

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

**“DESARROLLO E IMPLEMENTACIÓN DE CONTROLES DE
SEGURIDAD INFORMÁTICA PARA EL SISTEMA ERP
ACADEMIUM DE LA UNIDAD EDUCATIVA JAVIER, SIGUIENDO
LA NORMA ISO 27001”**

TRABAJO DE TITULACIÓN

Previa la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Iván Isaac Solís Granda

GUAYAQUIL – ECUADOR

AÑO

2016

AGRADECIMIENTO

Agradezco a mi familia por el apoyo incondicional que me han dado durante años para que pueda seguir con mis estudios profesionales.

Por los diferentes consejos que me han ayudado y que han hecho que sigan en el camino correcto de manera profesional y personal.

A mi linda novia que me ha brindado su apoyo y su comprensión en la realización de la maestría y la tesis.

Agradezco a mi tutor por haberme apoyado en las revisiones y hacer que mi trabajo de tesis se haya culminado con éxito.

Y un agradecimiento a Dios por estar a mi lado cuidándome todos los años de mi vida.

DEDICATORIA

A Dios por haberme cuidado tantos años, a mis padres y hermanos por estar ahí conmigo con su apoyo.

A todos los seres queridos que han estado conmigo.

TRIBUNAL DE SUSTENTACIÓN

DIRECTOR MSIG/MSIA

ING. LENÍN FREIRE

DIRECTOR DEL PROYECTO DE GRADUACIÓN

MGS. NESTOR ARREAGA

MIEMBRO DEL TRIBUNAL

MGS. ALBERT ESPINAL

DECLARACIÓN EXPRESA

“Declaro de forma expresa que todo el contenido de esta Tesis de Grado es de mi completa autoría y responsabilidad, por lo que doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”

Iván Isaac Solís Granda

RESUMEN

Desarrollar e Implementar controles de seguridad informática para el sistema ERP Academium de la Unidad Educativa Javier, siguiendo la norma ISO 27001. Para llevar a cabo la aplicación de los controles lo primero que debemos realizar es una evaluación de riesgos que podría sufrir la aplicación web tomando en cuenta todas las vulnerabilidades existentes y el impacto que causarían para la institución.

Después haremos un inventario de los activos de la información y escogeremos la metodología Magerit para realizar el análisis y gestión de riesgos de los sistemas informáticos. La importancia de utilizar esta metodología es para identificar los riesgos existentes en la organización y aplicar estrategias para la protección de ellos.

Según las vulnerabilidades encontradas escogeremos los mejores controles de la norma ISO 27001:2013 y crearemos nuevas políticas de seguridad que deberán ser seguidas por el personal de la institución. La norma ISO también nos provee de recomendaciones y mejores prácticas para la gestión de la seguridad informática y así preservar la confidencialidad, integridad y disponibilidad de la información.

Por último, elaboramos un plan de trabajo e implementamos de los controles en el servidor y por medio de la evaluación de riesgos podremos evidenciar que estas han sido mitigadas las vulnerabilidades.

ÍNDICE GENERAL

AGRADECIMIENTO.....	I
DEDICATORIA.....	II
TRIBUNAL DE SUSTENTACIÓN.....	III
DECLARACIÓN EXPRESA.....	IV
RESUMEN.....	V
ÍNDICE GENERAL.....	VII
ÍNDICE DE FIGURAS.....	XI
ÍNDICE DE TABLAS	XII
INTRODUCCIÓN.....	XIII
1 GENERALIDADES.....	1
1.1 ANTECEDENTES	1
1.2 DESCRIPCIÓN DEL PROBLEMA	2
1.3 SOLUCIÓN PROPUESTA.....	3
1.4 OBJETIVO GENERAL.....	4
1.5 OBJETIVOS ESPECÍFICOS.....	4
1.6 METODOLOGÍA.....	4
2 MARCO TEÓRICO.....	6
2.1 SEGURIDAD INFORMÁTICA.....	6
2.2 ACTIVO DE LA INFORMACIÓN.....	7
2.3 ERP	8

2.4	ESTÁNDARES Y NORMAS APLICABLES A LA SEGURIDAD	
	INFORMÁTICA	10
2.5	NORMA ISO/IEC 27001	11
2.6	METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGO	13
3	LEVANTAMIENTO DE INFORMACIÓN.....	17
3.1	ARQUITECTURA TI	17
3.2	ESTRUCTURA ORGANIZACIONAL	21
3.2.1	MISIÓN	21
3.2.2	VISIÓN.....	21
3.2.3	POLÍTICA INFORMÁTICA	21
3.3	ORGANIGRAMA INSTITUCIONAL	21
3.4	DESCRIPCIÓN DE LOS PROCESOS POR DEPARTAMENTO.....	22
3.5	DETERMINACIÓN DEL ALCANCE DEL PROYECTO	23
4	ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD.....	25
4.1	ANÁLISIS DE RIESGOS	25
4.2	IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS.....	27
4.3	DEPENDENCIAS DE LOS ACTIVOS.....	29
4.4	VALORACIÓN DE LOS ACTIVOS.....	31
4.5	DIMENSIONAMIENTO DE LOS ACTIVOS.....	32
4.6	IDENTIFICACIÓN DE LAS AMENAZAS.....	34
4.7	VALORACIÓN DE LAS AMENAZAS	37

4.8	EVALUACIÓN DE RIESGO.....	38
5	IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	43
5.1	ELABORACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO.....	43
5.2	IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO.....	45
5.2.1	SELECCIÓN DE CONTROLES BASADOS EN LA NORMA ISO 27001	45
5.3	DECLARACIÓN DE APLICABILIDAD DE LOS CONTROLES SELECCIONADOS	46
5.4	DEFINICIÓN DE POLÍTICAS DE SEGURIDAD.....	51
5.4.1	POLÍTICAS Y NORMAS INTERNAS.....	52
5.4.2	POLÍTICAS GENERALES.....	52
5.4.3	POLÍTICAS DE SEGURIDAD A NIVEL FÍSICO	54
5.4.4	ACTUALIZACIÓN DE PAQUETES DEL SISTEMA OPERATIVO	55
5.4.5	POLÍTICAS DE SEGURIDAD A NIVEL LÓGICO	55
5.4.6	POLÍTICAS DE ACCESO	57
5.4.7	POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN	58
5.4.8	POLÍTICAS DE MANTENIMIENTO DE EQUIPOS.....	58
5.4.9	POLÍTICAS DE USO DEL ERP ACADEMIUM.....	59
6	ELABORACIÓN DE CASO DE USO Y ANALISIS DE RESULTADOS.....	61
6.1	ELABORACIÓN DEL CASO DE USO.	61
6.2	HARDENING EN EL SERVIDOR DE ACADEMIUM.....	62

6.3	ROLES Y RESPONSABILIDADES.....	62
6.4	IMPLEMENTACIÓN DE CONTROLES.....	63
6.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.....	64
6.6	EVALUACIÓN Y DOCUMENTACIÓN DE LOS CONTROLES DE LA NORMA EN EL ERP	66
	CONCLUSIONES Y RECOMENDACIONES.....	70
	BIBLIOGRAFÍA.....	73
	ANEXO A.....	74
	ANEXO B.....	75

ÍNDICE DE FIGURAS

Figura 1.2 Gestión de riesgos.....	13
Figura 2.2 Metodología Magerit.....	14
Figura 3.3 Diseño de la red Academium.....	19
Figura 4.3 Topología de la red de datos - Bloque Secundaria.....	20
Figura 5.3 Topología de la red de datos - Bloque Primaria.....	20
Figura 6.4 Elementos del análisis de riesgos potenciales.....	26
Figura 7.4 Dependencia de activos.....	30
Figura 8.6 Recurso de Hardware para el servidor Academium.....	66

ÍNDICE DE TABLAS

Tabla 1 Fases de la mejora continua.....	12
Tabla 2 Procesos por Departamento.....	22
Tabla 3 Inventario de activos.....	28
Tabla 4 Criterio de valoración.....	32
Tabla 5 Valoración de los activos.....	33
Tabla 6 Amenaza por activo.....	35
Tabla 7 Probabilidad de ocurrencia.....	38
Tabla 8 Degradación del valor.....	38
Tabla 9 Niveles de aceptación del riesgo.....	39
Tabla 10 Evaluación de riesgo.....	40
Tabla 11 Declaración de aplicabilidad.....	46
Tabla 12 Implementación de controles.....	63

INTRODUCCIÓN

Los sistemas ERP, integran toda la información de diferentes departamentos en un solo repositorio o base de datos para luego ser utilizado y gestionado dependiendo de la necesidad de la institución. Estos sistemas otorgan un apoyo a los clientes dando tiempos rápidos de respuesta y usa de manera eficiente la información, para la toma de decisiones oportunas.

Academium es un ERP que integra módulos financieros y académicos automatizando los procesos de negocios de la institución y nos permite realizar el análisis contable y administrativo. El sistema está desarrollado bajo una plataforma web amigable para el usuario y puede ser accedido desde el internet.

Desde la implementación de Academium en la institución, hemos comenzado a tener diferentes ataques en el servidor de otras IP externas, por lo cual pone en peligro la información que tenemos almacenada. Y siendo la información, el principal activo de toda institución debemos salvaguardarla para que no sea manipulada o vista por cualquier persona que no tenga autorización.

La información debe cumplir con la disponibilidad, confiabilidad e integridad para lo cual vamos a realizar un análisis de gestión de riesgos y conocer todas la vulnerabilidades que tenemos en este momento. El análisis que vamos a realizar contara con la ayuda de la metodología Magerit, y bajo el estándar de la de la norma ISO27001:2013 escogeremos los mejores controles para aplicarlos en el servidor.

CAPÍTULO 1:

GENERALIDADES

1.1 ANTECEDENTES

La Unidad Educativa **Javier** ha adquirido un nuevo ERP llamado **Academium** para llevar en conjunto la parte administrativa (contabilidad, compras, ventas, recursos humanos, tesorería) y la parte educativa.

El objetivo de adquirir el **ERP Academium** es que los demás colegios de la red jesuitas con diferentes sedes en el país tengan el mismo aplicativo y así llevar un control de la aplicación a un nivel macro.

El número de procesos de las demás unidades educativas es menor a los que se maneja en la Unidad Educativa Javier, por lo que tenemos muchas más

transacciones al día y se maneja un gran flujo de información tanto la parte administrativa como la parte académica.

Esto hace que tengamos que salvaguardar la información y estar preparado para cualquier eventualidad.

Desde la implementación del **ERP Academium** se le configuró un IP pública para que la aplicación pueda ser visitada desde cualquier parte, pero en los últimos meses hemos sufrido de ataques de otras IP, esto lo podemos constatar en el registro de acceso del servidor.

Al ser un sitio web siempre habrá personas que quieran vulnerarlo y poderse extraer o modificar la información de la base de datos y al ser un **ERP** que maneja información contable de la institución al perderse no se tendría la seguridad o la confiabilidad de realizar los cobros de las pensiones, comprar y pagar a los proveedores, realizar los presupuestos de cada área, realizar los roles de pagos de los empleados y visualizar la cartera de los años anteriores de los padres de familia.

1.2 DESCRIPCIÓN DEL PROBLEMA

En listamos los siguientes riesgos de seguridad

- Los ataques externos o fuera de la institución a través del internet son constante, con un alto riesgos de que ingresen al servidor y comprometan la información almacenada.
- Los ataques internos o dentro de la institución a través de la red no son muy comunes pero tampoco existen tampoco los debidos controles o políticas de seguridad en la red.

- La integridad de los datos estarían siendo comprometidas por no tener políticas de control de acceso al servidor y a la base de datos.
- El servidor no cuenta con las actualizaciones de parches del sistema operativo ocasionando un mal funcionamiento del servidor.
- No ha habido un debido hardening del servidor por lo cual tenemos muchos servicios que consumen los recursos.
- No se cuenta con un servidor de respaldo que almacene la misma información que el servidor de producción por lo que si el servidor de producción se daña, en ese momento se tendría que levantar un respaldo de la aplicación y de la base de datos en otro servidor, causando malestar a los usuarios.

En la actualidad contamos con un firewall que está haciendo frente a cualquier ataque externo al servidor, pero nos falta políticas y controles de seguridad que nos ayudarían a minimizar los riesgos de seguridad.

Al definir los controles necesarios en la Unidad Educativa Javier nos servirán para las demás instituciones de la red jesuitas que utilizan el **ERP Academium**.

1.3 SOLUCIÓN PROPUESTA

Desarrollo e implementación de controles de seguridad informática utilizando la norma ISO 27001.

La norma también nos proveerá de recomendaciones y mejores prácticas para la gestión de la seguridad informática y así preservar la confidencialidad, integridad y disponibilidad de la información.

1.4 OBJETIVO GENERAL

- Implementar controles de seguridad informática para el sistema **ERP Academium** de la Unidad Educativa Javier, siguiendo la norma ISO 27001.

1.5 OBJETIVOS ESPECÍFICOS

- Levantar la información de la arquitectura tecnológica de la aplicación **Academium** en la Unidad Educativa Javier.
- Identificar los posibles riesgos de seguridad informática de la aplicación **Academium**.
- Diseñar un sistema de gestión de seguridad de la información para la aplicación **Academium**.
- Establecer procedimientos y políticas de seguridad en el departamento de sistemas basados en la norma ISO 27001.

1.6 METODOLOGÍA

Para la implementación de un sistema de gestión de seguridad informática vamos a realizar las siguientes tareas:

- Realizar una evaluación de riesgos que podría sufrir la aplicación web tomando en cuenta todas las vulnerabilidades existentes y el impacto que causarían para la institución.

- Hacer un inventario de activos de la información que contribuyen en el buen funcionamiento del **Academium** con sus respectivos responsables.
- Realizar un análisis de riesgos considerando los activos más importantes.
- Escoger los controles más adecuados para la implementación de la norma y poder afrontar los riesgos de seguridad.
- Elaborar un plan de trabajo para la implementación de los controles.
- Realizar actividades de monitoreo de los controles.
- Planificar casos de pruebas para evidenciar el cumplimiento de los controles seleccionados de la norma.
- Realizar el informe de la evaluación de riesgos de los casos de pruebas después de aplicar los controles seleccionados.
- Documentar los controles seleccionados utilizados en los casos de prueba.

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD INFORMÁTICA

La seguridad informática es un conjunto de medidas preventivas [1] que nos ayuda a proteger la información almacenada ante cualquier posible ataque o intromisión manteniendo su integridad, disponibilidad y confidencialidad.

Para ello aplica diferentes técnicas y protocolos de seguridad a nivel lógico y de la red asegurando los activos más importantes de la organización.

La seguridad informática se enfoca en la protección a nivel físico (hardware) y lógico (software) minimizando las amenazas y vulnerabilidades para la protección del sistema informático.

Teniendo en cuenta que la información es el activo más importante de la organización debe cumplir los siguientes aspectos.

- **Integridad:** Consiste en mantener la información libre de modificaciones de personas o procesos no autorizados. La integridad garantiza que la información no sea alterada y que sea completa.
- **Disponibilidad:** Es el acceso libre a la información a las personas o procesos que tengan autorización. Preservando la continuidad de la información en todo momento y evitando interrupciones.
- **Confidencialidad:** Consiste en no divulgar la información antes cualquier persona o entidad que no tenga la debida autorización. La confidencialidad asegura el acceso a la información y minimiza los privilegios del acceso según el rol de las personas.

2.2 ACTIVO DE LA INFORMACIÓN

Un activo es todo aquello que tiene valor para su empresa y que debe ser protegido.

Los activos de la información se consideran recursos (hardware y software) que contienen información y componen un proceso de comunicación a partir de la generación de la información que inicia desde el emisor y utilizando un medio de transmisor hasta el receptor.

Existen tres tipos de activos:

- **Personal:** Todos los usuarios que interactúan con el sistema y que tienen acceso a los datos e información.

- **Sistemas e Infraestructura:** Se refiere a los componentes físicos que nos ayuda a gestionar y almacenar la información.
- **Datos e Información:** Principal activo de la información, se refiere a la información almacenada en medios magnéticos o físicos.

Para llevar un control de los activos de la información es importante definir políticas y realizar el inventario de los activos.

Según el activo que se quiere proteger tenemos dos tipos de seguridad:

- **Seguridad Física:** Es la aplicación de mecanismos dentro y fuera del Centro de Computo que aseguran la protección de los equipos físicos. Estos mecanismos consisten en barreras físicas y procedimientos de control que nos ayudan a la prevención de amenazas físicas.
- **Seguridad Lógica:** Es el complemento de la seguridad física, consiste en la aplicación de controles lógicos que nos ayudan a la protección de software y de la información contra alguna intromisión no autorizada.

2.3 ERP

Se define como ERP (Enterprise Resource Planning - Planificación de Recursos Empresariales) [2] a un conjunto de sistemas de gestión de información o módulos que están integrados entre si y automatizan los procesos operativos y productivos de una empresa.

Los sistemas de planificación de recursos empresariales se caracterizan por estar compuestos de módulo asociados, entre los más importantes tenemos [2]:

- Finanzas: Mantiene la información de la tesorería de la empresa, financiación (préstamos), inversiones, contabilidad, etc.
- Compras: Mantiene la información y gestión de las compras (aprovisionamientos) de la empresa, proveedores, etc.
- Ventas: Mantiene la información y gestión de las ventas. Datos de ventas, partidas expedidas, precios de venta, etc.
- Logística: Mantiene la información y gestión de los almacenes, stocks, transportes, etc.
- Recursos humanos: Mantiene la información y gestión del personal, nóminas, categorías laborales, horas extra, impuestos, etc.
- CRM (Customer Relationship Management o Sistema de gestión de relaciones con clientes): Es un subsistema que mantiene la información y gestión de las relaciones con clientes (datos, contratos, etc.).

Al tener un solo acceso a la base de datos, el ERP funciona como un sistema integrado. El ERP puede ser modular o configurable dependiendo de la necesidad de la empresa.

Los ERP modulares cuentan con diferentes módulos que ya están predefinidos y gestionan los diferentes departamentos. En cambio que los

ERP configurables tiene módulos que pueden ser modificados para que sea adaptable a la necesidad de la empresa.

Los objetivos principales de los sistemas ERP son [2]:

- Optimización de los procesos empresariales.
- Acceso a la información.
- Posibilidad de compartir información entre todos los componentes de la organización.
- Eliminación de datos y operaciones innecesarias de reingeniería.

El propósito fundamental de un ERP es otorgar apoyo a los clientes del negocio, tiempos rápidos de respuesta a sus problemas, así como un eficiente manejo de información que permita la toma oportuna de decisiones y disminución de los costos totales de operación.

2.4 ESTÁNDARES Y NORMAS APLICABLES A LA SEGURIDAD INFORMÁTICA

Toda organización ya sea pequeña o grande debe tener un sistema de gestión eficiente que proteja los recursos de la organización. Por lo que se debe identificar y detectar los riesgos o vulnerabilidades de la organización y adoptar las mejoras normas para reducir el impacto de sobre sus recursos.

Al implementar un sistema de gestión de seguridad de la información (SGSI) en una organización, nos aseguramos que seguimos un proceso sistematizado y documentado que garantiza que la información va a estar

protegida por medio de la selección de controles de seguridad adecuados y proporcionales.

La norma ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) [3], que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

A partir de la norma ISO 27000 han surgido un gran número de estándares ISO con sus diferentes normas que implementan un sistema de gestión de seguridad de la información a cualquier tipo de organización.

2.5 NORMA ISO/IEC 27001

La norma ISO 27001 es un estándar para la seguridad de la información (Information technology - Security techniques – Information security management systems - Requirements) que establece los requisitos para implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando del ciclo de Deming y siguiendo el modelo PDCA (Plan - Do - Check - Act) para los procesos de la organización.

Tabla 1. Fases de la mejora continua

Fase Planificación (Establecer el SGSI)	Establecer políticas, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.
Fase Ejecución (implementar y gestionar el SGSI)	Implementar y gestionar el SGSI de acuerdo a su política, controles, procesos y procedimientos.
Fase Seguimiento (monitorizar y revisar el SGSI)	Medir y revisar las prestaciones de los procesos del SGSI.
Fase Mejora (mantener y mejorar el SGSI)	Adoptar acciones correctivas y preventivas basadas en auditorías y revisiones internas o en otra información relevante, a fin de alcanzar la mejora continua del SGSI.

La actualización de la norma ISO 27001 - 2013 incluye el Anexo A que se conforma de 14 dominios, 35 objetivos de control (una descripción de lo que se desea alcanzar con la aplicación de controles) y 114 controles de seguridad, que pueden ser seleccionados e implementados como parte del proceso de tratamiento de riesgos [3].

Lo más relevante de la norma ISO 27001 es el análisis y gestión de los riesgos basado en los procesos de negocio y servicios de IT. [4]

2.6 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGO

El análisis de riesgo permite estimar la magnitud de los riesgos que puede sufrir una organización y dependiendo del entorno se toma decisiones de gestión y asignación de recursos.

En cambio que el tratamiento de riesgos va a recopilar las actividades que nos ayudan a salvaguardar a la organización de las amenazas a las que está expuesta.

Ambas actividades, el análisis de riesgo y el tratamiento de riesgo se denomina Gestión de Riesgos.



Figura 1.2: Gestión de riesgos

Entre las metodologías usadas en la gestión de riesgos, vamos a implementar la metodología Magerit.

Magerit es la metodología de análisis y gestión de riesgos [5] que permite concienciar a los responsables sobre la existencia de los riesgos en la organización.

Ofrece una metodología sistemática para analizar los riesgos y planificar el tratamiento de los riesgos.

Y valoriza los activos que interactúan con el ambiente de la organización y sus dependencias determinando su vulnerabilidad e implementando los controles necesarios para la mejora y disminución de los riesgos.

En la actualidad Magerit se encuentra en el versión 3, esta versión sigue la terminología ISO 31000 que implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información[6].

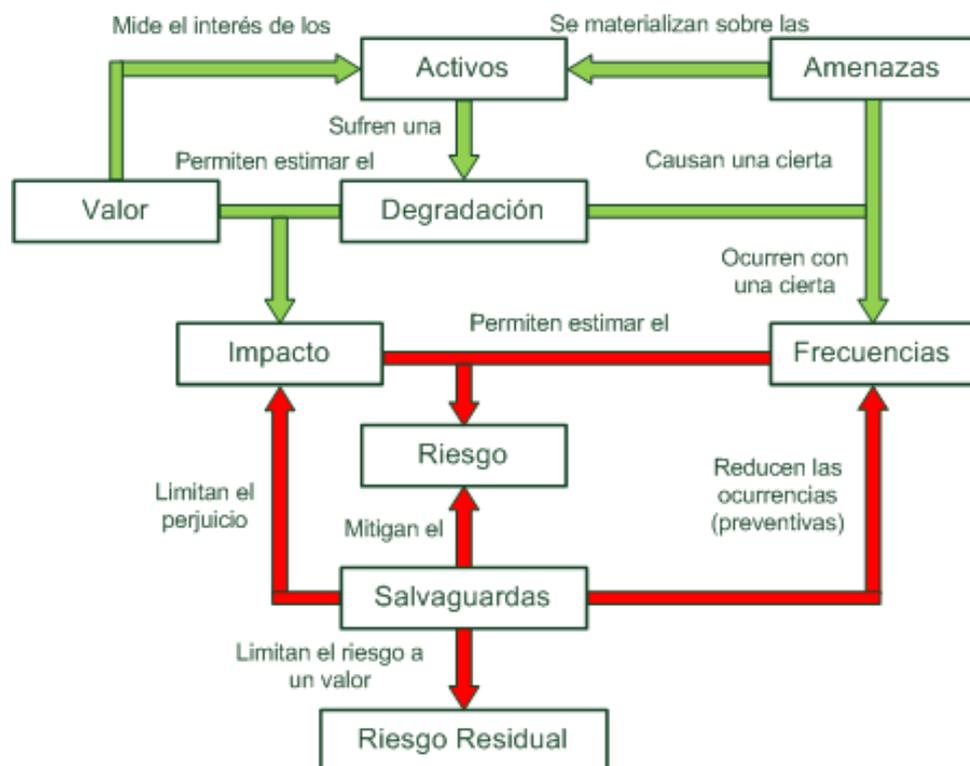


Figura 2.2: Metodología Magerit

El análisis de riesgos proporciona una metodología que se detalla a continuación [7]:

- Toma de datos: Determina el alcance del análisis y los elementos a los cuales vamos a aplicar la metodología.
- Dimensionamiento: Da un valor a cada activo que este dentro del alcance de análisis de riesgos y agrupamos a los activos por su valor. También determina los parámetros por los cuales vamos a evaluar los activos como la vulnerabilidad, impacto, efectividad del control de seguridad.
- Análisis de activos: Identifica todos los activos que intervienen en los procesos de negocio de la organización.

Una vez identificados se los comienza a clasificar de la siguiente manera

- Activos Físicos.
 - Activos Lógicos.
 - Activos de entorno e infraestructura.
 - Activos intangibles.
- Análisis de amenazas: Identifica todas las posibles amenazas que puede ocurrir en la organización.

Las amenazas se categorizan de la siguiente manera.

- Accidentes
- Errores.
- Amenazas intencionales presenciales.
- Amenazas intencionales remotas.

- Valoración de impactos: Determina el impacto de una vulnerabilidad sobre un activo.
- Análisis de riesgo intrínseco: Determina el valor del riesgo a través del valor del activo por la vulnerabilidad e impacto.
- Influencia de salvaguardas: Gestiona el riesgo implementando la mejor solución para reducirlo.
- Análisis de riesgo efectivo: Determina el valor de riesgo efectivo después de haber aplicado la mejor solución.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1 ARQUITECTURA TI

La institución cuenta con un departamento de sistemas que da soporte a todos sus empleados.

Entre los roles que desempeña el departamento de sistemas en la UE Javier tenemos:

- Programación de nuevas aplicaciones web.
- Soporte a usuarios.
- Administración de la red.

- Administración los perfiles de usuarios
- Respaldo de información(Base de datos y Aplicaciones)
- Mantenimiento de hardware y software.
- Administración de los salones de audio y video.

El Centro de Computo tiene un sistema de ventilación y racks acordes a los equipos instalados, pero no cuenta con un sistema de control de acceso, que permita mantener una información básica como de cuándo y quien ingreso al centro de datos.

La aplicación **Academium**, que es la aplicación Core de la institución, se encuentra instalada en un equipo clon tipo escritorio con las siguientes características:

- Sistema Operativo CentOS Linux Release 6.0 Versión 2.632.71.e16.x86_64 GNU_Linux
- Servidor Apache Versión 5.0
- PHP 5.3.3
- IP Interna: 192.168.7.240
- IP Externa: 190.95.215.181

En este momento el equipo no presta las mejores condiciones para trabajos de misión crítica, además el mismo equipo hace las funciones de equipo de producción y desarrollo, es decir mientras atiende a los usuarios, está atendiendo los cambios y modificaciones, lo que puede provocar interrupciones o lentitud en el sistema.

A continuación se detalla la infraestructura de red que actualmente tiene el colegio Javier.

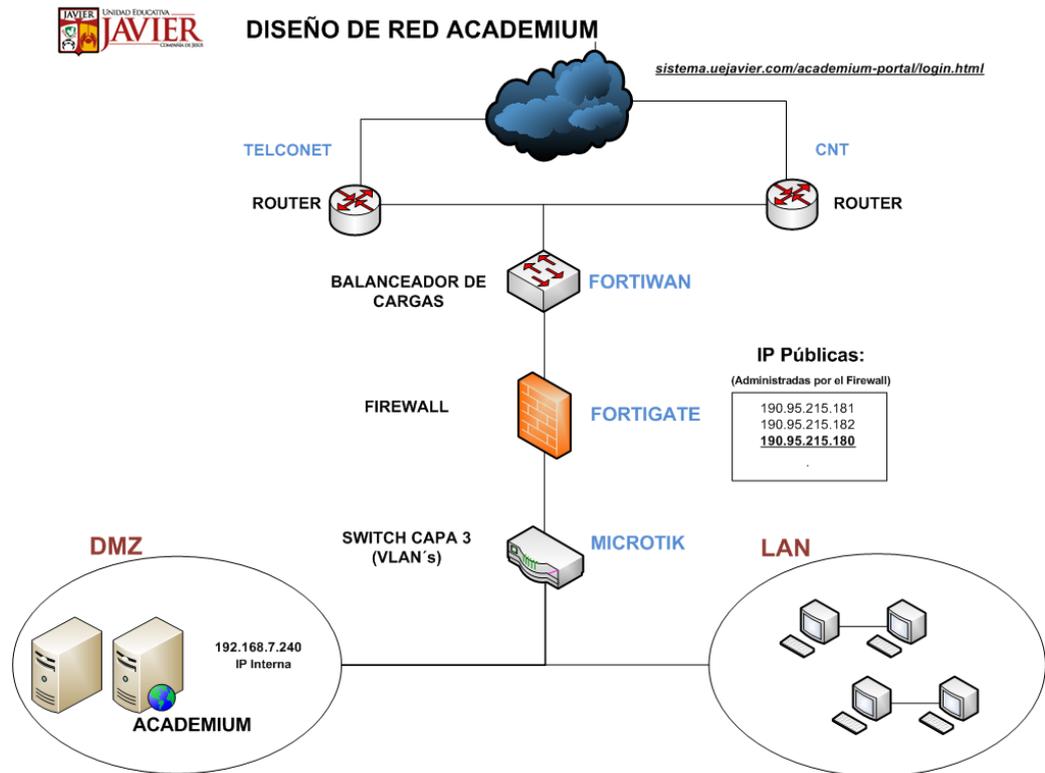


Figura 3.3: Diseño de la red Academium

NOTA: Vale indicar que existen estándares de seguridad del software utilizado en los diferentes servidores Linux, los cuales son los siguientes:

Sistema Operativo CentOS Linux Release 6.0 Versión 2.632.71.e16.x86_64

GNU_Linux

Motor de base de datos MySql Versión 5.1.40

PHP Versión 5.3.3

Apache versión 5.0

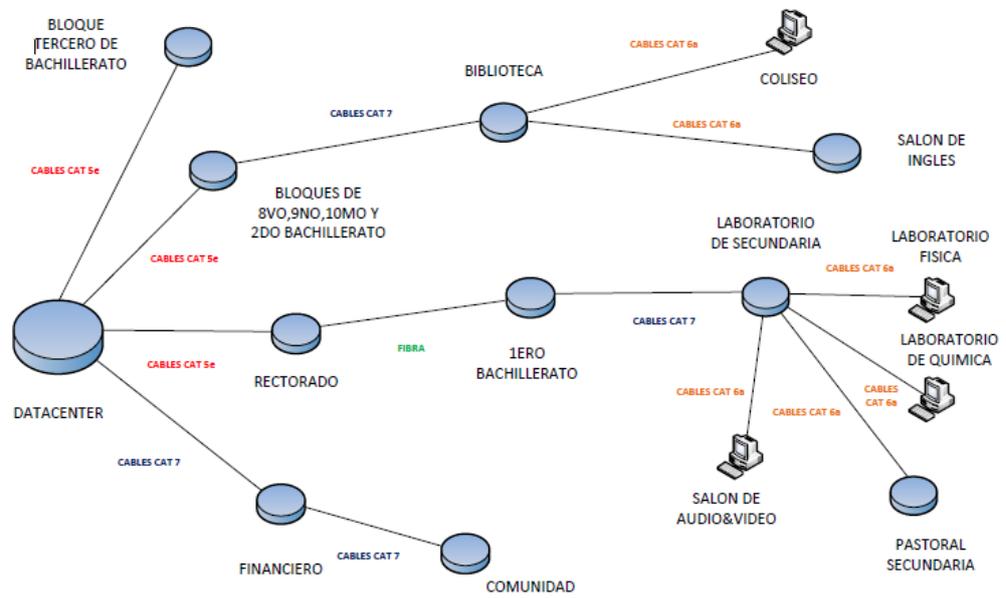


Figura 4.3: Topología de la red de datos - Bloque Secundaria

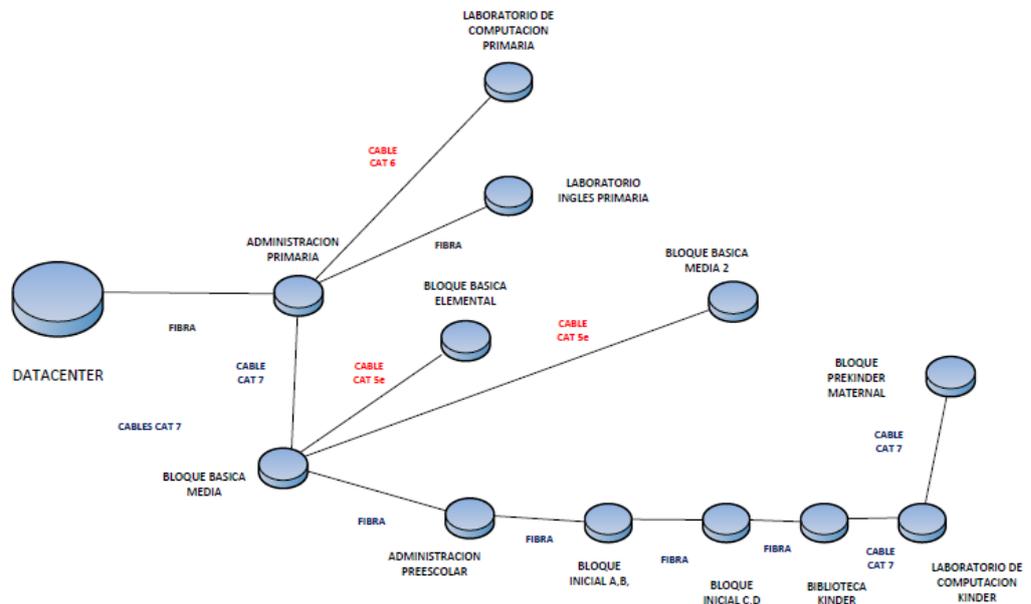


Figura 5.3: Topología de la red de datos - Bloque Primaria

3.2 ESTRUCTURA ORGANIZACIONAL

3.2.1 MISIÓN

Evangelizar a la familia Javeriana y forjar hombres y mujeres con liderazgo ignaciano y excelencia integral al servicio de los demás, con alto espíritu de solidaridad, respeto intercultural y comprometido con el desarrollo global.

3.2.2 VISIÓN

Ser una comunidad educativa de excelencia internacional que forma niños, niñas y jóvenes fortalecidos en la pedagogía Ignaciana, en la ciencia y la justicia, con una profunda experiencia de Dios, capaces de asumir desafíos, edificar y contribuir con una sociedad más justa y equitativa.

3.2.3 POLÍTICA INFORMÁTICA

Las políticas y estándares de seguridad informática tienen por objetivo establecer normas y obligaciones de todo el personal comprometido en el uso de los servicios informáticos proporcionados por la UE Javier.

3.2.4 ORGANIGRAMA INSTITUCIONAL

Ver Anexo A "Organigrama Institucional".

3.3 DESCRIPCIÓN DE LOS PROCESOS POR DEPARTAMENTO

La norma ISO 27001 implementa un sistema de gestión de seguridad de la información (SGSI), que identifica los procesos de negocios que realiza la institución.

Cada proceso debe estar contenido por el departamento que lo realiza, a continuación detallaremos los departamentos y los procesos que realiza cada uno.

Tabla 2. Procesos por Departamento

Contabilidad	El departamento de contabilidad se encarga de garantizar que los registros de todas las operaciones realizadas en Academium se presenten en los informes contables que son entregados cada mes a la Gerencia. Entre los informes que son entregados tenemos los estados resultados, estado de flujo efectivo, conciliaciones bancarias, balances generales y anexos.
Compras	El departamento de compras se encarga de realizar las órdenes de compra, solicitudes de provisión, el ingreso y egreso de materiales e insumos. También se registran las facturas de compras de bienes inventariados y de servicios. Y generan los pagos a los proveedores para así dar de baja el saldo que se le adeuda.
Nómina y Talento Humano	El departamento de nómina y talento de humano se encarga de ingresar los nuevos empleados, crear los nuevos roles y departamentos. Se registran los préstamos y anticipos que son otorgados a los empleados. Y crean los roles de pagos para después enviar el archivo con los saldos al banco para pagar los sueldos.
Facturación,	El departamento de facturación, cobranza y becas se

Cobranzas y Becas	<p>encarga del proceso de matriculación, realizar las facturas masivas de pensiones de todos los estudiantes de la institución, otorgar el descuento por becas y facturar los servicios que ofrece la institución como alquiler de capilla, etc.</p> <p>Realizan la gestión de cobranzas por medio de los estados de cuentas de cada cliente o padre de familia. Se crea los archivos de los bancos para enviar a debitar a los padres de familia en sus cuentas o tarjetas.</p> <p>Y las facturas que se generar se envían a autorizar por medio del web service del SRI.</p>
Académico	<p>En lo que respecta al área académica, el ERP es parametrizado para seguir las normas del Ministerio de Educación como por ejemplo las equivalencias, los parciales, los cursos y las materias.</p> <p>Se crean los trimestres, se registran las notas de los alumnos y se envía a calcular los promedios de cada parcial.</p> <p>Después de cada trimestre se imprimen las libretas y los certificados de promociones.</p> <p>También nos ayuda a realizar el seguimiento de cada alumno, ingresando sus incidentes que haya tenido dentro de la institución.</p>

3.4 DETERMINACIÓN DEL ALCANCE DEL PROYECTO

Después de haber sido aceptado el proyecto por el departamento de sistema, se va a disponer de todos los recursos existentes para garantizar la seguridad de la información de la institución.

La información que maneja el colegio Javier de acuerdo a su importancia debe ser protegida usando las medidas de seguridad necesarias. Y se va a definir los siguientes objetivos que debe cumplir el proyecto.

- Diseñar una planificación de la seguridad de la información para la institución.
- Analizar el estado actual e identificar las vulnerabilidades y amenazas.
- Escoger los mejores controles de seguridad para salvaguardar la información.

El dominio del proyecto cubrirá los procesos de los departamentos de contabilidad, compras, nomina, facturación y académico.

CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD

4.1 ANÁLISIS DE RIESGOS

Como se había mencionado en los capítulos anteriores vamos a usar la metodología Magerit para realizar el análisis y gestión de riesgos de los sistemas informáticos.

La importancia de utilizar esta metodología es para identificar los riesgos existentes en la organización y aplicar estrategias para la protección de ellos.

Para seguir la metodología debemos realizarlos los siguientes pasos.

1. Determinar los activos relevantes para la Organización (su interrelación y su valor)
2. Determinar las amenazas que están expuestos los activos.
3. Determinar qué salvaguardas son eficaces frente al riesgo.
4. Estimar el impacto del activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto

Por lo general Magerit exige seguir los pasos 1, 2, 4 y 5, y posteriormente el paso 3, ya que inicialmente la organización no cuenta con salvaguardas.

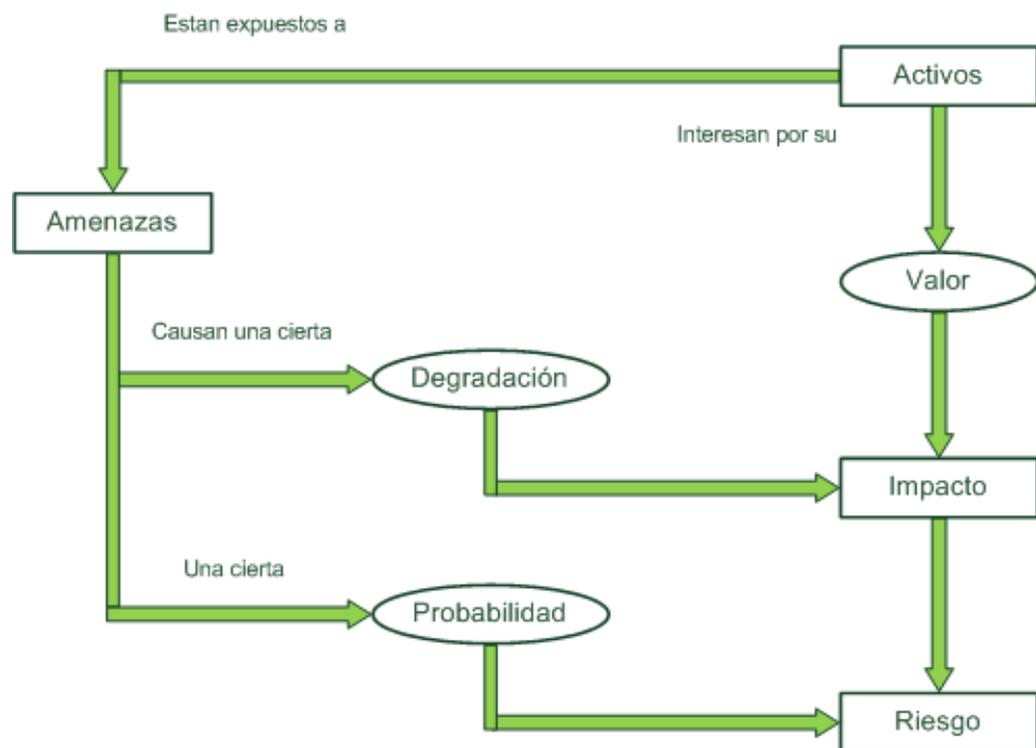


Figura 6.4: Elementos del análisis de riesgos potenciales

4.2 IDENTIFICACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS

Para identificar los activos se consultó al departamento de sistemas, que proceso son los más crítico para la institución. Y clasificaremos los activos tomando como base el Libro II de la metodología Magerit versión 3 descrita a continuación:

- **[D] Datos/Información.** Es lo más importante para una organización y lo que debe ser salvaguardado. Dependiendo de cuál importante es la información o datos se va a determinar su nivel de confidencialidad.
- **[SW] Aplicaciones (Software).** Llamados también como programas, aplicativos, desarrollos, etc. Es cualquier tarea automatizada que se realiza en un equipo informático.
- **[HW] Equipos Informáticos (Hardware).** Son los equipos físicos que dan una utilidad a la organización y que puede ser reemplazado si tiene algún desperfecto.
- **[S] Servicios.** Tareas externas o internas que necesita la organización para realizar sus procesos.
- **[AUX] Equipamiento auxiliar.** Son los medios físicos que apoyan a la infraestructura de la organización.
- **[COM] Redes de comunicaciones.** Son los activos que hacen referencia a la contratación de servicios por terceros.

Tabla 3. Inventario de activos

Código	Activo	Clasificación	Descripción
D-001	Respaldo de la base de datos	Datos/Información	Archivos de respaldo de la base de datos.
D-002	Respaldo del código fuente de Academium	Datos/Información	Archivo comprimido del respaldo de la aplicación.
D-003	Información académica	Datos/Información	Datos del estudiante, calificaciones, notas de conducta, promedios, etc.
D-004	Información financiera	Datos/Información	Datos sobre los balances, presupuestos, cuentas contables, cuentas bancarias, costos, saldo de proveedores, etc.
D-005	Información del personal de la institución	Datos/Información	Datos sobre los contratos, sueldos, datos personales de los empleados (docentes y administrativos), nomina, etc.
D-006	Información financiera de los padres de familia	Datos/Información	Datos financieros de los padres de familia, cuentas bancarias, número de tarjetas de crédito y débito, etc.
D-007	Base de Datos de Academium	Datos/Información	Base de Datos MySQL, que almacena los datos académicos, financieros y del personal.
SW-001	Motor de base de datos	Aplicaciones (Software)	Repositorio que nos ayuda a almacenar la información registrada.
SW-002	Sistema	Aplicaciones	Software que administra el

	operativo del Servidor	(Software)	hardware y software del equipo.
SW-003	Sistema Web - Academium	Aplicaciones (Software)	Sistema de planificación de recursos empresariales.
HW-001	Servidor	Equipos informáticos (Hardware)	Equipo que contiene la aplicación Academium y la base de datos.
AUX-001	Cortafuego	Equipamiento auxiliar	Hardware y software que administra los accesos y permisos a la red y al servidor.
COM-001	Red LAN	Redes de comunicaciones	Sistema de comunicación entre los equipos y el servidor dentro de la institución.
S-001	Autorización de facturas y notas de créditos al SRI.	Servicios	Envío del XML de las facturas y notas de crédito al web service del SRI
S-002	Envío de las facturas y notas de créditos por correo.	Servicios	Las facturas o notas de crédito una vez autorizadas por el SRI se envían al correo del padre de familia.
S-003	Envío de los roles de pagos por correo.	Servicios	Para optimizar el proceso de entrega de los roles de pagos a los empleados se implementó el envío de correo de sus roles.

4.3 DEPENDENCIAS DE LOS ACTIVOS

Existen activos esenciales en la organización que manejan la información y los servicios. Estos activos son llamados activos superior mientras que los activos más prosaicos o de menor importancia son llamados activo inferior.

Un “activo superior” depende de otro “activo inferior” cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior.

Es decir al materializarse la amenaza del activo inferior este afecta directamente al activo superior.

Y para determinar la dependencia entre nuestros activos identificados anteriormente crearemos el siguiente gráfico.

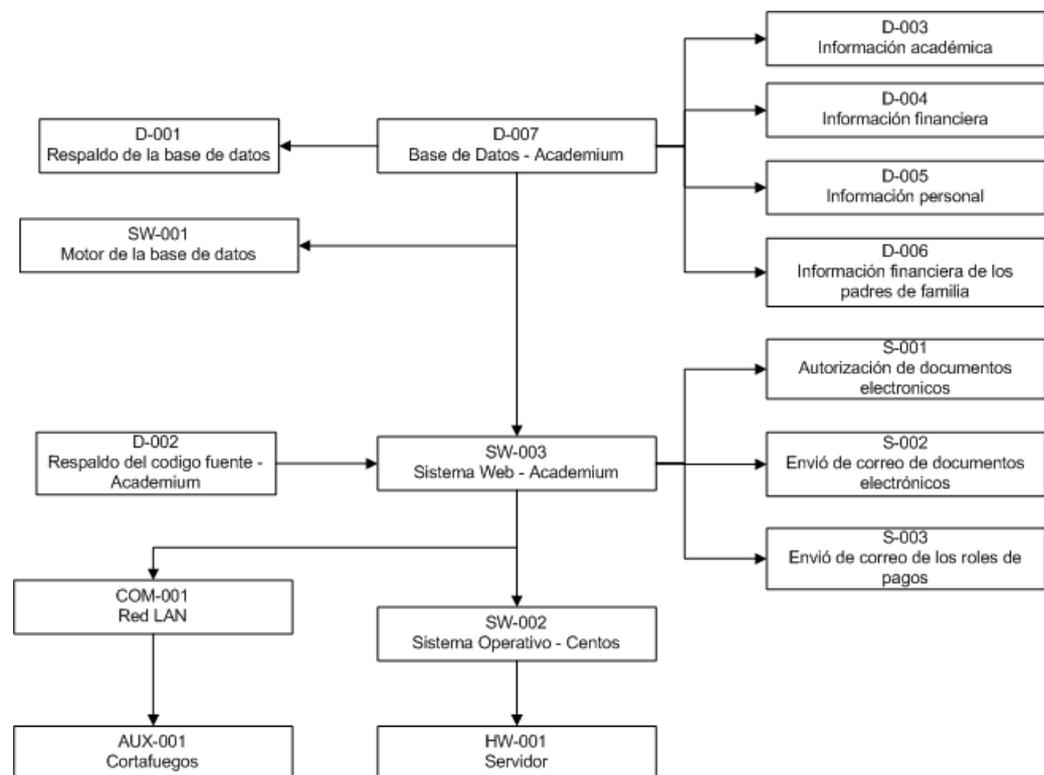


Figura 7.4: Dependencia de activos

Dentro de las dependencias entre los activos que se destacan es el sistema operativo ya que es el sistema base en donde corre el servidor web de

aplicación y la base de datos. Luego de eso tenemos la aplicación web y la base de datos en donde se guarda toda la información de la institución.

Y finalmente tenemos las consultas y los reportes que son generados por las personas y que deben ser información fiable para los clientes.

4.4 VALORACIÓN DE LOS ACTIVOS

Una vez identificados los activos, procedemos asignarle un valor de importancia, este valor debe ser cuantitativo (escala numérica) o cualitativo (escala de nivel) y consiste en valorar los activos de acuerdo a las dimensiones de interés que propone la norma ISO 27001:2013

El valor de un activo es el promedio de la integridad, disponibilidad y confidencialidad.

Notación de la fórmula:

VA: Valor del activo

VI: Valor de la integridad

VD: Valor de la disponibilidad

VC: Valor de la confidencialidad

Formula:

$$VA = \frac{VI + VD + VC}{3}$$

Los criterios de valorización deben ser claros y concisos para que sea entendible por todos los participantes.

Para cuantificar el valor de cada activo usamos la escala de Likert y asignamos un valor de 1 si el impacto es muy bajo y de 5 si el impacto es muy alto, tomando en cuenta los siguientes criterios.

Tabla 4. Criterio de valoración

	Valor	Criterio
5	Muy alto	Daño muy grave a la organización
4	Alto	Daño grave a la organización
3	Medio	Daño importante a la organización
2	Bajo	Daño menor a la organización
1	Despreciable	Irrelevante a efectos prácticos

4.5 DIMENSIONAMIENTO DE LOS ACTIVOS

El dimensionamiento nos ayuda a definir que atributos o cualidades tiene un activo. Y el valor que se obtenga va hacer del impacto de la materialización de las amenazas sobre el activo.

Un activo debe ser considerado por las siguientes dimensiones:

- Confidencialidad [C]: Que consecuencias tendría si personas no autorizadas tienen acceso a la información de débitos bancarios?

- Disponibilidad [D]: Que hacer si no se puede acceder a la aplicación web por algún sabotaje?
- Integridad [I]: Que hacer si la red ha sido hackeada?

Tabla 5. Valoración de los activos

Código	Activo	Dimensiones			Valor promedio
		Disponibilidad	Confidencialidad	Integridad	
D-001	Respaldos de la base de datos	10	10	10	10
D-002	Respaldo del código fuente de Academium	7	7	10	8
D-003	Información académica	10	10	10	10
D-004	Información financiera	10	10	10	10
D-005	Información del personal	10	10	10	10
D-006	Información financiera de los padres de familia	10	10	10	10
D-007	Base de Datos de Academium	10	10	10	10
SW-001	Motor de base de datos	10	10	10	10
SW-002	Sistema operativo del Servidor	9	9	8	8.67
SW-003	Sistema Web - Academium	10	8	9	9
HW-001	Servidor	10	9	9	9.33
AUX-001	Cortafuego	8	8	8	8
COM-001	Red LAN	8	9	10	9
S-001	Autorización de facturas y notas de créditos al	7	7	9	7.67

	SRI.				
S-002	Envío de las facturas y notas de créditos por correo.	7	7	9	7.67
S-003	Envío de los roles de pagos por correo.	7	7	9	7.67

4.6 IDENTIFICACIÓN DE LAS AMENAZAS

Después de identificar todos los activos involucrados en los procesos de la organización, vamos a identificar las amenazas que afectan a cada activo.

Las amenazas son eventos que pueden desencadenar un incidente en la organización, provocando daños materiales o pérdidas inmateriales en sus activos.

Las amenazas más típicas que puede sufrir un activo son:

- De origen natural [N]: Desastres naturales de cualquier naturaleza (terremotos, inundaciones, tsunamis, etc.)
- Del entorno (de origen industrial) [I]: Desastres industriales (fuego, fallos eléctricos, etc.)
- Causadas por las personas de forma accidental [E]: Personas con acceso al sistema que causan problemas de forma accidental.
- Causadas por las personas de forma deliberada [A]: Personas con acceso al sistema que causan problemas de forma deliberada por algún motivo.

Se debe considerar que la materialización de una amenaza es porque existen vulnerabilidades que son fáciles de explotar por su falta de controles y salvaguardias.

Tabla 6. Amenaza por activo

Código	Activo	Amenaza	Vulnerabilidad
D-001	Respaldos de la base de datos	[E.1] Deterioro del archivo de respaldo de la base de datos	Respaldo inadecuado
D-002	Respaldo del código fuente de Academium	[E.1] Deterioro del archivo de respaldo	Respaldo inadecuado
D-003	Información académica	[A.1] Robo de la información. [A.2] Manipulación de la información académica [E.2] Acceso sin permiso a la información	Falta de controles de seguridad en la aplicación No existen una fortaleza en las contraseñas de los usuarios Restricción de accesos a los perfiles de usuario
D-004	Información financiera	[A.1] Robo de la información. [A.2] Manipulación de la información académica [E.2] Acceso sin permiso a la información	Falta de controles de seguridad en la aplicación No existen una fortaleza en las contraseñas de los usuarios Restricción de accesos a los perfiles de usuario
D-005	Información del personal	[A.1] Robo de la información. [A.2] Manipulación de la información académica [E.2] Acceso sin permiso a la información	Falta de controles de seguridad en la aplicación No existen una fortaleza en las contraseñas de los usuarios Restricción de accesos a los perfiles de usuario
D-006	Información financiera de los padres de familia	[A.1] Robo de la información. [A.2] Manipulación de la información académica [E.2] Acceso sin permiso a la información	Falta de controles de seguridad en la aplicación No existen una fortaleza en las contraseñas de los usuarios Restricción de accesos a los perfiles de usuario
D-007	Base de Datos de Academium	[A.1] Robo de la información. [A.3] Acceso no autorizado	Acceso libre al servidor de la base de datos. Mala administración en la creación de usuario y asignación de permisos

SW-001	Motor de base de datos	[I.1] Servicio del MySQL no arranca [E.3] Manipulación del archivo de configuración	Mala configuración del archivo de configuración del MySQL Falta de control del acceso al servidor de base de datos.
SW-002	Sistema operativo del Servidor	[E.4] Inestabilidad en el sistema operativo por mantenimiento o actualización. [I.2] Avería a nivel de hardware o software [E.5] Envío de información no autorizada desde el servidor [E.6] Acceso sin restricción a los usuarios [A.4] Acceso no autorizado al servidor	Instalación de parches de software sin haberlo probados. Ausencia de mantenimientos preventivos a los equipos. Partes defectuosas de fábrica. Puertos abiertos del sistema operativo Instalación de paquetes sin previa inspección. No existe una gestión de los usuarios del sistema operativo. Mala configuración del iptables
SW-003	Sistema Web - Academium	[A.5] Modificación del código fuente de la aplicación [I.3] Servicio del Apache no arranca	Acceso libre al servidor de aplicación. Nuevas actualización en el código fuente Mala configuración del apache.
HW-001	Servidor	[I.4] Falla o avería del hardware por apagones de luz. [N.1] Incendio [N.2] Daño por agua [N.3] Desastres naturales	Apagones por motivo externos del proveedor. Acceso libre al servidor de la base de datos. Fuga de agua por tuberías. Ausencia de diseño antisísmico del centro de datos.
AUX-001	Cortafuego	[A.6] Acceso no autorizado [I.5] Falla del sistema operativo [I.4] Falla o avería del hardware por apagones de luz.	Falta de control de los accesos a los usuarios. Sistema operativo obsoleto. Apagones por motivo externos del proveedor.
COM-001	Red LAN	[I.6] Caída de la red por hardware. [A.7] Acceso no autorizado a la red [A.8] Envío erróneo de paquetes de internet	Desgastes del equipo por motivo natural. Falta de restricción de privilegios en la red. Falta de control de envío y recepción de paquetes.

S-001	Autorización de facturas y notas de créditos al SRI.	[A.9] No se pueda autorizar ni enviar por correo. [E.7] La información no es la correcta	Mala configuración de los iptables. Alteración de la información.
S-002	Envío de las facturas y notas de créditos por correo.	[A.9] No se pueda autorizar ni enviar por correo. [E.7] La información no es la correcta	Mala configuración de los iptables. Alteración de la información.
S-003	Envío de los roles de pagos por correo.	[A.9] No se pueda autorizar ni enviar por correo. [E.7] La información no es la correcta	Mala configuración de los iptables. Alteración de la información.

4.7 VALORACIÓN DE LAS AMENAZAS

Las amenazas no siempre provocan el mismo efectos en las dimensiones de valoración de un activo, para ello debemos determinar que tanto perjudica la amenaza a un activo y una forma de hacerlo es estimando la frecuencia de ocurrencia y el porcentaje de degradación.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

- Probabilidad de Ocurrencia
- Porcentaje de Degradación

La probabilidad de ocurrencia se modela de manera cualitativamente por medio de la siguiente escala nominal:

Tabla 7. Probabilidad de ocurrencia

	Valor	Rango	Vulnerabilidad
MA	5	Muy frecuente	A diario
A	4	Frecuente	Mensualmente
M	3	Normal	Una vez al año
B	2	Poco frecuente	Cada varios años
MB	1	Muy poco frecuente	Siglos

En cambio que el impacto tiene la siguiente escala:

Tabla 8. Degradación del valor

Valor	Rango
1	Muy bajo
2	Bajo
3	Media
4	Alto
5	Muy alto

4.8 EVALUACIÓN DE RIESGO

Identificado los activos, las amenazas y las vulnerabilidades que ocurren en la institución se procede a calcular el riesgo.

El riesgo se calcula tomando la probabilidad de ocurrencia de una amenaza por el valor del impacto de la materialización de una amenaza sobre un activo.

$$\text{Riesgo} = \text{Probabilidad} * \text{Impacto}$$

Para entender los riesgos vamos a usar la siguiente tabla:

Tabla 9. Niveles de aceptación del riesgo

Valor	Riesgo
0 - 5	Despreciable
6 - 10	Bajo
11 - 15	Medio
16 - 20	Alto
21 - 25	Muy alto

Tabla 10. Evaluación de riesgo

Código	Activo	Amenaza	Probabilidad	Impacto	Riesgo
D-001	Respaldo de la base de datos	[E.1] Deterioro del archivo de respaldo de la base de datos	2	3	6
D-002	Respaldo del código fuente de Academium	[E.1] Deterioro del archivo de respaldo	2	3	6
D-003	Información académica	[A.1] Robo de la información.	3	5	15
		[A.2] Manipulación de la información académica	4	5	20
		[E.2] Acceso sin permiso a la información	4	4	16
D-004	Información financiera	[A.1] Robo de la información.	3	5	15
		[A.2] Manipulación de la información académica	4	5	20
		[E.2] Acceso sin permiso a la información	4	4	16
D-005	Información del personal	[A.1] Robo de la información.	3	5	15
		[A.2] Manipulación de la información académica	4	5	20
		[E.2] Acceso sin permiso a la información	4	4	16
D-006	Información financiera de los padres de familia	[A.1] Robo de la información.	3	5	15
		[A.2] Manipulación de la información académica	4	5	20
		[E.2] Acceso sin permiso a la información	4	4	16
D-007	Base de Datos de Academium	[A.1] Robo de la información.	1	5	5
		[A.3] Acceso no autorizado	2	5	10
SW-001	Motor de base de datos	[I.1] Servicio del MySQL no arranca	2	5	10
		[E.3] Manipulación del archivo de configuración	1	5	5
SW-002	Sistema operativo del Servidor	[E.4] Inestabilidad en el sistema operativo por	3	4	12

		mantenimiento o actualización.			
		[I.2] Avería a nivel de hardware o software	1	4	4
		[E.5] Envío de información no autorizada desde el servidor	5	4	20
		[E.6] Acceso sin restricción a los usuarios	4	4	16
		[A.4] Acceso no autorizado al servidor	4	5	20
SW-003	Sistema Web - Academium	[A.5] Modificación del código fuente de la aplicación	4	4	16
		[I.3] Servicio del Apache no arranca	2	5	10
HW-001	Servidor	[I.4] Falla o avería del hardware por apagones de luz.	3	5	10
		[N.1] Incendio	1	5	5
		[N.2] Daño por agua	1	5	5
		[N.3] Desastres naturales	1	5	5
AUX-001	Cortafuego	[A.6] Acceso no autorizado	1	3	3
		[I.5] Falla del sistema operativo	2	3	6
		[I.4] Falla o avería del hardware por apagones de luz	1	3	3
COM-001	Red LAN	[I.6] Caída de la red por hardware.	3	5	15
		[A.7] Acceso no autorizado a la red	3	4	9
		[A.8] Envío erróneo de paquetes de internet	5	3	15
S-001	Autorización de facturas y notas de créditos al SRI.	[A.9] No se pueda autorizar ni enviar por correo.	3	4	9
		[E.5] La información no es la correcta	3	5	15
S-002	Envío de las facturas y notas de créditos por correo.	[A.9] No se pueda autorizar ni enviar por correo.	3	4	12
		[E.5] La información no es	3	5	15

		la correcta			
S-003	Envío de los roles de pagos por correo.	[A.9] No se pueda autorizar ni enviar por correo.	3	4	12
		[E.4] La información no es la correcta	3	5	15

CAPÍTULO 5

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1 ELABORACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO.

La gestión de riesgo permite analizar todas las amenazas que pueden ocurrir en la institución y tomar las mejores decisiones para mitigarlas.

Después de identificar las amenazas y de realizar la evaluación de riesgos, se elabora un plan de tratamiento de riesgos, que consiste en seleccionar los controles necesarios para prevenir y evitar los riesgos.

Existen 4 estrategias para realizar el tratamiento del riesgo:

- Reducir

Seleccionar e implementar los controles adecuados a fin de disminuir los riesgos.

Para reducir los riesgos los controles deben evitar que una vulnerabilidad sea explotada por alguna amenaza.

La selección de los controles se lo puede hacer revisando el Anexo A de la norma ISO 27001-2013

- Transferir

Cuando el riesgo es difícil de hacerlo aceptable, es recomendable transferirlo a una tercializadora o aseguradora.

El ente externo tendrá que aplicar los controles pertinentes para volver el riesgo a un nivel aceptable.

- Evitar

Es la acción de cambiar las actividades de negocio o cambiar la forma en que se lleva un proceso, con el fin de evitar la ocurrencia del riesgo.

Para cambiar una actividad, antes debe haber un mutuo acuerdo con el departamento involucrado de la actividad.

- Aceptar

Cuando el riesgo no puede ser reducido por la aplicación de controles y su costo es demasiado alto para la implementación, entonces debemos aceptar el riesgo.

Deben existir criterios de aceptación de riesgos para poder clasificar, pero antes estar de acuerdo con la gerencia.

5.2 IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO.

5.2.1 SELECCIÓN DE CONTROLES BASADOS EN LA NORMA ISO 27001

Los controles seleccionados o salvaguardas deben enfocarse a las estrategias del plan de tratamiento de riesgo, para hacer frente a las amenazas a las está expuesta la institución.

El objetivo de las salvaguardas es mitigar los riesgos, reduciendo las frecuencias de las amenazas y limitando el daño que esta causa.

Del anexo A de la norma ISO 27001-2013 vamos a escoger los controles que nos ayudara a mitigar y controlar los riesgos existentes.

Ver Anexo B "Selección de controles basados en la norma ISO 27001-2013"

Después de implementar los controles seleccionados y mitigar los riesgos latentes en la organización, debemos enfocarnos en los riesgos residuales. Estos riesgos residuales son aquellos que a pesar de haber implementado los controles no se lo puede mitigar del todo.

Los riesgos residuales deben ser reducidos de forma que se conviertan en riesgos aceptables para la institución.

Los riesgos residuales deben ser debidamente documentados e informados por la gerencia para conocimiento general.

5.3 DECLARACIÓN DE APLICABILIDAD DE LOS CONTROLES SELECCIONADOS

La declaración de aplicabilidad debe tener los objetivos de control y controles que se han escogido del Anexo A de la norma para el establecimiento del SGSI.

Tabla 11. Declaración de aplicabilidad

Control Anexo A ISO 27001-2013	Objetivo de control	Aplicabilidad	Justificación
A.5 Políticas de la seguridad de la información			
A.5.1.1	Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	SI	Se debe definir un manual de políticas de seguridad de la información para la institución. Este manual debe ser aprobada por la gerencia y se socializado a los empleados dentro de la institución.
A.5.1.2		SI	Las políticas del manual deben ser revisadas y actualizadas periódicamente para agregar algún control que nos ayude a la continuidad del negocio.
A.6 Organización de la seguridad de la información			
A.6.1.1	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	SI	Definir un responsable que estará a cargo de toda la seguridad de la información (dueños de los activos, usuarios, etc.)
A.6.1.2		SI	Los roles y responsabilidades deben estar claramente definidos y documentados para que no haya un uso indebido del activo.
A.6.1.3		SI	Mantener contacto con las autoridades responsables de la seguridad de la información.
A.6.1.4		SI	Mantener contactos con el especialista o ingeniero de seguridad para cualquier consulta o

			novedad que se presente en la institución.
A.6.1.5		SI	Todo proyecto de nivel informático debe seguir las políticas de seguridad de la información.
A.7 Seguridad de los recursos humanos			
A.7.1.1	Asegurar que los empleados y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran.	SI	Antes de la contratación de un nuevo empleado, se debe revisar sus antecedentes según el reglamento interno y proporcionarle solo la información que tendrá va a tener disponible.
A.7.1.2		SI	Establecer responsabilidades sobre la seguridad de la información, definidos en el acuerdo contractual para los empleados o contratistas.
A.7.2.1		SI	La gerencia debe exigir que se cumplan las políticas de seguridad a sus empleados y contratistas.
A.7.2.2	Asegurar de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	SI	Se debe explicar o capacitar a los empleados o contratistas sobre las políticas de seguridad de la información.
A.7.2.3		SI	Si existe alguna contravención sobre las políticas de seguridad se deberá seguir el reglamento internos sobre la sanción.
A.7.3.1	Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	SI	Si un empleado o contratista sale de la institución, se debe deshabilitar su usuario y cualquier acceso al activo que tenía a su cargo.
A.8 Gestión de activos			
A.8.11		SI	Identificar los activos de información y realizar un inventario.
A.8.1.2	Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.	SI	Definir un propietario por cada activo.
A.8.1.3		SI	Identificar, documentar e implementar el uso de la información y de los activos asociados.
A.8.2.1	Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su	SI	Clasificar la información en función a su disponibilidad, criticidad e integridad.
A.8.2.2		SI	Crear procedimientos para el

	importancia para la organización.		etiquetado de la información de acuerdo a su clasificación
A.9 Control de acceso			
A.9.1.2	Limitar el acceso a información y a instalaciones de procesamiento de información.	SI	Se debe definir políticas de control de acceso a los usuarios de la red y a los empleados que tenga que usar algún servicio en la institución.
A.9.2.1	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios	SI	Establecer políticas de gestión de usuarios, para la asignación de usuario y mantenimiento.
A.9.2.3		SI	Definir perfiles de acceso para cada usuario.
A.9.3.1	Hacer que los usuarios rindan cuentas por las salvaguardas de su información de autenticación.	SI	Los usuarios deben seguir la política del cambio de contraseña. Esta política debe establecer las reglas que debe cumplir como la longitud mínima y el tipo de caracteres permitidos.
A.9.4.1	Evitar el acceso no autorizado a sistemas y aplicaciones	SI	Definir perfiles de usuario a las aplicaciones.
A.9.4.2		SI	Toda aplicación debe tener la opción de ingresar por medio de un usuario y contraseña.
A.9.4.3		SI	Habilitar el cambio de contraseña después de un periodo de tiempo.
A.11 Seguridad física y del entorno			
A.11.1.1	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	SI	La infraestructura del centro de datos debe cumplir con los requerimientos mínimos de seguridad y el acceso debe estar controlado por un sistema de acceso.
A.11.1.4		SI	La gerencia debe diseñar planes para la protección física de los servidores en caso de algún desastre natural.
A.11.2.3	Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.	SI	El cableado eléctrico de los equipos debe brindar la seguridad pertinente para cualquier eventualidad.
A.11.2.4		SI	Los equipos deben tener un mantenimiento programado para asegurar la disponibilidad e

			integridad del servicio o de los datos.
A.12 Seguridad de las operaciones			
A.12.1.2	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	SI	Los cambios de configuración deben ser ejecutados en un ambiente de prueba siguiendo el procedimiento establecido en las políticas de seguridad. Una vez probado deben ser documentados y pasados a producción.
A.12.2.1	Asegurar de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	SI	Revisar periódicamente las capacidades del servidor y de los servicios que la institución maneja.
A.12.3.1	Proteger contra la pérdida de datos.	SI	Se debe establecer políticas de respaldos de la base de datos y de la aplicación. Esta política debe comprender que los respaldos deben ser almacenados en dispositivos extraíbles.
A.12.4.1	Registrar eventos y generar evidencia.	SI	Registrar todas las transacciones que el usuario realiza en las aplicaciones.
A.12.4.3		SI	Guardar en los log del servidor cualquier modificación a los archivos de configuración.
A.12.6.1	Prevenir al aprovechamiento de las vulnerabilidades técnicas.	SI	La configuración de los iptables en el servidor debe ser probados en un servidor de pruebas y solo dar permisos a los puertos necesarios evitando los ataques externos.
A.12.6.2		SI	La instalación de nuevos software debe ser restringido y solo el departamento de sistema debe instalar el nuevo software después de haberlo revisado.
A.12.7	Minimizar el impacto de las actividades de	SI	Definir un plan de control de auditoría que no afecte en los

	auditoría de sistemas de información.		horarios laborales en donde el sistema tiene mayor demanda.
A.13 Seguridad de las comunicaciones			
A.13.1.1	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	SI	La red LAN de la institución debe contar que los requerimientos mínimos de seguridad.
A.13.1.2		SI	Identificar los mecanismos de seguridad de la infraestructura de red de la institución.
A.13.1.3		SI	Identificar las diferentes subredes que tienen la institución y las medidas de protección que tiene cada subred.
A.13.2.1	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	SI	La información enviada a través del web services debe ser correcta y no tener perdida en el proceso de transferencia.
A.13.2.3		SI	El envío de las facturas por medio de la mensajería electrónica debe contar con los seguridades apropiadas de acuerdo a los establecido en las políticas de seguridad.
A.14 Adquisición, desarrollo y mantenimiento de sistemas			
A.14.2.2	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	SI	Se debe implementar una política de gestión de cambios en la aplicación, este requiere que los cambios realizados deban ser probados en servidores de prueba y después pasarlos a producción.
A.14.2.3		SI	Se debe implementar políticas al momento de cambiar de servidor. Antes de realizar cualquier actualización o cambio de plataforma debemos realizar las pruebas necesarias, evitando el riesgo de la disponibilidad de los servicios en producción.
A.14.2.4		SI	Las actualizaciones o cambios de paquetes de software deben ser probados en servidores de prueba antes de pasarlo a producción.
A.14.2.6		SI	Establecer ambiente de pruebas en

			donde se puedan realizar cualquier actualización o modificación.
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			
A.17.1.1	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	SI	La institución debe planificar procesos para continuidad de negocio. Estos procesos deben estar alineados con las políticas y cumplir los requerimientos de la seguridad de la información.
A.17.1.2		SI	Desarrollar un proceso para la continuidad de negocio en casos de desastres o amenazas.
A.17.2.1	Asegurar la disponibilidad de instalaciones de procesamiento de información.	SI	Implementar planes de restauración asegurando la continuidad del negocio y la disponibilidad.
A.18 Cumplimiento			
A.18.1.3	Cumplimiento de requisitos legales y contractuales.	SI	Proteger los registros ante pérdida, destrucción y falsificación.
A.18.1.4		SI	Asegurar la protección y privacidad de los datos como lo exigen el reglamento interno y las cláusulas contractuales.

5.4 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD

Una vez realizado el análisis y escoger los controles para mitigar los riesgos a los que está expuesto el ERP Academium, vamos elaborar un manual de políticas de seguridad.

Las políticas de seguridad vana mitigar todas las vulnerabilidades encontradas en el análisis que hemos realizado en los capítulos anteriores.

El objetivo de las políticas es que el personal de la institución se comprometa con el proceso de seguridad.

5.4.1 POLÍTICAS Y NORMAS INTERNAS

Para el desarrollo de las políticas y normas se va a estructurar en base a los siguientes criterios:

- Políticas Generales.
- Políticas de seguridad a nivel físico.
- Actualización de paquetes del Sistema Operativo
- Políticas de seguridad a nivel lógico.
- Políticas de respaldos y recuperación de información.
- Políticas de mantenimiento de equipos.
- Políticas de uso del ERP Academium.

5.4.2 POLÍTICAS GENERALES

- Toda persona que ingresa a la UE Javier, debe tener una inducción sobre las políticas de seguridad, la utilización de recursos y el uso de los activos de la información.
- También aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.
- Todo el personal nuevo de la UE Javier, deberá ser notificado al Departamento de Sistemas, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para

la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del empleado, anular y cancelar los derechos otorgados como usuario informático.

- Llevar un inventario de todos los activos indispensables para la institución, cada activo debe tener un responsable y deberá ser parte de los procesos de negocio.
- Este inventario debe ser actualizado para cada periodo lectivo.
- Toda información que sea producida por el personal de la institución es de propiedad de la institución.
- Los usuarios solo puede manipular la información que tienen acceso, tal como lo estimula su contrato. Y es responsable de las acciones que están causan.
- Todo incidente o problema con el ERP Academium debe ser reportado al Departamento de Sistemas vía correo electrónico o telefónica.
- Al momento que el usuario se aleje de su computadora por un periodo de tiempo, la sesión de Windows debe bloquearse.
- Es responsabilidad del usuario evitar en todo momento la fuga de información de la UE Javier, que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

5.4.3 POLÍTICAS DE SEGURIDAD A NIVEL FÍSICO

- Está prohibido ingresar un Equipo Informático de Terceros sin contar con la autorización correspondiente de parte del Rector o del Coordinador de Sistemas.
- La instalación de un equipo informático de propiedad de Terceros dentro de la Institución deberá contar con la aprobación del Coordinador de Sistemas.
- El Centro de Cómputo de la UE Javier es un área restringida, por lo que solo el personal autorizado por el Departamento de Sistemas y el Rector puede acceder a él.
- El Coordinador del Departamento de Sistemas deberá llevar un registro escrito de todas las visitas autorizadas a los Centros de Cómputo restringidos.
- Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar malestar en sus actividades.
- Todo personal que tenga acceso al centro de datos debe contar con su tarjeta de identificación.
- El acceso al centro de datos será limitado, solo el personal autorizado y con previa autorización del coordinador o responsable del Departamento de Sistemas de la institución.
- Debe haber extintores contra fuego dentro y fuera del centro de datos.

- Todos los servidores deben estar conectados a una red de alimentación de energía ininterrumpida(UPS)
- Se prohíbe el ingreso de alimentos o bebida dentro del centro de datos.
- Todo equipo sea local o portátil debe estar conectado a la red de la institución para asignarle los accesos respectivos en la red.

5.4.4 ACTUALIZACIÓN DE PAQUETES DEL SISTEMA OPERATIVO

- Se debe mantener un esquema de actualización de las herramientas y del kernel del sistema operativo.
- El esquema de actualización consiste en tener una réplica del servidor de producción al cual vamos a probar las nuevas actualizaciones y ver su desarrollo. Una vez que haya pasado el periodo de pruebas se podrá certificar los paquetes a instalar en el servidor de producción.

5.4.5 POLÍTICAS DE SEGURIDAD A NIVEL LÓGICO

- Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la UE Javier, que no esté autorizado por el Departamento de Sistemas.
- Los usuarios de la UE Javier no deben establecer redes de área local, conexiones remotas a redes internas o externas,

intercambio de información con otros equipos de cómputo utilizando carpetas compartidas o el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la UE Javier, sin la autorización del Departamento de Sistemas y el Rector.

- Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Departamento de Sistemas, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la UE Javier, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.
- Todas las computadoras deben tener instalado un software antivirus empresarial.
- Se debe verificar las actualizaciones de las bases de datos del antivirus en cada computadora.
- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y notificar al Departamento de Sistemas para la revisión y erradicación del virus.
- Los equipos con sistema operativo Windows debe tener activo el firewall para mitigar ataques externos.
- La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

- Las contraseñas deben tener al menos 3 referencias: números, letras mayúsculas, letras minúsculas, caracteres especiales y una longitud mínima de 8 caracteres.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlo.
- Al finalizar cada periodo lectivo, se hace un respaldo de la información de todas las computadoras que son utilizadas por los docentes y debe ser almacenada en el File Server.
- No usar contraseñas similares para acceder a otros sistemas como el correo electrónico o para acceder al equipo.
- Utilizar herramientas como iptables para realizar el filtrado de paquetes de acuerdo a las direcciones IP y puertos.
- Los servicios innecesarios que están instalados en el servidor por defecto deben ser deshabilitado.
- Revisar periódicamente las auditorias del servidor y de los servicios, manteniendo un esquema de revisión:
 - Accesos y permisos a los archivos y directorios
 - Acceso a los usuarios
 - Contraseñas de usuarios

5.4.6 POLÍTICAS DE ACCESO

- Los accesos al servidor debe seguir una política de acceso y usuarios seguros.

- Los usuarios con acceso al Shell deben tener contraseñas complejas y ser cambiadas periódicamente.
- Crear usuarios no root y otorgarle los permisos de acuerdo a las tareas que realizaran.
- Usar el usuario root para ejecutar comandos privilegiados.
- Utilizar el protocolo SSH para realizar conexiones entrantes y salientes de manera segura.

5.4.7 POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

- Realizar un cronograma de respaldos de la base de datos y de la aplicación Academium.
- Los respaldos de la base de datos se realizaran dos veces en el día
- El respaldo de la aplicación se realizaran dos veces por mes.

5.4.8 POLÍTICAS DE MANTENIMIENTO DE EQUIPOS

- Antes de encender la computadora verifique que esté en buenas condiciones.
- Si nota que el equipo presenta algún desperfecto, notifíquelo al Departamento de Sistemas.
- Al finalizar la jornada de trabajo, debe apagar el equipo y no dejarlo en estado de hibernación o suspensión.
- No consumir bebidas o comer en frente de la estación de trabajo.

- Las computadoras deben estar protegido por UPS para contrarrestar los apagones y picos de voltaje.
- El mantenimiento correctivo de las computadoras lo debe realizar el personal del Departamento de Sistemas.
- Cada nuevo periodo lectivo se debe realizar un mantenimiento preventivo a todas las computadoras.

5.4.9 POLÍTICAS DE USO DEL ERP ACADEMIUM

- Todo usuario debe quedar registrado en la Base de Datos Usuarios y Roles. La creación de un nuevo usuario y/o solicitud para la asignación de otros permisos dentro del sistema de la UE Javier, deberá de venir acompañado del requerimiento y autorización del Coordinador de Recursos Humanos, de lo contrario no se le dará trámite a dicho requerimiento.
- El Departamento de Sistemas, en cabeza del Coordinador de Sistemas o su delegado en caso de ausencia, será la responsable de ejecutar los movimientos de altas, bajas o cambios de perfil de los usuarios mediante la respectiva Solicitud de Alta/Baja/Cambio.
- Para el uso del ERP Academium, debe ser abierto por Internet Explorer o por el Mozilla Firefox.
- Si se utiliza Internet Explorer debe activarse la Vista de Compatibilidad y agregar la dirección pública del sistema.

- El Departamento de Sistemas no se responsabiliza de los inconvenientes que tiene la aplicación cuando este es abierto con Google Chrome.
- Se debe borrar dos veces al mes el historial de navegación del explorador para que la aplicación no se demore en sus procesos.
- Antes de aplicar cualquier modificación o actualización en el Academium, esta debe ser probada en un ambiente de pruebas.
- Cada nuevo requerimiento debe ser notificado al Departamento de Sistemas, para revisarlo con las partes involucradas y definir tiempos de desarrollo.

CAPÍTULO 6

ELABORACIÓN DE CASO DE USO Y ANÁLISIS DE RESULTADOS

6.1 ELABORACIÓN DEL CASO DE USO.

En este capítulo elaboraremos un caso de uso al cual vamos a aplicar todos los controles antes mencionados en los capítulos anteriores, mitigando los riesgos latentes en los procesos críticos de la institución.

Aplicaremos el sistema de gestión de seguridad de la información que define una política de seguridad de la información.

6.2 HARDENING EN EL SERVIDOR DE ACADEMIUM.

El ERP Academium, es una aplicación web que originalmente fue instalado en un servidor con las características antes mencionadas.

- Sistema Operativo CentOS Linux Release 6.0 Versión 2.632.71.e16.x86_64 GNU_Linux
- Motor de base de datos MySql Versión 5.1.40
- PHP Versión 5.3.3
- Apache versión 5.0

El servidor se encuentra detrás de un firewall físico (Fortigate) que es monitoreado por el administrador de red de la institución y con soporte técnico de la compañía Telconet que también nos proporciona el servicio de Internet.

El servidor Academium cuenta con las mínimas configuraciones de seguridad que el proveedor de la aplicación ha realizado.

Pero debido a los diferentes ataques en meses anteriores y al continuo uso del servidor no solo para el sistema Academium sino para los demás aplicativos que se están llevando para el padre de familia. Debemos conocer todas las vulnerabilidades y aplicar los controles de la norma ISO.

6.3 ROLES Y RESPONSABILIDADES

El Departamento de Sistemas está encargado de hacer cumplirlas normas de seguridad, gestionando la protección de la información y de los recursos con los que cuenta el departamento.

Los roles designados que se responsabilizaran de la planificación e implementación de los controles de seguridad son:

- Coordinadora de IT, es el responsable de elaborar el manual de políticas de seguridad informática, siempre con supervisión y autorización del Rectorado.

6.4 IMPLEMENTACIÓN DE CONTROLES

Identificando las amenazas comenzaremos aplicar los siguientes controles descritos en los capítulos anteriores.

Tabla 12. Implementación de controles

Amenaza	Vulnerabilidad	Salvaguardas
[I.1] Servicio del MySQL no arranca	Mala configuración del archivo de configuración del MySQL	A.12.1.2 Gestión de cambios. A.12.4.3 Registros del administrador y del operador.
[E.4] Inestabilidad en el sistema operativo por mantenimiento o actualización.	Instalación de parches de software sin haberlo probados.	A.12.6.2 Restricciones sobre la instalación de software.
[E.5] Transferencia de información no autorizada desde el servidor	Instalación de paquetes sin previa inspección.	A.12.2.1 Controles contra códigos maliciosos. A.13.1.2 Seguridad de los servicios de la red.
[A.4] Acceso no autorizado al servidor	Mala configuración del iptables	A.12.6.1 Gestión de las vulnerabilidades técnicas. A.13.1.1 Controles de redes. A.13.2.1 Políticas y procedimientos de

		transferencia de información.
[A.5] Modificación del código fuente de la aplicación	Acceso libre al servidor de aplicación.	A.9.1.1 Política de control de acceso. A.14.2.2 Política de desarrollo. A.14.2.2 Procedimientos de control de cambios en sistemas.
[I.3] Servicio del Apache no arranca	Nuevas actualización en el código fuente. Mala configuración del apache.	A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. A.14.2.4 Restricción en los cambios a los paquetes de software. A.14.2.6 Ambiente de desarrollo seguro.
[I.5] Falla del sistema operativo	Sistema operativo obsoleto.	A.17.1.1 Planificación de la continuidad de la seguridad de la información. A.17.1.2 Implementación de la continuidad de la seguridad de la información.
[A.9] No se pueda autorizar ni enviar por correo.	Mala configuración de los iptables.	A.13.2.3 Mensajería electrónica.

6.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas aplicadas para mantener seguro al servidor fueron las siguientes:

Actualización de paquetes en el sistema operativo

- Se debe mantener un esquema de actualización de las herramientas y del kernel del sistema operativo.
- El esquema de actualización consiste en tener una réplica del servidor de producción al cual vamos a probar las nuevas actualizaciones y ver

su desarrollo. Una vez que haya pasado el periodo de pruebas se podrá certificar los paquetes a instalar en el servidor de producción.

Políticas de acceso

- Los accesos al servidor debe seguir una política de acceso y usuarios seguros.
- Los usuarios con acceso al Shell deben tener contraseñas complejas y ser cambiadas periódicamente.
- Crear usuarios no root y otorgarle los permisos de acuerdo a las tareas que realizaran.
- Usar el usuario root para ejecutar comandos privilegiados.
- Utilizar el protocolo SSH para realizar conexiones entrantes y salientes de manera segura.

Cortafuegos

- Utilizar herramientas como iptables para realizar el filtrado de paquetes de acuerdo a las direcciones IP y puertos.

Desinstalar servicios innecesarios

- Los servicios innecesarios que están instalados en el servidor por defecto deben ser deshabilitado.

Habilitar las auditorias

Revisar periódicamente las auditorias del servidor y de los servicios, manteniendo un esquema de revisión:

- Accesos y permisos a los archivos y directorios
- Acceso a los usuarios
- Contraseñas de usuarios

6.6 EVALUACIÓN Y DOCUMENTACIÓN DE LOS CONTROLES DE LA NORMA EN EL ERP

Siguiendo las recomendaciones de la norma ISO-27001 comenzaremos previniendo cualquier vulnerabilidad técnica que tenga el servidor.

Para ello adquirimos un nuevo servidor HP Proliant ML-350 G9 con un sistema operativo autónomo VMware ESXi Versión 6.0, el VMware nos va a permitir virtualizar el servidor **Academium**.

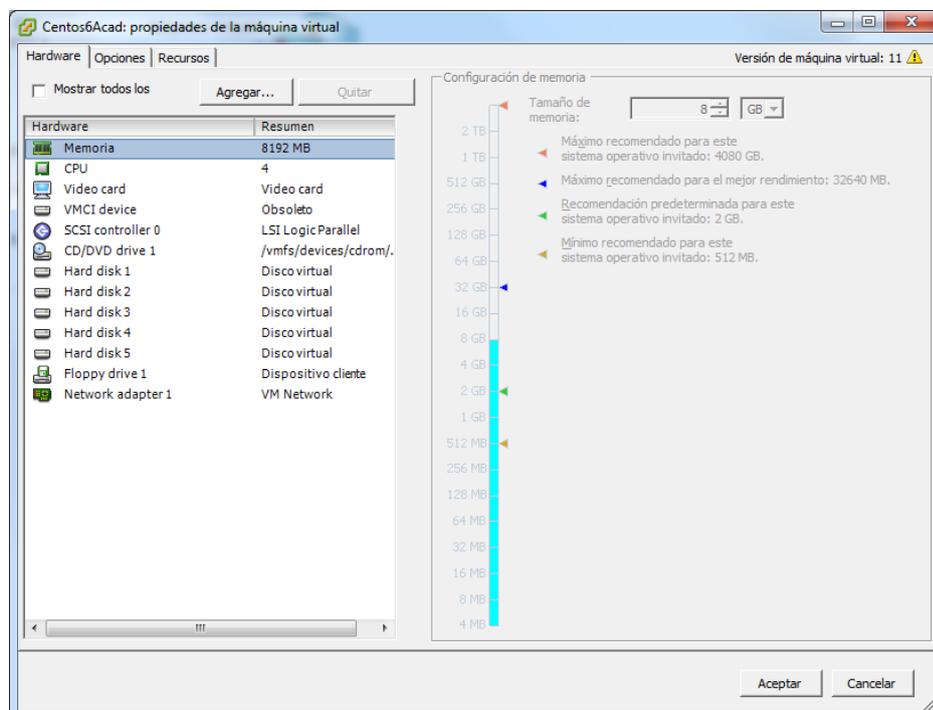


Figura 8.6. Recurso de Hardware para el servidor Academium

En servidor de Academium va a contar con el sistema operativo CentOS Linux 6.x, de 32 bits, esta distribución supera en funcionalidad a versiones más antiguas de CentOS.

Después de la instalación del CentOS, realizamos las actualizaciones del sistema operativo accionando el comando *yum update*, e instalamos el servidor http Apache 2.2.5 y PHP 5.6.30.

Con los nuevos controles aplicados en el archivo de configuración del apache se pudo mitigar las siguientes fallas de seguridad.

Ocultar la versión del apache.

Asegurarse que el servidor *httpd* se ejecute con el usuario apache.

Proteger el directorio Server Root, limitando los permisos de usuario.

Denegar el acceso a los directorios raíz y al contenido de los directorios. El servidor Academium tiene que mostrar contenido público dentro de la intranet.

Desactivación de ejecuciones de scripts CGI en cualquier directorio.

Impedir que los usuarios puedan modificar los archivos *.htaccess* los cuales pueden anular las configuraciones de seguridad que se han realizado.

Desactivación de módulos innecesarios que están instalados en el servidor.

Activación del modo seguro del apache, este módulo nos va ayudar a filtrar peticiones maliciosas recibidas por el servidor web.

Activación del módulo `mod_ssl`, protegerá el intercambio de tráfico entre el cliente y el servidor.

Las configuraciones de seguridad del servicio `mysql` fueron activadas ejecutando el `mysql_secure_installation`, este script se asegurara de establecer una contraseña al usuario administrador de la base de datos, eliminar el usuario anónimo y eliminar la base de datos de test.

Para controlar y mitigar las diferentes vulnerabilidades que tiene PHP es necesario realizar las configuraciones de varios parámetros, entre ellos tenemos:

Des habilitación de la salida de errores en las páginas web, ya que pueden revelar información sensible.

Asegurarse que las ejecuciones de script PHP solo estén contenidas en el fichero **`/var/www`**

Deshabilitar funciones específicas de PHP que pueden ser utilizados por atacantes para realizar inyección de código malicioso.

La configuración del `IPTABLES` se realizó tomando en cuenta los servicios y puertos que vamos a utilizar y se bloqueó los demás puertos que no necesitamos.

Con los nuevos controles aplicados al servidor hemos tenido una gran mejoría en el tráfico provocado por el servidor `Academium`, no existen los picos de información que enviaba anteriormente el antiguo servidor.

Para el nuevo periodo de matriculación 2017-2018, los directivos propusieron que tengamos un portal de matriculación en línea en donde los padres de familias tengan acceso al sistema para actualizar sus datos y del estudiante, dentro de sus funcionalidades el padre de familia puede realizar pagos en línea de la reserva de cupo.

El portal de matriculación se alimenta de la misma información que el ERP Academium y toda la información ingresada o modificada va a estar relacionada con el modulo académico y módulo de pensiones.

Para el desarrollo del portal de matriculación y de la funcionalidad del botón de pago, la institución financiera Pacificard solicito que el sitio web tenga instalado un Certificado Digital SSL emitida por una entidad autorizada.

Con ayuda de Security Data, se obtuvo el certificado digital, el cual se lo instalo en el dominio sistema.uejavier.com y con ello nos aseguramos que todas los sitios web dentro del servidor Academium este protegidos.

Y con los controles implementados de acuerdo a la norma ISO 27001, Pacificard certifico el sitio web de Matriculación en Línea como un sitio seguro para realizar transacciones

Ya estamos realizando el desarrollo para el botón de pago con la institución Diners Club Ecuador y por ende también vamos a ser validado por la institución como sitio seguro.

CONCLUSIONES Y RECOMENDACIONES

1. La información es el principal activo de información que una empresa debe resguardar y para ello se debe aplicarse todo tipo de salvaguardas para minimizar al máximo cualquier vulnerabilidad existente.
2. La información debe cumplir con tres principios fundamentales como son la integridad, confidencialidad e integridad, estos componentes nos va ayudar para realizar la gestión de seguridad de información.
3. Toda empresa que desea asegurar la información, debe seguir con un sistema de gestión eficiente que maneje sus recursos. Y en el caso de la Unidad Educativa Javier, se va a tomar la Norma ISO 27001, que nos va a proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

4. Para realizar el análisis de riesgos existen muchas metodologías en el campo de la gestión de riesgo. Magerit es la metodología que nos va ayudar para valorizar los activos que interactúan con el ambiente de la organización y sus dependencias determinando su vulnerabilidad e implementando los controles necesarios para la mejora y disminución de los riesgos.
5. Una vez determinado los riesgos a los que está expuesto el servidor de Academium, procedemos a buscar los mejores controles a aplicar, para ellos tomaremos el estándar ISO 27001-2013.
6. Antes de realizar la implementación de los controles, la directiva aprobó la compra de un nuevo servidor físico de mayores características, por lo que el sistema Academium fue migrado al nuevo servidor.
7. En el fortalecimiento del servidor web se realizó una búsqueda en varias páginas en internet y libros sobre seguridad informática.
8. Una vez aplicados los controles en el servidor y en el sitio web, vemos una gran mejoraría en el canal de internet. Ya no tenemos picos altos de información saliente del servidor y muchos de los protocolos que no son utilizados fueron inhabilitados.
9. La mayoría de los controles implementados son internos, por lo que los usuarios finales no perciben los cambios realizados.
10. Para el área académica, como es costumbre, antes de comenzar el año lectivo se realizó una explicación sobre las políticas de seguridad informática que tiene la institución, en donde se les enseña la importancia de seguir las políticas y normas de seguridad y el manejo seguro de sistema Academium.

11. Las nuevas políticas fueron acogidas sin problema por el personal académico.
12. Por último, fuimos certificados como sitio seguro, para realizar transacciones bancarias, esto fue porque se implementó el botón de pago para el sitio de matriculación en línea.

Recomendaciones

13. Realizar la concientización y divulgación de las políticas de seguridad al personal administrativo y docentes. Debemos crear una cultura en donde la seguridad de la información no se responsabiliza del área de sistema sino de la alta gerencia.
14. La institución debe tener en cuenta que la seguridad de la información es un proceso que nunca termina y siempre debe ser revisado y actualizado de manera continúa.
15. El departamento de sistema debe ser capacitado sobre temas de seguridad informática y que tenga en conocimiento de la Norma ISO 27001-2013, a fin de determinar posibles vulnerabilidades
16. Después de haber realizado el análisis de riesgos y obtener los controles de seguridad respectivos, estos deben ser implementados a la mayor brevedad posible.
17. Es recomendable que la institución tenga un plan de contingencia ante cualquier amenaza.

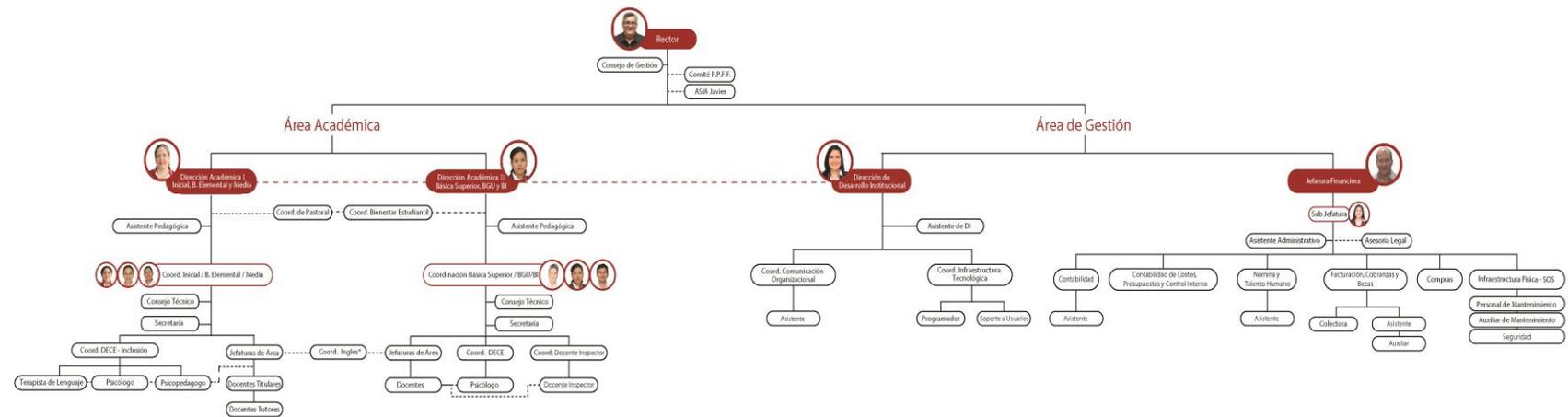
BIBLIOGRAFÍA

- [1] Wikipedia. (2016). Seguridad Informática. 12-08-2016, de Enciclopedia de la Seguridad Informática Sitio web
https://es.wikipedia.org/wiki/Seguridad_de_la_informacion.
- [2] aprenderaprogramar.com. ¿Qué es y para qué sirve un ERP? Software empresarial. SAP, Sage, Oracle, Microsoft Dynamics, Infor LN, etc. 12-08-2016, Sitio web.
http://aprenderaprogramar.com/index.php?option=com_content&view=article&id=889:ique-es-y-para-que-sirve-un-erp-software-empresarial-sap-sage-oracle-microsoft-dynamics-infor-ln-etc-&catid=57:herramientas-informaticas&Itemid=179
- [3] PriteshGupta.com. (2005). El portal de ISO 27001 en Español. 12-08-2016, Sitio web <http://www.iso27000.es/iso27000.html#seccion1>
- [4] Carlos Manuel Fernández. (2012). La norma ISO 27001 del Sistema de Gestión de la Seguridad Informática. 12-08-2016
- [5] Wikipedia. (2014). Magerit (metodología). 12-08-2016, Sitio web
[https://es.wikipedia.org/wiki/Magerit_\(metodología\)](https://es.wikipedia.org/wiki/Magerit_(metodología))
- [6] MAGERIT. (2016). Metodología de Análisis de Riesgos: Magerit. 12-08-2016, Sitio web <http://www.gr2dest.org/metodologia-de-analisis-de-riesgos-magerit>.
- [7] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.

ANEXO A

ORGANIGRAMA INSTITUCIONAL

ORGANIGRAMA



Simbología
 * Solo para los Jefes de Área de Inglés
 ---- Apoyo

ANEXO B

SELECCIÓN DE CONTROLES BASADOS EN LA NORMA ISO 27001-2013

Código	Activo	Amenaza	Vulnerabilidad	Salvaguardas
D-001	Respaldos de la base de datos	[E.1] Deterioro del archivo de respaldo de la base de datos	Respaldo inadecuado	A.12.3.1 Respaldo de la información.
D-002	Respaldo del código fuente de Academium	[E.1] Deterioro del archivo de respaldo	Respaldo inadecuado	A.12.3.1 Respaldo de la información.
D-003	Información académica	[A.1] Robo de la información.	Falta de controles de seguridad en la aplicación.	A.9.4.2 Procedimiento de ingreso seguro. A.9.3.1 Uso de información de autenticación secreta. A.12.4.1 Registros de eventos
		[A.2] Manipulación de la información académica	No existen una fortaleza en las contraseñas de los usuarios	A.9.4.3 Sistema de gestión de contraseñas.
		[E.2] Acceso sin permiso a la información	Restricción de accesos por los perfiles de usuario	A.9.2.3 Gestión de derechos de acceso privilegiados. A.9.4.1 Restricción de acceso a la información.
D-004	Información financiera	[A.1] Robo de la información.	Falta de controles de seguridad en la aplicación	A.9.4.2 Procedimiento de ingreso seguro. A.9.3.1 Uso de información de autenticación secreta. A.12.4.1 Registros de eventos
		[A.2] Manipulación de la información académica	No existen una fortaleza en las contraseñas de los usuarios	A.9.4.3 Sistema de gestión de contraseñas.
		[E.2] Acceso sin permiso a la información	Restricción de accesos a los perfiles de usuario	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.4.1 Restricción de acceso a la información.

D-005	Información del personal	[A.1] Robo de la información.	Falta de controles de seguridad en la aplicación	A.9.4.2 Procedimiento de ingreso seguro. A.9.3.1 Uso de información de autenticación secreta. A.12.4.1 Registros de eventos
		[A.2] Manipulación de la información académica	No existen una fortaleza en las contraseñas de los usuarios	A.9.4.3 Sistema de gestión de contraseñas.
		[E.2] Acceso sin permiso a la información	Restricción de accesos a los perfiles de usuario	A.9.2.3 Gestión de derechos de acceso privilegiados. A.9.4.1 Restricción de acceso a la información.
D-006	Información financiera de los padres de familia	[A.1] Robo de la información.	Falta de controles de seguridad en la aplicación	A.9.4.2 Procedimiento de ingreso seguro. A.9.3.1 Uso de información de autenticación secreta. A.12.4.1 Registros de eventos
		[A.2] Manipulación de la información académica	No existen una fortaleza en las contraseñas de los usuarios	A.9.4.3 Sistema de gestión de contraseñas.
		[E.2] Acceso sin permiso a la información	Restricción de accesos a los perfiles de usuario	A.9.2.3 Gestión de derechos de acceso privilegiados. A.9.4.1 Restricción de acceso a la información.
D-007	Base de Datos de Academium	[A.3] Acceso no autorizado	Mala administración en la creación de usuario y asignación de permisos	A.9.1.2 Acceso a redes y a los servicios en red A.9.2.1 Registro y cancelación del registro de usuarios. A.9.2.3 Gestión de derechos de acceso privilegiados.
SW-001	Motor de base de datos	[I.1] Servicio del MySQL no arranca	Mala configuración del archivo de configuración del MySQL	A.12.1.2 Gestión de cambios. A.12.4.3 Registros del administrador y del operador.
SW-002	Sistema operativo del Servidor	[E.4] Inestabilidad en el sistema operativo por mantenimiento o actualización.	Instalación de parches de software sin haberlo probados.	A.12.6.2 Restricciones sobre la instalación de software.
		[E.5] Transferencia de información no autorizada desde el servidor	Instalación de paquetes sin previa inspección.	A.12.2.1 Controles contra códigos maliciosos. A.13.1.2 Seguridad de los servicios de la red.

		[E.6] Acceso sin restricción a los usuarios	No existe una gestión de los usuarios del sistema operativo.	A.12.7 Controles de auditorías de sistema de información.
		[A.4] Acceso no autorizado al servidor	Mala configuración del iptables	A.12.6.1 Gestión de las vulnerabilidades técnicas. A.13.1.1 Controles de redes. A.13.2.1 Políticas y procedimientos de transferencia de información.
SW-003	Sistema Web - Academium	[A.5] Modificación del código fuente de la aplicación	Acceso libre al servidor de aplicación.	A.9.1.1 Política de control de acceso. A.14.2.2 Política de desarrollo. A.14.2.2 Procedimientos de control de cambios en sistemas.
		[I.3] Servicio del Apache no arranca	Nuevas actualización en el código fuente. Mala configuración del apache.	A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación. A.14.2.4 Restricción en los cambios a los paquetes de software. A.14.2.6 Ambiente de desarrollo seguro.
HW-001	Servidor	[I.4] Falla o avería del hardware por apagones de luz.	Apagones por motivo externos del proveedor.	A.11.1.1 Perímetro de seguridad física. A.11.1.4 Protección contra amenazas externas y ambientales. A.17.1.1 Planificación de la continuidad de la seguridad de la información. A.17.1.2 Implementación de la continuidad de la seguridad de la información. A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.
AUX-001	Cortafuego	[I.5] Falla del sistema operativo	Sistema operativo obsoleto.	A.17.1.1 Planificación de la continuidad de la seguridad de la información. A.17.1.2 Implementación de la continuidad de la

				seguridad de la información.
COM-001	Red LAN	[I.6] Caída de la red por hardware.	Desgastes del equipo por motivo natural.	A.11.2.3 Seguridad del cableado. A.11.2.4 Mantenimiento de equipos. A.13.1.1 Controles de redes.
		[A.7] Acceso no autorizado a la red	Falta de restricción de privilegios en la red.	A.13.1.2 Seguridad de los servicios de la red. A.13.1.3 Separación en las redes.
		[A.8] Envío erróneo de paquetes de internet	Falta de control de envío y recepción de paquetes.	A.13.2.1 Políticas y procedimientos de transferencia de información.
S-001	Autorización de facturas y notas de créditos al SRI.	[A.9] No se pueda autorizar ni enviar por correo.	Mala configuración de los iptables.	A.13.2.3 Mensajería electrónica.
		[E.7] La información no es la correcta	Alteración de la información.	A.18.1.3 Protección de registros. A.18.1.4 Privacidad y protección de información de datos personales.
S-002	Envío de las facturas y notas de créditos por correo.	[A.9] No se pueda autorizar ni enviar por correo.	Mala configuración de los iptables.	A.13.2.3 Mensajería electrónica.
		[E.7] La información no es la correcta	Alteración de la información.	A.18.1.3 Protección de registros. A.18.1.4 Privacidad y protección de información de datos personales.
S-003	Envío de los roles de pagos por correo.	[A.9] No se pueda autorizar ni enviar por correo.	Mala configuración de los iptables.	A.13.2.3 Mensajería electrónica.
		[E.7] La información no es la correcta	Alteración de la información.	A.18.1.3 Protección de registros. A.18.1.4 Privacidad y protección de información de datos personales.