, $this->mode),
$this->number);
                        $tmp_iv = $this->cambiarTam($this->iv, 16);
                        $tmp_key = $this->tamanio_key($this->keyA);
                        $this->encript = mcrypt_encrypt($this->encryption,
$tmp_key, $this->message, $this->mode, $tmp_iv);
                        $this->cryptM = $this->encript;
                        return(array("crypt" => $this->encript));
                }
                function des_encriptar(){
                        //$this->iv =
mcrypt_create_iv(mcrypt_get_iv_size($this->encryption, $this->mode),
$this->number);
                        $tmp_iv = $this->cambiarTam($this->iv, 16);
                        $tmp_key = $this->tamanio_key($this->keyA);
                        $this->encript = mcrypt_decrypt($this->encryption,
$tmp_key, $this->cryptM, $this->mode, $tmp_iv);
                        return(array("dcrypt" => $this->encript));
                }
                function tamanio_key($key){
```

```
                $tamanio = strlen($key);
                $tmp_string = "";
                $tam_restante = 0;
                $tmp_key = "";

                if($tamanio == 16) $tmp_key = $key;
                elseif($tamanio == 24) $tmp_key = $key;
                elseif($tamanio == 32) $tmp_key = $key;
                elseif($tamanio > 0 && $tamanio < 16){
                        $tam_restante = 16 - $tamanio;
                        for($i = 0; $i < $tam_restante; $i++)
$tmp_string .= "".$this->numberLetter($i);
                        $tmp_key = $key."".$tmp_string;
                }
                elseif($tamanio > 16 && $tamanio < 24){
                        $tam_restante = 24 - $tamanio;
                        for($i = 0; $i < $tam_restante; $i++)
$tmp_string .= "".$this->numberLetter($i);
                        $tmp_key = $key."".$tmp_string;
                }
                elseif($tamanio > 24 && $tamanio < 32){
                        $tam_restante = 32 - $tamanio;
                        for($i = 0; $i < $tam_restante; $i++)
$tmp_string .= "".$this->numberLetter($i);
                        $tmp_key = $key."".$tmp_string;
                }
                elseif($tamanio > 32){
                        $tmp_key = substr($key,0,32);
                }
                else $tmp_key = "";

                return($tmp_key);
        }
        function numberLetter($number){
                $tmp_letter_number = "";
                switch($number){
                        case 0: $tmp_letter_number = $number;
break;
                        case 1: $tmp_letter_number = $number;
break;
                        case 2: $tmp_letter_number = $number;
break;
                        case 3: $tmp_letter_number = $number;
break;
                        case 4: $tmp_letter_number = $number;
break;
                        case 5: $tmp_letter_number = $number;
break;
                        case 6: $tmp_letter_number = $number;
break;
                        case 7: $tmp_letter_number = $number;
break;
                        case 8: $tmp_letter_number = $number;
break;
```

```
                                case 9: $tmp_letter_number = $number;
break;
                                case 10: $tmp_letter_number = "a"; break;
                                case 11: $tmp_letter_number = "c"; break;
                                case 12: $tmp_letter_number = "d"; break;
                                case 13: $tmp_letter_number = "e"; break;
                                case 14: $tmp_letter_number = "f"; break;
                                case 15: $tmp_letter_number = "g"; break;
                                case 16: $tmp_letter_number = "h"; break;
                                case 17: $tmp_letter_number = "i"; break;
                                case 18: $tmp_letter_number = "j"; break;
                                case 19: $tmp_letter_number = "k"; break;
                                case 20: $tmp_letter_number = "l"; break;
                                case 21: $tmp_letter_number = "m"; break;
                                case 22: $tmp_letter_number = "n"; break;
                                case 23: $tmp_letter_number = "o"; break;
                                case 24: $tmp_letter_number = "p"; break;
                                case 25: $tmp_letter_number = "q"; break;
                                case 26: $tmp_letter_number = "r"; break;
                                case 27: $tmp_letter_number = "s"; break;
                                case 28: $tmp_letter_number = "t"; break;
                                case 29: $tmp_letter_number = "u"; break;
                                case 30: $tmp_letter_number = "v"; break;
                                case 31: $tmp_letter_number = "w"; break;
                                case 32: $tmp_letter_number = "x"; break;
                                case 33: $tmp_letter_number = "y"; break;
                                case 34: $tmp_letter_number = "z"; break;
                                case 35: $tmp_letter_number = "@"; break;
                                default: $tmp_letter_number = "+"; break;
                        }
                        return($tmp_letter_number);
                }
                public function cambiarTam($letter, $size){
                        $tamanio = strlen($letter);
                        $tmp_string = "";
                        $tam_restante = 0;
                        $tmp_letter = "";

                        if($tamanio == $size) $tmp_letter = $letter;
                        elseif($tamanio > 0 && $tamanio < $size){
                                $tam_restante = $size - $tamanio;
                                for($i = 0; $i < $tam_restante; $i++)
$tmp_string .= "".$this->numberLetter($i);
                                $tmp_letter = $letter."".$tmp_string;
                        }
                        elseif($tamanio > $size) $tmp_letter =
substr($letter, 0, $size);
                        else $tmp_letter = "";

                        return($tmp_letter);
                }
                public function setKey($key){$this->keyA = $key;}
                public function setEncryption($encryption){$this-
>encryption = $encryption;}
                public function setMode($mode){$this->kmode = $mode;}
```

```
		public function setIv($iv){$this->iv = $iv;}
	}
	class HashD{
		private $pass;
		private $options;
		private $algoritmo;

		function __construct(){
			$this->algoritmo = "tiger192,3";//'ripemd160', md5, tiger192,3
			$this->options = [
				'cost' => 12,
			];
		}
		function pass_hasc(){
			return(password_hash($this->pass, PASSWORD_BCRYPT, $this->options));
		}
		function hashR(){
			return(hash($this->algoritmo, $this->pass));
		}

		function setPass($el){$this->pass = $el;}
		function setOptions($el){$this->options = $el;}
		function setAlgoritmo($el){$this->algoritmo = $el;}
	}
?>
```

D. PARA LA RECOLECCIÓN DE DATOS DEL MÓDULO REPORTES DEL SISTEMA

```
<?php
	header("Content-Type: application/json");
	require_once("all.php");

	$option = isset($_POST["op"]) ? $_POST["op"] : (isset($op) ? $op : "incidenciaSoft");
	$option = isset($_GET["op"]) ? $_GET["op"] : $option;
	$anioI = isset($_GET["anioi"]) ? $_GET["anioi"] : date("Y");
	$anioF = isset($_GET["aniof"]) ? $_GET["aniof"] : date("Y");
	$anioI = ($anioI!="") ? $anioI : date("Y");
	$anioF = ($anioF!="") ? $anioF : date("Y");

	$fechaI = $anioI."-01-01";
	$fechaF = $anioF."-12-31";
	if(!isset($actual)) session_start();
	$md = new ManagerDb();

	switch($option){
		case "riesgo":
			$q = "SELECT *, COUNT(fecha) AS cant FROM `items` WHERE (fecha>='".$fechaI."' AND fecha<='".$fechaF."') AND correo='".$_SESSION["S"]["USER"]."' GROUP BY fecha, riesgo ORDER BY riesgo";
```

```
                        $datos = $md->obtenerDatos($q, "");
                        $dRecol = isset($datos["datos"]) ? $datos["datos"] :
array();

                        $label = array();
                        $data = array();
                        $datosR = array();
                        foreach($dRecol as $k => $v){
                                $fecha = $v["fecha"];
                                $fecha = explode("-", $fecha);
                                array_push($label,                $md-
>fechaWinthNumber($fecha[1]));
                                array_push($data, $v["cant"]);
                        }
                        $datosR["label"] = $label;
                        $datosR["data"] = $data;
                        $datosR["title"] = "Cantidad de riesgos";
                        print_r(json_encode($datosR));
                        break;
                case "riesgoFC":
                        $Nval = [
                                "Ninguna de las opciones",
                                "La organizacion no a contmeplado la
realizacion de acciones en este sentido",
                                "Se realizan acciones de manera puntual",
                                "Se realizan acciones de manera
sistematica (planificadas y periodicas)",
                                "Se realizan acciones conforme a una
metodología/proceso/procedimiento",
                                "Las acciones que se realizan estan
integradas en los procesos de organizacion"
                        ];
                        $fechaI = $anioI."-01-01";
                        $fechaF = $anioI."-12-31";
                        $q = "SELECT valor, gruoup, fecha, hora,
COUNT(gruoup) AS cant FROM `items` WHERE (fecha>='".$fechaI."'
AND fecha<='".$fechaF."') AND correo='".$_SESSION["S"]["USER"]."'
GROUP BY valor, fecha ORDER BY fecha ASC";

                        $datos = $md->obtenerDatos($q, "");
                        $dRecol = isset($datos["datos"]) ? $datos["datos"] :
array();

                        $label = array();
                        $dataR = array();
                        $datosR = array();
                        foreach($dRecol as $k => $v){
                                $fecha = $v["fecha"];
                                $fecha = explode("-", $fecha);
                                if(!in_array($md-
>fechaWinthNumber($fecha[1]), $label)){
                                        array_push($label,        $md-
>fechaWinthNumber($fecha[1]));
                                }
                        }
```

```
                        $c = 1;
                        $datosR["month"] = $label;
                        $datosR["datos"] = array();
                        $datosR["titles"] = $Nval;
                        foreach($label as $kk => $vv){
                                $d = array();
                                $d["titulo"] = "";
                                $d["month"] = $vv;
                                //-----------------
                                $NvalC = [0,0,0,0,0,0];
                                $val = [[0], [1,2,3], [4,5,6], [7,8,9], [10,11,12],
[13]];

                                $vs = array();
                                $cn = array();
                                $nC = 0;
                                foreach($dRecol as $ks => $vss){
                                        $fecha = $vss["fecha"];
                                        $fecha = explode("-", $fecha);
                                        if($vv                ==                $md-
>fechaWinthNumber($fecha[1])){
                                                array_push($vs,
intval($vss["valor"]));

        if(isset($cn["ca".$vss["valor"]]))       $cn["ca".$vss["valor"]]       +=
intval($vss["cant"]);
                                                else $cn["ca".$vss["valor"]] =
intval($vss["cant"]);
                                        }
                                }
                                for($i=0;$i<count($NvalC);$i++){
                                        $_vs = $val[$i];
                                        for($j=0;$j<count($_vs);$j++){
                                                if(in_array($_vs[$j],       $vs))
$NvalC[$i]+=$cn["ca".$_vs[$j]];
                                        }
                                }
                                $nC++;
                                //-----------------

                                $d["data"] = $NvalC;//$dataR;
                                array_push($datosR["datos"], $d);
                                $dataR = array();
                                $c++;
                        }
                        print_r(json_encode($datosR));
                        break;
                case "impacto":
                        $q = "SELECT *, COUNT(fecha) AS cant FROM
`items` WHERE (fecha>='".$fechaI."' AND fecha<='".$fechaF."') AND
correo='".$_SESSION["S"]["USER"]."' GROUP BY fecha, impacto
ORDER BY impacto";

                        $datos = $md->obtenerDatos($q, "");
```

```
                $dRecol = isset($datos["datos"]) ? $datos["datos"] :
array();

                $label = array();
                $dataR = array();
                $datosR = array();
                foreach($dRecol as $k => $v){
                        $fecha = $v["fecha"];
                        $fecha = explode("-", $fecha);
                        if(!in_array($md-
>fechaWinthNumber($fecha[1]), $label)){
                                array_push($label,          $md-
>fechaWinthNumber($fecha[1]));
                        }
                }

                $c = 1;
                $datosR["month"] = $label;
                $datosR["datos"] = array();
                $datosR["titles"] = ["Alto", "Intermedio", "Bajo"];
                foreach($label as $kk => $vv){
                        $d = array();
                        $d["titulo"] = "";
                        $d["month"] = $vv;

                        foreach($dRecol as $k => $v){
                                $fecha = $v["fecha"];
                                $fecha = explode("-", $fecha);

                                if($vv          ==          $md-
>fechaWinthNumber($fecha[1])){
                                        if($v["impacto"] == "Alto"){
                                                $dataR[0] = $v["cant"]
* 1;
                                        }
                                        if($v["impacto"]          ==
"Intermedio"){
                                                $dataR[1] = $v["cant"]
* 1;
                                        }
                                        if($v["impacto"] == "Bajo"){
                                                $dataR[2] = $v["cant"]
* 1;
                                        }
                                }
                        }
                        $dataR[0] = isset($dataR[0]) ? $dataR[0] : 0;
                        $dataR[1] = isset($dataR[1]) ? $dataR[1] : 0;
                        $dataR[2] = isset($dataR[2]) ? $dataR[2] : 0;

                        $d["data"] = $dataR;
                        array_push($datosR["datos"], $d);
                        $dataR = array();
                        $c++;
                }
```

```
                        print_r(json_encode($datosR));
                        break;
                case "verificacion":
$q = "SELECT v.*, COUNT(v.estado) AS cant FROM `verificacion` AS v
WHERE (v.correo='".$_SESSION["S"]["USER"]."') AND
(v.fecha>='".$fechaI."' AND v.fecha<='".$fechaF."') GROUP BY v.estado,
v.fecha";

                        $datos = $md->obtenerDatos($q, "");
                        $dRecol = isset($datos["datos"]) ? $datos["datos"] :
array();

                        $label = array();
                        $dataR = array();
                        $datosR = array();
                        foreach($dRecol as $k => $v){
                                $fecha = $v["fecha"];
                                $fecha = explode("-", $fecha);
                                if(!in_array($md-
>fechaWinthNumber($fecha[1]), $label)){
                                        array_push($label, $md-
>fechaWinthNumber($fecha[1]));
                                }
                        }

                        $c = 1;
                        $datosR["month"] = $label;
                        $datosR["datos"] = array();
                        $datosR["titles"] = ["Finalizado", "En proceso", "Por
verificar"];
                        foreach($label as $kk => $vv){
                                $d = array();
                                $d["titulo"] = "";
                                $d["month"] = $vv;

                                foreach($dRecol as $k => $v){
                                        $fecha = $v["fecha"];
                                        $fecha = explode("-", $fecha);

                                        if($vv == $md-
>fechaWinthNumber($fecha[1])){
if($v["estado"] == "Finalizado"){
$dataR[0] = $v["cant"] * 1;
        }
if($v["estado"] == "En proceso"){
$dataR[1] = $v["cant"] * 1;
}
                                                if($v["estado"] == "Por
verificar"){
                                                        $dataR[2] = $v["cant"]
* 1;
                                                }
                                        }
                                }
                                $dataR[0] = isset($dataR[0]) ? $dataR[0] : 0;
```

```
                                $dataR[1] = isset($dataR[1]) ? $dataR[1] : 0;
                                $dataR[2] = isset($dataR[2]) ? $dataR[2] : 0;

                                $d["data"] = $dataR;
                                array_push($datosR["datos"], $d);
                                $dataR = array();
                                $c++;
                        }
                        print_r(json_encode($datosR));
                        break;
                default:  print_r(json_encode(array("error"=>"sin  datos")));
break;
        }?>
```

E. EXIT: PARA EL CIERRE DE SESIÓN DEL SISTEMA

```
<?php
        header("Content-Type: application/json");
        session_start();
        $rs = array();
        if(isset($_POST["salir"])){
                if(isset($_SESSION["S"]) && $_POST["salir"] == "si"){
                        unset($_SESSION["S"]);
                        //session_destroy();
                        $rs["response"] = "exito";
                }elseif($_POST["salir"] == "comprobar"){
                        if(!isset($_SESSION["S"]))  $rs["response"]  =  "no
existe";
                        else $rs["response"] = "existe";
                }else{
                        $rs["response"] = "salir";
                }
        }
        print_r(json_encode($rs));
?>
```

F. MYPHP: PARA EXPORTAR UNA LA BASE DE DATOS DEL SISTEMA

```
<?php
define("DB_USER", 'root');
define("DB_PASSWORD", '');
define("DB_NAME", 'control');
define("DB_HOST", 'localhost');
define("BACKUP_DIR", '../copiaBd');
define("TABLES", '*');
define("CHARSET", 'utf8');
define("GZIP_BACKUP_FILE", true);
class Backup_Database {
   var $host;
   var $username;
   var $passwd;
   var $dbName;
   var $charset;
   var $conn;
   var $backupDir;
   var $backupFile;
```

```
   var $gzipBackupFile;

        public $nameFile;

   public function __construct($host, $username, $passwd, $dbName, $charset = 'utf8') {
      $this->host          = $host;
      $this->username      = $username;
      $this->passwd        = $passwd;
      $this->dbName        = $dbName;
      $this->charset       = $charset;
      $this->conn          = $this->initializeDatabase();
      $this->backupDir     = BACKUP_DIR ? BACKUP_DIR : '.';
      $this->backupFile                    = 'copiaDb-'.$this->dbName.'-'.date("Ymd_His", time()).'.sql';
      $this->gzipBackupFile      = defined('GZIP_BACKUP_FILE') ? GZIP_BACKUP_FILE : true;
   }

   protected function initializeDatabase() {
      try {
         $conn = mysqli_connect($this->host, $this->username, $this->passwd, $this->dbName);
         if (mysqli_connect_errno()) {
            throw new Exception('ERROR connecting database: ' . mysqli_connect_error());
            die();
         }
         if (!mysqli_set_charset($conn, $this->charset)) {
            mysqli_query($conn, 'SET NAMES '.$this->charset);
         }
      } catch (Exception $e) {
         print_r($e->getMessage());
         die();
      }

      return $conn;
   }
   public function backupTables($tables = '*') {
      try {
         /**
         * Tables to export
         */
         if($tables == '*') {
            $tables = array();
            $result = mysqli_query($this->conn, 'SHOW TABLES');
            while($row = mysqli_fetch_row($result)) {
               $tables[] = $row[0];
            }
         } else {
            $tables = is_array($tables) ? $tables : explode(',',$tables);
         }

         $sql = 'CREATE DATABASE IF NOT EXISTS `'.$this->dbName."`;\n\n";
```

```
        $sql .= 'USE '.$this->dbName.";\n\n";

        /**
        * Iterate tables
        */
        foreach($tables as $table) {
            $this->obfPrint("Haciendo copia de la tabla: `".$table."`...".str_repeat('.', 20-strlen($table)), 0, 0);

            /**
             * CREATE TABLE
             */
            $sql .= 'DROP TABLE IF EXISTS `'.$table.'`;';
            $row = mysqli_fetch_row(mysqli_query($this->conn, 'SHOW CREATE TABLE `'.$table.'`'));
            $sql .= "\n\n".$row[1].";\n\n";

            /**
             * INSERT INTO
             */

            $row = mysqli_fetch_row(mysqli_query($this->conn, 'SELECT COUNT(*) FROM `'.$table.'`'));
            $numRows = $row[0];

            // Split table in batches in order to not exhaust system memory
            $batchSize = 1000; // Number of rows per batch
            $numBatches = intval($numRows / $batchSize) + 1; // Number of while-loop calls to perform
            for ($b = 1; $b <= $numBatches; $b++) {

                $query = 'SELECT * FROM `'.$table.'` LIMIT '.($b*$batchSize-$batchSize).','.$batchSize;
                $result = mysqli_query($this->conn, $query);
                $numFields = mysqli_num_fields($result);

                for ($i = 0; $i < $numFields; $i++) {
                    $rowCount = 0;
                    while($row = mysqli_fetch_row($result)) {
                        $sql .= 'INSERT INTO `'.$table.'` VALUES(';
                        for($j=0; $j<$numFields; $j++) {
                            if (isset($row[$j])) {
                                $row[$j] = addslashes($row[$j]);
                                $row[$j] = str_replace("\n","\\n",$row[$j]);
                                $sql .= ""$row[$j]."" ;
                            } else {
                                $sql.= 'NULL';
                            }

                            if ($j < ($numFields-1)) {
                                $sql .= ',';
                            }
                        }

                        $sql.= ");\n";
```

```
                }
            }

            $this->saveFile($sql);
            $sql = '';
        }

        $sql.="\n\n\n";

        $this->obfPrint(" OK");
    }

    if ($this->gzipBackupFile) {
        $this->gzipBackupFile();
    } else {
        $this->obfPrint('Exito al guardar archivo en: ' . $this->backupDir.'/'.$this->backupFile, 1, 1);
    }
} catch (Exception $e) {
    print_r($e->getMessage());
    return false;
}

return true;
}
protected function saveFile(&$sql) {
    if (!$sql) return false;

    try {

        if (!file_exists($this->backupDir)) {
            mkdir($this->backupDir, 0777, true);
        }

        file_put_contents($this->backupDir.'/'.$this->backupFile, $sql, FILE_APPEND | LOCK_EX);

    } catch (Exception $e) {
        print_r($e->getMessage());
        return false;
    }

    return true;
}
protected function gzipBackupFile($level = 9) {
    if (!$this->gzipBackupFile) {
        return true;
    }

    $source = $this->backupDir . '/' . $this->backupFile;
    $dest =  $source . '.zip';

    $this->obfPrint('Finalizado con exito .... ', 1, 0);
    //$this->obfPrint('El archivo fue comprimido y guardado en ' . $dest . '... ', 1, 0);
```

```
                $this->nameFile = $dest;

        $mode = 'wb' . $level;
        if ($fpOut = gzopen($dest, $mode)) {
            if ($fpIn = fopen($source,'rb')) {
                while (!feof($fpIn)) {
                    gzwrite($fpOut, fread($fpIn, 1024 * 256));
                }
                fclose($fpIn);
            } else {
                return false;
            }
            gzclose($fpOut);
            if(!unlink($source)) {
                return false;
            }
        } else {
            return false;
        }

        $this->obfPrint('OK');
        return $dest;
    }
    public function obfPrint ($msg = '', $lineBreaksBefore = 0,
$lineBreaksAfter = 1) {
        if (!$msg) {
            return false;
        }

        $output = '';

        if (php_sapi_name() != "cli") {
            $lineBreak = "<br />";
        } else {
            $lineBreak = "\n";
        }

        if ($lineBreaksBefore > 0) {
            for ($i = 1; $i <= $lineBreaksBefore; $i++) {
                $output .= $lineBreak;
            }
        }

        $output .= $msg;

        if ($lineBreaksAfter > 0) {
            for ($i = 1; $i <= $lineBreaksAfter; $i++) {
                $output .= $lineBreak;
            }
        }

        echo $output;

        if (php_sapi_name() != "cli") {
            ob_flush();
```

```
        }

        flush();
    }
}

error_reporting(E_ALL);
set_time_limit(900);

if (php_sapi_name() != "cli") {
    echo '<div style="font-family: monospace;">';
}

$backupDatabase = new Backup_Database(DB_HOST, DB_USER,
DB_PASSWORD, DB_NAME);
$result = $backupDatabase->backupTables(TABLES, BACKUP_DIR) ?
'OK' : 'KO';
$backupDatabase->obfPrint('Resultado de comprension: ' . $result, 1);
echo "<input type='hidden' id='resultC' value='".$result."'>";
echo "<input type='hidden' id='resultFile' value='".$backupDatabase-
>nameFile."'>";

if (php_sapi_name() != "cli") {
    echo '</div>';
}
```

G. OPEN SERVER: CONEXIÓN DE LA BASE DE DATOS CON LOS MÓDULOS PARA EJECUTAR CONSULTAS EN LA BASE DE DATOS

```
<?php
        class OpenServ{
                private $servS;
                private $userS;
                private $passS;
                private $enlaceS;
                public $dbS;
                public $cnS;
                public $infoConS;
                public $rsS;
                public $datos;

                function __construct(){
                        $this->servS = "localhost";
                        $this->userS = "root";
                        $this->passS = "";
                        $this->dbS = "control";
                        $this->enlaceS = null;
                        $this->infoConS = [];
                        $this->datos = null;
                }
                function enlace(){
                        try{
```

```
                $this->enlaceS = mysqli_connect($this->servS, $this->userS, $this->passS, $this->dbS) or die("No existe base de datos");
                return($this->enlaceS);
            }catch(Exception $e){
                $this->infoConS["r"] = "Error0";
                return($this->infoConS);
            }
        }
        function respuesta(){
            try{
                $this->rsS = mysqli_query($this->enlace(), $this->cnS);
                return($this->rsS);
            }catch(Exception $e){
                $this->infoConS["r"] = "Error0";
                return($this->infoConS);
            }
        }
        function conect(){
            if (!$this->respuesta()){
                $this->infoConS["r"] = "Error en la ejecucion";
                mysqli_close($this->enlaceS);
                //exit();
                return($this->infoConS);
            }
            return($this->rsS);
        }
        function ejecutarConsulta(){
            $datos = array();
            $this->rsS = $this->conect();
            if(is_array($this->rsS)){
                $datos["response"] = "Error";
                //return($this->rsS);
                return($datos);
            }else{
                while($fila = mysqli_fetch_assoc($this->rsS)) $datos["datos"] = $fila;
                if(isset($datos["datos"])) $datos["response"] = "Exito";
                else $datos["response"] = "SinDatos";
                mysqli_free_result($this->rsS);
                mysqli_close($this->enlaceS);
                return $datos;
            }
        }
        function ejecutarConsultaR(){
            $datos = array();
            $this->rsS = $this->conect();
            if(is_array($this->rsS)){
                $datos["response"] = "Error";
                //return($this->rsS);
                return($datos);
            }else{
```

```
                                $cont = 0;
                                while($fila = mysqli_fetch_assoc($this->rsS)){
                                        $datos["datos"][$cont] = $fila;
                                        $cont++;
                                }
                                $cont = 0;
                                if(isset($datos["datos"])) $datos["response"] = "Exito";
                                else $datos["response"] = "SinDatos";
                                mysqli_free_result($this->rsS);
                                mysqli_close($this->enlaceS);
                                return $datos;
                        }
                }
                function ejecutarConsultaD(){
                        $datos = array();
                        if (!$this->respuesta()){
                                $this->infoConS["r"] = "Error";
                                mysqli_close($this->enlaceS);
                                return($this->infoConS);
                        }else{
                                //while($fila = mysqli_fetch_array($this->rsS)) $datos[] = $fila;
                                $datos["r"] = "Exito";
                                return($datos);
                        }
                }
                function setCns($cnS){$openServer->cnS = $cnS;}
                function __destruct(){}
        }?>
```

H. UPCALL: PARA SUBIR UN ARCHIVO AL SISTEMA, COMO EN EL MÓDULO EVALUACIÓN DE RIESGOS

```
<?php
        header("Content-Type: application/json");
        require_once("openServer.php");
        require_once("uploadGeneral.php");
        session_start();
        $fm = new fileManager();

        if(isset($_FILES['archivo'])){
                $fm->fileO = $_FILES['archivo'];
                $rutaF = md5(md5($_SESSION["S"]["USER"]));
                if(isset($_GET['ruta'])){
                        $fm->rutaArchivo = "filesS/";
                }
                if(isset($_GET["nombre"])) $fm->tmp_name = $_GET["nombre"];
                else $fm->tmp_name = date("dmyst");
                print_r(json_encode($fm->uploadFile()));
        }else print_r(array("estado" => "Error"))
?>
```

I. USUARIO: PARA MODIFICAR LOS DATOS DEL USUARIO

```
<?php
	require_once("../actions/openServer.php");
	class Usuario{
		public $correo;
		public $codigo;
		public $nombres;
		public $apellido;
		public $imagen;
		public $cargo;//1: administrador, 2: usuario, 3: bloqueado
		public $contrasena;
		public $datoU;
		public $estado;
		public $rs = array();
		//limites
		public $lim_min = 0;
		public $lim_max = 15;

		//contactos
		public $c_contacto;
		public $c_correo;
		public $c_usuario;
		public $c_tipo;

		function __construct(){
			$this->correo = "";
			$this->codigo = "";
			$this->nombres = "";
			$this->apellido = "";
			$this->imagen = "";
			$this->cargo = "";
			$this->contrasena = "";
			$this->estado = 1;
		}
		function login(){
			session_start();
			//session_id("SEG01");
			$openServer = new OpenServ();
			$openServer->cnS = "SELECT * FROM `usuario` WHERE `correo`='".$this->correo."' AND contrasena='".$this->contrasena."'";
			//echo $openServer->cnS;
			$this->rs = $openServer->ejecutarConsulta();
			//print_r($this->rs);
			if($this->rs["response"] == "Exito"){
				if(empty($this->rs["datos"]["correo"]) || $this->rs["datos"]["correo"] != ""){
					$_SESSION["S"]["USER"] = $this->rs["datos"]["correo"];
					$_SESSION["S"]["PASS"] = $this->rs["datos"]["contrasena"];
				}
				if($_SESSION["S"]["USER"] == ""){
```

```
                                session_destroy();
                        }
                }
                return($this->rs);
        }
        function obtenerDatos(){
                $openServer = new OpenServ();
                $openServer->cnS = "SELECT * FROM `usuario` WHERE `correo`='".$this->correo."' AND contrasena='".$this->contrasena."'";
                $this->rs = $openServer->ejecutarConsulta();
                return($this->rs);
        }
        function obtenerDatosWid(){
                $openServer = new OpenServ();
                $openServer->cnS = "SELECT * FROM `usuario` WHERE `correo`='".$this->correo."'";
                $this->rs = $openServer->ejecutarConsulta();
                return($this->rs);
        }
        function agregarUsuario(){
                $res = array();
                $openServer = new OpenServ();
                if($this->comprobarUsuario()["r"] == 1){
                        $this->rs["r"] = "El correo ya esta registrado";
                }else{
                        $this->rs["r"] = "El correo no esta registrado";
                        $openServer->cnS = "INSERT INTO `usuario`(`correo`, `codigo`, `nombres`, `apellido`, `imagen`, `cargo`, `contrasena`, estado) VALUES ('".$this->correo."', '".$this->codigo."', '".$this->nombres."', '".$this->apellido."', '".$this->imagen."', '".$this->cargo."', '".$this->contrasena."', '".$this->estado."')";
                        $this->rs = $openServer->ejecutarConsultaD();
                        if($this->rs["r"] == "Exito"){
                                //$this->createFolder();
                                $res["r"] = $this->rs["r"];
                                $res["datos"] = $this->obtenerDatos()["datos"];
                        }
                }
                return($res);
        }
        function comprobarUsuario(){
                $openServer = new OpenServ();
                if ($this->c_correo != "") $sql = "SELECT * FROM `usuario` WHERE `correo`='".$this->c_correo."'";
                else $sql = "SELECT * FROM `usuario` WHERE `correo`='".$this->correo."'";
                $openServer->cnS = $sql;
                $this->datoU = $openServer->ejecutarConsulta();
                $this->rs["rr"] = $this->datoU;
```

```
                        if($this->datoU["response"] == "Error" || $this->datoU["response"] == "SinDatos") $this->rs["r"] = "0";
                        else $this->rs["r"] = "1";
                        return($this->rs);
                }
                function createFolder(){
                        $path = "../users/";
                        $myFolder = md5(md5($this->correo));
                        $path = $path.$myFolder;
                        if(!mkdir($path, 0755, true)) return("Creado");
                        else return("noCreado");
                }
                function buscarUsuarioWNU(){
                        $openServer = new OpenServ();
                        $openServer->cnS = "SELECT * FROM `usuario` WHERE correo LIKE '%".$this->nombres."%' OR nombres LIKE '%".$this->nombres."%' LIMIT 0, 10";
                        $this->rs = $openServer->ejecutarConsultaR();
                        return($this->rs);
                }       }?>
```

8.2.2. CÓDIGO FUENTE DEL SISTEMA

A. MÓDULO ACTIVOS

```
<?php
    require_once("../actions/usuario.php");
    require_once("../actions/contactos.php");
    require_once("../actions/all.php");

    session_start();
    $usu = new Usuario();
    //print_r($_SESSION);
    $nombresApellido = "Aqui estamos :)";
    if(!isset($_SESSION["S"])) header("location:../");
    $usu->correo = $_SESSION["S"]["USER"];
    $usu->contrasena = $_SESSION["S"]["PASS"];
    $d = $usu->obtenerDatos();
    if(isset($d["datos"]["correo"])){
            if($d["datos"]["correo"] != ""){
                    $nombresApellido = $d["datos"]["nombres"]." ".$d["datos"]["apellido"];
            }else{
                    header("location:../");
            }
    }else{
            session_destroy();
            header("location:../");
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Activos</title>
    <link rel="icon" href="../img/system/icon.png">
    <link rel="stylesheet" href="../style/sty.css">
```

```
    <link rel="stylesheet" href="../style/menu.css">
    <!--<link rel="stylesheet" href="../plug/css/jquery-ui.css">-->
    <link rel="stylesheet" href="../plug/css/bootstrap.min.css">
    <link rel="stylesheet" href="../plug/css/font-awesome.min.css">
    <link rel="stylesheet" href="../style/sty.css">
    <link rel="stylesheet" href="../style/snd.css">
    <link rel="stylesheet" href="../style/reset.css">
    <link rel="stylesheet" href="../style/menuAutocomplete.css">
    <script src="../plug/js/jquery-2.1.1.min.js"></script>
    <!--<script src="../plug/js/jquery-ui.js"></script>-->
    <script src="../plug/js/tether.min.js"></script>
    <script src="../plug/js/bootstrap.min.js"></script>
    <script src="../script/snd.js"></script>
    <script src="../script/sc.js"></script>
    <script src="../script/usuario.js"></script>
    <script src="../script/sms-snd.yvv.js"></script>
    <script src="../script/funciones.js"></script>
    <script src="../script/autocomplete.js"></script>
    <script src="../script/insti.js"></script>
    <script src="../script/all.js"></script>
</head>
<body class="table-l">
    <header class="menu-min" id="menuMin">
            <div class="menuP">
                    <!--<img src="" alt="File" id="cargarImagenPage">-
->
                    <div          class="menu-item-min          evMenu"
id="cargarImagenPage">
                            <i class="fa fa-university fa-2x"></i>
                    </div>
                    <p id="cargarNombrePage">Institucion</p>
            </div>
            <div class="usuario-menu">
                    <p><?=$nombresApellido;?></p>
                    <div>
                            <i class="fa fa-caret-down fa-2x"></i>
                            <ul>
                                    <li          id="cerrarSesion">Cerrar
sesion</li>
                            </ul>
                    </div>
            </div>
    </header>
    <section class="container-menu menu-flotante hidden"><!--show-
->
            <?php require("menu.php"); ?>
    </section>
    <?php
            $con = new ManagerDb();
            $usuA = new Contactos();

            $query = "SELECT * FROM `mensajer` WHERE
correo='".$_SESSION["S"]["USER"]."'";
            $rs      =      $con->obtenerDatos($query,      ["min"=>0,
"max"=>100]);
```

```
            if(isset($rs["datos"])){
                $attrTag = 'class="contenedor pading-con" window-
text="mensajes"';
                $filesA = 'class="files listar_p"';
                $disButton = "";
            }else{
                $attrTag = '';
                $filesA = 'class="files"';
                $disButton = "hiddenButtom";
            }
    ?>
    <section class="contenedor pading-con" window-text="mensajes"
id="contenedoUnico"><!-- class="contenedor pading-con"-->
            <div id="files" class="files listar_p">
                <?php
                    $actual = true;
                    require_once('windows/listarInsti.php');
                ?>
            </div>
    </section>
    <div class="masArchivos rotateAnim" data-toggle="modal" data-
target="#nuevoInsti">
            <i class="fa fa-plus fa-5x"></i>
    </div>
    <!-- ventana new -->
    <div class="modal fade" id="nuevoInsti">
            <div class="modal-dialog" role="document">
                <form                    class="modal-content"
action="javascript:addInsti('#newInsti')" id="newInsti">
                    <div class="modal-header">
                        <h5>Nueva activo</h5>
                        <button type="button" class="close"
data-dismiss="modal" aria-label="close">
                            <span                    aria-
hidden="true">&times;</span>
                        </button>
                    </div>
                    <div class="modal-body">
                        <div class="form-group">
                            <label for="nombre_act">
                                Nombre
                            </label>
                            <input              type="text"
name="nombre_act"       class="form-control"       id="nombre_act"
placeholder="Nombre del activo" required>
                        </div>
                        <div class="form-group">
                            <label for="cant_act">
                                Cantidad
                            </label>
                            <input          type="number"
name="cant_act"           class="form-control"          id="cant_act"
placeholder="min: 1" min="1" value="1" required>
                        </div>
```

```
                                    <div class="form-group">
                                        <label for="categ_act">
                                            Categoria
                                        </label>
                                        <select     name="categ_act"
id="categ_act" class="form-control" required="">
<option value="Servicios">Servicios</option>
<option value="Información">Información</option>
<option value="Hardware">Hardware</option>
<option value="Software">Software</option>
<option value="Soporte">Soporte</option>
<option value="Instalaciones">Instalaciones</option>
<option value="Personal">Personal</option>
<option value="Comunicaciones">Comunicaciones</option>
                                        </select>
                                    </div>
                                    <div class="form-group">
                                        <label for="propie_act">
                                            Propietario
                                        </label>
                                        <input                type="text"
name="propie_act"          class="form-control"          id="propie_act"
placeholder="Propietario" required>
                                    </div>
                                    <div class="form-group">
                                        <label for="confid_act">
                                            Confidencialidad
                                        </label>
                                        <select     name="confid_act"
id="confid_act" class="form-control" required="">
<option value="0">Muy baja</option>
<option value="2.5">Baja</option>
<option value="5">Regular</option>
<option value="7.5">Alta</option>
<option value="10">Muy alta</option>
                                        </select>
                                    </div>
                                    <div class="form-group">
                                        <label for="integri_act">
                                            Integridad
                                        </label>
                                        <select     name="integri_act"
id="integri_act" class="form-control" required="">
<option value="0">Muy baja</option>
<option value="2.5">Baja</option>
<option value="5">Regular</option>
<option value="7.5">Alta</option>
<option value="10">Muy alta</option>
                                        </select>
                                    </div>
                                    <div class="form-group">
                                        <label for="dispo_act">
                                            Disponibilidad
                                        </label>
```

```
                                        <select name="dispo_act"
id="dispo_act" class="form-control" required="">
<option value="0">Muy baja</option>
<option value="2.5">Baja</option>
<option value="5">Regular</option>
<option value="7.5">Alta</option>
<option value="10">Muy alta</option>
                                        </select>
                                    </div>
                                </div>
                                <div class="modal-footer">
                                    <button type="submit" class="btn
btn-primary">Aceptar</button>
                                </div>
                            </form>
                        </div>
                    </div>
                    <!-- ventana edit -->
                    <div class="modal fade" id="editInsti">
                        <div class="modal-dialog" role="document">
                            <form class="modal-content"
action="javascript:updaInsti('#editInstiD')" id="editInstiD">

                            </form>
                        </div>
                    </div>
                </body>
                <script>
                    indice = 7;
                    init.showTextCut(".sms-mu", 20);
                    init.showTextCut(".nomApeCorto", 20);
                    init.showTextCut(".titulo", 15);
                    init.showTextCut(".t1", 7);
                    $(function () {
                        $('[data-sms="sms"]').tooltip();
                    });
                    //autocompleteN("contacto", "");
                    var snd = new Snd();
                    //cargarSmsRec({min: 0, max: 15});
                </script>
                </html>
```

B. MÓDULO EVALUACIÓN

```
<?php
    require_once("../actions/openServer.php");
    require_once("../actions/usuario.php");
    require_once("../actions/archivo.php");
    require_once("../actions/all.php");

    session_start();
    $usu = new Usuario();
    $arch = new Archivo();
    $mgd = $md = new ManagerDb();
    $all = new All();
    //print_r($_SESSION);
```

```
    $nombresApellido = "Aqui estamos :)";
    if(!$_SESSION["S"]) header("location:../");
    $usu->correo = $_SESSION["S"]["USER"];
    $usu->contrasena = $_SESSION["S"]["PASS"];
    $d = $usu->obtenerDatos();
    if(isset($d["datos"]["correo"])){
        if($d["datos"]["correo"] != ""){
            $nombresApellido = $d["datos"]["nombres"]."
".$d["datos"]["apellido"];
        }else{
            header("location:../");
        }
    }else{
        session_destroy();
        header("location:../");
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Evaluacion de riesgo</title>
    <link rel="icon" href="../img/system/icon.png">
    <link rel="stylesheet" href="../plug/css/font-awesome.min.css">
    <link rel="stylesheet" href="../plug/css/bootstrap.min.css">
    <link rel="stylesheet" href="../style/sty.css">
    <link rel="stylesheet" href="../style/menu.css">
    <link rel="stylesheet" href="../style/animacion.css">
    <link rel="stylesheet" href="../style/mostrar.css">
    <link rel="stylesheet" href="../style/alert.css">
    <script src="../plug/js/jquery-2.1.1.min.js"></script>
    <script src="../plug/js/tether.min.js"></script>
    <script src="../plug/js/bootstrap.min.js"></script>
    <script src="../script/funciones.js"></script>
    <script src="../script/sc.js"></script>
    <script src="../script/snd.js"></script>
    <script src="../script/arch.js"></script>
    <script src="../script/upload.js"></script>
    <script src="../script/carpeta.js"></script>
    <script src="../script/alert.js"></script>
    <script src="../script/all.js"></script>
</head>
<body class="table-l">
    <header class="menu-min" id="menuMin">
        <div class="menuP">
            <!--<img src="" alt="File" id="cargarImagenPage">-
->
            <div class="menu-item-min evMenu"
id="cargarImagenPage">
                <i class="fa fa-tasks fa-2x"></i>
            </div>
            <p id="cargarNombrePage">Evaluacion de
riesgo</p>
        </div>
        <div class="usuario-menu">
```

```
                    <p><?=$nombresApellido;?></p>
                    <div>
                        <i class="fa fa-caret-down fa-2x"></i>
                        <ul>
                            <li id="cerrarSesion">Cerrar sesion</li>
                        </ul>
                    </div>
                </div>
            </header>
            <section class="container-menu menu-flotante hidden"><!--show-->
                <?php require("menu.php"); ?>
            </section>
            <section class="contenedor"><!-- window-text="archivos"-->
                <div class="files conOv" id="evaluaciones">
                    <?php
                        $actual = '';
                        include("windows/listarevalu.php");
                    ?>
                </div>
                <!--<div class="comentarios">
                    <div class="com">
                        <img src="../img/system/man.svg" alt="person">
                        <article class="textComent">Lorem ipsum dolor sit amet, consectetur adipisicing elit. Libero tempora soluta voluptas, impedit facere, perferendis pariatur accusamus quis debitis animi, voluptatibus veritatis labore excepturi aspernatur! Dolorum voluptatem, quasi illum tempore!</article>
                    </div>
                </div>-->
            </section>
            <div class="masArchivos rotateAnim" onClick="cargarItems('#evaluaciones')"><i class="fa fa-plus fa-5x"></i></div>

            <!-- ventana new -->
            <div class="modal fade" id="nuevaEvaluacion">
                <div class="modal-dialog" role="document">
                    <form class="modal-content" action="javascript:subirAr()" id="formularioAdd" method="post" enctype="multipart/form-data"><!--subirAr()-->
                        <div class="modal-header">
                            <h5>Ingrese los datos corectamente</h5>
                            <button type="button" class="close" data-dismiss="modal" aria-label="close">
                                <span aria-hidden="true">&times;</span>
                            </button>
                        </div>
                        <div class="modal-body">
                            <input type="hidden" id="idItemAddAdjunt" name="idItemAddAdjunt" value="" required>
```

```
                                    <div class="form-group">
                                        <label for="oportunidad">
                                            Oportunidad de
mejora
                                        </label>
                                        <textarea
name="oportunidad" id="oportunidad" rows="3" placeholder="Ingrese
alguna oportunidad de mejora" class="form-control"
required></textarea>
                                    </div>
                                    <div class="form-group">
                                        <label for="puntos">
                                            Puntos fuertes
                                        </label>
                                        <textarea name="puntos"
id="puntos" rows="3" placeholder="Ingrese algun punto fuerte"
class="form-control" required></textarea>
                                    </div>
                                    <div class="form-group">
                                        <label for="observaciones">
                                            Observaciones
                                        </label>
                                        <textarea
name="observaciones" id="Observaciones" rows="3"
placeholder="Ingrese la Observaciones" class="form-
control"></textarea>
                                    </div>
                                    <div class="form-group">
                                        <label>
                                            Archivo
                                        </label>
                                        <div class="form-control"
onClick="$('#codp').click()">
                                            <div class="btn btn-
info"><i class="fa fa-plus"></i></div>
                                            <span
id="nombreArchivo" style="margin-left: 10px;" class="">Agragar
archivo</span>
                                        </div>
                                        <input type="file"
name="codp" class="form-control-file" id="codp" style="display:
none;">
                                        <small id="fileHelp"
class="form-text text-muted">
                                            El tamaño del archivo
no debe superar los 2mb
                                        </small>
                                    </div>
                                </div>
                                <div class="modal-footer">
                                    <button type="submit" class="btn
btn-primary">Aceptar</button>
                                    <button type="button" class="btn
btn-secondary" data-dismiss="modal">cerrar</button>
                                </div>
```

```
                    </form>
                </div>
            </div>
            <!-- ventana new -->
            <div class="modal fade" id="infoAdjunt">
                <div class="modal-dialog" role="document">
                    <div class="modal-content">
                        <div class="modal-header">
                            <h5>Informacion</h5>
                            <button type="button" class="close"
data-dismiss="modal" aria-label="close">
                                <span aria-
hidden="true">&times;</span>
                            </button>
                        </div>
                        <div class="modal-body"
id="datosInformacion">
                            Espere un momento ...
                        </div>
                        <div class="modal-footer">
                            <button type="button" class="btn
btn-secondary" data-dismiss="modal">cerrar</button>
                        </div>
                    </div>
                </div>
            </div>
            <!--alert modal-->
            <div class="modal fade" id="alertModal">
                <div class="modal-dialog" role="document">
                    <div class="modal-content">
                        <div class="modal-header">
                            <h5>Advertencia</h5>
                            <button type="button" class="close"
data-dismiss="modal" aria-label="close">
                                <span aria-
hidden="true">&times;</span>
                            </button>
                        </div>
                        <div class="modal-body text-success"
id="altext">
                            Las contraseñas no coinciden
                        </div>
                    </div>
                </div>
            </div>
        </body>
        <script>
            indice = 0;
            init.showTextCut(".textComent", 100, true);
            init.showTextCut(".titulo", 100, false);
            init.showButtons(".contenedor");
            init.exitAll();
            //////
            /*document.onauxclick = function(){return false;};
            snd.posicionClick("files");*/
```

```
    //
    //cargarArchivo("#codp", $("#nombreFile"));

    $('#opcionesModal').on('click', function (e) {
            $("body").css("padding", 0);
    });
    $('#alertModal').on('click', function (e) {
            $("body").css("padding", 0);
    });
    $('#enviarModal').on('click', function (e) {
            $("body").css("padding", 0);
    });
    $('#compartirModal').on('click', function (e) {
            $("body").css("padding", 0);
    });

    //////////////
    var filesCount = 0;
    uploadFile = false;
    $("#codp").change(function(e) {
            tamaAr = e.target.files[0].size;
            $("#nombreArchivo").html(e.target.files[0].name);
            var d = new Date();
            d = d.toLocaleTimeString() + "" + d.toDateString();
            var archivosS = e.target.files;
            var dataS = {
                    tmp_name:                       d.toString().split("
").join("").split(":").join("").split("-").join(""),
                    data: new FormData($("#formularioAdd")[0])
            };
            if (archivosS.length > 0) {
                    dataS.data.append("archivo", archivosS[0]); //
            }
//          console.log(dataS);
            datoEnv = "";
            archivo = dataS.data;
            uploadFile = true;
    });
</script>
</html>
```

C. MÓDULO VERIFICACIÓN

```
<?php
    require_once("../actions/openServer.php");
    require_once("../actions/usuario.php");
    require_once("../actions/archivo.php");
    require_once("../actions/all.php");

    session_start();
    $usu = new Usuario();
    $arch = new Archivo();
    $mgd = $md = new ManagerDb();
    $all = new All();
```

```
    //print_r($_SESSION);
    $nombresApellido = "Aqui estamos :)";
    if(!$_SESSION["S"]) header("location:../");
    $usu->correo = $_SESSION["S"]["USER"];
    $usu->contrasena = $_SESSION["S"]["PASS"];
    $d = $usu->obtenerDatos();
    if(isset($d["datos"]["correo"])){
            if($d["datos"]["correo"] != ""){
                    $nombresApellido = $d["datos"]["nombres"]."
".$d["datos"]["apellido"];
            }else{
                    header("location:../");
            }
    }else{
            session_destroy();
            header("location:../");
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Evaluacion de riesgo | verificacion</title>
    <link rel="icon" href="../img/system/icon.png">
    <link rel="stylesheet" href="../plug/css/font-awesome.min.css">
    <link rel="stylesheet" href="../plug/css/bootstrap.min.css">
    <link rel="stylesheet" href="../style/sty.css">
    <link rel="stylesheet" href="../style/menu.css">
    <link rel="stylesheet" href="../style/animacion.css">
    <link rel="stylesheet" href="../style/mostrar.css">
    <link rel="stylesheet" href="../style/alert.css">
    <script src="../plug/js/jquery-2.1.1.min.js"></script>
    <script src="../plug/js/tether.min.js"></script>
    <script src="../plug/js/bootstrap.min.js"></script>
    <script src="../script/funciones.js"></script>
    <script src="../script/sc.js"></script>
    <script src="../script/snd.js"></script>
    <script src="../script/arch.js"></script>
    <script src="../script/upload.js"></script>
    <script src="../script/carpeta.js"></script>
    <script src="../script/alert.js"></script>
    <script src="../script/all.js"></script>
</head>
<body class="table-l">
    <header class="menu-min" id="menuMin">
            <div class="menuP">
                    <!--<img src="" alt="File" id="cargarImagenPage">-
->
                    <div class="menu-item-min evMenu"
id="cargarImagenPage">
                            <i class="fa fa-tasks fa-2x"></i>
                    </div>
                    <p id="cargarNombrePage">Evaluacion de
riesgo</p>
            </div>
```

```
            <div class="usuario-menu">
                <p><?=$nombresApellido;?></p>
                <div>
                    <i class="fa fa-caret-down fa-2x"></i>
                    <ul>
                        <li id="cerrarSesion">Cerrar
sesion</li>
                    </ul>
                </div>
            </div>
    </header>
    <section class="container-menu menu-flotante hidden"><!--show-
->
            <?php require("menu.php"); ?>
    </section>
    <section class="contenedor"><!-- window-text="archivos"-->
            <div class="files conOv" id="evaluaciones">
                <?php
                    $actual = '';
                    include("windows/listarevaluVer.php");
                ?>
            </div>
    </section>
    <div class="modal fade" id="alertModal">
            <div class="modal-dialog" role="document">
                <div class="modal-content">
                    <div class="modal-header">
                        <h5>Advertencia</h5>
                        <button type="button" class="close"
data-dismiss="modal" aria-label="close">
                            <span aria-
hidden="true">&times;</span>
                        </button>
                    </div>
                    <div class="modal-body text-success"
id="altext">
                        Las contraseñas no coinciden
                    </div>
                </div>
            </div>
    </div>
</body>
<script>
    indice = 3;
    init.showTextCut(".textComent", 100, true);
    init.showTextCut(".titulo", 100, false);
    init.showButtons(".contenedor");
    init.exitAll();
    /*document.onauxclick = function(){return false;};
    snd.posicionClick("files");*/
    //
    //cargarArchivo("#codp", $("#nombreFile"));
    $('#opcionesModal').on('click', function (e) {
            $("body").css("padding", 0);
    });
```

```
    $('#alertModal').on('click', function (e) {
        $("body").css("padding", 0);
    });
    $('#enviarModal').on('click', function (e) {
        $("body").css("padding", 0);
    });
    $('#compartirModal').on('click', function (e) {
        $("body").css("padding", 0);
    });

    var filesCount = 0;
    uploadFile = false;
    $("#codp").change(function(e) {
        tamaAr = e.target.files[0].size;
        $("#nombreArchivo").html(e.target.files[0].name);
        var d = new Date();
        d = d.toLocaleTimeString() + "" + d.toDateString();
        var archivosS = e.target.files;
        var dataS = {
            tmp_name:                    d.toString().split("
").join("").split(":").join("").split("-").join(""),
            data: new FormData($("#formularioAdd")[0])
        };
        if (archivosS.length > 0) {
            dataS.data.append("archivo", archivosS[0]); //
        }
//      console.log(dataS);
        datoEnv = "";
        archivo = dataS.data;
        uploadFile = true;
    });
```

D. MÓDULO REPORTE

```
<?php
    require_once("../actions/openServer.php");
    require_once("../actions/usuario.php");
    require_once("../actions/archivo.php");
    require_once("../actions/all.php");

    session_start();
    $usu = new Usuario();
    $arch = new Archivo();
    $mgd = $md = new ManagerDb();
    $all = new All();
    //print_r($_SESSION);
    $nombresApellido = "Aqui estamos :)";
    if(!$_SESSION["S"]) header("location:../");
    $usu->correo = $_SESSION["S"]["USER"];
    $usu->contrasena = $_SESSION["S"]["PASS"];
    $d = $usu->obtenerDatos();
    if(isset($d["datos"]["correo"])){
        if($d["datos"]["correo"] != ""){
            $nombresApellido    =    $d["datos"]["nombres"]."
".$d["datos"]["apellido"];
        }else{
            header("location:../");
```

```
            }
    }else{
            session_destroy();
            header("location:../");
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Reporte</title>
    <link rel="icon" href="../img/system/icon.png">
    <link rel="stylesheet" href="../style/sty.css">
    <link rel="stylesheet" href="../style/menu.css">
    <link rel="stylesheet" href="../plug/css/bootstrap.min.css">
    <link rel="stylesheet" href="../plug/css/font-awesome.min.css">
    <link rel="stylesheet" href="../style/snd.css">
    <link rel="stylesheet" href="../style/reset.css">
    <script src="../plug/js/jquery-2.1.1.min.js"></script>
    <script src="../plug/js/tether.min.js"></script>
    <script src="../plug/js/bootstrap.min.js"></script>
    <script src="../script/snd.js"></script>
    <script src="../script/sc.js"></script>
    <script src="../script/Chart.min.js"></script>
    <script src="../script/utils.js"></script>
    <script src="../script/all.js"></script>
</head>
<body class="table-l">
    <header class="menu-min" id="menuMin">
            <div class="menuP">
                    <!--<img src="" alt="File" id="cargarImagenPage">-
->
                    <div          class="menu-item-min          evMenu"
id="cargarImagenPage">
                            <i class="fa fa-bar-chart fa-2x"></i>
                    </div>
                    <p id="cargarNombrePage">Reporte</p>
            </div>
            <menu class="nav menuPermisos">
                    <li class="nav-item dropdown">
                            <a class="nav-link dropdown-toggle" data-
toggle="dropdown" href="#" role="button" aria-haspopup="true" aria-
expanded="false" link_s="">Evaluacion</a>
                            <div class="dropdown-menu">
                                    <a              class="dropdown-item
btnMenuPer" href="javascript:repo01()" link_s="">Segun nivel</a>
                                    <!--<a          class="dropdown-item
btnMenuPer"        href="javascript:repo02()"        link_s="">Segun
impacto</a>-->
                                    <div                 class="dropdown-
divider"></div>
                                    <form              class="form-group"
style="width: 250px;padding: 0 20px;">
                                            <?php
```

```
    require_once("../actions/all.php");
    $md = new ManagerDb();

    if(!isset($_SESSION["S"]["USER"])) session_start();

    $q = "SELECT fecha FROM `items` WHERE
correo="'.$_SESSION["S"]["USER"]."'";
    $datos = $md->obtenerDatos($q, "");
    $dRecol = isset($datos["datos"]) ? $datos["datos"] : array();
    $fechas = array();
    foreach($dRecol as $k => $v){
    $fechaS = $v["fecha"];

    $fechaS = explode("-", $fechaS);

    if(!in_array($fechaS[0], $fechas)){

    array_push($fechas, $fechaS[0]);
                                                        }
                                                    }
                                            ?>
                                            <labe
for="anioSe">Seleccione el año inicio</labe>
                                            <select name="anioSe"
id="anioSe" class="form-control">
                                                <?php

    foreach($fechas as $k => $v){
                                                ?>
                                                <option
value="<?=$v;?>"><?=$v;?></option>
                                                <?php } ?>
                                            </select>
                                        </form>
                                    </div>
                                </li>
                                <li class="nav-item dropdown">
                                    <a class="nav-link dropdown-toggle" data-
toggle="dropdown" href="#" role="button" aria-haspopup="true" aria-
expanded="false" link_s="">Verificacion</a>
                                    <div class="dropdown-menu">
                                        <a class="dropdown-item
btnMenuPer" href="javascript:repo03()" link_s="">Segun estado</a>
                                        <div class="dropdown-
divider"></div>
                                        <form class="form-group"
style="width: 250px;padding: 0 20px;">
                                            <?php

    require_once("../actions/all.php");
                                                $md = new
ManagerDb();

    if(!isset($_SESSION["S"]["USER"])) session_start();
```

```
                                                $q = "SELECT
fecha FROM `items` WHERE correo='".$_SESSION["S"]["USER"]."'";
                                                $datos = $md-
>obtenerDatos($q, "");
                                                $dRecol =
isset($datos["datos"]) ? $datos["datos"] : array();
                                                $fechas =
array();

    foreach($dRecol as $k => $v){

    $fechaS = $v["fecha"];
    $fechaS = explode("-", $fechaS);
    if(!in_array($fechaS[0], $fechas)){
    array_push($fechas, $fechaS[0]);
                                                        }
                                                }
                                        ?>
    <labe for="anioSev">Seleccione año inicio</labe>
    <select name="anioSev" id="anioSev" class="form-control">
                                                <?php

    foreach($fechas as $k => $v){
                                                ?>
                                                <option
value="<?=$v;?>"><?=$v;?></option>
                                                <?php } ?>
                                        </select>
                                        <labe
for="anioSv">Seleccione año fin</labe>
                                        <select name="anioSv"
id="anioSv" class="form-control">
                                                <?php

    foreach($fechas as $k => $v){
                                                ?>
                                                <option
value="<?=$v;?>"><?=$v;?></option>
                                                <?php } ?>
                                        </select>
                                </form>
                        </div>
                </li>
                <li class="nav-item dropdown">
                        <a class="nav-link dropdown-toggle" data-
toggle="dropdown" href="#" role="button" aria-haspopup="true" aria-
expanded="false" link_s="">Activos</a>
                        <div class="dropdown-menu">
                                <a class="dropdown-item
btnMenuPer" href="javascript:cargarActivos('#evaluaciones')"
link_s="">Reporte</a>
                                <!--<a class="dropdown-item
btnMenuPer" href="#" link_s="">Comparacion</a>-->
```

```
                                    <div class="dropdown-
divider"></div>
                                    <form class="form-group"
style="width: 200px;padding: 0 20px;">
                                        <?php

    require_once("../actions/all.php");
                                            $md = new
ManagerDb();

    if(!isset($_SESSION["S"]["USER"])) session_start();

                                            $q = "SELECT
fecha FROM `activo` WHERE correo='".$_SESSION["S"]["USER"]."'";
                                            $datos = $md-
>obtenerDatos($q, "");
                                            $dRecol =
isset($datos["datos"]) ? $datos["datos"] : array();
                                            $fechas =
array();

    foreach($dRecol as $k => $v){
    $fechaS = $v["fecha"];
    $fechaS = explode("-", $fechaS);
    if(!in_array($fechaS[0], $fechas)){
    array_push($fechas, $fechaS[0]);
                                                }
                                            }
                                        ?>
                                        <div class="form-group">
                                            <label
for="categ_repor">
                                                Categoria
                                            </label>
                                            <select
name="categ_repor" id="categ_repor" class="form-control"
required="">
<option value="-">Sin categoria</option>
<option value="Servicios">Servicios</option>
<option value="Información">Información</option>
<option value="Hardware">Hardware</option>
<option value="Software">Software</option>
<option value="Soporte">Soporte</option>
<option value="Instalaciones">Instalaciones</option>
<option value="Personal">Personal</option>
<option value="Comunicaciones">Comunicaciones</option>
                                            </select>
                                        </div>
                                        <div class="form-group">
                                            <div class="form-
group">
                                                <label
for="reporte_anio_activo">
                                                    Año
                                                </label>
```

```
                                                    <select
name="reporte_anio_activo"  id="reporte_anio_activo"  class="form-
control" required="">
                                                        <?php
foreach($fechas as $k => $v){ ?>

    <option value="<?=$v;?>"><?=$v;?></option>
                                                        <?php
} ?>
                                                    </select>
                                                    <label
for="reporte_mes_activo">
                                                        Mes
                                                    </label>
                                                    <select
name="reporte_mes_activo"  id="reporte_mes_activo"  class="form-
control" required="">

    <option value="01">Enero</option>
    <option value="02">Febrero</option>
    <option value="03">Marzo</option>
    <option value="04">Abril</option>
    <option value="05">Mayo</option>
    <option value="06">Junio</option>
    <option value="07">Julio</option>
    <option value="08">Agosto</option>
    <option value="09">Setiembre</option>
    <option value="10">Octubre</option>
    <option value="11">Noviembre</option>
    <option value="12">Diciembre</option>
                                                    </select>
                                                </div>
                                            </div>
                                        </form>
                                    </div>
                                </li>
                            </menu>
                            <div class="usuario-menu">
                                <p><?=$nombresApellido;?></p>
                                <div>
                                    <i class="fa fa-caret-down fa-2x"></i>
                                    <ul>
                                        <li          id="cerrarSesion">Cerrar
sesion</li>
                                    </ul>
                                </div>
                            </div>
    </header>
    <section class="container-menu menu-flotante hidden"><!--show-
->
                            <?php require("menu.php"); ?>
    </section>
    <section class="contenedor"><!-- window-text="archivos"-->
                            <div  class="files  conOv"  id="evaluaciones"  style="width:
900px; margin: auto; padding: 0 50px;padding-bottom: 50px;">
```

```
                    <canvas id="reporte01" width="400" height="400"></canvas>
                </div>
    </section>
    <footer></footer>
</body>
<script>
    indice = 2;
    init.showTextCut(".textComent", 100, true);
    init.showTextCut(".titulo", 25, true);

    var ctx = document.getElementById("reporte01");

    function repo001(){
        var url = "../actions/datos.php";
        var data_ = {
            op: "riesgo",
            anioi: $("#anioSe").val(),
            aniof: $("#anioS").val()
        };
        var Json = $.getJSON(url, data_, function(r){
            if(r.data){
                data =  {
                    "labels": r.label,
                    "datasets": [{
                        "label": r.title,
                        "data": r.data,
                        "fill": false,
                        "backgroundColor": [ "rgba(255, 99, 132, 0.2)", "rgba(255, 159, 64, 0.2)", "rgba(255, 205, 86, 0.2)", "rgba(75, 192, 192, 0.2)", "rgba(54, 162, 235, 0.2)", "rgba(153, 102, 255, 0.2)", "rgba(201, 203, 207, 0.2)" ],
                        "borderColor": [ "rgb(255, 99, 132)", "rgb(255, 159, 64)", "rgb(255, 205, 86)", "rgb(75, 192, 192)", "rgb(54, 162, 235)", "rgb(153, 102, 255)", "rgb(201, 203, 207)" ],
                        "borderWidth": 1
                    }]
                };
                options = {"scales": {"yAxes": [{ "ticks": {"beginAtZero": true }}]}};
                var grafica = new Chart(ctx, {
                    type: 'bar',
                    data: data,
                    options: options
                });
            }else{
                $("#evaluaciones").html("");
                $("#evaluaciones").append($("<p class='text-center' style='margin: auto;'>").html("No tienes datos aun!! ..."));
            }
        });
        Json.fail(function() {
```

```
    //$("#contenedorGrafica").append($("<div>").html("Sin datos, intente mas tarde"));
                console.log("Ocurrio un error al obtener los datos");
            });
    }
    function repo01(){
            var url = "../actions/datos.php";
            var data_ = {
                op: "riesgoFC",
                anioi: $("#anioSe").val(),
                aniof: $("#anioS").val()
            };
            var Json = $.getJSON(url, data_, function(r){
                eliminarTag();
                redimencion(1);
                if(r.month.length>0){
                    var color = Chart.helpers.color;

                    var datos = r.datos;
                    var dataSet = [];
                    var colors = [

    color(window.chartColors.grey).alpha(0.5).rgbString(),
    color(window.chartColors.red).alpha(0.5).rgbString(),
    color(window.chartColors.orange).alpha(0.5).rgbString(),
    color(window.chartColors.yellow).alpha(0.5).rgbString(),
    color(window.chartColors.green).alpha(0.5).rgbString(),
    color(window.chartColors.blue).alpha(0.5).rgbString()
                    ];
                    var colorB = [
                        window.chartColors.grey,
                        window.chartColors.red,
                        window.chartColors.orange,
                        window.chartColors.yellow,
                        window.chartColors.green,
                        window.chartColors.blue
                    ];
                    var options = {
                        scales: { "yAxes": [{ "ticks": { "beginAtZero": true } }]},
                        responsive: true,
                        legend: {
                            position: 'bottom',
                            fullWidth: false
                        },
                        title: {
                            display: true,
                            text: 'Segun impacto'
                        };

                    for(var i=0;i<r.titles.length;i++){
                        var d = [];
                        for(var j=0;j<r.month.length;j++){
                            d.push(datos[j].data[i]);
```

```
                                        }
                                        var dA = {
                                                label: r.titles[i],
                                                backgroundColor: colors[i],
                                                borderColor: colorB[i],
                                                borderWidth: 1,
                                                data: d
                                        };
                                        dataSet.push(dA);
                                }
                                var barChartData = {
                                        labels: r.month,
                                        datasets: dataSet
                                };
                                var grafica = new Chart(ctx, {
                                        type: 'bar',
                                        data: barChartData,
                                        options: options
                                });
                        }else{
                                $("#evaluaciones").html("");
                                $("#evaluaciones").append($("<p
class='text-center' style='margin: auto;'>").html("No tienes datos aun!!
..."));
                        }
                });
                Json.fail(function() {

    //$("#contenedorGrafica").append($("<div>").html("Sin        datos,
intente mas tarde"));
                        console.log("Ocurrio un error al obtener los datos");
                });
    }
    function repo02(){
                var url = "../actions/datos.php";
                var data_ = {
                        op: "impacto",
                        anioi: $("#anioSe").val(),
                        aniof: $("#anioS").val()
                };
                var Json = $.getJSON(url, data_, function(r){
                        eliminarTag();
                        redimencion(1);
                        if(r.month.length>0){
                                var color = Chart.helpers.color;

                                var datos = r.datos;
                                var dataSet = [];
                                var colors = [

    color(window.chartColors.red).alpha(0.5).rgbString(),
    color(window.chartColors.green).alpha(0.5).rgbString(),
    color(window.chartColors.orange).alpha(0.5).rgbString()
                                ];
                                var colorB = [
```

```
                                        window.chartColors.red,
                                        window.chartColors.green,
                                        window.chartColors.orange
                                ];
                                var options = {
                                        scales: { "yAxes": [{ "ticks": { "beginAtZero": true } }]},
                                        responsive: true,
                                        legend: {
                                                position: 'top',
                                        },
                                        title: {
                                                display: true,
                                                text: 'Segun impacto'
                                        }
                                };
                                        for(var i=0;i<r.titles.length;i++){
                                        var d = [];
                                        for(var j=0;j<r.month.length;j++){
                                                d.push(datos[j].data[i]);
                                        }
                                        var dA = {
                                                label: r.titles[i],
                                                backgroundColor: colors[i],
                                                borderColor: colorB[i],
                                                borderWidth: 1,
                                                data: d
                                        };
                                        dataSet.push(dA);
                                }
                                var barChartData = {
                                        labels: r.month,
                                        datasets: dataSet
                                };
                                var grafica = new Chart(ctx, {
                                        type: 'bar',
                                        data: barChartData,
                                        options: options
                                });
                        }else{
                                $("#evaluaciones").html("");
                                $("#evaluaciones").append($("<p class='text-center' style='margin: auto;'>").html("No tienes datos aun!! ..."));
                        }
                });
                Json.fail(function() {

    //$("#contenedorGrafica").append($("<div>").html("Sin datos, intente mas tarde"));
                        console.log("Ocurrio un error al obtener los datos");
                });
    }
    function repo03(){
                var url = "../actions/datos.php";
```

```
		var data_ = {
			op: "verificacion",
			anioi: $("#anioSev").val(),
			aniof: $("#anioSv").val()
		};
		var Json = $.getJSON(url, data_, function(r){
			eliminarTag();
			redimencion(1);
			if(r.month.length>0){
				var color = Chart.helpers.color;

				var datos = r.datos;
				var dataSet = [];
				var colors = [

    color(window.chartColors.red).alpha(0.5).rgbString(),

    color(window.chartColors.green).alpha(0.5).rgbString(),

    color(window.chartColors.orange).alpha(0.5).rgbString()
				];
				var colorB = [
					window.chartColors.red,
					window.chartColors.green,
					window.chartColors.orange
				];
				var options = {
					scales: { "yAxes": [{ "ticks": {
"beginAtZero": true } }]},
					responsive: true,
					legend: {
						position: 'top',
					},
					title: {
						display: true,
						text: 'Segun impacto'
					}
				};

				for(var i=0;i<r.titles.length;i++){
					var d = [];
					for(var j=0;j<r.month.length;j++){
						d.push(datos[j].data[i]);
					}
					var dA = {
						label: r.titles[i],
						backgroundColor: colors[i],
						borderColor: colorB[i],
						borderWidth: 1,
						data: d
					};
					dataSet.push(dA);
				}
				var barChartData = {
					labels: r.month,
```

```
                                        datasets: dataSet
                                    };
                                    var grafica = new Chart(ctx, {
                                        type: 'bar',
                                        data: barChartData,
                                        options: options
                                    });
                                }else{
                                    $("#evaluaciones").html("");
                                    $("#evaluaciones").append($("<p
class='text-center' style='margin: auto;'>").html("No tienes datos aun!!
..."));
                                }
                            });
                            Json.fail(function() {

    //$("#contenedorGrafica").append($("<div>").html("Sin datos,
intente mas tarde"));
                                console.log("Ocurrio un error al obtener los datos");
                            });
                        }
                        function eliminarTag(){
                            $("#evaluaciones").html("");
                            $("#evaluaciones").append('<canvas id="reporte01"
width="400" height="400">');
                            ctx = document.getElementById("reporte01");
                        }
                        repo01();
                        $('.btnMenuPer').on('click', function (e) {
                            $('.btnMenuPer').removeClass('active');
                            $(this).addClass('active');
                        });
                    </script>
                    </html>
```

E. MODULO COPIA DE SEGURIDAD

```
<?php
    require_once("../actions/usuario.php");
    require_once("../actions/contactos.php");
    require_once("../actions/all.php");

    session_start();
    $usu = new Usuario();
    //print_r($_SESSION);
    $nombresApellido = "Aqui estamos :)";
    if(!isset($_SESSION["S"])) header("location:../");
    $usu->correo = $_SESSION["S"]["USER"];
    $usu->contrasena = $_SESSION["S"]["PASS"];
    $d = $usu->obtenerDatos();
    if(isset($d["datos"]["correo"])){
        if($d["datos"]["correo"] != ""){
            $nombresApellido = $d["datos"]["nombres"]."
".$d["datos"]["apellido"];
        }else{
            header("location:../");
```

```
            }
    }else{
            session_destroy();
            header("location:../");
    }
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Copias de seguridad</title>
    <link rel="icon" href="../img/system/icon.png">
    <link rel="stylesheet" href="../style/sty.css">
    <link rel="stylesheet" href="../style/menu.css">
    <!--<link rel="stylesheet" href="../plug/css/jquery-ui.css">-->
    <link rel="stylesheet" href="../plug/css/bootstrap.min.css">
    <link rel="stylesheet" href="../plug/css/font-awesome.min.css">
    <link rel="stylesheet" href="../style/snd.css">
    <link rel="stylesheet" href="../style/reset.css">
    <link rel="stylesheet" href="../style/menuAutocomplete.css">
    <script src="../plug/js/jquery-2.1.1.min.js"></script>
    <!--<script src="../plug/js/jquery-ui.js"></script>-->
    <script src="../plug/js/tether.min.js"></script>
    <script src="../plug/js/bootstrap.min.js"></script>
    <script src="../script/snd.js"></script>
    <script src="../script/sc.js"></script>
    <script src="../script/usuario.js"></script>
    <script src="../script/sms-snd.yvv.js"></script>
    <script src="../script/funciones.js"></script>
    <script src="../script/autocomplete.js"></script>
    <script src="../script/all.js"></script>
</head>
<body class="table-l">
    <header class="menu-min" id="menuMin">
            <div class="menuP">
                    <!--<img src="" alt="File" id="cargarImagenPage">-
->
                    <div          class="menu-item-min          evMenu"
id="cargarImagenPage">
                            <i class="fa fa-copy fa-2x"></i>
                    </div>
                    <p          id="cargarNombrePage">Copias          de
seguridad</p>
            </div>
            <div class="usuario-menu">
                    <p><?=$nombresApellido;?></p>
                    <div>
                            <i class="fa fa-caret-down fa-2x"></i>
                            <ul>
                                    <li          id="cerrarSesion">Cerrar
sesion</li>
                            </ul>
                    </div>
            </div>
    </header>
```

```
    <section class="container-menu menu-flotante hidden"><!--show-
->
        <?php require("menu.php"); ?>
    </section>
    <section class="contenedor pading-con" window-
text="mensajes"><!-- class="contenedor pading-con"-->
        <div id="itemsFolder" class="listar_p">
            <?php
                $actual = "";
                include("windows/listarCop.php");
            ?>
        </div>
    </section>
    <!--delete modal-->
    <div class="modal fade" id="delModal">
        <div class="modal-dialog modal-lg" role="document">
            <div class="modal-content">
                <div class="modal-header">
                    <h5>Realizar copia</h5>
                    <button type="button" class="close"
data-dismiss="modal" aria-label="close">
                        <span aria-
hidden="true">&times;</span>
                    </button>
                </div>
                <div class="modal-body">
                    <div class="alert alert-success">
                        <p>Se realizara una copia de
seguridad de toda la base de datos relacionado con este sistema</p>
                        <hr>
                        <div
id="resultadoCopy"></div>
                    </div>
                </div>
                <div class="modal-footer">
                    <button type="button" class="btn
btn-success" onClick="realizarCopia('#resultadoCopy')">Hacer copia
ahora</button>
                </div>
            </div>
        </div>
    </div>

    <div class="masArchivos rotateAnim" data-toggle="modal" data-
target="#delModal"><i class="fa fa-plus fa-5x"></i></div>
</body>
<script>
    indice = 4;
    init.showTextCut(".sms-mu", 20);
    init.showTextCut(".nomApeCorto", 20);
    $(function () {
        $('[data-sms="sms"]').tooltip();
    });
    autocompleteN("contacto", "");
    var snd = new Snd();
```

```
cargarSmsRec({min: 0, max: 15});
function descargar(e){
        e.preventDefault;
        link = e.getAttribute("data-link");
        if(confirm("esta seguro de descargar el archivo?")){
                window.open(link, "_blank");
        }       }
```

F. CODIGO PARA EL MENÚ

```
<nav class="menu-buble">
    <a href="#" class="homeButton btn-buble menu-barra"><i
class="fa fa-bars fa-5x"></i></a>

    <a href="evaluacion.php" class="btn-buble blue showmesaje">
            <i class="fa fa-tasks fa-5x"></i>
            <span class="message-label show-title">Evaluacion de
riesgo</span>
    </a>
    <!--<a href="upload.php" class="btn-buble green showmesaje">
            <i class="fa fa-cloud-upload fa-5x"></i>
            <span class="message-label show-title">Subir
archivo(s)</span>
    </a>-->
    <a href="verificacion.php" class="btn-buble purple showmesaje">
            <i class="fa fa-check-square-o fa-5x"></i>
            <span class="message-label show-
title">Verificacion</span>
    </a>
    <a href="reporte.php" class="btn-buble red showmesaje">
            <i class="fa fa-bar-chart fa-5x"></i>
            <span class="message-label show-title">Reportes</span>
    </a>
    <a href="configuracion.php" class="btn-buble green
showmesaje">
            <i class="fa fa-cog fa-5x"></i>
            <span class="message-label show-title">Usuario</span>
    </a>
    <a href="copia.php" class="btn-buble orange showmesaje">
            <i class="fa fa-copy fa-5x"></i>
            <span class="message-label show-title">Copias de
seguridad</span>
    </a>
    <a href="activos.php" class="btn-buble lightblue showmesaje">
            <i class="fa fa-laptop fa-5x"></i>
            <span class="message-label show-title">Activos</span>
    </a>
</nav>}
```