

**Análisis de Riesgos de la Seguridad de la Información para la Institución
Universitaria Colegio Mayor Del Cauca**

**John Jairo Perafán Ruiz
Mildred Caicedo Cuchimba**

**Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería
Especialización en Seguridad Informática
Popayán
2014**

**Análisis de Riesgos de la Seguridad de la Información para la Institución
Universitaria Colegio Mayor Del Cauca**

**John Jairo Perafán Ruiz
Mildred Caicedo Cuchimba**

**Tesis de grado para optar por el título:
Especialista En Seguridad Informática**

**Asesor:
Francisco Solarte Solarte
Ingeniero de Sistemas**

**Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas Tecnología e Ingeniería
Especialización en Seguridad Informática
Popayán
2014**

Contenido

1	Introducción	13
2	Planteamiento Del Problema	14
2.1	Formulación Del Problema	14
3	Justificación	15
4	Objetivos.....	16
4.1	General.....	16
4.2	Específicos	16
5	Marco Referencial.....	17
5.1	Antecedentes.....	17
5.2	Marco Teórico.....	19
5.3	Marco Conceptual.....	24
5.4	Marco Contextual.....	29
5.4.1	Nombre De La Empresa.....	29
5.4.2	Reseña Histórica	29
5.4.3	Misión.....	29
5.4.4	Visión	29
5.4.5	Política De Calidad.....	29
5.4.6	Naturaleza Jurídica	30
5.4.7	Estructura Académico – Administrativa.....	31
5.5	Marco Legal.....	31
6	Diseño Metodológico	34
6.1	Investigación Aplicada	34
7	Informe Técnico	36
7.1	Activos De Información.....	38
7.2	Ethical hacking. Análisis de Vulnerabilidades	40
7.2.1	Evaluación De Vulnerabilidades	41
8.....		42
7.2.2	Mapa De Red	45
7.2.3	Mapa Software (S.I. Académico)	46

8.1	Resumen Informativo Y Funcional Sistemas De Información Sensibles	47
8.1.1	Sistema De Reserva De Salas De Reunión. (MRBS)	47
8.1.2	GLPI	47
8.1.3	Sistema De Información Académico Y De Gestión. (SIAG)	48
8.2	Resumen Del Diagnóstico De Servicios Más Relevantes	50
8.3	Análisis Y Evaluación De Riesgos Basado En Magerit V.3	52
8.3.1	Proceso P1: Planificación	53
8.3.2	Proceso P2: Análisis De Riesgos	54
8.3.3	Proceso P3: Estimación Del Estado De Riesgo	83
8.3.4	Interpretación De Los Resultados	88
9	Controles	91
9.1	Mecanismos De Control De Activos	92
9.2	Resumen De Controles	95
10	Políticas De Seguridad Informática	98
10.1	Seguridad Relacionada Al Personal	99
10.1.1	Funcionarios	99
10.1.2	Capacitación	99
10.1.3	Incidentes Y Atención A Usuarios	100
10.2	Seguridad Lógica	100
10.2.1	Control De Acceso	100
10.2.2	Administración De Acceso De Usuarios	101
10.2.3	Uso De Contraseñas	102
10.2.4	Responsabilidades De Los Usuarios	102
10.2.5	Uso Del Correo Electrónico	103
10.2.6	De Acceso A Terceros	103
10.2.7	De Acceso a La Red	104
10.2.8	De Backups	104
10.2.9	Servidores	105
10.2.10	Equipos De Cómputo	105
10.3	Responsabilidades Y Procedimientos Operativos	105
10.3.1	Protección Contra Software Malicioso	106
10.3.2	Mantenimiento	106

10.3.3	Control de Medios de Almacenamiento	106
10.4	Seguridad Física.....	106
10.4.1	De Los Equipos.....	106
10.5	Seguridad Legal	107
10.5.1	Licenciamiento De Software	107
11	Recomendaciones	108
12	Conclusiones.....	109
13	Bibliografía	110
14	Anexos	114
14.1	Anexo A: Clasificación De Los Activos	114
14.2	Anexo B : Valoración De Activos – Escala Estándar	115
14.3	Anexo C: Encuesta Aplicada	119
14.4	Anexo D: Catalogo De Salvaguardas	124
14.5	Anexo E: Valoración De Riesgos.....	128
14.6	Anexo D: Propuesta; Formato de Política De Seguridad.....	133

Lista de Tablas

Tabla 1. Evaluación de Vulnerabilidades	41
Tabla 2: Activos de información	55
Tabla 3: Escala de valoración activos	61
Tabla 4: Valoración activos tipo: aplicaciones	62
Tabla 5: Valoración activos tipo: servicios	64
Tabla 6: Valoración activos tipo: redes de comunicaciones.....	66
Tabla 7: Valoración activos tipo: equipamiento informático	66
Tabla 8: Valoración activos tipo: Equipamiento informático	68
Tabla 9: Valoración activos tipo: instalaciones	68
Tabla 10: Valoración activos tipo: personal	69
Tabla 11: Valor frecuencia de amenazas.....	71
Tabla 12: Valor degradación de amenazas	71
<i>Tabla 13: Valoración de Amenazas Tipo: Aplicaciones Informáticas.....</i>	<i>72</i>
Tabla 14: Valoración de Amenazas Tipo: servicios	73
Tabla 15 Valoración de Amenazas Tipo: redes de comunicaciones.....	74
Tabla 16: Valoración de Amenazas Tipo: equipamiento informático	75
Tabla 17: Valoración de Amenazas Tipo: equipamiento auxiliar	77
Tabla 18: Valoración de Amenazas Tipo: instalaciones.....	77
Tabla 19 Valoración de Amenazas Tipo: personal.....	78
Tabla 20: Salvaguardas: protecciones generales u horizontales	79
Tabla 21: Salvaguardas: protección de los datos/información	80
Tabla 22: Salvaguardas: Protección de los Servicios	81
Tabla 23: Salvaguardas: Protección de las aplicaciones (Software).....	82
Tabla 24: Salvaguardas Activos: Protección de los equipos (Hardware)	82
Tabla 25: Salvaguardas protección de las comunicaciones	83
Tabla 26: Valores estimación de impacto	84
Tabla 27: Valoración impacto en activos de información	85
Tabla 28: valores de frecuencia	86
Tabla 29: Criterios de valoración para estimación de riesgo	86
Tabla 30: Valoración de riesgo en activos de información.....	87
Tabla 31: Clasificación de controles	97
Tabla 32: Valoración de Riesgos	128
Tabla 33: Matriz de Riesgos	132

Lista de Figuras

Figura 1: Estructura de MAGERIT	23
Figura 2: Organigrama Institucional	31
Figura 3: Logo IUCMC	36
Figura 4: Ciclo mejora continua PHVA.....	36
Figura 5 : Diagrama de Interconexión general IUCMC	39
Figura 6: Interfaz Sistema de reservas	47
Figura 7: Interfaz GLPI en la institución	48
Figura 8: Módulo de Gestión Académica – SIAG.....	49
Figura 9: Evaluación de activos de la institución.....	49
Figura 10 : Tabla riesgo acumulado.....	50
Figura 11: Obtención registros DNS	51
Figura 12: Enumeración Sitio Web	51
Figura 13: Vulnerabilidades detectadas – Qualys online	52
Figura 14: Dependencia de activos tipo Aplicaciones informáticas.....	56
Figura 15: Dependencia de activos tipo servicios.....	56
Figura 16: Dependencia de activos tipo: equipamiento informático	57
Figura 17: Dependencia de activos tipo: Aplicaciones Informáticas	57
Figura 18: Dependencia de activos tipo Redes de comunicaciones	58
Figura 19: Recorrido Bottom-Up activos personal	58
Figura 20: Recorrido Bottom-Up activos Equipamiento informático.....	59
Figura 21: Recorrido Bottom-Up activos redes de comunicaciones.....	59
Figura 22: Recorrido Bottom-Up activos Equipamiento auxiliar	60
Figura 23: Recorrido Bottom-Up activos Instalaciones	60
Figura 24: Recorrido Bottom-Up activos Aplicaciones	61

1 Introducción

Hoy en día los sistemas de información son el alma de organizaciones, empresas y entidades, el grado de responsabilidad reposa en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantener teniendo una adecuada sistematización y documentación.

El tratamiento de la información abarca aspectos que van desde el manejo de documentos en medio físico como el proceso de almacenaje y recuperación conocido también como proceso de gestión documental, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, si existen, claro está, incluyendo además los sistemas físicos de protección y accesibilidad a sitios o áreas restringidas.

Es por esto que los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos; los equipos de cómputo almacenan información, la procesan y la transmiten a través de redes y canales de comunicación, abriendo nuevas posibilidades y facilidades a los usuarios, pero se deben considerar nuevos paradigmas en estos modelos tecnológicos y tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total es muy alto (aunque en la realidad no es alcanzable idealmente), y las organizaciones no están preparadas para hacer este tipo de inversión.

Se tiene la falsa percepción de que la seguridad de la información es una tarea imposible de aplicar, en realidad, con esfuerzo, el conocimiento necesario y el apoyo constante de las directivas se puede alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad propias.

La Institución Universitaria Colegio Mayor del Cauca es una entidad en crecimiento que debe involucrar dentro de sus procesos buenas prácticas encaminadas a la protección de la información; razón por la cual es necesario el desarrollo del análisis de riesgo de la seguridad de la información aplicado a cada uno de los activos de información.

El análisis de riesgo permite realizar un diagnóstico para conocer las debilidades y fortalezas internas encaminadas en la generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática que hacen parte de un Sistema de Gestión de Seguridad de la Información (SGSI), además de facilitar su continuo monitoreo a través de procesos de auditorías y mejoras continuas.

2 Planteamiento del Problema

La Institución Universitaria Colegio Mayor del Cauca, no tiene un sistema de seguridad de la información que permita la gestión de vulnerabilidades, riesgos y amenazas a las que normalmente se ve expuesta la información presente en cada uno de los procesos internos, no se tienen estandarizados controles que lleven a mitigar delitos informático o amenaza a los que están expuestos los datos comprometiendo la integridad, confidencialidad y disponibilidad de la información.

Existen procedimientos creados subjetivamente por iniciativa y experiencia de los miembros del equipo TIC; por ejemplo, no existe una política de uso de claves de usuario, en los servidores se realiza el cambio de claves de acceso a criterio del personal responsable de cada uno de ellos sin una periodicidad y bitácora definida; los administrativos y docentes no hacen uso de claves de acceso, por lo que cualquier persona puede tener acceso a los equipos de cómputo que se les ha asignado.

La Institución Universitaria tiene muchos inconvenientes dentro del manejo de la información debido a que ha ido creciendo paulatinamente y no se ha tomado conciencia de la importancia de asegurar la información existente; a medida que avanza es necesario adoptar y crear políticas que regulen las buenas prácticas en cada una de las transacciones, procesos y recursos relacionados con la información y para esto, es indispensable realizar el análisis de riesgos de la seguridad de la información, incluyendo los activos que directa e indirectamente están ligados a este proceso, como lo dicta la metodología Magerit.

De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de riesgos; muy seguramente en un futuro cercano podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento como lo pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros.

2.1 Formulación del Problema

¿Cómo identificar y tratar los riesgos que afecten la seguridad de la información de La Institución Universitaria Colegio Mayor del Cauca, con el fin de definir e implementar a futuro un Sistema de Gestión de Seguridad de la Información, mediante el análisis de riesgos?

3 Justificación

Hoy día la Institución Universitaria Colegio Mayor del Cauca, tiene una infraestructura tecnológica en crecimiento, de la cual dependen muchos de los procesos, dependencias y el funcionamiento tanto administrativo como académico. Gran parte de la información institucional, se encuentra en los equipos del personal administrativo y docente, otra parte en los buzones de correo, también existe información en formato físico y por último la que se encuentra almacenada en sistemas de información; pero se evidencia que no hay políticas de control que puedan proveer un adecuado tratamiento de este valioso activo como es la información sensible de la Institución Universitaria Colegio Mayor del Cauca.

En la actualidad las empresas y organizaciones de cualquier tipo de índole deben considerar dentro de sus planes de gobierno el aseguramiento de la información generando políticas y controles bien sea en busca de garantizar la continuidad del negocio o de una certificación como carta de presentación y de distinción ante la competencia. La institución Universitaria debe tomar conciencia de la necesidad de alinear sus objetivos institucionales, asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma.

Este es uno de los retos que debe asumir la institución para estar acorde a los modelos y estándares actuales; para ello es necesario empezar con la ejecución del análisis de riesgos de la seguridad de la información que en un futuro será la base para implementar el sistema de gestión de seguridad de la información (SGSI), que permitirá mantener un modelo de negocio estable logrando un valor agregado y posicionamiento a nivel regional.

Se debe tener un análisis de riesgos para la Institución Universitaria Colegio Mayor del Cauca con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos; teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos acorde a las directrices nacionales e internacionales que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas de seguridad y que de esta forma se logren los objetivos institucionales.

4 Objetivos

4.1 General

Realizar el análisis de riesgos que permita generar controles para minimizar la probabilidad de ocurrencia e impacto de los riesgos asociados con las vulnerabilidades y amenazas de seguridad de la información existentes en la Institución Universitaria Colegio Mayor del Cauca.

4.2 Específicos

- Identificar y clasificar los activos de información presentes en la Institución Universitaria Colegio Mayor del Cauca
- Aplicar una metodología de evaluación de riesgos que permita definir las vulnerabilidades y amenazas de seguridad existentes, y evaluar los riesgos de acuerdo a la escala definida por la metodología Magerit.
- Sugerir mecanismos de control y gestión que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.
- Elaborar un informe de recomendaciones donde se muestre los hallazgos que permita definir un Sistema de seguridad de la información ajustada a la realidad de la Institución Universitaria Colegio Mayor del Cauca.

5 Marco Referencial

5.1 Antecedentes

Partiendo de la necesidad de determinar el estado de seguridad de la información mediante un diagnóstico en la Institución Universitaria Colegio Mayor del Cauca y en vista de que actualmente se tiene una estructura institucional con la dotación y tecnología necesarias para desarrollarlas, se plantea realizar el análisis de riesgos a partir de la revisión de algunos antecedentes en la materia.

Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27000), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo ISM3); sin embargo, en la especificación de los mismos no se afronta su aplicación a un grupo empresarial, lo cual requiere consideraciones adicionales. Existe una metodología en implantación de un SGSI para un grupo empresarial jerárquico¹, en donde se describe la importancia de implantar un SGSI que permita dotar de seguridad todos los procesos productivos de las empresas de cualquier tipo y tamaño, muestra una metodología clara para realizar análisis de riesgo en un ambiente empresarial.

Muchos de los planteamientos y problemas en seguridad informática se encaminan a protegerse contra accesos no autorizados, pero este es un problema sencillo de resolver, ya que durante años se han desarrollado y perfeccionado algoritmos matemáticos para el cifrado de datos, para el intercambio seguro de información, para garantizar el correcto funcionamiento del software, que se ha

¹ PALLAS MEGA, Gustavo. Metodología de implantación de un SGSI en un grupo empresarial jerárquico. Universidad república de Montevideo (Uruguay), 2009.

traducido en herramientas capaces de proporcionar soluciones rápidas y sencillas a problemas técnicos de seguridad. Desafortunadamente, no es suficiente simplemente arreglar los errores o eliminar las fallas técnicas de seguridad. El problema va mucho más allá. La Seguridad Informática es un problema cultural, en el que el usuario juega un rol protagónico. La metodología para el aseguramiento de entornos informatizados - MAEI², resalta la importancia de tener una metodología clara para realizar un análisis de riesgos e identificar claramente vulnerabilidades, riesgos y amenazas presentes en los activos de información, ser gestionados y que permita optimizar los procesos organizacionales.

De igual forma también la existen lineamientos establecidos en la norma internacional UNE/ISO 27001, que establece las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). Esta norma establece un enfoque por procesos basado en el ciclo Deming, que plantea la gestión de la seguridad como un proceso de mejora continua, a partir de la repetición cíclica de cuatro fases como lo son planificar, hacer, verificar y actuar. Dentro de las especificaciones de la norma se establece un esquema documental del SGSI, que debe mantenerse actualizado, disponible y enmarcado en un índice, especialmente si la empresa desea superar un proceso de certificación, tal como lo describe un proceso de implantación de un SGSI³, el cual expone claramente los lineamientos que deben seguirse para implantar un Sistema de Gestión de Seguridad de la Información en un entorno real, describiendo el proceso para realizar el análisis de riesgo y sus fases futuras.

² BISOGNO, María Victoria. Metodología para el aseguramiento de entornos informatizados – MAEI. Buenos Aires – Argentina. Universidad de Buenos Aires, 2004.

³ AVILA ARZUZA, Maribel. Implantación de un SGSI. Barcelona- España - Universitat Oberta de Catalunya, 2012.

5.2 Marco Teórico

Seguridad de la Información

Se podría definir como seguridad de la información a un estado específico de la misma sin importar su formato, que nos indica un nivel o un determinado grado de seguridad de información, por ejemplo, que está libre de peligro, daño o riesgo, o por el contrario que es vulnerable y puede ser objeto de materialización de una amenaza. Las vulnerabilidades, el peligro o el daño de la misma es todo aquello que pueda afectar su funcionamiento directo y la esencia en sí de la información, o en su defecto los resultados que se obtienen de la consulta, administración o procesamiento de ella.

Garantizar un nivel de protección total es virtualmente imposible⁴, la seguridad de la información en la práctica a un nivel total o de completitud no es alcanzable porque no existe un sistema seguro al ciento por ciento. Existe un planteamiento denominado Desarrollo de una metodología para la auditoría de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la dirección provincial de pichincha del consejo de la judicatura⁵, donde se afirma que la información está expuesta a un mayor rango de amenazas y vulnerabilidades. “La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo de

⁴ ISO 2700. Sistema de gestión de seguridad de la información. Términos de uso información iso27000.es ©, 2012

⁵ PAREDES F. Geomayra y VEGA N. Mayra. Desarrollo de una metodología para la auditoría de riesgos Informáticos (físicos y lógicos) y su aplicación al Departamento de informática de la dirección provincial de pichincha del consejo de la judicatura. Provincia de Chimborazo- Ecuador Escuela Superior Politécnica De Chimborazo, 2011.

conversación”. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene⁶.

La seguridad de la información protege a una organización que la adopte como parte de su visión y misión de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los posibles daños y maximizar el retorno de las inversiones y sus las oportunidades. La información digital o en papel y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de la información es importante en negocios tanto del sector público como del privado para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos.⁷

Es necesario que exista seguridad en el activo más importante de la organización por las siguientes razones:

⁶ RUIZ L. Hernando. RESOLUCION 160-005326 Política de Seguridad de la información de la Superintendencia de Sociedades. 2008.

⁷ NTP-ISO/IEC 1779. Norma técnica Peruana. EDI, Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2007, p.8.

- ✓ Gran variedad de Riesgos y Amenazas: Fraudes, espionaje, sabotaje, vandalismo, incendio, inundación, hacking, virus, denegación de servicio, etc; Provenientes de múltiples fuentes.
- ✓ Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información interconectados.
- ✓ La mayoría de los sistemas de información no han sido diseñados para ser seguros.

Análisis de Riesgos Informáticos

Antes de definir lo que es el análisis de riesgos, tenemos que considerar lo que es un riesgo, a continuación se exponen las siguientes definiciones:

Según Fernando Izquierdo Duarte⁸: “El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos”.

Según Alberto Cancelado González: “El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas”.

Según Martín Vilches Troncoso⁹: “El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio.

⁸ IZQUIERDO D, Fernando. La administración y los riesgos. [en line]. EN: Maxitana C, Jennifer D. (Auditor en control de gestión). Tesis: Administración de riesgos de tecnología de información de una empresa del sector informático. Guayaquil – Ecuador: Escuela Superior politécnica del Litoral, 2005. P.39. http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-33960.pdf

⁹ VILCHES T, Martín. El riesgo [en line]. EN: Machuca C, John. (Magister en Contabilidad y Auditoría). Tesis Guía para la evaluación del sistema de riesgo operativo en la Cooperativa de Ahorro y Crédito Jardín Azuayo. Cuenca – Ecuador. Universidad de Cuenca, 2011. P.21. <http://dspace.ucuenca.edu.ec/bitstream/123456789/2729/1/tm4487.pdf>

Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado”.

Ahora bien el proceso de análisis de riesgos debe ser el más importante de la gestión de la seguridad de la información de una organización, de aquí parte la gestión de los riesgos, que es en últimas con la que se decide tomar la decisión de eliminarlos, ignorarlos, mitigarlos y controlarlos, es decir aplicar la gestión de riesgos basados en la compleja tarea de determinar, analizar, evaluar y clasificar los activos de información más importantes según la criticidad de los mismos.

Actualmente se han tratado de clasificar los diferentes tipos de riesgos para que sea más fácil la aplicación de un análisis de los mismos, entre los más comunes están los riesgos de negocios, inherentes, de auditoría, operativos y de control, profesionales y de tecnología entre otros. Además a nivel general se debe tener claro el objetivo del análisis de riesgo estableciendo a su vez una escala valorativa y con cierta regla de priorización de los mismos, luego de que se tiene una escala definida y los riesgos catalogados y organizados todo se debe condensar en una matriz que muestre realmente el nivel de impacto según nuestra escala de valoración, buscando establecer al final el estado actual en materia de seguridad de la información.

Metodología de Análisis de Riesgos

Son desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: Las cuantitativas y las cualitativas, de las que existen gran cantidad de ambas clases y sólo se centrará en la utilizada para el proyecto y caso de estudio específico en la Institución Universitaria. La metodología que el proyecto adopta es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información): El esquema completo de Etapas, Actividades y Tareas del Sub-modelo de Procesos

de MAGERIT¹⁰ el cual puede aplicarse o no en su totalidad, dependiendo de la complejidad misma del proyecto es el siguiente:

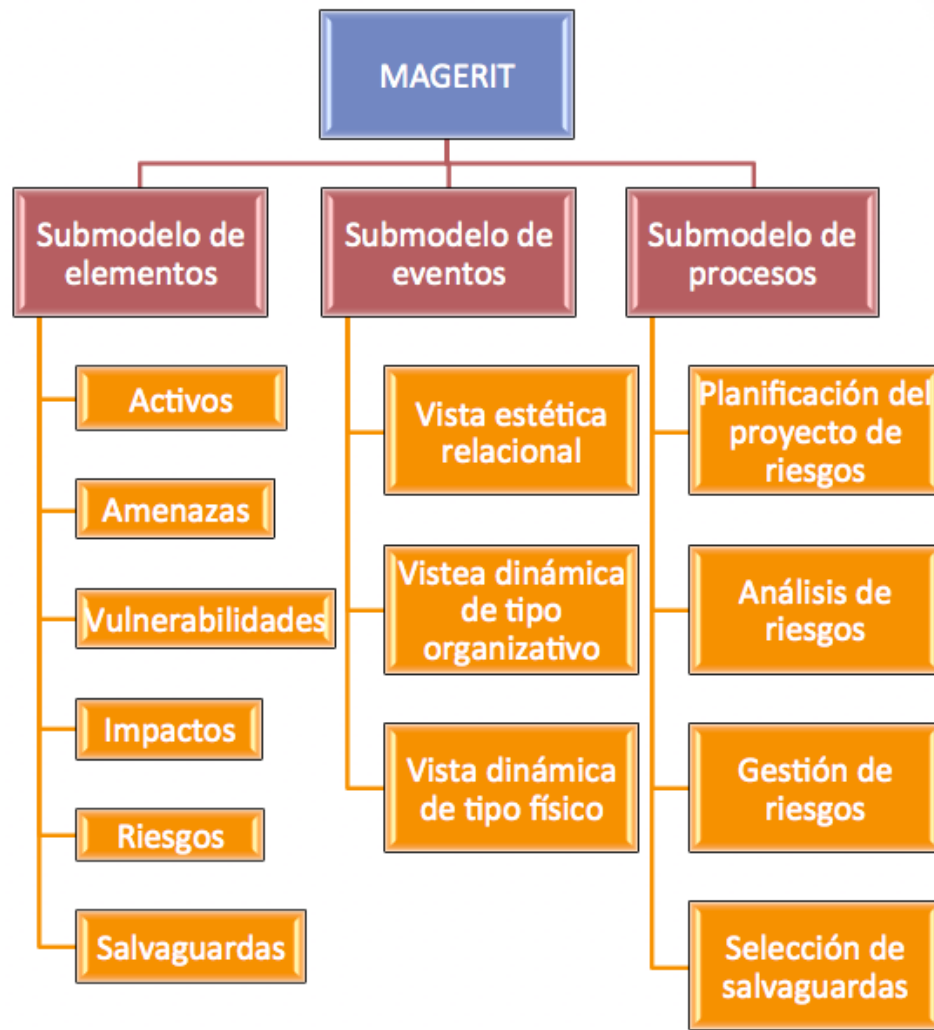


Figura 1: Estructura de MAGERIT

Auditoría Informática

La auditoría informática comprende gran variedad de conceptos, parámetros y normativas tendientes a mejorar procesos y procedimientos internos a nivel

¹⁰ BOLAÑOS, María C y ROCHA G. Mónica. 25 de marzo de 2014. Auditoría de SI. Magerit V3(Metodología de Analisis y Gestion de Riesgos de los Sistemas de Informacoin).[en línea]: <http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-analisis-y-gestin-de-riesgos-de-los-sistemas-de-informacion>.

organizacional, por medio de mecanismos de control interno; algunos métodos se basan en buenas prácticas de gobierno corporativo o la aplicación de transparencia en el actuar de las organizaciones vista como un activo más de la misma y encaminada o proyectada en términos de eficiencia corporativa.

Según el autor Fernando Pons en un artículo publicado en la revista nuevas tecnologías, En sus inicios, el auditor informático surge como un apoyo a los tradicionales equipos de auditoría. Su labor de apoyo consistía básicamente en la obtención de información financiera de los sistemas de información en los que residía y tratarla, con herramientas específicas para cantidades masivas de datos así facilitar la labor de los equipos de auditoría financiera.

Entre las grandes ventajas que el apoyo del auditor informático ofrecía era el dar la validación del total de la información revisada o auditada, en lugar de los habituales procedimientos de muestreo. Dicha labor continúa siendo hoy día una de las principales tareas del auditor informático. Actualmente es fácil encontrar auditores informáticos manipulando información para validar información compleja de obtener, tal como lo es la información del ámbito financiero, información académica en instituciones de educación superior, o en ámbitos productivos el de la amortización de inmovilizados o la valoración de existencias. Conforme el auditor, indaga y cuestiona o valora cada dato en un proceso organizacional va profundizando su conocimiento en la gestión de los negocios importantes de la organización y a su vez es capaz de plantear objetivos de control que tratarán de proteger la información en su totalidad o parcialmente de acuerdo a las funciones organizacionales y a la definición de límites de acuerdo a los niveles de criticidad de la información identificados por cada organización.

5.3 Marco Conceptual

El activo más importante que tiene una organización es la información y, por lo tanto, deben existir lineamientos claros que permitan su aseguramiento sin dejar

de lado la seguridad física aplicada a los equipos donde se encuentra almacenada.

Dichos lineamientos o técnicas están dadas por la seguridad lógica y aspectos de la seguridad física que permite la creación de barreras y procedimientos que resguardan la información y permiten el acceso a ella única y exclusivamente a personal autorizado.

Hoy en día existe en el mercado gran variedad de dispositivos electrónicos móviles como netbooks, computadores portátiles, tabletas, smartphones etc., convirtiéndose en blanco de posibles ataques y búsquedas de debilidades entre ellas, fraude electrónico, robo de identidad, denegación de servicios entre muchos otros.

La gestión de la seguridad debe ser planteada tanto en la parte lógica como física a través de los planes de contingencia, políticas de seguridad y aplicación de normativas.

Características de un Sistema Seguro:

Confidencialidad: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

Integridad: Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen. De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella

La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de ocurrencia de algún problema.

Otras características y conceptos que se relacionan con el proyecto y deben ser tenidos en cuenta por su composición teórica son los siguientes:

Control de acceso a los recursos: Se entiende como la regulación de quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Auditoría: Son los mecanismos para poder determinar qué es lo que está ocurriendo en el sistema, qué es lo que hace cada uno de los usuarios, los tiempos y fechas de dichas acciones.

Metodología de auditoría: Permite de una manera adecuada presentar una guía procedimental para que se efectúen tareas, actividades y tareas tendientes a realizar el proceso de revisión preliminar, revisión de controles, diagnósticos y comparación de estados actuales en materia de seguridad, finalizando con informes que presentan los resultados de la aplicación metodológica.

Magerit: Es un tipo de metodología que es una guía de referencia para realizar procesos de análisis de riesgos al igual que provee lineamientos para la gestión de riesgos en sistemas informáticos y todos los aspectos que giran alrededor de ellos en las organizaciones para lograr muchas de las metas planteadas al interior de las mismas y buscando cumplir las políticas de buen gobierno. El proyecto en mención se basa en esta metodología para poder efectuar el proceso de análisis de riesgos logrando identificar los activos, las amenazas, determinar tanto los riesgos como los impactos potenciales y se recomiendan como proceder a elegir las salvaguardas o contra medidas para minimizar los riesgos.

Papeles de trabajo: Hacen referencia al material de evidencia que el auditor maneja para recolectar datos o constancia escrita del trabajo que se está realizando, para este caso aplica la utilización de formatos.

SGSI¹¹: Un Sistema de gestión de la seguridad de la información, es como su nombre lo expresa un sistema que se encarga de proveer una cantidad de mecanismos y herramientas basados en la norma ISO 27001 y tiene por objetivo conocer al interior de la institución a los que puede estar expuesta la información, define como se deben gestionar los riesgos y debe ser un marco de referencia para la institución el cual debe ser conocido por todo el personal y debe estar sometido a una revisión y a un proceso de mejora constante.

Los anteriores aspectos deben ser tenidos en cuenta al momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto aspectos importantes para que así los usuarios y los sistemas realicen sus procedimientos de la mejor manera posible, de forma concreta y clara además se debe tener presente los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan las políticas para no generar un ambiente de tensión y/o agresión.

La seguridad informática esta creada para velar y proteger los activos informáticos, en aras de garantizar la integridad, disponibilidad y confidencialidad de los datos propios de una organización, independiente de su tamaño, tipo o razón social.

La información.

Es uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y personal capacitado, previendo que usuarios externos y no autorizados puedan acceder a ella sin autorización. Evitando que corra el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o

¹¹COLOMBIA. ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009.

que sea manipulada; llegando a obtener posteriormente datos erróneos e incompletos.

Dentro de esta variable se contempla la accesibilidad y disponibilidad funciones de la seguridad informática que permiten asegurar el acceso a la información y poder disponer de ella en el momento oportuno, incluyendo los backups para que en caso de que se presenten daños o pérdida de datos, producto de accidentes, atentados o desastres, se pueda subir una copia y evitar catástrofes organizacionales o suspensión de servicios, que en ocasiones trae como consecuencia altas pérdidas económicas.

La infraestructura computacional.

Parte esencial para gestionar, administrar y almacenar la información indispensable dentro del normal funcionamiento de la Institución. El papel que desempeña la seguridad informática en este punto es velar que el hardware (parte física) tengan un óptimo funcionamiento y logre evitar problemas relacionados con robo, incendios, desastres naturales, bloqueos, fallas en el suministro eléctrico, vandalismo, entre otros que lleguen a afectar directamente la infraestructura informática.

Los usuarios.

Son las personas que están directamente involucradas con la infraestructura tecnológica, comunicaciones y administradores de la información. La seguridad informática debe establecer normas que minimicen los riesgos tanto de información como de su infraestructura, dentro de dichas normas de debe contemplar, horarios de acceso, restricciones físicas y lógicas, permisos, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo esto debe estar regido por estándares y normas que minimicen los riesgos y el impacto en caso de llegar a presentar un siniestro.

5.4 Marco Contextual

5.4.1 Nombre de la Empresa

Institución Universitaria Colegio Mayor Del Cauca

5.4.2 Reseña Histórica¹²

La Institución Universitaria Colegio Mayor del Cauca es una Institución Pública, fundada bajo el Gobierno presidencial de Alberto Lleras Camargo con la LEY 48 DE 1945, por la cual se fomenta la creación de Colegios Mayores de Cultura Femenina.

En sus inicios se llamó "Colegio Mayor de Cultura Popular del Cauca", abre sus puertas a las jóvenes de Popayán el 13 de Noviembre de 1967, como una alternativa de educación formal, aunque no se denominaba, en ese entonces, educación superior, acoge mujeres de la ciudad y rompe la tradición de sus homólogos del país recibiendo en su primera promoción algunos pocos varones.

Por medio del Decreto 5858 del 03 de septiembre del 2008 se concede la reforma estatutaria conducente a cambio de carácter académico de institución tecnológica a institución Universitaria. Y en el primer semestre del año 2010 brinda las carreras profesionales en Administración de empresas y Arquitectura.

5.4.3 Misión

Institución Universitaria Pública, fundamentada en principios y valores; contribuimos al desarrollo social formando personas competentes a través de programas tecnológicos, profesionales universitarios y de postgrado, en las áreas del arte, las ingenierías, las ciencias sociales y la administración

5.4.4 Visión

Consolidarnos como una institución de educación superior pública, posicionada en la región por su excelencia académica, la calidad en sus procesos y la pertinencia social de sus programas.

5.4.5 Política de Calidad

¹² COLOMBIA. INSTITUCION UNIVERSITARIA COLEGIO MAYOR DEL CAUCA. <http://www.colmayorcauca.edu.co/unimayor/page/historia-institucional>

La Institución Universitaria Colegio Mayor del Cauca tiene el compromiso social de formar personas con competencias intelectuales, éticas y estéticas; implementando programas con pertinencia para la construcción de región, buscando el mejoramiento continuo de los procesos en cumplimiento de su misión y visión

5.4.6 Naturaleza Jurídica

La Institución Universitaria Colegio Mayor Del Cauca, es un establecimiento público del orden departamental, de carácter académico, con personería jurídica, autonomía administrativa, patrimonio independiente y con domicilio en la ciudad de Popayán.

Según la Ley 30 de 1992, las instituciones universitarias son instituciones facultadas para adelantar programas de formación en ocupaciones, programas de formación académica en profesiones o disciplinas y programas de especialización.

Actualmente la Institución Universitaria Colegio Mayor del Cauca ofrecen los siguientes programas académicos:

Programas Profesionales

- Arquitectura
- Administración Financiera
- Administración de Empresas
- Diseño Visual
- Ingeniería Informática

Programas Tecnológicos

- Delineante de Arquitectura e Ingeniería
- Desarrollo de Software
- Gestión Empresarial
- Gestión Comercial y de Mercados
- Gestión Financiera

Cursos De Extensión

- Inglés Infantil
- Inglés Adultos
- Curso de Música
- Curso de Pintura

Educación Continuada

- Diplomado en Arquitectura y Urbanismo Sostenible

Posgrados

- Especialización en Administración de la Información y Bases de Datos

5.4.7 Estructura Académico – Administrativa



Figura 2: Organigrama Institucional

5.5 Marco Legal

En la actualidad las empresas de carácter público privado, son empresas que realmente invierten muy poco o nada en el aseguramiento tanto de sus recursos como de sus activos, incluyendo el más importante: La información. Al no implementar mecanismos de seguridad en las redes de computadores llevan no sólo a pérdidas sustanciales de dinero si no a estar por fuera de las exigencias del mundo actual, la mayoría de las transacciones que involucran información se realizan a través de redes y el uso de internet.

Utilizar estándares como ISO27000¹³, (específicamente un SGSI) contribuye a establecer procesos de reconocimiento y control en las áreas de una organización, dentro del área de sistemas se debe dar gran importancia la creación y adaptación de mecanismos, políticas de procesos que permitan asegurar y mejorar la seguridad informática.

Para suplir esta necesidad la Institución Universitaria debe tomar como soporte el los estándares de la norma ISO/IEC 27000 las siguientes y legislaturas tanto nacionales como internacionales:

¹³ CALDER, Alan. Implementing information security based on ISO 27001/ISO 27002, ISBN 9087538189, 2012.

Norma ISO/IEC 2700¹⁴ : Familia de estándares donde especifica claramente los parámetros sobre seguridad de la información, para desarrollar, implementar y mantener los sistemas de gestión de seguridad de la información, entre ellos:

- ✓ **Norma ISO/IEC 27001:** Define los requisitos para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información).
- ✓ **Norma ISO/IEC 27002:** (anterior ISO 17799). Es una guía de buenas prácticas, describe los controles a seguir dentro del marco de la seguridad de la información; enmarcados en 11 dominios, 39 objetivos de control y 133 controles.
- ✓ **Norma ISO/IEC 27003:** Proporciona ayuda y orientación sobre la implementación de un SGSI, incluye el método PHVA (planear, hacer verificar y actuar) contribuyendo con revisiones y mejora continua.
- ✓ **Norma ISO/IEC 27004:** Especificará las métricas y técnicas de medición para determinar la eficacia de un SGSI y de sus controles. Aplicable específicamente en la fase del hacer (Do); de acuerdo con el método PHVA.
- ✓ **Norma ISO/IEC 27005:** Suministra directrices para la gestión del riesgo en la seguridad de la información.

Ley 1273 de 2009: sobre los delitos informáticos y la protección de la información y de datos en Colombia.¹⁵

MAGERIT: “Metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno”.¹⁶

Magerit¹⁷ está compuesta por tres libros, el libro I, describe el método a seguir para la ejecución del análisis de riesgos. El libro II; catálogo de elementos

¹⁴ ISO 27000 Directory. [en línea] <http://www.27000.org/>

¹⁵ COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES (MinTIC).

¹⁶ Portal administración electrónica. MAGERIT v3: Metodología de Analisis y Gestion de Riesgos de los sistemas de información. [en línea]. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ

¹⁷ DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método Libro II: Catálogo de Elementos, Libro III: Guía de Técnicas. 2012

discriminados en: activos, amenazas, vulnerabilidades, impacto, riesgo y salvaguardas. Y el libro III, es la guía de técnicas para realizar el análisis final y gestión de riesgos, se puede aplicar técnicas cualitativas o cuantitativas.

6 Diseño Metodológico

6.1 Investigación Aplicada

Cuyo propósito es la solución de problemas específicos para mejorar la calidad de vida de las sociedades, este tipo de investigación está vinculada a la investigación pura, en el caso particular del análisis de riesgos informáticos en la Institución Universitaria Colegio Mayor del Cauca, este tipo de investigación permite la búsqueda de una posible solución a los problemas conocidos o que aún se desconocen de acuerdo a los riesgos informáticos que se pueden presentar o que se están presentando en la institución, tratando de dar una solución práctica a una problemática definida a través de respuestas a las necesidades que la investigación sugiere y que puede valerse de algún proceso sistemático para el desarrollo como tal del proyecto. Se podría asociar la siguiente frase para explicar de mejor forma lo que implica la utilización de la investigación aplicada.

En la investigación aplicada “El objetivo es predecir un comportamiento específico en una configuración muy específica” dice Keith Stanovich, científico cognitivo y autor de “How to think straight about psychology” (2007, p.106).¹⁸

La investigación aplicada esta soportada en aportes teóricos y el desarrollo de actividades tendientes a determinar las posibles causas del problema y evidenciar los hallazgos, que más adelante y gracias a los resultados de la investigación, proporcionaran un marco de trabajo en búsqueda de la aplicabilidad de las posibles soluciones.

Como parte del desarrollo de la investigación aplicada, se plantean a nivel general actividades que tratan de dimensionar y atacar el problema mencionado para brindar al final del proyecto las posibilidades que tiene la institución para adoptar un plan de mejora, de acuerdo a los resultados que se obtengan a partir del análisis de riesgos. Algunas de estas actividades se mencionan a continuación.

- Definición de los objetivos del proyecto y delimitación del alcance de acuerdo al problema planteado.
- Análisis de fuentes de datos y recopilación de información: Esta etapa busca recolectar la mayor cantidad de información posible con respecto al estado actual, estudios o proyectos que tengan relación con el análisis de riesgos y en general en materia de seguridad informática en la institución

¹⁸ Román Valdes Cesardari. Enero 2014. Recurso digital: generación del conocimiento. [en línea] : <http://issuu.com/lizbethfuentes6/docs/m2-t1>

- Generación del plan de trabajo y establecimiento de plazos de tiempo: Esta actividad hace referencia a la generación de un cronograma de actividades a nivel general que establezca límites de tiempo y asignación de tareas para lograr el desarrollo del proyecto.
- Recolección de documentos organizacionales: Para realizar el análisis de riesgos es importante conocer el entorno y contexto en el que se basa la Institución objeto de estudio, conocer su estructura organizacional, forma de operación, lineamientos, normatividad y reglamentaciones en las que se ampara, entre otras.
- Reconocimiento del entorno y del ámbito de trabajo: Se requiere realizar una valuación de activos, infraestructura y visita de los lugares físicos donde tendrá aplicación el proceso de análisis de riesgos.
- Desarrollo de análisis de riesgos: Gracias al plan de trabajo y la determinación de los componentes a evaluar, se recogen datos que permitan demostrar posibles deficiencias o fallas que puedan llegar a materializarse.
- Identificación de vulnerabilidades: Se enfoca en el desarrollo de actividades y/o la aplicación de herramientas sobre sistemas de información, aplicaciones web, sistemas de comunicación o servicios de red y los activos de información críticos con el objetivo de determinar su estado actual desde el punto de vista de seguridad de la información.
- Análisis de vulnerabilidades: Luego de obtener las evidencias se realiza un compendio y organización de todos estos datos, con información relevante que permita determinar focos de falla.
- Análisis de los datos, hallazgos de debilidades y generación de recomendaciones: Con la información, datos obtenidos se genera una matriz con la valoración de los riesgos obtenidos, sugerencias y recomendaciones.
- Discusión de resultados y obtención de la conclusión: paralelo a la generación del informe técnico, se realiza un resumen ejecutivo que muestre de una manera general y objetiva los resultados del proyecto.
- Presentación del informe definitivo a las directivas de la Institución: Se prepara la sustentación del proyecto para socializar el trabajo realizado.

7 Informe Técnico



Figura 3: Logo IUCMC

Para la ejecución del análisis de riesgos se adopta el ciclo de mejora continua PHVA¹⁹ como lo recomienda la norma ISO/IEC 27001



Figura 4: Ciclo mejora continua PHVA

Etapa 1:

La primera etapa fue un reconocimiento de infraestructura física y tecnológica así como la recolección de documentación e información relevante para el desarrollo del proyecto:

- Información contextual de la institución
- Manuales de configuración por parte de fabricantes o elaborados por personal del área en cuanto a servicios, servidores y dispositivos de red.

¹⁹ PHVA ¿Qué es el ciclo PHVA?. Enero 09 de 2010. Blog de Seguridad informática. [en línea]. <http://securityjeifer.wordpress.com/tag/phva/>

- Estudios o contrataciones relacionados con seguridad de la información.
- Manuales de usuario, manuales de operación de sistema de información propios o de terceros.
- Procesos y procedimientos definidos del personal de soporte técnico o de atención a usuarios para la solución de incidencias.

Etapa 2:

En esta fase luego de comprender la estructura organizacional y su manera de operación, basada en el modelo de negocio (actividad principal) de la institución, se clasifican activos por criticidad, se definen planes para realizar y obtener datos sobre el estado de seguridad a nivel hardware y software de equipos, servicios, procesos y procedimientos; además de conseguir información con respecto a instalaciones físicas.

- Visitas a los sitios físicos donde se encuentran los equipos de comunicación, seguridad perimetral, almacenamiento y procesamiento de datos para tomar evidencias de las condiciones actuales.
- Clasificación de los activos de información más críticos que pueden detener el normal funcionamiento de la IUCMC en caso de falla.
- Solicitud formal de cuentas de prueba y acceso en modo invitado a servidores y equipos de comunicación, tales como firewalls, switches y routers, con el fin de tomar evidencia del proceso y forma de configuración de cada dispositivo y/o sistema operativo.
- Solicitud de acceso a la documentación de la red, se evidencio el diseño lógico (Definición de segmentos, diseño de direccionamiento, diagramas lógicos, VLANs), privilegios y características de cuentas de usuario, perfiles de cuentas de acceso, políticas definidas en los firewall.

Etapa 3:

Con la información obtenida y el otorgamiento de acceso restringido sobre ciertos servicios, equipos o servidores y conociendo el direccionamiento e infraestructura tecnológica, se procede con el montaje de un escenario de pruebas, basado en herramientas de escaneo y análisis para detectar posibles vulnerabilidades a nivel de servicios, protocolos o puertos; pruebas sobre conformación de contraseñas, modos de acceso y en general test que se encaminan a determinar el estado actual de seguridad en la infraestructura de red e información a nivel general.

- Se realiza una selección de herramientas y entornos para realizar las diferentes pruebas que tienen aplicabilidad en el contexto del proyecto. La mayoría de herramientas utilizadas son herramientas de tipo ethical hacking y versiones libres, aunque se hizo uso de herramientas en línea y versiones de prueba.
- se realiza un análisis y enumeración de puertos, protocolos y servicios para determinar el estado actual de puertos disponibles, abiertos y cerrados, que

será el punto de partida del análisis de riesgos informáticos sobre los servicios de red y aplicaciones definidas por su criticidad.

- Se utilizan las herramientas de escaneo de vulnerabilidades previamente seleccionadas, se evaluaron aspectos importantes como intentos de acceso por fuerza bruta sobre aplicativos web, tipo de codificación y/o cifrado de contraseñas y fortaleza de las mismas, se realizaron pruebas de acceso entre subredes y segmentos con tal de evadir sistemas de protección física y lógica como Vlans en switches, sistema VPN y políticas de restricción entre zonas configuradas en firewall; por otro lado se realizaron pruebas de escalamiento de privilegios y acceso remoto. Cabe aclarar que muchas de las pruebas se aplicaron sobre máquinas virtualizadas, creando de esta forma un ambiente de pruebas que no comprometiera los sistemas críticos que están en producción.
- Con los datos obtenidos, se realiza un análisis y clasificación de activos de información en riesgo para definir y sugerir controles o salvaguardas, ayudando de esta manera a minimizar el impacto de materialización de amenaza detectada.

7.1 Activos de Información

En la actualidad la Institución Universitaria Colegio Mayor del Cauca tiene los siguientes activos de información e infraestructura tecnológica:

Servidores y Equipos de Intercambio de Datos

- La institución posee doce (13) servidores
- Tres (3) equipos de protección perimetral firewall (Unified Threat Management) tipo Fortigate.
- Cuatro (4) zonas de acceso inalámbrico con potencia media-alta.
- Redes de comunicación e Internet
 - Se tienen treinta y cuatro (34) switches de red.
 - El router principal pertenece al ISP.

Sistemas de Comunicación y Voz

- La sede principal cuenta con un sistema de telefonía convencional o mini central telefónica PBX (Private Branch Exchange).
- PBX Virtual con un total de 24 extensiones VoIP distribuidas en las tres sedes.

Sistemas de Seguridad, Prevención y Control de Acceso

- Sensores de movimiento y alarmas de seguridad.
- Cámaras de seguridad IP.
- Sistemas de aire acondicionado.

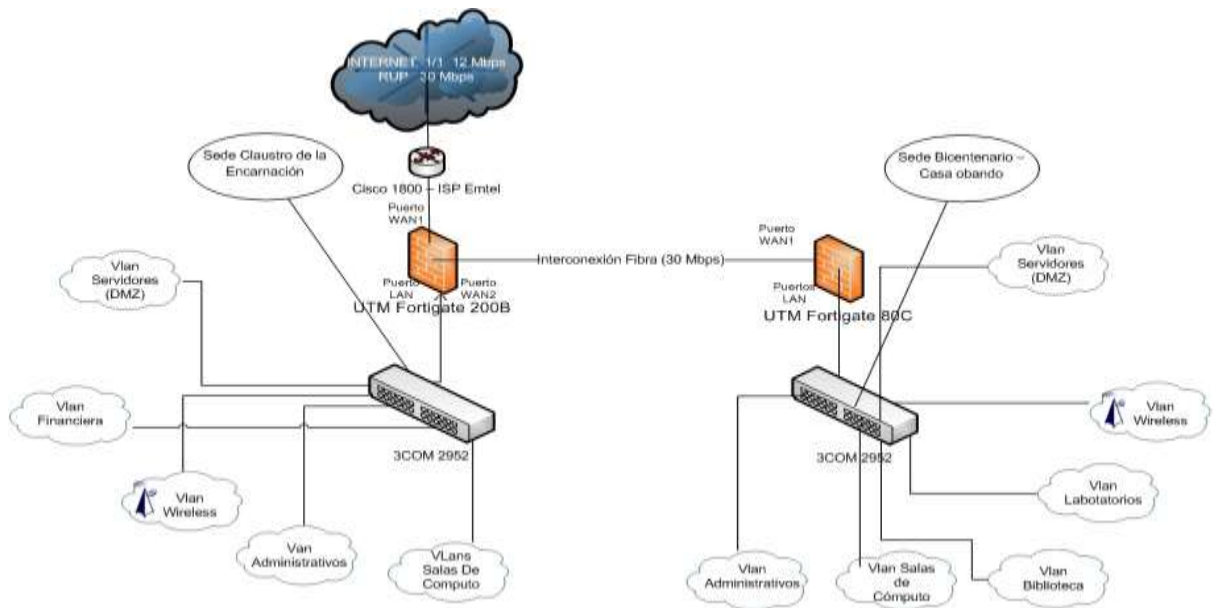
- Extintores de diferentes tipos según la ubicación del extintor, entorno, equipos y elementos de cada sitio.

Equipos de Cómputo

- En total se dispone de trescientos ochenta y un (381) equipos de cómputo, distribuidos en seis (6) salas de cómputo y cuatro (4) laboratorios de uso estudiantil sumando 270 equipos. Ciento once (111) equipos de cómputo de uso administrativo y docente.

Diseño General Red de Datos IUCMC

Figura 5 : Diagrama de Interconexión general IUCMC



7.2 Ethical hacking. Análisis de Vulnerabilidades


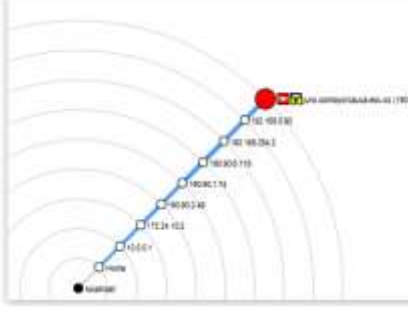

Este informe técnico pretende dar a conocer algunas de las pruebas, análisis y resultados obtenidos con base a herramientas utilizadas y teniendo presente a nivel de guía la metodología Magerit v.3 para el análisis y gestión de los riesgos encontrados así como las posibles fallas, amenazas o vulnerabilidades que se pueden presentar en la Institución Universitaria Colegio Mayor del Cauca y que afecten directa o indirectamente la seguridad de la información que administra o manipula el personal administrativo y docente.

Es de anotar que se hace especial énfasis en los servicios que actualmente se prestan en la institución y que son la base fundamental del funcionamiento institucional diario, donde se pueden presentar fallas, daños o alteraciones a dichos servicios e información por la ausencia de procedimientos, políticas, planes y mecanismos que garanticen la confiabilidad, confidencialidad y disponibilidad de la información e infraestructura tecnológica presente y futura de la institución.

A continuación se presentan algunos de los servicios y sistemas de información más relevantes para la institución donde recaen vulnerabilidades y amenazas resumidas en el cuadro de evaluación de vulnerabilidades:

7.2.1 Evaluación De Vulnerabilidades

Tabla 1. Evaluación de Vulnerabilidades

Prueba efectuada	Activo de información	Fecha y duración	Encargado de prueba	Conclusiones
<p>1. Se realizó enumeración de puertos, servicios y protocolos - Identificación de direccionamiento público y privado IPv4 en los segmentos 190.5.199.xxx/28 y 10.20.30.xxx/26 respectivamente. Prueba efectuada con herramientas como ping, nslookup, nmap, dns-stuff on line, dns fierce y zenmap en Windows.</p>  	<p>UTM (Unified Threat Management) Fortigate 200B – Fortigate 80C – Mapeo a Direcciones de Servidores Web y Servidor SIAG.</p>	<p>Noviembre 9 de 2013 – 3pm a 6pm (Direcciones Públicas) Noviembre 16 de 2013 9 am a 12 pm (Direcciones Privadas)</p>	<p>Mildred Caicedo C. John Jairo Perafán R.</p>	<p>El firewall de protección perimetral es bastante restrictivo a nivel del direccionamiento público, aunque fue fácilmente identificable puertos abiertos en la mayoría de direcciones públicas y obedecen a las políticas de restricción de servicios y protocolos en el firewall. A nivel interno se detectaron muchos más puertos abiertos ya que no se han definido políticas restrictivas entre zonas. Un ejemplo fue que obtuvimos información de todos los servicios y versiones instaladas además de puertos abiertos disponibles en cada IP asociada a los servidores.</p> 
<p>2. Luego de tener identificados puertos y servicios específicos de los activos más significativos de la Institución se ejecutaron herramientas de pruebas para encontrar y analizar</p>	<p>Servidores de sitios web críticos, por direcciones públicas, Servidor SIAG, Servidores de Sistemas de</p>	<p>Noviembre 29 (6 pm) hasta 30 de noviembre (3 pm) 2013.</p>	<p>John Jairo Perafán Ruiz – Mildred Caicedo C.</p>	<p>Los resultados de estos análisis nos arrojan en su mayoría unos ID dependiendo de la herramienta y corresponden a ID de Open Source Vulnerability Data Base que es la Base</p>

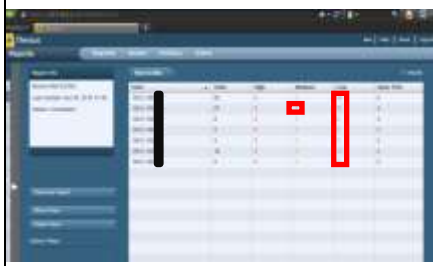
vulnerabilidades, entre ellas Nessus, OWASP wte y Nikto, las cuales basan su análisis de vulnerabilidades de acuerdo a bases de datos con las últimas detecciones de fallos a nivel de sistemas operativos, aplicativos o servicios.



8

Información Logística (MRBS, GLPI e Inventario)

de datos de Vulnerabilidades de código abierto que podemos encontrar en el sitio web <http://www.osvdb.org>, ingresamos al sitio y podemos buscar la información referente a cualquiera de los IDS o vulnerabilidades encontradas por Nikto. Owasp centra su análisis a las vulnerabilidades de servicios y servidores web al igual que Nessus. Se encuentran vulnerabilidades a nivel de versiones obsoletas en sistemas operativos, versiones con altos riesgos de amenazas y vulneración en servidores web como apache y agujeros en IIS.




3. Se realizaron pruebas al sistema de Información Académico y de Gestión SIAG. Primero en su conformación y estructura, en el desarrollo de módulos web, a nivel de scripts, variables y Chequeo de código de bajo rendimiento.

Módulos internos y externos del sistema de información de SIAG, tales como Gestión Académica, liquidación, sistema de reportes, admisiones, evaluación docente, registro en línea, labor docente, consulta notas,

Diciembre 6 de 2013 horas de la noche.

Manuel E. Prado (Responsable desarrollo y Mantenimiento SIAG).

Bajo el uso del programa badboy, se pudo evidenciar compromisos en el rendimiento de algunos módulos en cuanto al nivel de carga de procesamiento del servidor frente a un script que saturaba con muchas transacciones al servidor provocando denegación de servicio después de un corto periodo de tiempo. Es de aclarar que la prueba interna fue la que permitió establecer estos resultados; las pruebas

	<p>sistema de promedios y control académico entre otros.</p>			<p>desde Internet fueron abortadas por el Sistema de Prevención contra Intrusos (IPS) y el escaneo de vulnerabilidades. Badboy es una herramienta diseñada para ayudar en las pruebas y el desarrollo de aplicaciones dinámicas complejas como el caso de los módulos y aplicaciones del SIAG que es el sistema de información más importante para la Institución.</p>
<p>4. Pruebas de conformación de contraseñas en archivos shadow, copia de los archivos originales de sistemas web de acceso a SIAG y a servidores web en sistemas operativos Linux.</p>	<p>Aplicativos y módulos web en SIAG y sitios web en servidores apache, ISS desde Linux o Windows.</p>	<p>Enero 10 de 2014.</p>	<p>John Perafán R.</p>	<p>Con la herramienta JohnTheRipper, se pudo comprobar que no existen contraseñas seguras, muchas de las contraseñas de usuario para acceso a sistemas Linux, o a aplicativos web en el SIAG son fácilmente descifrables.</p>

5. Pruebas de penetración aprovechando las vulnerabilidades encontradas con las herramientas de escaneo de vulnerabilidades, las pruebas se realizaron con herramientas tipo httpprint comparando las firmas de versiones del web server objeto de análisis con las listas de explotación y fallas a nivel de configuración o codificación.



Servidores y aplicativos web que enlazan a módulos o sistemas de información sensibles. Los servicios y servidores puestos a prueba fueron virtualizados en VMWare 7 con copias exactas de su información y configuración como resultado de la creación de un ambiente de pruebas.

Diciembre 2013 – Enero 2014.

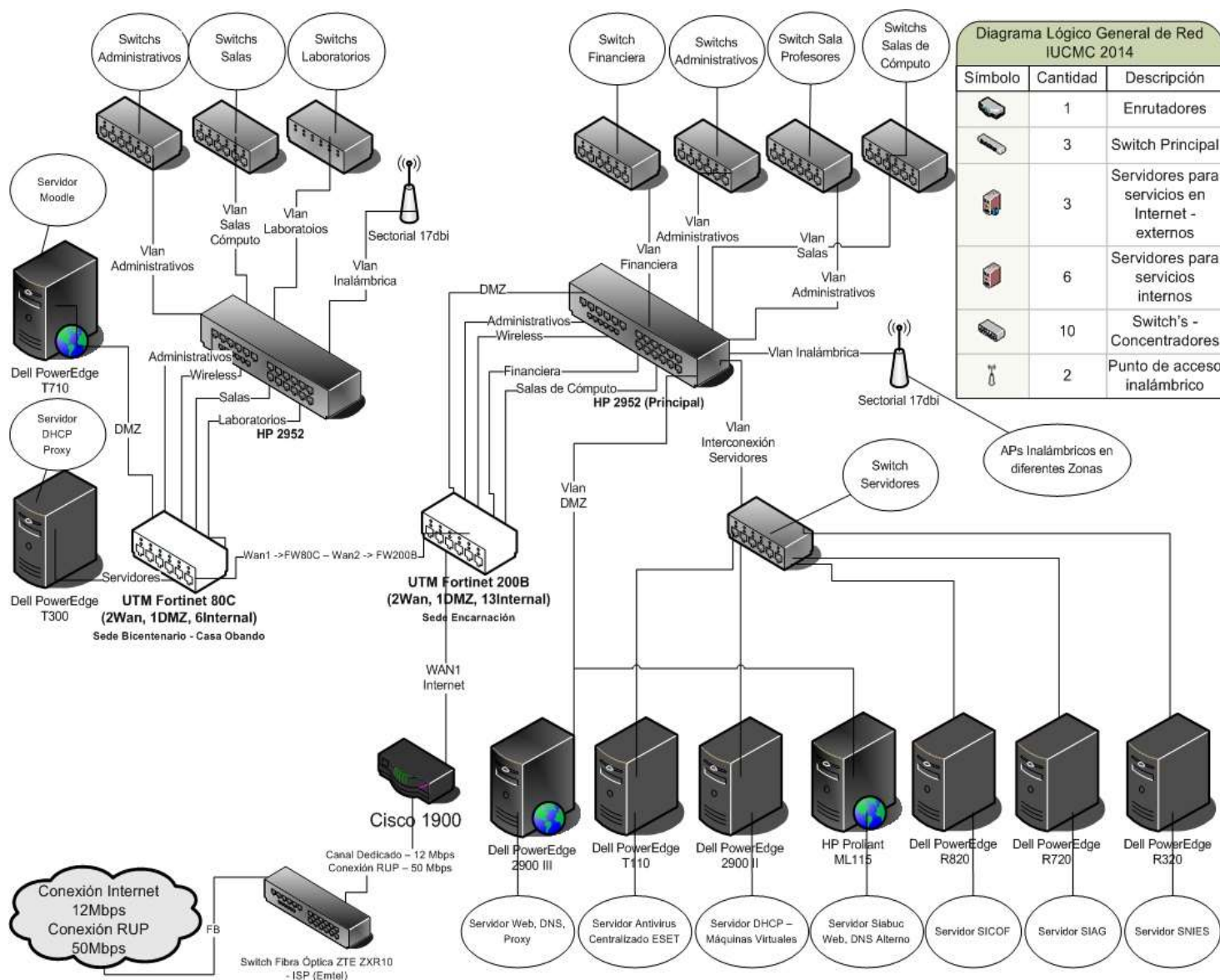
Mildred Caicedo C. - John Jairo Perafán R. - Manuel E. Prado (Responsable mantenimiento y desarrollo SIAG) - Gabriel M. Melo A. (Web Master)

La explotación de vulnerabilidades en el ambiente de pruebas demostró que existen fallas de seguridad, como agujeros por falta de actualizaciones en webserver, aplicación de parches de seguridad, malas prácticas para la asignación de passwords y problemas en algoritmos de cifrado de las mismas, errores de codificación segura que permiten ejecutar ataques tipo SQL Injection. Este framework además de los ataques por fuerza bruta, permite configurar peticiones especiales que pueden evadir al IPS con módulos como el mod_security y RnDCase aunque no fue posible evaluarlo en el entorno real para comprobar la efectividad del IPS.



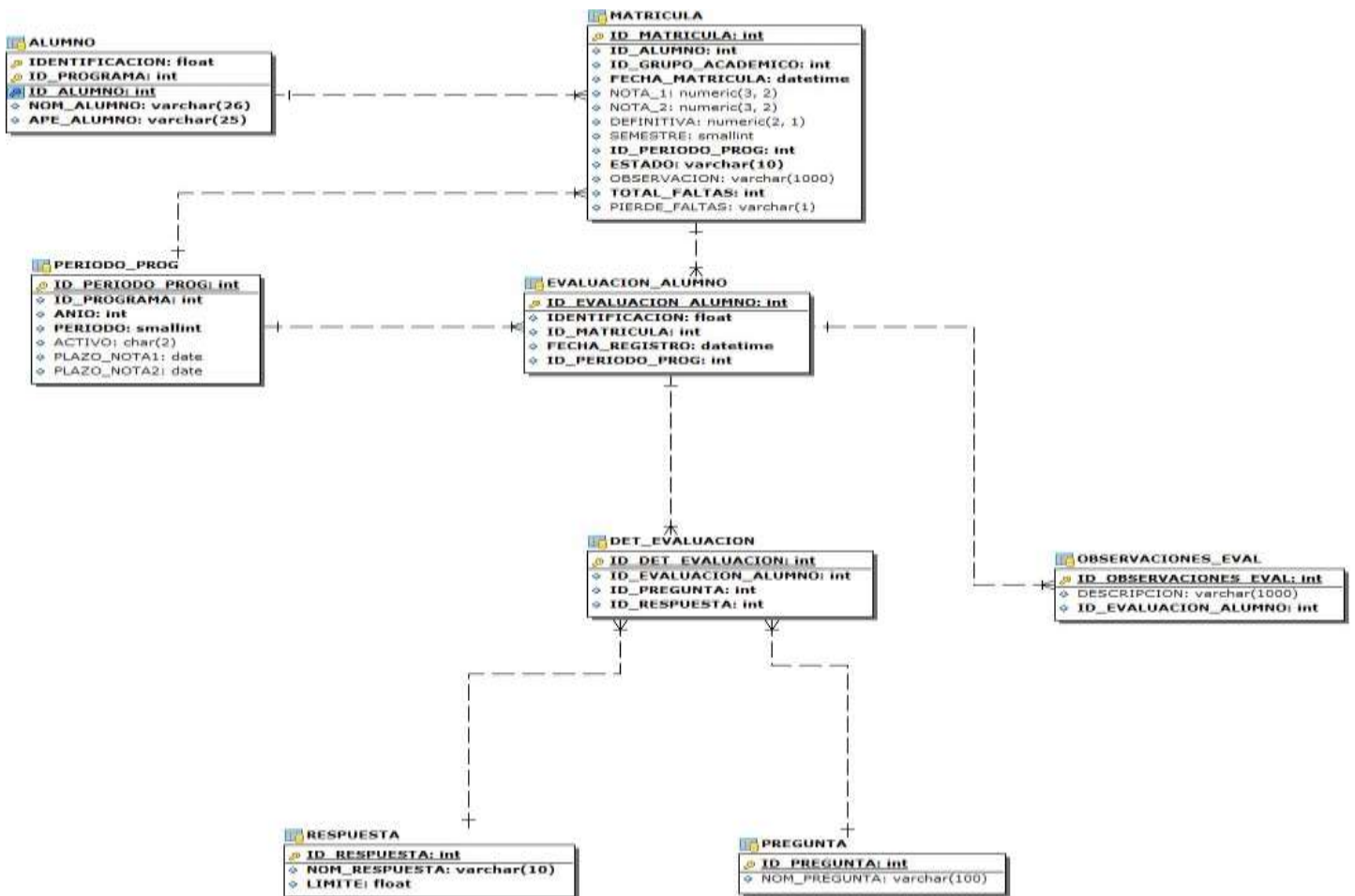
Fuente: Esta investigación

7.2.2 Mapa de Red



Fuente: Esta investigación

7.2.3 Mapa Software (S.I. Académico)



Fuente: Esta investigación

8.1 Resumen Informativo y Funcional Sistemas de Información Sensibles

8.1.1 Sistema De Reserva De Salas De Reunión. (MRBS)

MRBS (Meeting Room Booking System) es un sistema de uso interno para registrar las reservas de los salones de clases, salas de conferencia, salas de cómputo y demás salas de reuniones que existen dentro de las tres sedes de la Institución. Es GPL, la aplicación web gratis con PHP y MySQL/pgsqli.



Figura 6: Interfaz Sistema de reservas

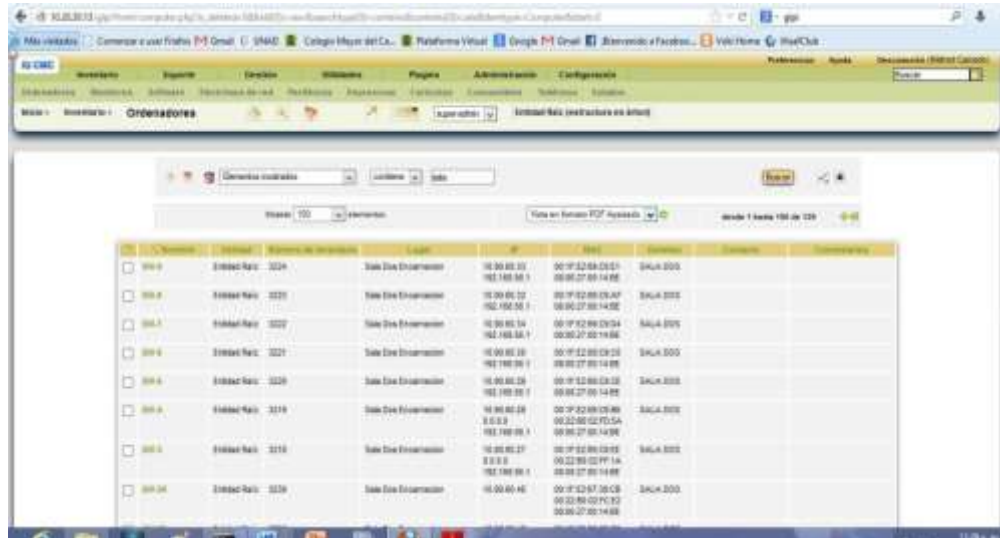
Cualquier persona puede acceder para consultar este sistema desde cualquier terminal conectado a la red de la Institución para obtener información actualizada de salas, laboratorios y salones de clase, su disponibilidad y ocupación en un momento dado.

8.1.2 GLPI

Es aplicación Web escrita en PHP, que permite registrar y administrar el inventario del hardware y del software de la Institución. Funciona internamente y es software libre distribuido bajo licencia GPL, que nos ofrece facilidad para la administración de recursos informáticos.

El usuario administrador posee todos los permisos, le permite crear usuarios, cambiar contraseña de usuarios, adicionar elementos al inventario, generar reportes, generar y asignar incidencias, hacer modificaciones al sistema.

Figura 7: Interfaz GLPI en la institución



8.1.3 Sistema de Información Académico y de Gestión. (SIAG)

El sistema de información SIAG es tal vez el más importante ya que está ligado al quehacer institucional, fue un sistema que nació como proyecto de grado y ha evolucionado a tal punto que integra gran variedad de módulos que incluyen entre otros matrículas, historial y reportes personalizados o a medida, reporte y consulta de notas, faltas, admisiones y un módulo de liquidación que se integra con el sistema financiero, incluye un sistema de evaluación docente (SICEDD – Sistema de Información para control de evaluación y desempeño docente) y un sistema de información arte mayor y extensión (AMEX -SIA).

El módulo de gestión académica es la principal aplicación del Sistema de Información Académico y de Gestión de la institución y el acceso a él debe contar con un proceso que garantice la autenticidad del funcionario que ingresa a administrar el aplicativo ya que en este se realiza todo el proceso académico importante de los estudiantes matriculados en programas de formación regulares y contempla desde la admisión del estudiante hasta el historial académico del mismo, pasando por aspectos como los prerrequisitos de matrículas inter-semestrales, promedios ponderados, alumnos matriculados académicamente, materias, gestión de alumno-plan, evaluación certificativa, registro de notas y más.



Figura 8: Módulo de Gestión Académica – SIAG

Con los activos más importantes previamente identificados se procede a realizar la valuación de riesgos. Proceso base para poder identificar su nivel de importancia y criticidad dentro del modelo de negocio de la Institución Universitaria Colegio Mayor del Cauca, a continuación se observan los resultados de la valuación de activos en la herramienta.

Código	Descripción	Valor	Riesgo	Impacto	Ponderación
01	Caja de negocio				
01.01	INVESTIDO EN EL PROCESO DE REGISTRO EN LINEA	0	10		
01.02	INVESTIDO EN EL PROCESO DE FORMALIZACIÓN DE INSCRIPCIÓN EN LINEA	0	0		
02	Servicios asociados				
02.01	Equipamiento				
02.01.01	SWI Sistema de Información Académico y de Gestión	10	10	10	
02.01.02	SWR Sistema de atención de las Salas de reuniones	4	4	4	
02.01.03	SLP Administrativa de Instalación Estudiantil	4	4	4	
02.01.04	SAI Sistema de Información Científica e Investigativa	10	10	10	10
02.01.05	SWW Servidor Web - Colaboración Académica	10	10	10	10
02.01.06	SWP Servidor Proxy	5	5		
02.01.07	EHWI Equipos				
02.01.07.01	SWI Servidor de Servicios de Dominio Local	0	0	0	
02.01.07.02	SWR Servidor Proxy Local	4	4	4	
02.01.07.03	SLP Servidor de Instalación Estudiantil	5	5	5	
02.01.07.04	SAI Servidor Web - Colaboración Académica	8	8	8	8
02.01.07.05	SWP Servidor Proxy	10	10	10	10
02.01.07.06	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.07	SWR Servidor Proxy Local	10	10	10	10
02.01.07.08	SLP Servidor de Instalación Estudiantil	10	10	10	10
02.01.07.09	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.10	SWP Servidor Proxy	8	8	8	8
02.01.07.11	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.12	SWR Servidor Proxy Local	7	7	7	
02.01.07.13	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.14	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.15	SWP Servidor Proxy	7	7	7	
02.01.07.16	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.17	SWR Servidor Proxy Local	7	7	7	
02.01.07.18	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.19	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.20	SWP Servidor Proxy	7	7	7	
02.01.07.21	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.22	SWR Servidor Proxy Local	7	7	7	
02.01.07.23	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.24	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.25	SWP Servidor Proxy	7	7	7	
02.01.07.26	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.27	SWR Servidor Proxy Local	7	7	7	
02.01.07.28	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.29	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.30	SWP Servidor Proxy	7	7	7	
02.01.07.31	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.32	SWR Servidor Proxy Local	7	7	7	
02.01.07.33	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.34	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.35	SWP Servidor Proxy	7	7	7	
02.01.07.36	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.37	SWR Servidor Proxy Local	7	7	7	
02.01.07.38	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.39	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.40	SWP Servidor Proxy	7	7	7	
02.01.07.41	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.42	SWR Servidor Proxy Local	7	7	7	
02.01.07.43	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.44	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.45	SWP Servidor Proxy	7	7	7	
02.01.07.46	SWI Servidor de Servicios de Dominio Local	7	7	7	
02.01.07.47	SWR Servidor Proxy Local	7	7	7	
02.01.07.48	SLP Servidor de Instalación Estudiantil	7	7	7	
02.01.07.49	SAI Servidor Web - Colaboración Académica	7	7	7	
02.01.07.50	SWP Servidor Proxy	7	7	7	

Figura 9: Evaluación de activos de la institución.

Posteriormente la herramienta arroja los resultados obtenidos con los datos de la valuación de activos y se procede con la identificación de las amenazas. La utilización de una metodología como Magerit y de la EAR PILAR, nos facilita llegar a la identificación de los riesgos tal como se muestra en la siguiente figura, aunque cabe anotar que este proceso está bastante resumido solo con las

actividades más relevantes que le permitan al lector entender cuál debería ser el proceso adecuado para realizar el análisis de los riesgos y su posterior tratamiento a partir de la definición de controles o salvaguardas y de igual manera a partir de la identificación de los activos más críticos poder definir la línea base que nos facilitara el proceso de Ethical Hacking o Pentest con herramientas que nos permitan tener resultados más aproximados de las verdaderas fallas en sistemas de información, aplicaciones web, entre otros..

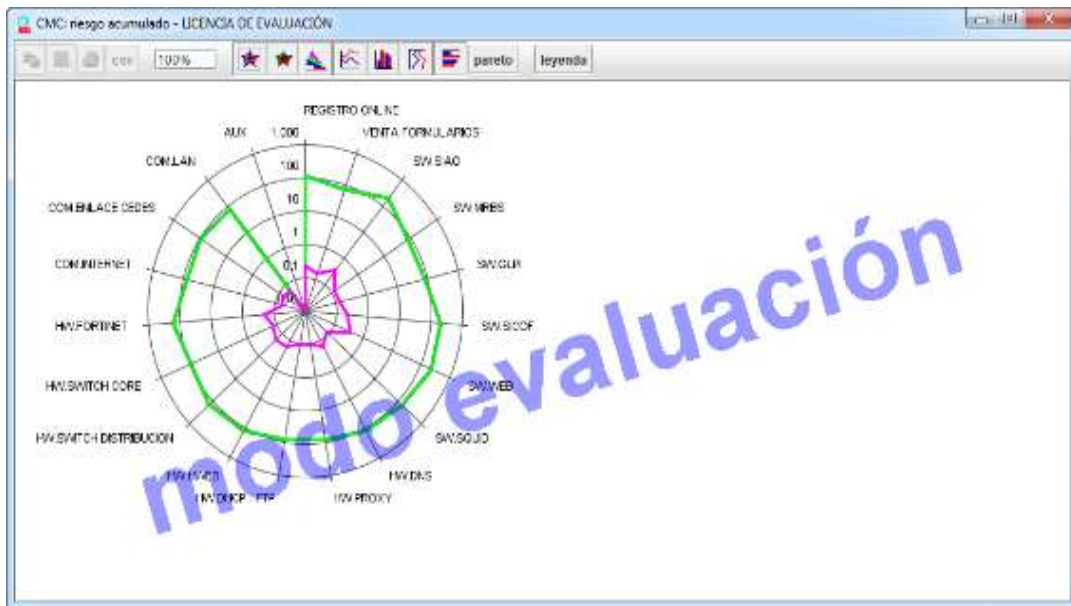


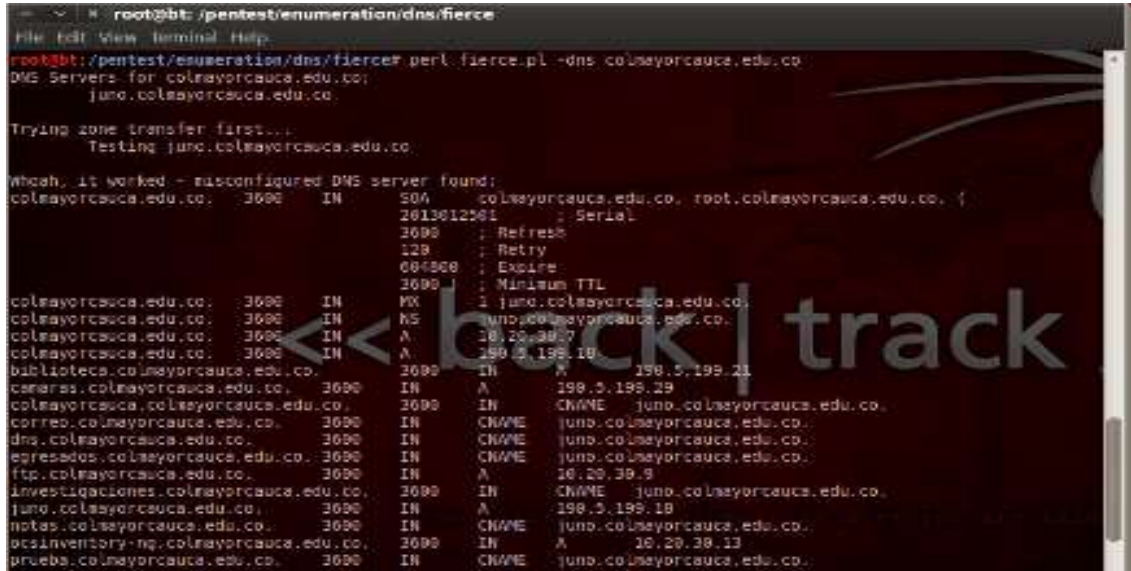
Figura 10 : Tabla riesgo acumulado

A partir de este análisis se procede entonces con la preparación y definición del plan de vulnerabilidades, Pentest o Ethical Hacking, el cual se debe apalancar de igual manera en la conceptualización de algunos estándares adicionales; como los activos más críticos en la institución son las aplicaciones que están ligadas al uso de un servicios web se utilizaron algunas recomendaciones dadas por OWASP.

8.2 Resumen del Diagnóstico de Servicios más Relevantes

Para realizar las primeras pruebas que nos indicaran la carencia de controles, nos enfocaremos en el desarrollo de una prueba de intrusión a uno de los servicios de la Institución.

Se procedió a identificar la dirección IP del servidor que aloja el servicio, luego con la IP se procede a buscar más información del sitio como hosting, propietario, DNS, tipo de servidor web, entre otra información para ello hacemos uso de una herramienta en línea.



```
root@bt: /pentest/enumeration/dns/fierce
root@bt: /pentest/enumeration/dns/fierce perl fierce.pl -dns colmayorcauca.edu.co
DNS Servers for colmayorcauca.edu.co:
juno.colmayorcauca.edu.co

Trying zone transfer first...
Testing juno.colmayorcauca.edu.co

Whoah, it worked - misconfigured DNS server found:
colmayorcauca.edu.co. 3698 IN SOA colmayorcauca.edu.co. root.colmayorcauca.edu.co. {
2613612561 ; Serial
3698 ; Refresh
128 ; Retry
604800 ; Expire
3698 ; Minimum TTL
colmayorcauca.edu.co. 3698 IN MX 1 juno.colmayorcauca.edu.co.
colmayorcauca.edu.co. 3698 IN NS juno.colmayorcauca.edu.co.
colmayorcauca.edu.co. 3698 IN A 18.20.38.7
colmayorcauca.edu.co. 3698 IN A 198.5.199.18
biblioteca.colmayorcauca.edu.co. 3698 IN A 198.5.199.21
canarias.colmayorcauca.edu.co. 3698 IN A 198.5.199.29
colmayorcauca.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
correo.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
dns.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
egresados.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
ftp.colmayorcauca.edu.co. 3698 IN A 18.20.38.9
investigaciones.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
juno.colmayorcauca.edu.co. 3698 IN A 198.5.199.18
notas.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
ocsinventory-ng.colmayorcauca.edu.co. 3698 IN A 18.20.38.13
prueba.colmayorcauca.edu.co. 3698 IN CNAME juno.colmayorcauca.edu.co.
```

Figura 11: Obtención registros DNS

Posteriormente se realizó un escaneo de puertos al servidor previamente identificado para conocer los servicios y puertos que están habilitados en el servidor.

Luego se realizaron algunas tareas tendientes a obtener la enumeración de servicios web en ese servidor.

Figura 12: Enumeración Sitio Web



```
root@bt: /pentest/enumeration/web/whatweb
root@bt: /pentest/enumeration/web/whatweb whatweb colmayorcauca.edu.co
http://colmayorcauca.edu.co [200] Adobe-Flash, HTTPServer[Debian Linux][Apache/2.2.9 (Debian)], Frame, ActiveX, Apache[2.2.9], YouTube, Country[ESTADOS UNIDOS], IP 18.20.38.7, JQuery, Lightbox, HTML5, Google-Analytics[UA-31401470-1], Title[Universidad Tecnológica del Cauca]
root@bt: /pentest/enumeration/web/whatweb?
```

Posteriormente se efectuaron análisis de vulnerabilidades utilizando para ello varias herramientas como Nikto, openvas, nessus, w3af, entre otras, todas

lanzadas desde la distribución de herramientas libres para hacking ético Backtrack y algunas herramientas en línea como Qualys.

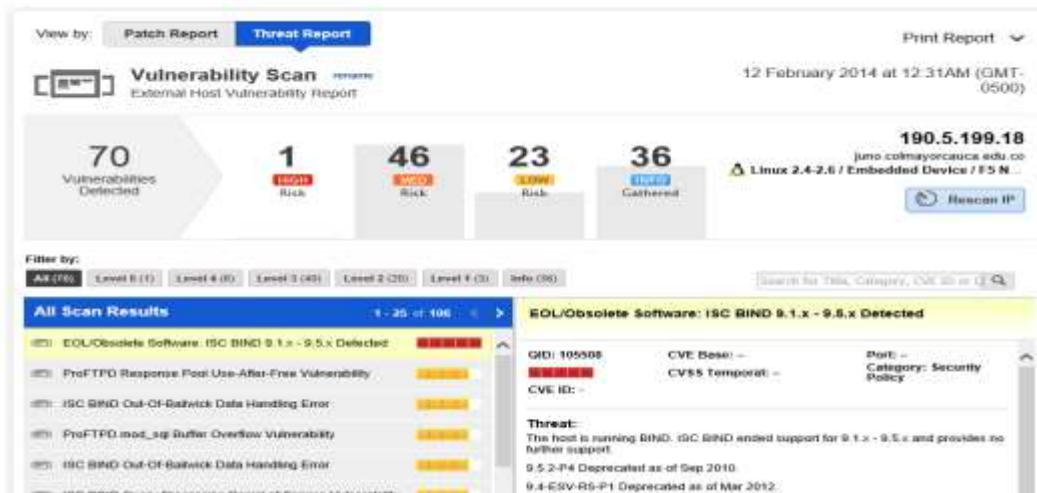


Figura 13: Vulnerabilidades detectadas – Qualys online

En general estas son algunas de las tantas pruebas realizadas a los activos identificados previamente en el análisis de riesgos, sin embargo es importante recalcar que toda prueba de penetración o testeo se debe preparar y si es contratada con un tercero se debe establecer un acuerdo de confidencialidad. Firmados los acuerdos de confidencialidad, alcance y límites de las pruebas se deben definir y preparar las líneas base para los servicios a ser probados, la línea base corresponde a definir el tipo de pruebas, técnicas y herramientas a utilizar, para el caso en mención se tomaron líneas base para servicios web. Otro tema importante es mencionar que la seguridad no solo se mide sobre los recursos informáticos si no sobre todo el entorno donde se encuentran ubicados y trabajando dichos recursos, es decir se debe evaluar la seguridad lógica, la física y al ambiental, que requiere la utilización de técnicas como: la observación directa, la encuesta y por supuesto el hacking ético, para la evaluación de la parte física, a continuación se ilustran algunos ejemplos simples de revisiones a la seguridad.

8.3 Análisis y Evaluación de Riesgos Basado en Magerit V.3

Apoyados en la metodología Magerit se desarrollan tres procesos para el logro del proyecto “Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca”:

8.3.1 Proceso P1: Planificación

Esta etapa es muy importante porque es el marco de referencia para el desarrollo del proyecto.

8.3.1.1 Actividad A1.1: Estudio de Oportunidad.

Esta actividad tiene como objetivo específico, realizar un diagnóstico del estado de seguridad en que se encuentran los activos de información y los tecnológicos dentro de la IUCMC, además de motivar a la alta dirección para implementar un SGSI.

8.3.1.2 Actividad A1.2: Definición del Alcance y Objetivos del Proyecto

Después de haber recibido el aval para la realización del proyecto “Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca IUCMC”, se definen los límites y el dominio de trabajo y los objetivos para desarrollar exitosamente el proyecto.

Los objetivos han sido planteados con el propósito de realizar un concienzudo y real análisis de riesgos que lleven a una futura implementación del sistema de gestión de seguridad de la información de IUCMC.

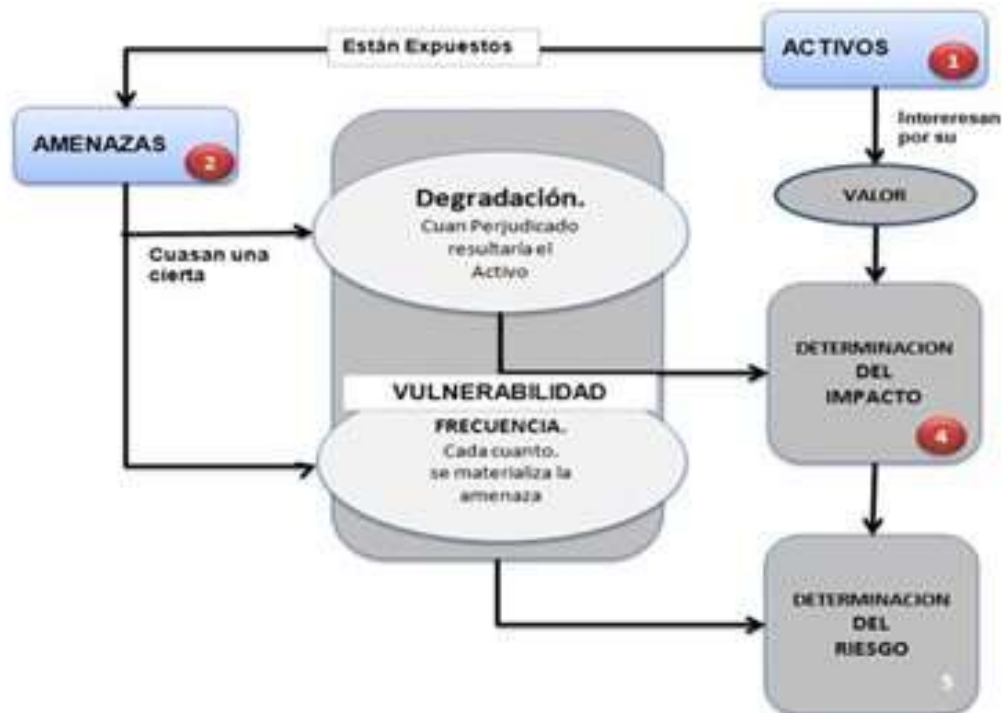
8.3.1.3 Actividad A1.3: Planificación del Proyecto

Es necesario realizar un cronograma de actividades que nos sirva como bitácora, para el desarrollo exitoso del proyecto.

8.3.1.4 Actividad A1.4: Lanzamiento del Proyecto.

Con el aval del asesor TIC de la IUCMC se inicia el proceso de análisis de riesgos y se adopta la técnica de observación directa y entrevista para la recolección de la información siendo estas las más apropiadas, ya que se tiene la ventaja de que los integrantes del equipo de trabajo está directamente involucrado con los procesos y sistemas informáticos existentes en la institución.

8.3.2 Proceso P2: Análisis de Riesgos



Fuente: <http://slideplayer.es/slide/1649894/>

Al igual que cualquier organización y/o empresa la Institución Universitaria Colegio Mayor del Cauca, está expuesta a múltiples riesgos razón por la cual debe considerar y dar importancia a los cambios o alteraciones que lleguen a afectar los activos informáticos evitando acciones negativas al normal funcionamiento.

Este es la parte crítica y quizás la razón de ser de MAGERIT, de la correcta aplicabilidad, clasificación y valoración de los activos depende el éxito del proyecto.

8.3.2.1 Actividad A2.1: Caracterización y Valoración de los Activos.

Esta actividad abarca las siguientes tareas (T2):

Tarea 2.1.1: Identificación de los Activos

Los activos presentes en la Institución Universitaria Colegio Mayor del Cauca, son identificados y clasificados tomando como base el Libro II de la metodología

MAGERIT versión 3, en donde nos presenta el catálogo de elementos (Ver Anexo A):

Tabla 2: Activos de información

TIPO	NOMBRE DEL ACTIVO
APLICACIONES INFORMATICAS	1. [SI_SIAG] Sistema de Información Académica y de Gestión. 2. [SI_SICOF] Sistema Contable y Financiero 3. [SI_SIABUC] Sistema de Automatización de Bibliotecas de la Universidad de Colima. 4. [SO] Sistema Operativo. 5. [HER_SW] Herramientas Software. 6. [ANT_VIR] Anti virus
SERVICIOS	7. [SV_S_WEB] Servidor Sitios Web. 8. [SV_PROXY] Servidor Proxy. 9. [SV_DNS] Servidor DNS 10. [SV_DHCP] Servidor DHCP 11. [SV_VoIP] Servidor Telefonía IP 12. [SV_BD] Servidor Bases de Datos 13. [SV_CAM] Servidor Cámaras IP 14. [SV_LSM_MOODLE] Servidor herramientas virtuales de aprendizaje.
REDES DE COMUNICACIONES	15. [RO_ISP] Router Proveedor de Servicios de Internet.
EQUIPAMIENTO INFORMatico	16. [FW_UTM] Firewall / Equipo Unificado contra Amenazas. 17. [PC] Equipos de computo 18. [SW_A] Switch Administrable
EQUIPAMIENTO AUXILIAR	19. [CAB_RED] Cableado de Red 20. [UPS] Sistema de Alimentación Ininterrumpida.
INSTALACIONES	21. [GAB] Gabinete de Red
PERSONAL	22. [AS_TIC] Asesor Tecnologías de Información y Comunicaciones 23. [TEC_ADMIN_II] Técnico Administrativo Grado II 24. [TEC_ADMIN_EX] Técnico Administrativo Experto 25. [CO] Contratista.

Fuente: Esta investigación

Tarea 2.1.2: Dependencias entre Activos

Recorrido Top – Down

- Dependencia de los activos del tipo APLICACIONES INFORMATICAS:
 - Las aplicaciones que lo soportan.
 - Los equipos que lo hospedan.
 - El personal del que depende.

Figura 14: Dependencia de activos tipo Aplicaciones informáticas.

- Dependencia de los activos del tipo SERVICIOS:
 - Los equipos que lo hospedan.
 - El personal que tiene acceso.

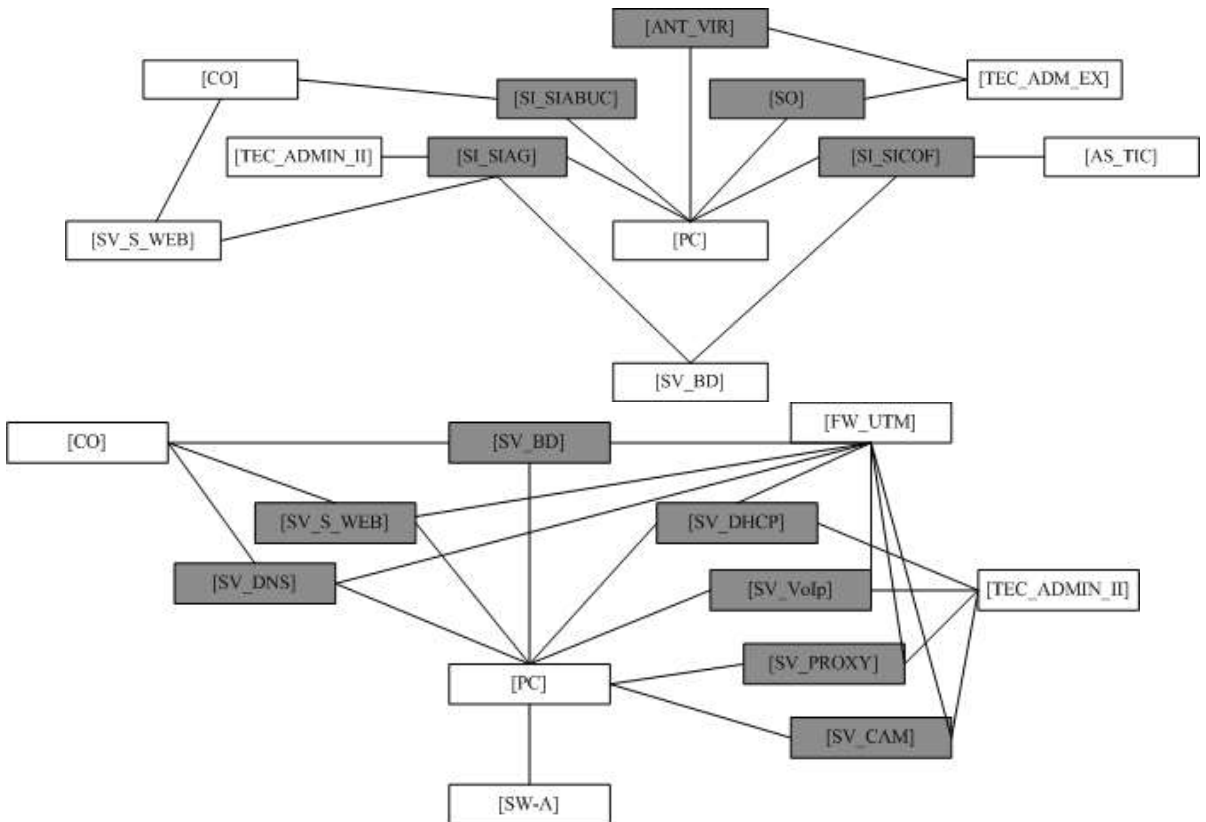


Figura 15: Dependencia de activos tipo servicios

- Dependencia de los activos del tipo EQUIPAMIENTO INFORMATICO:
 - Las instalaciones que lo acogen.
 - El personal que lo gestiona.

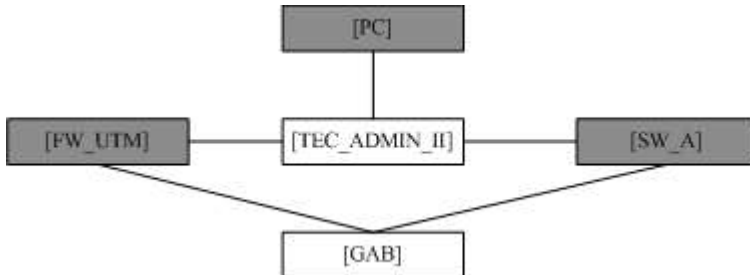


Figura 16: Dependencia de activos tipo: equipamiento informático

- Dependencia de los activos del tipo APLICACIONES INFORMATICAS:
 - ✓ Los equipos que lo hospedan.
 - ✓ El personal que tiene acceso.

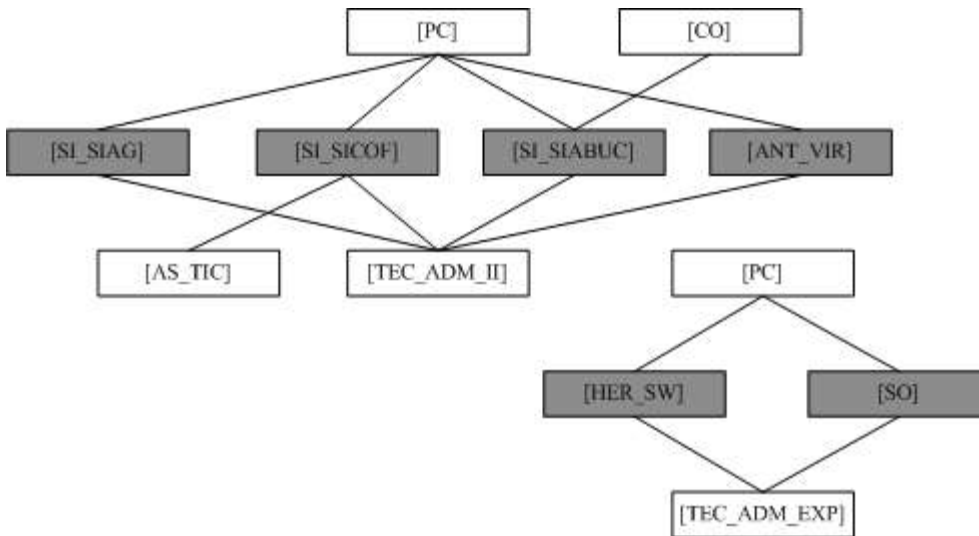


Figura 17: Dependencia de activos tipo: Aplicaciones Informáticas

- Dependencia de los activos del tipo REDES DE COMUNICACIONES de:
 - Las instalaciones.
 - El equipamiento auxiliar.

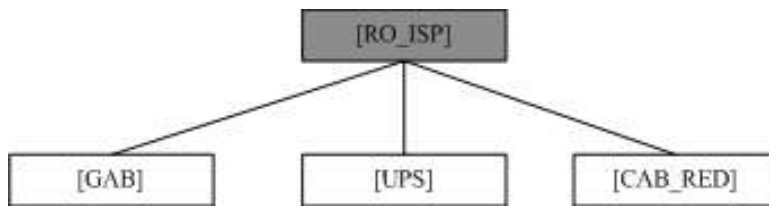


Figura 18: Dependencia de activos tipo Redes de comunicaciones

Recorrido Bottom – Up

- Los activos que son soportados por el tipo de activos PERSONAL son:
 - Los datos a los que tiene acceso.
 - Las aplicaciones que manejan.
 - Los equipos informáticos que gestiona.
 - Los servicios que gestionan.

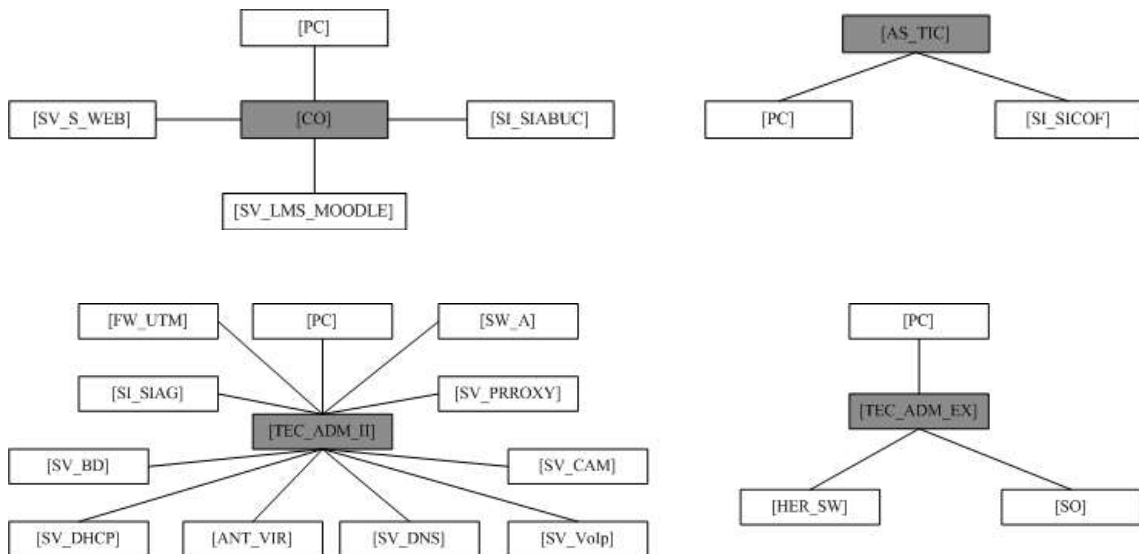


Figura 19: Recorrido Bottom-Up activos personal

- Los activos que son soportados por el tipo de activos EQUIPAMIENTO INFORMATICO:
 - Los servicios habilitan.
 - Los datos que hospeda.

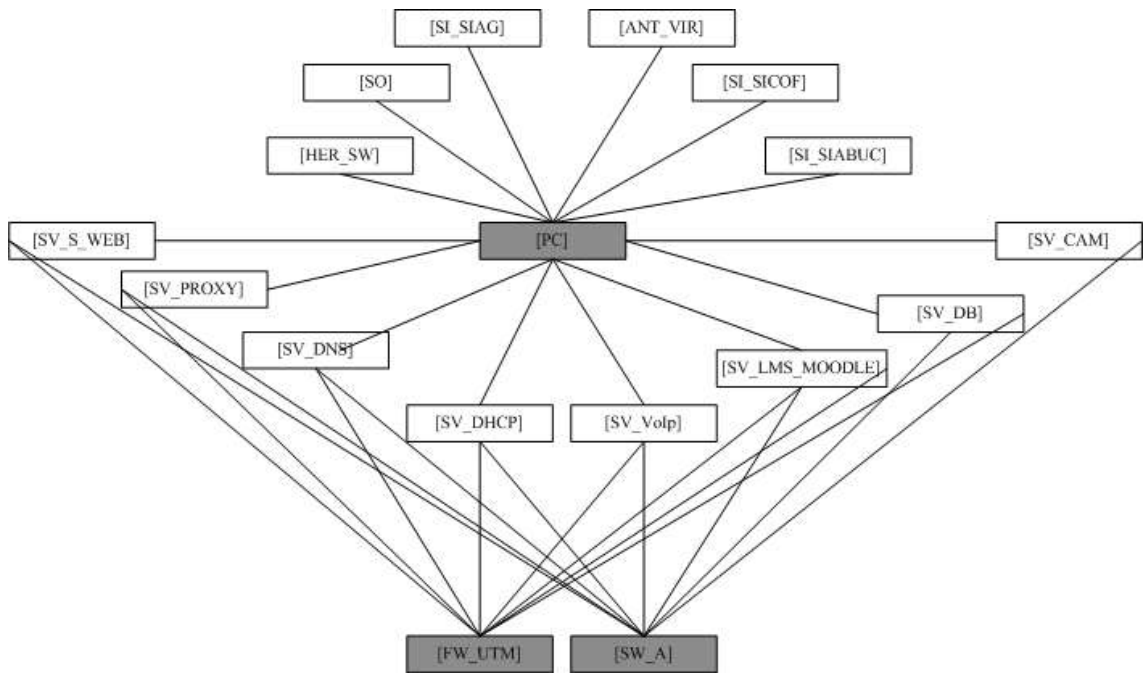


Figura 20: Recorrido Bottom-Up activos Equipamiento informático

- Los activos que son soportados por el tipo de activos REDES DE COMUNICACIONES:
 - Las aplicaciones que habilita.
 - Los servicios que habilita.

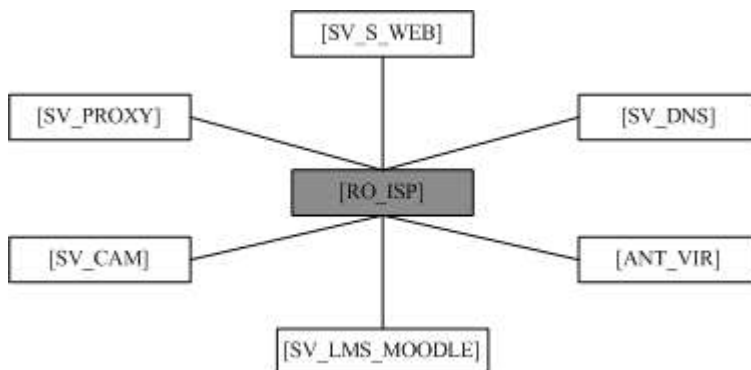


Figura 21: Recorrido Bottom-Up activos redes de comunicaciones

- Los activos que son soportados por el tipo de activos EQUIPAMIENTO AUXILIAR:
 - Las redes de comunicación.
 - Las aplicaciones que habilita.

- Los servicios que habilita.

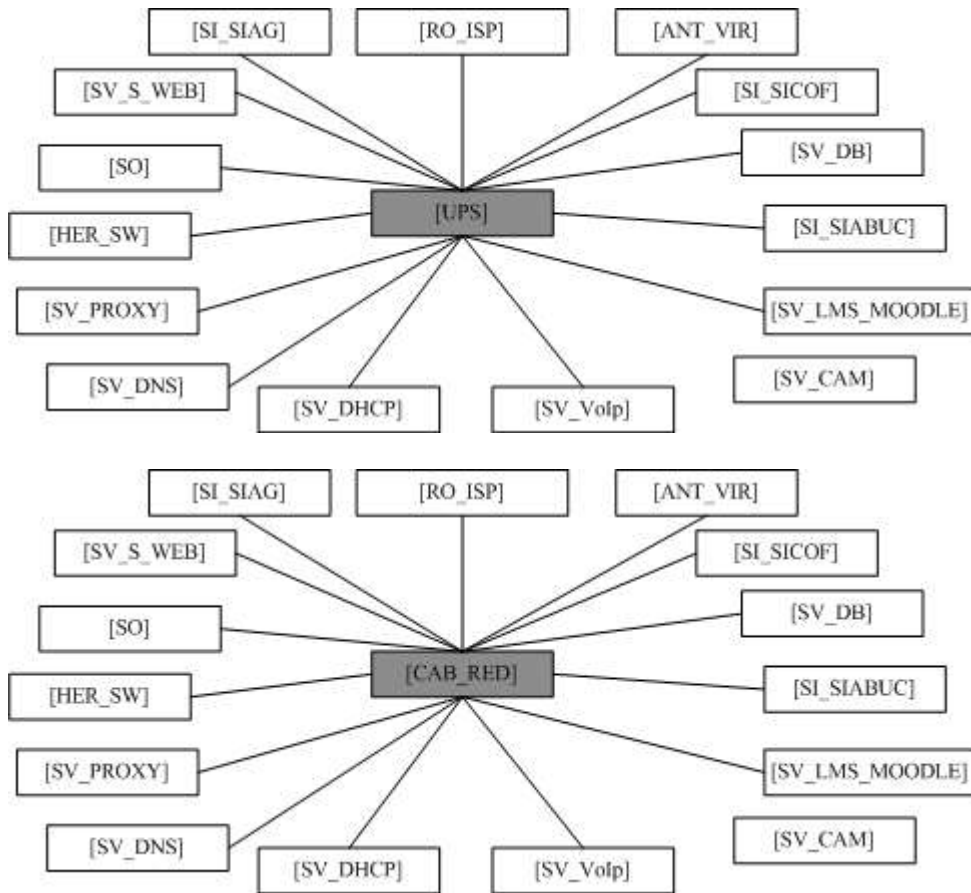


Figura 22: Recorrido Bottom-Up activos Equipamiento auxiliar

- Los activos que son soportados por el tipo de activos INSTALACIONES:
 - Los equipos informáticos que acoge.



Figura 23: Recorrido Bottom-Up activos Instalaciones

- Los activos que son soportados por el tipo de activos APLICACIONES:
 - Los servicios que habilita.

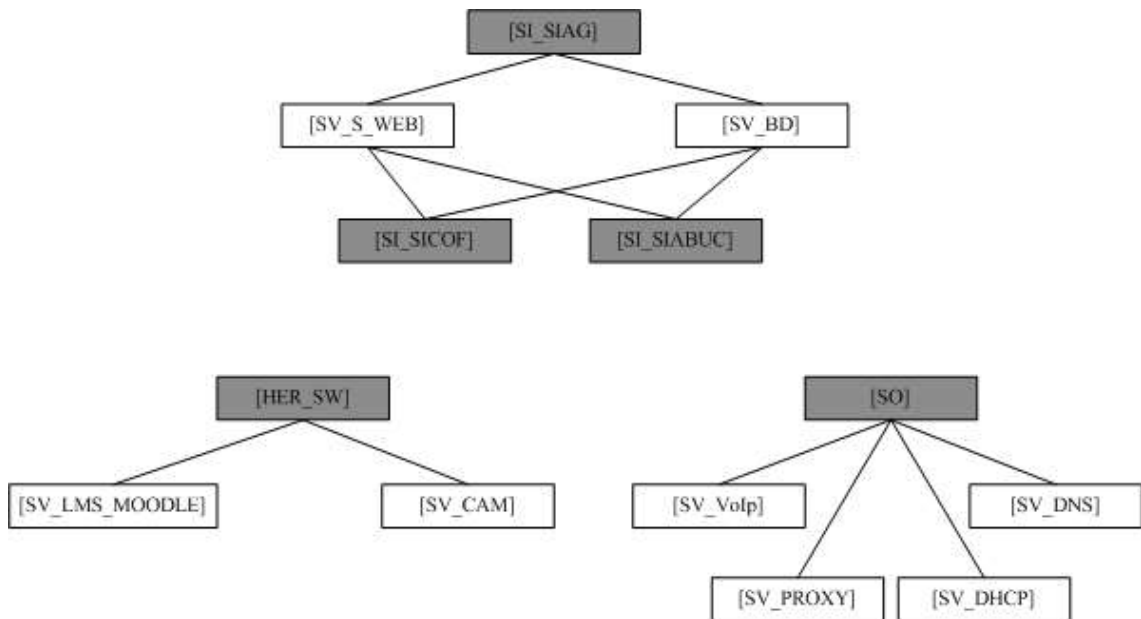


Figura 24: Recorrido Bottom-Up activos Aplicaciones

Tarea 2.1.3: Valoración de los Activos

- ✓ Para realizar el proceso de valoración de activos de acuerdo a la metodología MAGERIT Versión 3; se usa las siguientes dimensiones²⁰:
 - [D] disponibilidad
 - [I] integridad de los datos
 - [C] confidencialidad de la Información.
 - [A] Autenticidad
 - [T] trazabilidad

“Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión”.

Tabla 3: Escala de valoración activos

Valor			Criterio
10	Extremo	E	Daño extremadamente grave.
9	Muy Alto	MA	Daño Muy grave.
6-8	Alto	A	Daño grave.
3-5	Medio	M	Daño importante.

²⁰ Tomado de: 2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8. un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión”.

1-2	Bajo	B	Daño Menor.
0	Despreciable	D	Irrelevante a efectos prácticos.

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

El libro II- Catálogo de elementos de la metodología MAGERIT V.3, permite realizar la valoración de cada uno de los activos haciendo uso de la escala estándar (ver Anexo B Valoración de activos – Escala estándar)

Valoración de Activos Tipo: Aplicaciones

Tabla 4: Valoración activos tipo: aplicaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[SI_SIAG] Sistema de Información Académica y de Gestión ⁽¹⁾	[MA]	[MA]	[M]	[A]	[A]
[SI_SICOF] Sistema Contable y Financiero ⁽²⁾		[A]	[A]	[A]	
[SI_SIABUC] Sistema de Automatización de Bibliotecas de la Universidad de Colima. ⁽³⁾	[M]	[A]			
[SO] Sistema Operativo. ⁽⁴⁾	[MA]	[A]			
[HER_SW] Herramientas Software ⁽⁵⁾	[MA]	[A]			
[ANT_VIR] Antivirus ⁽⁶⁾	[A]				

Fuente: Esta Investigación

- (1) **[4.pi]** probablemente afecte a un grupo de individuos
- [5.lro]** probablemente sea causa de incumplimiento de una ley o regulación
- [9.si]** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
- [1.po]** pudiera causar protestas puntuales.

[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

[1.lg] Pudiera causar una pérdida menor de la confianza dentro de la organización

(2) [4.pi1] probablemente afecte a un grupo de individuos

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios

[5.da2] Probablemente cause un cierto impacto en otras organizaciones

[5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

[2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización

[4.crm] Dificulte la investigación o facilite la comisión de delitos

[8.lbl] Confidencial

(3) [4.pi1] probablemente afecte a un grupo de individuos

[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

[3.po] causa de protestas puntuales

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

[1.adm] pudiera impedir la operación efectiva de una parte de la Organización

[7.rto] RTO < 4 horas

(4) [6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[3.da] Probablemente cause la interrupción de actividades propias de la Organización

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(5) [6.pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente

[3.da] Probablemente cause la interrupción de actividades propias de la Organización

[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística

(6) [7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

Valoración de Activos Tipo: Servicios

Tabla 5: Valoración activos tipo: servicios

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[SV_S_WEB] Servidor Sitios Web. (7)		[MA]	[A]		
[SV_PROXY] Servidor Proxy. (8)	[E]	[A]			
[SV_DHCP] Servidor DHCP(9)	[M]	[A]			
[SV_VoIP] Servidor Telefonía IP	[B]	[B]			
[SV_BD] Servidor Bases de Datos(10)	[E]	[MA]		[MA]	[A]
[SV_CAM] Servidor Cámaras IP(11)	[B]				
[SV_LSM_MOODLE] Servidor herramientas virtuales de aprendizaje. (12)	[M]	[M]	[M]		

Fuente: Esta Investigación

(7) [6. pi2] probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

[7.lro] probablemente cause un incumplimiento grave de una ley o regulación

[1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

[5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local

(8) [6.pi1] probablemente afecte gravemente a un grupo de individuos

- [9.si]** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
- [9.da]** Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
- [6.po]** probablemente cause manifestaciones, o presiones significativas
- [3.adm]** probablemente impediría la operación efectiva de una parte de la Organización
- (9) [1.pi1]** pudiera causar molestias a un individuo
- [3.si]** probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
- [9.da]** Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
- [6.po]** probablemente cause manifestaciones, o presiones significativas
- [3.adm]** probablemente impediría la operación efectiva de una parte de la Organización
- (10) [6.pi1]** probablemente afecte gravemente a un grupo de individuos
- [9.si]** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
- [9.da]** Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
- [6.po]** probablemente cause manifestaciones, o presiones significativas
- [3.adm]** probablemente impediría la operación efectiva de una parte de la Organización
- [9.lg.a]** Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
- (11) [0.4]** no supondría daño a la reputación o buena imagen de las personas u organizaciones
- [4.crm]** Dificulte la investigación o facilite la comisión de delitos
- (12) [4.pi1]** probablemente afecte a un grupo de individuos
- [3.lro]** probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
- [9.si]** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
- [3.da]** Probablemente cause la interrupción de actividades propias de la Organización
- [3.adm]** probablemente impediría la operación efectiva de una parte de la Organización
- [3.lg]** Probablemente afecte negativamente a las relaciones internas de la Organización
- [6.lbl]** Difusión limitada

Valoración de Activos Tipo: Redes de Comunicaciones

Tabla 6: Valoración activos tipo: redes de comunicaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[RO_ISP] Router Proveedor de Servicios de Internet. . ⁽¹³⁾	[MA]	[A]			

Fuente: Esta Investigación

- (13) **[5.pi2]** probablemente quebrante seriamente leyes o regulaciones
[9.lro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
[10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
[9.cei.e] constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
[5.lg.b] Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

Valoración de Activos Tipo: Equipamiento Informático

Tabla 7: Valoración activos tipo: equipamiento informático

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[FW_UTM] Firewall / Equipo Unificado contra Amenazas. ⁽¹⁴⁾	[MA]	[A]	[MA]	[MA]	[A]
[PC] Equipos de cómputo ⁽¹⁵⁾	[M]	[M]	[MA]	[M]	
[SW_A] Switch Administrable ⁽¹⁶⁾	[M]	[M]	[MA]	[M]	

Fuente: Esta Investigación

- (14) **[6.pi2]** probablemente quebrante seriamente la ley o algún reglamento de protección de información personal

- [7.lro]** probablemente cause un incumplimiento grave de una ley o regulación
- [10.si]** probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
- [9.cei.e]** constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
- [9.da]** Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
- [6.po]** probablemente cause manifestaciones, o presiones significativas
- [7.olm]** Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
- [2.lg]** Probablemente cause una pérdida menor de la confianza dentro de la Organización
- (15)** **[5.pi1]** probablemente afecte gravemente a un individuo
- [3.lro]** probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
- [7.si]** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
- [7.cei.d]** proporciona ganancias o ventajas desmedidas a individuos u organizaciones
- [5.da]** Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
- [1.po]** pudiera causar protestas puntuales
- [3.lg]** Probablemente afecte negativamente a las relaciones internas de la Organización
- (16)** **[5.pi1]** probablemente afecte gravemente a un individuo
- [3.lro]** probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
- [7.si]** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
- [7.cei.d]** proporciona ganancias o ventajas desmedidas a individuos u organizaciones
- [7.da]** Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
- [6.po]** probablemente cause manifestaciones, o presiones significativas
- [9.olm]** Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
- [5.lg.b]** Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

Valoración de Activos Tipo: Equipamiento Auxiliar

Tabla 8: Valoración activos tipo: Equipamiento informático

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[CAB_RED] Cableado de Red ⁽¹⁷⁾	[A]	[M]			[M]
[FA_UPS] Sistema de Alimentación Ininterrumpida. ⁽¹⁸⁾	[M]				

Fuente: Esta Investigación

- (17) **[4.pi1]** probablemente afecte a un grupo de individuos
[3.si] probablemente sea causa de una disminución en la seguridad o dificulte la investigación de un incidente
[7.cei.d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[7.da] probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.adm] probablemente impediría la operación efectiva de la Organización
- (18) **[4.pi1]** probablemente afecte a un grupo de individuos
[3.si] probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización
[6.po] probablemente cause manifestaciones, o presiones significativas

Valoración de Activos Tipo: Instalaciones

Tabla 9: Valoración activos tipo: instalaciones

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[GAB] Gabinete de Red ⁽¹⁹⁾	[B]	[D]			

Fuente: Esta Investigación

- (19) [1.1ro] pudiera causar el incumplimiento leve o técnico de una ley o regulación.
 [1.si] pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Valoración de Activos Tipo: Personal

Tabla 10: Valoración activos tipo: personal

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[AS_TIC] Asesor de Tecnologías de Información y Comunicaciones ⁽²⁰⁾	[A]		[MA]		[A]
[TEC_ADMIN_II] Técnico Administrativo Grado II ⁽²¹⁾	[E]	[MA]	[MA]	[MA]	[A]
[TEC_ADMIN_EX] Técnico Administrativo Experto ⁽²²⁾	[MA]	[A]	[A]	[A]	[A]
[CO] Contratista. ⁽²³⁾	[MA]	[A]	[A]	[A]	[A]

Fuente: Esta Investigación

- (20) [6.pi1] probablemente afecte gravemente a un grupo de individuos
 [7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
 [3.cei.d] facilita ventajas desproporcionadas a individuos u organizaciones
 [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
 [5.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
 [6.po] probablemente cause manifestaciones, o presiones significativas
 [7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
 [5.adm] probablemente impediría la operación efectiva de más de una parte de la Organización
 [7.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
- (21) [6.pi1] probablemente afecte gravemente a un grupo de individuos

[9.iro] probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
[9.si] probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
[9.cei.b] de muy elevado valor comercial
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[3.po] causa de protestas puntuales
[10.olm] Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
[7.adm] probablemente impediría la operación efectiva de la Organización
[9.lg.b] Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
[4.crm] Dificulte la investigación o facilite la comisión de delitos

- (22) **[4.pi1]** probablemente afecte a un grupo de individuos
[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[9.cei.d] causa de muy significativas ganancias o ventajas para individuos u organizaciones
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[7.olm] Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
[7.adm] probablemente impediría la operación efectiva de la Organización
- (23) **[4.pi1]** probablemente afecte a un grupo de individuos
[7.si] probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[9.cei.d] causa de muy significativas ganancias o ventajas para individuos u organizaciones
[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
[6.po] probablemente cause manifestaciones, o presiones significativas
[5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
[3.adm] probablemente impediría la operación efectiva de una parte de la Organización

[2.Ig] Probablemente cause una pérdida menor de la confianza dentro de la Organización

8.3.2.2 Actividad A2.2: Caracterización Y Valoración De Las Amenazas

El objetivo de esta actividad es determinar la degradación del activo; proceso que consiste en evaluar el valor que pierde el activo (en porcentaje) en caso que se materialice una amenaza.

Estas Amenazas se han tomado del catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0

Para el desarrollo de esta actividad es necesario tener presente los rangos dados en los siguientes cuadros tanto de frecuencia como de degradación.

Frecuencia de Amenazas

Tabla 11: Valor frecuencia de amenazas

Valor			Criterio
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Degradación de las Amenazas

Tabla 12: Valor degradación de amenazas

Valor	Criterio	
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10%	B	Degradación BAJA del activo

1%	MB	Degradación MUY BAJA del activo
----	----	---------------------------------

Fuente: Magerit V.3 - Libro II - Catálogo de Elementos

Identificación y Valoración de Amenazas Tipo: Aplicaciones Informáticas

Tabla 13: Valoración de Amenazas Tipo: Aplicaciones Informáticas

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.1] Errores de los usuarios	F	MA	A			
[E.2] errores del administrador	FN	A				
[E.4] Errores de configuración	FN	A				
[E.14] Escapes de información	PF			A		
[E.18] Destrucción de información	PF	MA		A		
[A.11] Acceso no autorizado	FN	MA				
[A.15] Modificación de la información	PF		MA			

Fuente: Esta Investigación

Justificación de Amenazas – Aplicaciones Informáticas

[E.1] Errores de los usuarios: Se considera que este tipo de amenaza llegue a presentarse frecuentemente debido a que los usuarios o personal nuevo no es capacitado adecuadamente en el uso de los activos “aplicaciones informáticas” y su degradación es considerada de muy alto impacto en la dimensión de Disponibilidad porque dichos activos están directamente relacionados con los servicios y el modelo de negocio de la institución Universitaria Colegio Mayor del Cauca; en caso de materializarse esta amenaza se tendrá una paralización de casi el 90% de los servicios.

[E.2] errores del administrador: Se da un valor ALTO, ya que si llegase a presentar un “error del administrador” la disponibilidad de las aplicaciones y los servicios que ellos soportan se verá seriamente afectada y debido a que el personal encargado de la administración de estas aplicaciones es altamente calificado; la probabilidad de ocurrencia en POCO FRECUENTE.

[E.4] Errores de configuración: Se valora como de ALTA degradación porque debido a una mala configuración en los activos pertenecientes a las aplicaciones informáticas llevaría a ataques como intrusión, denegación de servicios, robo de

información, etc. Afectando directamente el corazón informático de la Institución Universitaria llevándola a un suspensión de los servicios ofrecidos.

[E.14] Escapes de información: Se considera que la afectación sería Alta para la dimensión de Confidencialidad, ya que si hay escape de información esta puede ser modificada o usada para beneficios propios llevando a pérdida de confianza Institucional.

[E.18] Destrucción de información: Dado el caso de llegarse a presentar esta amenaza las dimensiones más afectadas son la Disponibilidad y la Confidencialidad, porque los activos de las aplicaciones informáticas guardan toda la información que se maneja a diario dentro de los procesos de la Institución universitaria.

[A.11] Acceso no autorizado. La dimensión que afecta directamente es la Disponibilidad y se considera muy alta porque al presentarse una intrusión desencadenaría la materialización de las amenazas [E.14], [E.18] y [A.15] entre otras.

[A.15] Modificación de la información: Afectará directamente la dimensión de integridad en un nivel muy alto, porque de presentarse ataques de modificación de información se van a ver alterados los datos almacenados en los activos pertenecientes a este grupo, causando un caos informático y arrojando datos erróneos a la hora de las consultas y transacciones en cada uno de los procesos normalizados dentro de las labores institucionales.

Identificación y Valoración de Amenazas Tipo: Servicios

Tabla 14: Valoración de Amenazas Tipo: servicios

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.20] Vulnerabilidades de los programas	PF	MA				
[A.5] Suplantación de la identidad del usuario	FN			A	A	
[A.8] Difusión de Software dañino	FN	A				
[A.24] Denegación de Servicios	PF	MA				

Fuente: Esta Investigación

Justificación de Amenazas – Servicios

[E.20] Vulnerabilidades de los programas: La probabilidad de ocurrencia se consideró como PF y que afectará directamente la disponibilidad porque; los programas usados para dar soporte a los servicios implementados en la Institución universitaria primero son evaluados en ambientes de prueba antes de ponerlos en

funcionamiento. Pero en caso de sufrir un ataque por esta amenaza se experimentaría una suspensión de los servicios en un nivel muy alto, cerca al 100%.

[A.5] Suplantación de la identidad del usuario: Este es quizá una de las mayores amenazas visibles dentro de los servicios que ofrece la Institución debido a que no se han implementado normativas para el uso de contraseñas fuertes para el acceso a los servicios, por lo que se puede presentar con mucha frecuencia.

[A.8] Difusión de Software dañino: Esta amenaza es considerada de alto grado de degradación y que pudiese presentar en un nivel de frecuencia normal ; con afectación directa a la disponibilidad; debido a la gran cantidad de equipos de cómputo que están destinados para los alumnos y por la falta de concientización que hay sobre el uso de software licenciado.

[A.24] Denegación de Servicio, Se ha valorado de muy alta degradación en la dimensión de disponibilidad, porque se pueden llegar a presentar errores de programación que no permiten a usuarios autorizados acceder al sistema. Esta amenaza puede ser causa de una reacción en cadena con otras amenazas; pero con poca frecuencia de ocurrencia.

Identificación y Valoración de Amenazas Tipo: Redes de Comunicaciones.

Tabla 15 Valoración de Amenazas Tipo: redes de comunicaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.*] Desastres Naturales	PF	MA				MA
[I.5] Avería de origen físico o lógico	PN	MA				
[I.8] Fallo de Servicio de comunicaciones	PF	A				
[E.2] Errores del administrador	PF	A		A		
[A.4] Manipulación de Configuración.	PF			A	A	

Fuente: Esta Investigación

Justificación de Amenazas – Redes de Comunicaciones

[N.*] Desastres Naturales: Se puede llegar a presentar y la disponibilidad de los activos de redes de comunicaciones tendría un detrimento muy alto porque, el lugar donde este se encuentra no es el adecuado y al ser destruido, se caerían todos los servicios llevando a una paralización total de las actividades en los procesos.

[I.5] Avería de origen físico o lógico: Se considera que afecta la disponibilidad en un nivel MUY ALTO porque; las zonas (lugares) donde se han ubicado no son los más adecuados físicamente para su protección o por el contrario el proceso de instalación y/o configuración no fue el adecuado por mala manipulación.

[I.8] Fallo de Servicio de comunicaciones: El activo de redes de comunicaciones se ha calificado con grado de afectación en la disponibilidad de nivel Alto porque, se cuenta con un solo proveedor de Servicios de internet y se han presentado casos en que por algún fallo en las redes del proveedor se ha visto seriamente afectado los demás servicios configurados y suministrados internamente dentro de la Institución universitaria por varias horas, aunque estos casos se han presentado con muy poca frecuencia.

[E.2] Errores del administrador: Por errores del administrador se puede llegar a tener un Alto grado de degradación en las dimensiones de disponibilidad y confidencialidad ya que al no ser un dispositivo propio la administración está en manos de la Empresa prestadora de este servicio.

[A.4] Manipulación de Configuración: este ítem está ligado directamente con el numeral y las razones expuestas anteriormente en E.2.

Identificación y Valoración de Amenazas Tipo: Equipamiento Informático

Tabla 16: Valoración de Amenazas Tipo: equipamiento informático

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[N.1] Fuego.	PF	MA	MA	MA	MA	MA
[I.2] Daños por Agua.	PF	MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	PF	A				
[E.23] Errores de mantenimiento/ actualización de equipos (hardware).	FN	A				
[A.11] Acceso no	FN			A		

Autorizado.						
[A.23] Manipulación de los equipos.	FN			A		

Fuente: Esta Investigación

Justificación de Amenazas – Equipamiento Informático

[N.1] Fuego: Se consideró de muy alto impacto en todas las dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) al llegarse a presentar fuego como desastre natural porque se perdería todo el equipamiento informático que es el soporte de los demás activos de información como los relacionados en aplicaciones informáticas, servicios, redes de comunicaciones. No se tiene una protección contra esta amenaza, debido a que la institución ha ido adquiriendo estos activos de acuerdo a las necesidades sin ningún tipo de planeación y ningún soporte técnico de seguridad.

[I.2] Daños por Agua. La degradación se consideró como alta en disponibilidad y de poca frecuencia porque, el equipamiento informático se encuentra ubicado sin ninguna precaución, existe un centro de datos ubicado muy cerca de una zona de circulación pública con una ventana que da a la calle y otro centro de datos ubicado debajo de los ductos de aguas negras presentando además un riesgo potencial.

[I.5] Avería de origen físico o lógico: En nivel de degradación que puede presentarse en cuanto a averías de origen físico o lógico son altas afectando la disponibilidad de los activos “equipamiento informático” debido a que las zonas destinadas como centros de datos se usan además como zonas de almacenamiento de equipos de cómputo y cables de red obsoletos, cajas de cartón y gran variedad de material inflamable; otra razón es que la mayoría de equipamiento informático está sometido a largas jornadas de uso (salas de cómputo y laboratorios) con lo que se pueden presentar fallas de físicas o de des-configuración sin un control adecuado.

[E.23] Errores de mantenimiento/ actualización de equipos (hardware): La disponibilidad por errores de mantenimiento o actualización de equipos (hardware) es valorada como de Alto impacto porque, a pesar de contar con personal capacitado para realizar esta tarea no siempre se cuenta con el tiempo suficiente y se han presentado casos en que no es posible ejecutarla esta actividad de manera completa ya que el personal capacitado es contratado semestralmente al mismo tiempo que se inician las labores académicas y administrativas. No se tiene una política de mantenimiento que contrarreste esta amenaza.

[A.11] Acceso no Autorizado: La confidencialidad para este ítem dentro del equipamiento informático es alto debido a que no se tienen implementados normas de seguridad para el acceso a los centros de datos, aunque se controla el

acceso a través de una clave para desactivar la alarma de acceso, pero a estas zonas puede acceder cualquier persona sin tener un permiso especial de acceso, al igual que a las salas de cómputo donde puede acceder cualquier usuario sin restricción ni control alguno.

[A.23] Manipulación de los equipos. Se considera que el grado de degradación que se puede llegar a experimentar es alto en la dimensión de confidencialidad especialmente en los equipos de cómputo de la parte administrativa porque no se han tomado medidas o políticas de seguridad que concienticen a los usuarios en el uso exclusivo del personal contratado en la Institución y del uso de nombre de usuario y contraseña fuerte, y el bloqueo de los equipos en ausencia de estos. Pudiendo dar pie a accesos no autorizados a información y a extracción de partes hardware de los equipos.

Identificación y Valoración de Amenazas Tipo: Equipamiento Auxiliar

Tabla 17: Valoración de Amenazas Tipo: equipamiento auxiliar

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[I.5] Avería de origen físico o lógico	PF	A				

Fuente: Esta Investigación

Justificación De Amenazas – Equipamiento Auxiliar

[I.5] Avería de origen físico o lógico: La valoración del equipamiento auxiliar se realiza por observación directa y se considera que la degradación sería directamente a la disponibilidad en un nivel alto porque en una de las sedes (Claustro de la Encarnación) hay cables principales sin protección y existe algunas UPS expuestas al contacto directo con los usuarios.

Identificación y Valoración de Amenazas Tipo: Instalaciones

Tabla 18: Valoración de Amenazas Tipo: instalaciones

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[A.26] Ataque destructiva	PF	MA				

Fuente: Esta Investigación

Justificación de Amenazas – Instalaciones

[A.26] Ataque destructiva: Se ha considerado que la amenaza A.26 afectaría la disponibilidad del activo instalaciones en un nivel alto porque estos se encuentran sin ninguna protección, las tapas de protección de los gabinetes no tienen seguridad por lo que cualquier persona puede tener acceso a estos (Claustro de la Encarnación).

Identificación y Valoración de Amenazas Tipo: Personal

Tabla 19 Valoración de Amenazas Tipo: personal

Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
		D	I	C	A	T
[E.7] Deficiencia en la organización.	FN	A				
[E.15] Alteración accidental de la información	FN		A	A		
[A.30] Ingeniería Social	PF			A		

Fuente: Esta Investigación

Justificación De Amenazas – Personal

[E.7] Deficiencia en la organización. Se valora como frecuencia normal y de degradación de disponibilidad como Alta porque las directivas de la organización no contratan el personal suficiente para implementar el SGSI necesario dentro de la Institución universitaria y lograr minimizar todas estas amenazas encontradas, además de esto el poco personal se contrata semestralmente y el tiempo para realizar actividades como mantenimiento de equipos de cómputo es muy corto en relación con la cantidad de equipos existentes en la entidad educativa.

[E.15] Alteración accidental de la información: Se puede llegar a materializar la amenaza de alteración accidental de la información por el personal debido a la falta de capacitación y la mala comunicación que existe internamente en la institución universitaria, ya se ha mencionado que el personal nuevo que ingresa no es capacitado adecuadamente en sus labores y mucho menos en base al tema de seguridad informática. Por esta razón se puede ver afectada altamente la confidencialidad e integridad de los datos.

[A.30] Ingeniería Social: Hasta el momento no hemos tenido ningún tipo de inconveniente relacionado con la ingeniería social en el activo de personal, pero es una amenaza latente enlazada con las razones dadas en E.15. Y la falta de

concientización del personal en las mejores prácticas de seguridad informática. Llevando a una afectación Alta en la dimensión de confidencialidad.

La anterior valoración es producto de entrevistas casuales aplicadas con los funcionarios del área de TIC de la Institución universitaria colegio Mayor del Cauca y de encuesta aplicada. (Ver anexo C)

8.3.2.3 Actividad A2.3: Caracterización De Las Salvaguardas

La caracterización de salvaguardas se realiza de acuerdo al nivel de criticidad de los activos incluidos en el análisis de riesgos de la institución universitaria Colegio Mayor del Cauca, basados en el catálogo de elementos que proporciona Magerit v 3.0. (Ver anexo D)

Salvaguardas Activos: Protecciones Generales u Horizontales

Tabla 20: Salvaguardas: protecciones generales u horizontales

Salvaguardas	Dimensión	Evaluación
Control de acceso lógico	[A], [D], [C]	30%
Gestión de incidencias	[D], [C], [T], [A], [I]	50%
IDS/IPS Detección y prevención de intrusión	[C], [I], [A], [D]	70%

Fuente: Esta Investigación

Descripción de Salvaguardas

Control de acceso lógico: Existen medidas básicas para al acceso a las aplicaciones y servicios web a través de la autenticación de usuarios. Por medio de esta salvaguarda se logra proteger a los activos del tipo servicios y aplicaciones en la dimensión de Disponibilidad, Confidencialidad y Autenticidad de los usuarios del servicio, con una efectividad del 30%, la valoración se da porque a pesar de existir mecanismos básicos, no son los ideales y pueden ser fácilmente vulnerados.

Gestión de incidencias: Existe un sistema para la gestión y tratamiento de incidencias, en el cual los usuarios están en la capacidad de solicitar asistencia, hacer seguimiento a su solicitud y pueden calificar el servicio prestado. Esta salvaguarda ayuda a proteger a los activos de cualquier tipo dentro de la organización en las dimensiones de Disponibilidad, Confidencialidad, Autenticidad, Integridad y Trazabilidad del servicio, con una efectividad del 50%. La valoración de efectividad se debe porque en ocasiones el personal encargado de redireccionar las solicitudes no lo hace, o por su parte las atenciones se efectúan

pero nunca son cerradas presentando al final del semestre datos erróneos en los indicadores y resultados de satisfacción de usuario.

IDS/IPS: El sistema de protección perimetral integra un módulo de detección y prevención contra intrusos, este módulo protege de posibles intentos de acceso no autorizado desde Internet y también está activo en la red inalámbrica para proteger el acceso de los servicios y aplicaciones en las dimensiones de Confidencialidad, Integridad, Autenticidad y Disponibilidad. La medida de la efectividad se basa en que se han aplicado las reglas de detección por defecto en el dispositivo, pero se podrían establecer reglas a la medida de los servicios, aplicaciones o sistemas de información según cada requisito y nivel de acceso definido.

Salvaguardas Activos: Protección De Los Datos/Información

Tabla 21: Salvaguardas: protección de los datos/información

Salvaguardas	Dimensión	Evaluación
Copias de Seguridad de los Datos (Backup)	[I], [A], [C], [D], [T]	5%
Uso de firmas electrónicas	[C], [T], [A], [I]	50%

Fuente: Esta Investigación

Descripción De Salvaguardas

Copias de Seguridad de los Datos: Actualmente y luego del primer informe de riesgos entregado a las directivas, se está terminado el montaje de un sistema de copias de seguridad automatizado basado en un NAS (Network Attached Storage) para la información que se catalogue y organice de acuerdo a la criticidad y que será definida por el comité de gestión documental (archivo), se han iniciado pruebas para las copias de seguridad de servidores y Bases de Datos, luego para el resto de información que administre cada funcionario. Esta salvaguarda se aplica en todas y cada una de las dimensiones y su evaluación es baja ya que está en pruebas, además será el inicio del proyecto para integrar e implantar un sistema de gestión documental para la institución.

Uso de firmas electrónicas: Actualmente los líderes de procesos y personal que puede generar cualquier tipo de certificación interna o externa, posee un mecanismo de aplicación de certificación electrónica sobre cualquier documento que genere con el fin de mantener la Autenticidad, Confidencialidad, Integridad y Trazabilidad de la información. La valoración es considerada de esta manera porque no todos usan la firma digital para los documentos que generan por una parte, y los que la utilizan lo hacen regularmente.

Salvaguardas Activos: Protección De Los Servicios

Tabla 22: Salvaguardas: Protección de los Servicios

Salvaguardas	Dimensión	Evaluación
Se aplican perfiles de seguridad	[A], [I], [D]	80%
Protección de servicios y aplicaciones web	[I],[D]	40%
Voz sobre IP	[D]	50%

Fuente: Esta Investigación

Se aplican perfiles de seguridad: Los perfiles de seguridad son creados, configurados y aplicados a través de las políticas en firewalls y software de seguridad antivirus-antispyware, también se aplican en los sistemas operativos tipo servidor, los perfiles son aplicados dependiendo del tráfico entre zonas, acceso a servicios, servidores y protocolos. Su aplicación está relacionada con las dimensiones de Autenticidad, Integridad de los datos y Disponibilidad de la información y su valoración es alta, ya que es uno de los salvaguardas que más se tienen en consideración.

Protección de servicios y aplicaciones web: La protección de servicios así como de las diferentes aplicaciones web dispuestas a la comunidad académica y administrativa tiene salvaguardas basadas en herramientas de autenticación básicas, de igual forma se tratan de llevar medidas de seguridad esenciales para contrarrestar posibles ataques sobre los servicios críticos, aunque faltan medidas que mejoren los niveles de seguridad y acceso a los mismos que pueden comprometer la Integridad de las aplicaciones o la Disponibilidad de los servicios. La clasificación de la evaluación baja se da porque las medidas tomadas no son las mejores, ni las más eficientes, se deben mejorar los procesos para cifrar las contraseñas en algunos sistemas de información y por otro lado generar pautas para la creación, mantenimiento y uso en las mismas.

Voz sobre IP: El servicio de telefonía IP de la institución es brindado por un tercero, han surgido inconvenientes por ausencia del servicio, baja calidad en la transmisión y recepción de la voz y caídas en las llamadas en ciertas ocasiones, el proceso de TIC en la institución como medida alterna decidió implementar un sistema de voz sobre IP propio que está en prueba, con medidas de seguridad que pueden llegar a garantizar en cierta forma la Disponibilidad del servicio, aunque el cambio del sistema del brindado por el tercero al sistema propio se debe hacer manualmente y requiere de un periodo de tiempo corto para dar servicio a todos los clientes en cada una de las sedes; es por eso que la valoración se sitúa en esta escala.

Salvaguadas Activos: Protección De Las Aplicaciones (Software)

Tabla 23: Salvaguadas: Protección de las aplicaciones (Software)

Salvaguadas	Dimensión	Evaluación
Puesta en producción	[I], [D]	50%
Cambios (Actualizaciones y mantenimiento)	[I],[D], [T]	80%

Fuente: Esta Investigación

Puesta en producción: Los productos software en algunos casos son probados en ambientes virtuales para asegurar la compatibilidad, eficiencia y comportamiento de la aplicación antes de sacarla a un ambiente de producción para que la Integridad de los datos y la Disponibilidad esté acorde a lo esperado y la evaluación se asigna porque no existe un procedimiento para llevar este tipo de salvaguarda en su totalidad a la práctica.

Cambios (Actualizaciones y mantenimiento): Se procura mantener un control de versiones cuando se lanzan actualizaciones o mejoras del sistema de información académico, de igual modo el mantenimiento se hace en horarios fuera de los laborales para no perjudicar la normal operación del sistema, cumpliendo con las dimensiones de Disponibilidad, Integridad y Trazabilidad. La evaluación está relacionada con la mediana documentación que se genera en la aplicación del salvaguarda mencionado.

Salvaguadas Activos: Protección De Los Equipos (Hardware)

Tabla 24: Salvaguadas Activos: Protección de los equipos (Hardware)

Salvaguadas	Dimensión	Evaluación
Operación	[D]	60%
Cambios (Actualizaciones y mantenimiento)	[D], [T]	70%

Fuente: Esta Investigación

Operación: La manipulación de los equipos de cómputo se hace de acuerdo a pautas y recomendaciones del grupo de soporte y helpdesk, aunque en realidad no existe un procedimiento definido con buenas prácticas y consideraciones para el uso de los equipos. La Disponibilidad como dimensión está ligada a este salvaguarda, el criterio de evaluación se mantiene de acuerdo al trato del equipamiento a nivel general.

Cambios (Actualizaciones y mantenimiento): Las operaciones de mantenimiento y actualización se hacen de acuerdo a una programación definida semestralmente. En general se cumplen en su totalidad pero hace falta definir un

procedimiento estricto para el cumplimiento y seguimiento de labores en el ámbito preventivo, predictivo y correctivo así como de la calidad y efectividad de la asistencia a incidencias y que se relacionan con la dimensión de Disponibilidad y Trazabilidad.

Salvaguadas Activos: Protección De Las Comunicaciones

Tabla 25: Salvaguadas protección de las comunicaciones

Salvaguadas	Dimensión	Evaluación
Internet: Uso de? Acceso a?	[D], [C],[T]	90%
Seguridad Wireless (WiFi)	[D], [C]	50%

Fuente: Esta Investigación

Internet (Uso de? Acceso a?): Se aplican y monitorean perfiles para asegurar el acceso a internet, no solo en el perfil de seguridad aplicado se evalúan y restringen los accesos a sitios específicos o se aplican técnicas de webfiltering, también se gestiona tráfico y disponibilidad de ancho de banda, escaneo de posibles virus y capacidad de descarga en cuanto a un límite de tamaño por archivo. Se relacionan las dimensiones de Disponibilidad, Confidencialidad y Trazabilidad. La evaluación en general del salvaguarda se mantiene constante y en buenos criterios de efectividad.

Seguridad Wireless (WiFi): Se tiene la red inalámbrica separada física y lógicamente del resto de la red institucional, hay control en los protocolos de salida y entrada, se aplica control en ancho de banda y control de uso de aplicaciones p2p en conjunto con webfiltering y escaneo de virus y spam de salida, control de acceso entre usuarios o aislamiento AP. Se mantiene una relación con las dimensiones arriba citadas y su evaluación se asigna porque tanto el método de autenticación en la red como el acceso a la misma no es el más seguro.

8.3.3 Proceso P3: Estimación Del Estado De Riesgo

Actividad realizada con el propósito de analizar los datos recopilados en las actividades anteriores y evaluar el estado de riesgo, donde se incluye la estimación de impacto y riesgo. Se toma la siguiente escala para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- **MA:** muy alto
- **A:** alto •
- **M:** medio •
- **B:** bajo •
- **MB:** muy bajo

8.3.3.1 Actividad A.3.1: Estimación Del Impacto

El objetivo de esta actividad es determinar el alcance del daño producido sobre los activos de información en caso de llegarse a materializar una amenaza.

Se evalúa el grado de repercusión que pueda presentar cada activo, dentro de las dimensiones de valoración analizadas anteriormente como son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, haciendo uso de la siguiente tabla de doble entrada (ver tabla) propuestas por Magerit v.3.

Los activos con calificación Media deberán ser re-evaluados para mejorar, cambiar o adaptar nuevos controles, los de calificación Alta y muy alta deberán ser objeto atención Urgente.

Tabla 26: Valores estimación de impacto

IMPACTO		DEGRADACION				
		1%	10%	50%	80%	100%
VALOR	MA	M	A	A	MA	MA
	A	B	M	M	A	A
	M	MB	B	B	M	M
	B	MB	MB	MB	B	B
	MB	MB	MB	MB	MB	MB

Fuente: Magerit V.3 – Libro II - Catálogo de Elementos

Impacto acumulado: es el impacto potencial al que está expuesto el sistema tomando como base los valores obtenidos de los activos y valoración de las amenazas, sin tener en cuenta las salvaguardas actuales. Estos requieren atención inmediata.

Impacto residual: es el resultado de combinar el valor de los activos, la valoración de las amenazas y la efectividad de los salvaguardas aplicadas; los activos con resultado muy bajo o bajo (o casillas en blanco), son riesgos con los que se puede convivir pero que se tuvieron en cuenta dentro de los controles, políticas de seguridad y recomendaciones.

Tabla 27: Valoración impacto en activos de información

ACTIVO	AMENAZA	Impacto acumulado					Impacto residual					
		D	I	C	A	T	D	I	C	A	T	
APLICACIONES INFORMATICAS	[E.1] Errores de los usuarios	■	■	■								
	[E.2] errores del administrador	■										
	[E.4] Errores de configuración	■					■					
	[E.14] Escapes de información						■					
	[E.18] Destrucción de información			■								
	[A.11] Acceso no autorizado	■										
	[A.15] Modificación de la información							■	■			
SERVICIOS	[E.20] Vulnerabilidades de los programas	■										
	[A.5] Suplantación de la identidad del usuario								■	■		
	[A.8] Difusión de Software dañino	■										
	[A.24] Denegación de Servicios							■				
REDES DE COMUNICACIONES	[N.*] Desastres Naturales											■
	[I.5] Avería de origen físico o lógico									■		
	[I.8] Fallo de Servicio de comunicaciones									■		
	[E.2] Errores del administrador									■		
	[A.4] Manipulación de Configuración.									■	■	
EQUIPAMIENTO INFORMÁTICO	[N.1] Fuego.								■	■	■	■
	[I.2] Daños por Agua.								■	■	■	■
	[I.5] Avería de origen físico o lógico							■				
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware).							■				

Para la estimación del riesgo se toman los valores de la frecuencia de ocurrencia de cada amenaza frente a los activos e impacto acumulado ya que estos son los activos que necesitan una acción urgente.

Tabla 30: Valoración de riesgo en activos de información

ACTIVO	AMENAZA	IMPACTO					F	RIESGO
		D	I	C	A	T		
APLICACIONES INFORMATICAS	[E.1] Errores de los usuarios						F	
	[E.2] errores del administrador						FN	
	[E.4] Errores de configuración						FN	
	[E.14] Escapes de información						PF	
	[E.18] Destrucción de información						PF	
	[A.11] Acceso no autorizado						FN	
	[A.15] Modificación de la información						PF	
SERVICIOS	[E.20] Vulnerabilidades de los programas						PF	
	[A.5] Suplantación de la identidad del usuario						FN	
	[A.8] Difusión de Software dañino						FN	
	[A.24] Denegación de Servicios						PF	
REDES DE COMUNICACIONES	[N.*] Desastres Naturales						PF	
	[I.5] Avería de origen físico o lógico						FN	
	[I.8] Fallo de Servicio de comunicaciones						PF	
	[E.2] Errores del administrador						PF	
	[A.4] Manipulación de Configuración.						PF	
EQUIPAMIENTO INFORMATICO	[N.1] Fuego.						PF	
	[I.2] Daños por Agua.						PF	
	[I.5] Avería de origen físico o lógico						PF	
	[E.23] Errores de mantenimiento/ actualización de equipos						FN	

	(hardware).							
	[A.11] Acceso no Autorizado.						FN	
	[A.23] Manipulación de los equipos.						FN	
EQUIPAMIENTO AUXILIAR	[I.5] Avería de origen físico o lógico						PF	
INSTALACIONES	[A.26] Ataque destructiva						PF	
PERSONAL	[E.7] Deficiencia en la organización.						FN	
	[E.15] Alteración accidental de la información						FN	
	[A.30] Ingeniería Social						PF	

Fuente: Esta Investigación

8.3.4 Interpretación De Los Resultados

Los controles son adaptados de acuerdo al resultado obtenido en las tablas de la actividad A2.4 sobre estimación de riesgo teniendo en cuenta las necesidades y características de cada activo.

Hardware:

- ✓ Aunque se tiene personal para realizar mantenimiento hardware de tipo preventivo, correctivo y predictivo en los diferentes equipos de la institución tanto en salas de cómputo, equipos administrativos y equipos tipo servidor, la programación que se hace semestralmente no se cumple generalmente por la tardía contratación del personal.
- ✓ No se tienen definidos procedimientos para realizar mantenimiento correctivo y preventivo a nivel técnico, cada persona de soporte procede según el problema o incidencia de acuerdo a su experiencia y conocimiento, pero muchas veces la solución aunque puede ser exitosa no es la más efectiva o la más eficaz, por lo tanto se deben normalizar todos los procedimientos técnicos.
- ✓ No se tienen definidas restricciones para el uso de dispositivos de almacenamiento tipo USB, aunque se tiene un sistema de protección contra virus y spyware para minimizar los riesgos por contagio de virus, las unidades de almacenamiento USB pueden infectar fácilmente un sistema.
- ✓ Ante una falla irrecuperable de hardware en un equipo de cómputo de uso crítico, no se tienen estipulados planes de contingencia que permitan hacer un proceso de recuperación de una manera rápida y más grave aún es que no solo se pueda recuperar la información que se pueda comprometer.

Software:

- ✓ Todo el software que se adquiere, se usa o se desarrolla en la institución está licenciado, gracias a las renovaciones de licencia anuales o a las compras de licencias perpetuas. Existe un gran problema y es que no se tiene un control efectivo para la instalación de software ilegal, o restricciones que no permitan que cualquier usuario pueda instalar software sin la autorización o permiso por parte del personal técnico y/o de infraestructura tecnológica del área TIC.
- ✓ No se contemplan planes y procedimientos cuando se dan de baja equipos, cuando se actualizan o cuando se cambian, sobre todo con la información privada de carácter institucional que puedan llegar a contener dichos equipos.
- ✓ No se tienen procedimientos definidos, ni registros de la aplicación de actualizaciones de software o parches de seguridad en los sistemas base críticos.

Redes:

- ✓ La red se encuentra segmentada física y lógicamente en la totalidad de la sede Bicentenario-Casa Obando, en la sede Encarnación aún no se efectúa la segmentación de las diferentes subredes, lo cual además de ayudar a mejorar la seguridad de la red, mejora el rendimiento y reduce el tráfico innecesario. Se debe realizar esta actividad cuanto antes para disminuir la probabilidad de que se materialice cualquier amenaza.
- ✓ Los sistemas de protección perimetral que posee la institución, requieren anualmente de una renovación de la suscripción y licenciamiento para el funcionamiento de los módulos internos como el filtrado web de sitios, antivirus web, antispam / filtrado de email, firewall, sistema de prevención contra intrusos, escaneo de vulnerabilidades entre otros. En ciertas ocasiones por el proceso licitatorio al que se someten estas adquisiciones de licenciamiento, la institución ha estado expuesta a vulnerabilidades y amenazas de todo tipo porque el periodo efectivo de la licencia expira, y no se tienen planes de contingencia definidos ante falencias de gestión o administrativas en este sentido.
- ✓ Actualmente la sede principal y las dos subsedes alternas se comunican por medio de un enlace de fibra óptica a 30Mbps, en cuanto a servicios de red específicos institucionales y se provee el servicio de internet también por este medio. La redes en cada sede son diferentes a nivel de direccionamiento y los enlaces a servicios o servidores específicos son administrados por medio de mapeo interno de direcciones entre los Firewall y VLANs en los Switches, el problema ocasionado por este modelo de infraestructura tecnológica implementado, es que se crean cuellos de botella en el firewall-UTM (Unified Threat Management) que se tiene en funcionamiento, ya que no está diseñado para soportar el nivel de carga y tráfico de red actual. Es necesario replantear el esquema y modelo de red actual con el fin de unificar la red en las diferentes sedes con el fin de

mejorar en rendimiento, facilidad de administración y eliminación de posibles puntos de falla.

- ✓ Existen reglas de protección de acceso a nivel del firewall desde la red externa (Internet) a servicios y servidores específicos en la red de servidores DMZ (Desmilitarizada), esto se da en el direccionamiento externo o público; pero en el direccionamiento interno (Área Local), se puede obtener acceso por diferentes puertos a varios de los servicios restringidos desde redes como la Inalámbrica, que es una fuente de riesgo latente.

INSTALACIONES FÍSICAS:

- ✓ En la sede principal el estado del cableado estructurado no es la adecuada en su totalidad, aunque existe cableado tipo UTP categoría 6 casi en el 80% de la edificación, este no cumple con las normas mínimas de instalación en algunos casos; por ejemplo los armarios de cableado, patch-panel y patch-cord están en malas condiciones, desorganizados y sin seguridad alguna (Cualquier persona tiene acceso al cableado o switches dentro del armario). El cableado de red y eléctrico en la sede principal no está certificado por la norma RETIE (Reglamento Técnico de Instalaciones Eléctricas) y a nivel de red de datos en ANSI/TIA 568A-B.
- ✓ En cuanto a las condiciones ambientales y de seguridad en centros de cableado principal y servidores, no se tienen sistemas inteligentes de prevención contra incendios, no existen cámaras de seguridad en dichos sitios, los sistemas de aire acondicionado no siempre se encuentran encendidos, el control de acceso a estos lugares no es tan restrictivo, existe gran cantidad de material inflamable como cajas de cartón, muebles de madera y plástico cerca a equipos de comunicación y servidores.

9 Controles

Para especificar los controles de la IUCMC de acuerdo al ciclo PHVA se debe contemplar los siguientes:

- Controles relacionados con terceros: Cuando exista la necesidad de otorgar acceso a terceras partes a la información de la Empresa, los Responsables de los Sistemas de Información, llevarán a cabo este proceso, debidamente autorizado por el propietario de la información, teniendo en cuenta, entre otros aspectos:
 - ✓ El tipo de acceso requerido (físico/lógico y a qué recurso).
 - ✓ Los motivos para los cuales se solicita el acceso.
 - ✓ Los controles empleados por la tercera parte.
 - ✓ La incidencia del acceso en la seguridad de la información en la Institución.
 - ✓ Cumplimiento Institucional.

- Acuerdos de control de accesos que contemplen:
 - ✓ Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
 - ✓ Proceso de autorización de accesos y privilegios de usuarios.
 - ✓ Requerimiento para mantener actualizada una lista de personas autorizadas a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
 - ✓ Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
 - ✓ Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
 - ✓ Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
 - ✓ Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
 - ✓ Proceso claro y detallado de administración de cambios.
 - ✓ Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
 - ✓ Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
 - ✓ Controles que garanticen la protección contra software malicioso.
 - ✓ Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

9.1 Mecanismos De Control De Activos

Seguridad Física y Ambiental

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de los Sistemas de Información.

Controles de Acceso Físico

Los cuartos de comunicaciones y servidores se resguardarán mediante el empleo de controles de acceso físico, a fin de permitir el ingreso sólo al personal autorizado. Esta autorización es definida por el Comité de Seguridad Informática.

Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. Se tomará en cuenta las disposiciones y estándares en materia de sanidad y seguridad.

Se considerarán las amenazas de seguridad que representan los edificios y zonas aledañas.

Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecerán controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará respaldado a través de UPS y planta de energía con respaldo de un tiempo prudencial.

Mantenimiento de Equipos

La realización de tareas de mantenimiento preventivo al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Comité de Sistemas.

Controles Contra Software Malicioso

El Comité de Sistemas y de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso y designará el personal encargado para dichos controles.

Controles de Redes

El Área de TIC definirá controles para garantizar la seguridad de la infraestructura de comunicaciones y los servicios conectados en las redes de la Institución, contra el acceso no autorizado.

Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los firewalls

Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

Administración de Medios Informáticos Removibles.

Con el propósito de salvaguardar las copias de seguridad de los sistemas de información de la empresa, se dispone de un contrato con una empresa que custodia y salvaguarda la información que periódicamente es enviada según el procedimiento establecido para cada sistema.

Seguridad del Correo Electrónico

Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.

Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.

El acceso de usuarios remotos a las cuentas de correo electrónico.

El uso inadecuado por parte del personal.

Control de Acceso al Sistema Operativo

Identificación Automática de Terminales, El Área de TIC realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso y uso del Sistema Operativo a través del Controlador de Dominio.

Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, los operarios, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo.

Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

- Sugerir el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el procedimiento establecido para el manejo y uso de contraseñas.
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto anterior.
- Obligar a los usuarios a cambiar las contraseñas provisionales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Almacenar las contraseñas utilizando un algoritmo de cifrado.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

Control de Acceso a las Aplicaciones

- ✓ Restricción del Acceso a la Información. Los usuarios de los sistemas de aplicación, incluyendo al personal de TIC, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a los permisos otorgados de acuerdo al perfil solicitado por cada coordinador de área, Administradores o responsables de los Sistemas de Información.
- ✓ Validación de Datos de Entrada. Se validarán durante la etapa de diseño los controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Controles Criptográficos

Para la protección de claves de acceso a sistemas, datos y servicios.

Para el resguardo de información, en el proceso de generación de backups de los sistemas de información.

Seguridad de los Procesos de Desarrollo y Soporte

Procedimiento de Control de Cambios. Se implementarán controles durante la implementación de cambios verificando el cumplimiento del procedimiento establecido. Éstos garantizarán que se cumplan los procedimientos de seguridad y control.

Revisión Técnica de los Cambios en el Sistema Operativo Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad. Estas actividades serán ejecutadas por los administradores de los sistemas de información.

Para una mejor gestión de los controles, se ha realizado la siguiente clasificación de acuerdo a los objetivos de control (planteados en COBIT²¹)

9.2 Resumen De Controles

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Política de seguridad de información	
Documentar política de seguridad de información	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
Organización de la seguridad de la información	
Compromiso de la gerencia con la seguridad de la información	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.

²¹ ISACA Trust in, and value from, information systems. [en línea] <https://www.isaca.org/Pages/default.aspx>

Coordinación de la seguridad de información	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
Asignación de responsabilidades de la seguridad de la información	Se deben definir claramente las responsabilidades de la seguridad de la información.
Acuerdos de confidencialidad	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
Gestión de activos	
Inventarios de activos	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
Seguridad de los recursos humanos	
Roles y responsabilidades	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
Seguridad física y ambiental	
Perímetro de seguridad física	Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
Seguridad oficinas	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
Seguridad de computadores	
Ubicación protección equipo	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que llevan data o

	sostienen los servicios de información deben ser protegidos de la interceptación o daño.
Mantenimiento de equipo	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
Protección contra software malicioso	
Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
Copias de seguridad o backup (respaldo de información)	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
Gestión de seguridad de redes	
Controles de red	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
Seguridad de los servicios de red	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
Protección contra software malicioso	
Política de control de acceso	Se debe establecer, documentar y revisar la política de control de acceso.
Gestión de privilegios	Se debe restringir y controlar la asignación y uso de los privilegios.
Gestión de la clave del usuario	La asignación de claves se debe controlar a través de un proceso de gestión formal.
Control de acceso a redes	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.

Tabla 31: Clasificación de controles

Fuente: Esta investigación

10 Políticas De Seguridad Informática

Las políticas y los estándares establecidos, son lineamientos y referentes marco para la administración y conservación de los activos informáticos, los documentos y los archivos de la Institución Universitaria Colegio Mayor del Cauca.

Con la definición de las políticas de seguridad de la información, se establece al interior de la institución una cultura de calidad, operando de forma confiable y controlada, estructurando medidas y patrones técnicos de organización y administración de las tecnologías de la información y la comunicación, involucrando todo el equipo humano comprometido en la seguridad y el uso de los recursos informáticos. (ver anexo D).

En la institución universitaria Colegio mayor del Cauca los documentos, los archivos y la información son de carácter público y por lo tanto cumple con los objetivos esenciales de organización, clasificación, conservación y consulta en las diferentes fases del ciclo vital de los documentos.

Finalidad De La Política

Con el establecimiento de las políticas de seguridad informática, se da soporte a la producción, gestión, recuperación, conservación y difusión de los documentos y la información institucional, bajo las dimensiones de confiabilidad, integridad y autenticidad, características indispensables en el uso efectivo para la gestión institucional, toma de decisiones y como garantía de la prestación oportuna de los servicios que oferta el colegio mayor del Cauca.

Alcance

El alcance de las políticas de seguridad en el Colegio Mayor del Cauca debe estar ligada al PGD institucional (Programa de Gestión Documental) desde la producción o recepción de los documentos, el direccionamiento, tramite, consulta y conservación o disposición final según la normativa del área de archivo (por tratarse de administración de información en todos sus formatos), pasando por el reconocimiento de la información y los documentos como un activo estratégico para el cumplimiento misional, hasta la identificación y mitigación de riesgos.

Política De Seguridad Institucional

La información y los documentos contenidos y transportados en los recursos (activos) informáticos, serán clasificados, transmitidos, almacenados y custodiados de forma segura y controlada como soporte de los procesos institucionales misionales y de apoyo. El proceso institucional de gestión de recursos tecnológicos propondrá y controlara el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de la información automatizada en general.

Todo servidor o funcionario nuevo de la institución Universitaria Colegio Mayor del Cauca debe contar con la inducción sobre las políticas y estándares de seguridad informática, donde se dan a conocer las obligaciones y sanciones en que se puede incurrir en caso de incumplimiento.

10.1 Seguridad Relacionada Al Personal

10.1.1 Funcionarios

- ✓ Los usuarios y servidores de IUCMC, deben preservar y proteger los registros y la información utilizada en la infraestructura tecnológica, de igual forma protegerán la información almacenada o transmitida ya sea dentro de la red interna institucional, a otras dependencias, a sedes alternas o redes externas.
- ✓ Toda información producida y/o manipulada por los funcionarios se considera propiedad del Colegio Mayor del Cauca.
- ✓ Todos los archivos de computadores que sean proporcionados por personal externo o interno (programas, software, bases de datos, documentos y hojas de cálculo) que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus, utilizando el software antivirus autorizado en la institución antes de ejecutarse.
- ✓ Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- ✓ El funcionario deberá manipular únicamente la información necesaria para el desarrollo de las funciones estipuladas en el contrato.
- ✓ La información manipulada por el funcionario de la Institución no debe ser divulgada a terceros.
- ✓ Ningún funcionario tiene derecho sobre la información institucional que procede internamente.
- ✓ El usuario de la red IUCMC debe regirse por las normas y disposiciones de seguridad informática de la Institución Universitaria Colegio Mayor del Cauca
- ✓ El usuario es responsable de la información personal y acciones causadas por la manipulación de equipos de cómputo y red institucional.

10.1.2 Capacitación

- ✓ Los funcionarios y/o usuarios que hagan uso de la red de datos de la Institución deberán ser capacitados en temas básicos de seguridad de la información y específicos de acuerdo al área o función encomendada.
- ✓ Se debe tomar medidas de seguridad al realizar capacitaciones al personal interno o externo para que no comprometan los activos de información, dichas capacitaciones se deberán hacer en ambientes de prueba y/o simuladores.

- ✓ El responsable de TIC designara un equipo especializado en seguridad informática para realizar las capacitaciones a cada dependencia.
- ✓ El equipo de seguridad informática deberá planear e informar las fechas de las capacitaciones
- ✓ Las capacitaciones de seguridad informática deberán contar con el material de apoyo suficiente y acorde a la capacitación, además este deberá ser proporcionado a los usuarios.
- ✓ Las capacitaciones deberán hacerse en ambientes de prueba.
- ✓ Dentro de las capacitaciones deberán hacerse revisiones de los activos informáticos y servicios relacionadas con el tema.
- ✓ Es deber de los funcionarios y/o terceros asistir a las capacitaciones así como de acatar cada una de las disposiciones dispuestas en cada una de ellas.

10.1.3 Incidentes Y Atención A Usuarios

- ✓ Se efectuaran copias de respaldo o back-up como salvaguarda de información crítica de los procesos institucionales significativos, la realización de copias de respaldo o seguridad se harán periódicamente en los equipos administrativos y servidores. Las copias de seguridad deben rotularse para ser almacenados, se utilizara el software en la opción de back-up, o cd/DVD y la rotulación contenida, fecha de copia, asunto, código según TRD digital y se entregará a la oficina de TICS para almacenamiento y custodia.
- ✓ Todo incidente u ocurrencia de accidente de seguridad informática debe ser reportado oficialmente a TICS.
- ✓ Las solicitudes de atención a usuarios serán gestionadas a través del sistema GLPI y solucionadas en el menor tiempo posible.
- ✓ Se documentará detalladamente cualquier novedad que conduzca a poner en riesgo la seguridad de la información, posterior a la revisión de log o registros del sistema con el propósito de analizar la situación y crear o modificar controles en pro del aseguramiento informático.
- ✓ El administrador del sistema de incidencias (atención a usuarios) deberá priorizar las solicitudes y asignar el personal adecuado para dar solución a los problemas en los puestos de trabajo.

10.2 Seguridad Lógica

10.2.1 Control De Acceso

- ✓ El responsable de TIC proporcionará los documentos necesarios (formatos, guías, etc.) para el uso de los sistemas.

- ✓ Todo el personal o usuario informático nuevo de la institución deberá ser notificado a la oficina de TICS para asignarle derechos correspondientes, equipo, creación de usuario para la red y anulación en caso de retiro.
- ✓ De acuerdo a la norma ISO/IEC 27001:2005 A.10.1.3: Todos y cada uno de los contratistas y/o funcionarios, el personal de TICS, les entregará su rol en el sistema, definiendo sus privilegios. Por lo anterior, no es permitido que de un trabajador a otro se intercambien roles y/o cuentas para accesos al sistema. El responsable de la Oficina de TICS, tendrá un listado actualizado para velar por el cumplimiento.
- ✓ Las solicitudes de información de cualquier tipo debe hacerse por escrito ante el responsable de la dependencia o como lo tenga normalizado IUCMC, de no cumplirse se procederá a:
 - Informar de manera escrita al grupo de seguridad informática o en su defecto al responsable del área de TIC y/o dependencia a la que se realiza la solicitud
 - Negar en su totalidad la ejecución de la solicitud.
 - Denunciar a las autoridades competentes después de haber sido analizado el caso por el comité de seguridad informática.

10.2.2 Administración De Acceso De Usuarios

- ✓ Se considera usuarios de la red institucional a los alumnos, docentes, contratistas, administrativos y en general cualquier persona que haga uso de los servicios de la red.
- ✓ El comité o equipo de seguridad asignará a los usuarios con acceso a los sistemas e información de la Institución una cuenta de acceso previa clasificación y verificación de la función que desarrolla dentro de la Institución.
- ✓ Los alumnos son considerados como usuarios limitados, estos tendrán acceso a equipos de cómputo en una red especial y gozaran de servicios de internet y recursos compartidos, cualquier novedad o solicitud deberá ser evaluada y si es necesario deberá ser modificada este control.
- ✓ Todos los usuarios (incluido el personal de soporte técnico, como los operarios, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo.
- ✓ No se proporciona ningún tipo de servicio a los usuarios de cualquier índole, área, dependencia, o facultad sin haber cumplido todos los requerimientos para su autorización.
- ✓ La oficina de TICS deberá implementar un sistema de administración de contraseñas, donde se contemple los siguientes parámetros:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el procedimiento establecido para el uso de contraseñas
- Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto anterior.
- Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, no tenga acceso a información temporal o en tránsito de forma no protegida.

10.2.3 Uso De Contraseñas

Las contraseñas usadas por los usuarios deberán cumplir con los siguientes requisitos:

- ✓ Usar una combinación alfanumérica
- ✓ la contraseña debe tener una longitud mínima de 12 caracteres.
- ✓ La contraseña debe tener un periodo de vigencia, luego deberá ser cambiada por una nueva y diferente a la anterior.
- ✓ No deberá usarse datos personales, acrónimos ni datos directamente relacionado con el usuario.

10.2.4 Responsabilidades De Los Usuarios

- ✓ Es responsabilidad de los usuarios el uso que se haga de la cuenta de acceso y contraseña proporcionada a los sistemas y equipos de cómputo.
- ✓ El usuario deberá eliminar cualquier documento, colilla o archivo suministrado por el administrador del sistema y/o encargado de proporcionar la contraseña

para su acceso con el propósito de evitar suplantación de identidad y uso de la información tanto institucional como personal.

- ✓ Si no se cuenta con un sitio seguro para guardar la contraseña, se recomienda no hacerlo en papel, agenda o lugar de fácil acceso.
- ✓ El usuario es el único responsable del uso que dé al correo institucional o personal.
- ✓ El usuario deberá velar por la protección de acceso a su equipo de cómputo, a través del uso de protector de pantalla con contraseña que será activado manualmente al momento que requiera ausentarse.
- ✓ Los alumnos y personal en general es responsable de guardar su información personal, la institución Universitaria no se hace responsable por la pérdida de esta.
- ✓ Los usuarios deben reportar al responsable de TIC, personal técnico, área de TIC o equipo de seguridad cualquier daño, falla, riesgo o amenaza detectada.

10.2.5 Uso Del Correo Electrónico

- ✓ Los usuarios informáticos de la Institución Universitaria Colegio Mayor del Cauca, deben tratar los mensajes y los archivos adjuntos como información de propiedad de la institución.
- ✓ No se deben utilizar cuentas de correo electrónico asignadas a otros usuarios, ni recibir mensajes en cuentas de otros, si fuera necesario leer el correo de alguien más (mientras se encuentra por fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externo al Colegio Mayor del Cauca, a menos que cuente con una autorización de la oficina de TICS.
- ✓ Los usuarios informáticos de la Institución Universitaria Colegio Mayor del Cauca, podrán enviar información reservada o confidencial vía correo electrónico siempre y cuando vaya de manera encriptado y destinada exclusivamente a personas autorizadas y en ejercicio de funciones y responsabilidades institucionales.
- ✓ La oficina de TICS se reserva el derecho de monitorear las cuentas de usuario con actividad sospechosa que pongan en riesgo la seguridad de activos y de información Institucional.
- ✓ El correo electrónico institucional es un servicio gratuito y la Institución Universitaria no se responsabiliza por el mal uso que se dé.

10.2.6 De Acceso A Terceros

- ✓ Los proveedores, personal externo o personal que tenga algún tipo de relación con la Institución son considerados como usuarios terceros.

- ✓ El acceso a terceros será limitado en cuanto a privilegios y tiempo de acceso a los sistemas de información de la institución.
- ✓ Para suministrar permiso de acceso a usuarios externos o terceros este deberá presentar ante el área TIC o equipo (comité) de seguridad documento firmado de aceptación de confidencialidad.
- ✓ Los usuarios considerados terceros bene acatar cada una de las disposiciones de las políticas y normas de seguridad dispuestas internamente en la Institución además de las exigidas puntualmente dentro del contrato.

10.2.7 De Acceso a La Red

- ✓ Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada, en la cual los usuarios o funcionarios realicen exploración de los recursos informáticos en la red de la IUCMC, así como de las aplicaciones que sobre dicha red operan, con fines a detectar y explotar una posible vulnerabilidad.
- ✓ Los usuarios autorizados deberán tener una cuenta de acceso a la red proporcionada por la oficina de TIC.
- ✓ Los usuarios informáticos de las áreas o procesos de la IUCMC, no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de archivos (ftp) u otro tipo de protocolo para la transferencia de información, empleando la infraestructura de la red de la institución sin autorización de la oficina de TICS.
- ✓ La oficina de TICS deberá proporcionar los mecanismos de seguridad necesarios para realizar bloqueos, enrutamiento, filtrado de tráfico de red que garanticen el acceso controlado desde la red pública a la red interna y viceversa.
- ✓ Se deberán guardar periódicamente registros o logs de acceso a los sistemas.

10.2.8 De Backups

- ✓ Los backups deberán ser almacenados en un lugar exclusivo designado para este fin, garantizando su custodia, evitando posibles daños o hurto de personal interno y/o externo.
- ✓ Los backups eran usados exclusivamente en caso especiales.
- ✓ Los responsables de la seguridad informática deberán realizar procedimientos tanto para generar como para restaurar backups de información.
- ✓ Los backups de información deberán ser contemplados para suplir cualquier tipo de incidente, este procedimiento debe ser documentado.
- ✓ La información será clasificada de acuerdo a las tablas de retención documental emanadas del área de archivo y de acuerdo a esta priorización se

harán las atenciones a usuarios, personal administrativo y docente de la Institución.

10.2.9 Servidores

- ✓ La configuración de sistemas operativos de servidores es labor exclusiva del personal autorizado y de su administrador.
- ✓ Se deberán generar perfiles de usuario y asignar únicamente los permisos para acceso a los módulos que este debe manipular; no se dará acceso total a usuarios diferentes al administrador.
- ✓ El administrador deberá velar por la configuración adecuada de cada uno de los servicios que reposan en el servidor y eliminar los que por defecto se crean.

10.2.10 Equipos De Cómputo

- ✓ Los equipos de cómputo de docentes, administrativos, contratistas deberán tener configurada y hacer uso de cuantas de usuario y contraseña.
- ✓ Los usuarios de IUCMC, no deben mover o reinstalar, reubicar los equipos, ni retirar sellos de los mismos sin autorización.
- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente, destinada para archivos de programas y sistemas operativos generalmente /c:/
- ✓ Es prohibido que el usuario o funcionario distinto al personal autorizado abra o destape los equipos, asimismo cuando se requiera realizar cambios de reubicación en lugares físicos de trabajo o locativos, debe ser notificado con 3 días de anticipación a la oficina de TICS.
- ✓ El préstamo de portátiles o laptops tendrá que solicitarse en las secretarías de cada una de las facultades.

10.3 Responsabilidades Y Procedimientos Operativos

- ✓ Es responsabilidad del encargado de la oficina de TICS planear adecuadamente los horarios de mantenimiento en jornadas que no se obstaculice el normal funcionamiento de los equipos de administrativos, docentes y alumnos.
- ✓ Al terminar la jornada laboral los usuarios deberán dejar apagados los equipos de cómputo evitando el acceso no autorizado a terceros.

10.3.1 Protección Contra Software Malicioso

- ✓ Para prevenir infecciones de virus informático, los usuarios de la IUCMC, no deben hacer uso de software que no haya sido proporcionado y validado por la oficina de TICS. En el caso de sospecha de infección de virus, debe dejar de usar inmediatamente el equipo y notificar la sospecha a la oficina de TICS.
- ✓ El área de TIC o jefe a área deberá proporcionar software de protección como antivirus, antimalware y/o seguridad perimetral (firewall) para protección de la información manipulada y almacenada en los equipos de cómputo y servidores.

10.3.2 Mantenimiento

- ✓ El mantenimiento, preventivo y/o correctivo es una actividad exclusiva del personal de soporte técnico.
- ✓ Cuando se va a realizar mantenimiento en alguno de los equipos, se debe dar aviso con anticipación al usuario informático o servidor público.
- ✓ Es deber del personal de soporte técnico llevar registro de los mantenimientos y cambios realizados a los equipos de cómputo y de red.

10.3.3 Control de Medios de Almacenamiento

Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

10.4 Seguridad Física

10.4.1 De Los Equipos

- ✓ Se deberá reportar y registrar al momento de la entrada, en el área de recepción, los equipos de cómputo, de comunicaciones, medio de almacenamiento y herramientas que no sean propiedad de la institución
- ✓ Cuando un funcionario no autorizado o visitante requiera entrar a las salas donde se encuentran los servidores, debe solicitar autorización mediante comunicación interna a la oficina de TICS.
- ✓ Los equipos de cómputo, cables, UPS, subestación eléctrica, aires acondicionados, dispositivos de almacenamiento y de comunicación móvil o inalámbrica, deben estar amparados en pólizas contra robo, pérdida, daño o acceso no autorizado. Además, no será permitido el consumo de líquidos, alimentos, ni humo dentro de los centros de cómputo o salas donde reposen los equipos. [ISO/IEC 27001:2005 A.9.2]

10.5 Seguridad Legal

10.5.1 Licenciamiento De Software

- ✓ Se prohíbe en la Institución Universitaria Colegio Mayor del Cauca, instalar software y programas no autorizados y sin licenciamiento en la red de la IUCMC.
- ✓ Los programas o Software serán instalados única y exclusivamente por personal perteneciente al área de TIC (sistemas) o personal autorizado previa verificación de su legalidad.
- ✓ Los usuarios o funcionarios que requieran instalación de software deben justificar su uso, indicando el equipo donde se instalará y el período de tiempo que será usado.
- ✓ Se considera una falta grave que los usuarios, instalen cualquier tipo de programa en sus computadores, servidores, estación de trabajo u otros equipos conectados a la red del colegio mayor que no esté autorizado por la oficina de TICS.
- ✓ Se debe mantener por parte de la oficina de TICS el inventario actualizado de equipos, programas y licencias instaladas.

11 Recomendaciones

Se debe realizar la socialización del proyecto “análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca” para aprobar o mejorar la ejecución de los controles propuestos al interior de la IUCMC.

Implementación del Sistema de Gestión de Seguridad de la Información para proteger el activo más valioso “La Información”, para esto es necesario ccontratar personal capacitado en seguridad

Capacitar al personal del área de TIC o de sistemas en temas de seguridad informática para apoyar el proceso de capacitación a todo el personal involucrado con la IUCMC.

Evaluar y aprobar las políticas generadas dentro de este proyecto.

Los nuevos controles de seguridad resultado del análisis de riesgos deben ser puestos en funcionamiento a la mayor brevedad, toda vez que de esto depende la continuidad del negocio de la IUCMC.

Las directivas (la alta gerencia), deben tener en cuenta este estudio de seguridad informática, la aplicación e implementación del mismo además de incluir recursos necesarios para el desarrollo de la misma en el año 2015.

Los funcionarios de la institución deben recibir un ciclo de capacitación y socialización del desarrollo del proyecto para conocer y adoptar la política de cambio de seguridad informática en pro de las mejores prácticas.

Las directivas de la institución deben por medio del área de TIC y de los directos responsables en este campo posibilitar estos cambios, haciendo uso de jornadas pedagógicas de simulacro de desastre informáticos, y así poder comparar los beneficios de los nuevos controles de seguridad.

Incluir dentro de las tareas del equipo de TIC auditorias permanentes a los activos de información para actualizar controles y contribuir con el desarrollo de mejores prácticas relacionadas con la seguridad de la información.

12 Conclusiones

Finalizado el proyecto se logra alcanzar todos los objetivos planteados; los controles generados permiten mejorar y normalizar los procesos de la IUCMC aplicando los conceptos de seguridad de la información.

Aplicar la metodología MAGERIT para el análisis de riesgo es el primer paso para garantizar la seguridad de los activos de información y el normal funcionamiento interno de la IUCMC.

El análisis de riesgo aplicado, permite conocer de manera global el estado actual de la seguridad informática dentro de la IUCMC.

Los controles y políticas de seguridad de la información resultado de este análisis de riesgos pueden ser tomados como soporte para la implementación del SGSI; encaminado a:

Reducir el ambiente de riesgo vigente.

Disponer de las medidas de control interno necesarias.

Disminuir el grado de exposición de los sistemas que se procesan.

Incrementar la confiabilidad, integridad y disponibilidad de la información.

Optimizar los procesos orientados al cumplimiento de los objetivos de la Institución.

Conseguir disminuir el riesgo actual a su nivel mínimo.

La IUCMC actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de las directivas (alta gerencia) y de todo el personal es posible contrarrestar.

13 Bibliografía

[ARIA05] ARIAS RUIZ DE SOMAVIA, RAMÓN; Análisis de Riesgos del Sistema de Información clasificado de Isdefe. Informe interno de la empresa. 2005.

Ávila Arzuza, M. (2012). *Implantación de un SGSI*. (Trabajo Final de Máster). Universidad Oberta de Catalunya. Recuperado de <http://openaccess.uoc.edu/webapps/o2/handle/10609/14743>. Trabajo de grado para la implantación de un Sistema de Gestión de Seguridad de la Información en entorno real.

Bisogno, María Victoria (2004). Metodología para el aseguramiento de entornos informatizados – MAEI. Universidad de Buenos Aires (Argentina). Recuperado de: <http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenierainformatica>

BOLAÑOS, María C y ROCHA G. Mónica. 25 de marzo de 2014. Auditoria de SI. Magerit V3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).[en línea]: <http://asijav.weebly.com/auditoria-de-sistemas-de-informacioacuten/magerit-v3-metodologa-de-anlisis-y-gestin-de-riesgos-de-los-sistemas-de-informacion>.

CALDER, Alan. Implementing information security based on ISO 27001/ISO 27002, ISBN 9087538189, 2012. [en línea]. http://books.google.com.co/books/about/Implementing_information_security_based.html?hl=fil&id=515eAgAAQBAJ&redir_esc=y

Cevallos Michilena, Mario Andres, Metodología de seguridad informática con base en la norma ISO 27002 y en herramientas de prevención de intrusos para la red Administrativa del Gobierno Autónomo Descentralizado de San Miguel de Ibarra. <http://repositorio.utn.edu.ec/bitstream/123456789/2676/1/04%20RED%20027%20TESIS.pdf>

COBIT. ISACA Trust in, and value from, information systems. [en línea] <https://www.isaca.org/Pages/default.aspx>. Marco de referencia para optimizar y salvaguardas los recursos o activos de información y tecnológicos de cualquier empresa.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I: Método, Libro II: Catálogo de Elementos, Libro III: Guía de Técnicas.

Fisher, P. Royal. (1988). *Seguridad en los sistemas informáticos*. En. Díaz de Santos (Ed). Recuperado de http://books.google.es/books?hl=es&lr=&id=_Hu6Zu6VLP4C&oi=fnd&pg=PR7&dq=seguridad+en+los+sistemas+informaticos&ots=zPpF_P3Ab8&sig=i96QHUdE8kcXjq60XbjKg9r5V2w. El libro explica de manera sencilla y estructurada el diseño para la seguridad informática, haciendo énfasis en los puntos de control, colaboración de la alta dirección para la implementación de seguridad en los procesos organizacionales.

González Barroso, J. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid. Ministerio de Hacienda y Administraciones Públicas. Libro I de la metodología Magerit ofrece los lineamientos necesarios en el Proceso de Gestión de Riesgos dentro de un marco de trabajo para administrar los riesgos derivados del uso de tecnologías de la información.

González Barroso, Jesús. (2012). *Guía de Técnicas*. Madrid. Ministerio de Hacienda y Administraciones Públicas. Libro III de la metodología Magerit describe las técnicas usadas para hacer el Análisis de riesgos.

González Barroso, Jesús. (2012). *Catálogo de Elementos*. Madrid. Ministerio de Hacienda y Administraciones Públicas. (v.3.0): *Metodología de análisis y Gestión de riesgos los sistemas de información*. Libro número II de la metodología MAGERIT, estandariza los elementos objeto de proyecto de análisis necesarios para generar un inventario de activos, para luego hacer la administración de estos.

Hisham M. H. & Brunil D. R. (2009). *Asset Identification for Security Risk Assessment in Web Application: International Journal of Software Engineering*. Documento u artículo en formato pdf, ofrece información para identificar los riesgos en activos de seguridad, específicamente en aplicaciones Web.

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DEL CAUCA (2011), *Historia Institucional 1967-2011*. [En línea]. <http://www.colmayorcauca.edu.co/unimayor/page/historia-institucional>. Suministra información histórica y actual acerca del Colegio Mayor del Cauca.

Instituto Nacional de Tecnologías de la Comunicación (INTECO). *Implantación de un SGSI en la empresa*. [en línea]. http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf. Muestra de manera sencilla los conceptos y componentes necesarios dentro de la implementación del sistema de gestión de la seguridad de la información.

Ley 1273 de 2009. Ministerio de Tecnologías de la Información y de las Telecomunicaciones (MinTIC). [en línea]. <http://www.mintic.gov.co/portal/604/w3-article-3705.html>

Machuca Contreras John (2011). Tesis de maestría:Guía para la evaluación del sistema de riesgo operativo en la Cooperativa de Ahorro y Crédito Jardín Azuayo. Cuenca.140P.[en línea].
<http://dspace.ucuenca.edu.ec/bitstream/123456789/2729/1/tm4487.pdf>

Maxitana C, Jennifer D, Naranjo S. Bertha A. Administración de riesgos de tecnología de información de una empresa del sector informático. [en línea].
[https://www.dspace.espol.edu.ec/bitstream/123456789/15896/3/Resumen Cicyt.-Administración de Riesgos de TI de una empresa del sector Informático .pdf](https://www.dspace.espol.edu.ec/bitstream/123456789/15896/3/Resumen_Cicyt.-Administración_de_Riesgos_de_TI_de_una_empresa_del_sector_Informático.pdf)

NTP-ISO/IEC 1779, Norma técnica Peruana (2007). EDI, Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, Segunda edición.

Pallas M. Gustavo (2009). Tesis de Maestría en Ingeniería en Computación, Metodología de implantación de un SGSI en un grupo empresarial jerárquico. ISSN 1510 7264.

PAREDES F. Geomayra y VEGA N. Mayra (2011). Desarrollo de una metodología para la auditoría de riesgos Informáticos (físicos y lógicos) y su aplicación al Departamento de informática de la dirección provincial de pichincha del consejo de la judicatura. Escuela Superior Politécnica De Chimborazo (Ecuador).

PHVA ¿Qué es el ciclo PHVA? Enero 09 de 2010. Blog de Seguridad informática. [en línea]. <http://securityjeifer.wordpress.com/tag/phva/>. Conceptos enmarcados sobre la ejecución de este ciclo útil dentro de los procesos (sistemas) de gestión de la calidad, incluyendo los de seguridad de la información.

Plate, A. ISO/IEC 2700: *Sistema de Gestión de la de la Seguridad de la Información*. Recuperado de <http://datateca.unad.edu.co/contenidos/233004/24326153-Seminario-Iso-7001.pdf>

Portal administración electrónica. MAGERIT v3: Metodología de Análisis y Gestión de Riesgos de los sistemas de información. [En línea].
http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VCmVZhZRVJQ

Portantie,Fabian. La seguridad informática (libro pdf). [en línea]. <http://reduser.com>

Prevención y soluciones. ENI (Ed). Recuperado de <http://books.google.es/books?id=K8XdRni4t94C&printsec=frontcover&hl=es#v=onepage&q&f=false>

Ramírez, G. M. & Constain, G. E. (2012). *Modelos y estándares de la seguridad Informática*. Módulo de estudio de la Universidad Nacional Abierta y a Distancia, hace referencia a los modelos y estándares aplicables dentro de la seguridad informática

Román Valdes Cesardari(2014). Recurso digital Investigacion aplicada. [en linea]. <http://issuu.com/lizbethfuentes6/docs/m2-t1>

Royer, J.M. (2004) Seguridad en la informática de empresa: riesgos, amenazas,

RUIZ L. Hernando. RESOLUCION 160-005326 Política de Seguridad de la información de la Superintendencia de Sociedades. 2008.

Sabogal R., E. A. (2013) *Proyecto de seguridad informática I*. Módulo de estudio que presenta los lineamientos y recomendaciones para elaboración del anteproyecto y proyecto de grado requisito para optar por el título de especialistas en seguridad informático ofrecido por la UNAD.

14 Anexos

14.1 Anexo A: Clasificación De Los Activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Los datos son el combustible con el que opera una organización. La información es un activo abstracto que será almacenado en equipos o soportes de información y que puede ser transferido de un lugar a otro por los medios de transmisión de datos. Pertenecen a este grupo: ficheros, copias de respaldo, datos de configuración, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividad, código fuente, código ejecutable y datos de prueba
[S] Servicios	Función que satisface una necesidad de los usuarios, como: world wide web, acceso remoto a cuenta local, correo electrónico, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, servicio de directorio, gestión de identidades, gestión de privilegios, PKI - infraestructura de clave pública.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, que han sido automatizadas para su desempeño por un equipo informático, entre ellos están: desarrollo propio, desarrollo a medida (subcontratado), estándar, navegador web, servidor de presentación, servidor de aplicaciones, cliente de correo electrónico, servidor de correo electrónico, servidor de ficheros, sistema de gestión de bases de datos, monitor transaccional, ofimática, anti virus, sistema operativo, gestor de máquinas virtuales, servidor de terminales, sistema de backup.
[HW] Equipamiento informáticos (Hardware)	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, entre ellos podemos identificar: agendas electrónicas, equipo virtual, equipamiento de respaldo, periféricos dispositivos criptográficos, dispositivo de frontera, soporte de la red, concentradores, conmutadores, encaminadores, firewall, punto de acceso inalámbrico, etc.

[COM]	Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros. Medios de comunicación que tiene por objetivo transportar datos de un sitio a otro.
[Media]	Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o por largos periodos de tiempo. Ejemplo: CD-ROM, DVD, USB, Material Impreso.
[AUX]	Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos; como: fuentes de alimentación, cableado, armarios, mobiliario, equipos de climatización.
[L]	Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones. Ejemplo: cuartos, edificios, instalaciones de respaldo.
[P]	Personal	Personal relacionado con los sistemas de información; como: personal interno y externo, operadores, administradores de sistemas, desarrolladores de sistemas, contratistas y proveedores.
[SI]	Sistema de Información ²²	Conjunto de elementos interrelacionados que permiten la obtención, procesamiento, almacenamiento y distribución de la información para apoyar la toma de decisiones y el control en una organización.

14.2 Anexo B : Valoración De Activos – Escala Estándar

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	podría causar molestias a un individuo
	2.pi2	podría quebrantar de forma leve leyes o regulaciones

²² Adaptado para este proyecto y nombrado como aplicaciones informáticas.

1	1.pi1	podría causar molestias a un individuo
[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	podría causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
9	9.si	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
7	7.si	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	podría causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos

	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o

		logística (alcance local)
[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	podría impedir la operación efectiva de una parte de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos
[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar
[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4ue	RESTREINT UE
3	3.ue	RESTREINT UE

14.3 Anexo C: Encuesta Aplicada

Nombre de la empresa: Institución Universitaria Colegio Mayor del Cauca

Nombre de la persona entrevistada: Edgar A. Galvis C.

Cargo del entrevistado en la entidad: Asesor TIC

Fecha: 11/12/2013

ENCUESTA

A. Con respecto a los aspectos generales de la Seguridad en Redes

Pregunta: Indagar acerca de la disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, considerando componentes de la red como: Switches, Routers, Firewall, IPS/IDS, Gateway Antivirus de la empresa, desempeño de la Red, topología existente, con respecto a ello preguntar acerca de conexiones, componentes software y hardware utilizados, planos existentes y diseño.

R. /

Switches: Cerca del 60% de estos equipos de comunicación en los diferentes subcentros de cableado son de última tecnología a velocidades Gigabit Ethernet en marcas como Cisco, HP y Dell, lo cual garantiza en cierto grado la disponibilidad y el buen desempeño. Los Switches principales o de core en los centros de datos de cada sede están configurados de acuerdo a la segmentación del diseño de red y configurados en VLANs, lo cual minimiza los riesgos de acceso no autorizado entre subredes y elimina tráfico innecesario. El control de acceso físico es deficiente, ya que muchos de los Switches aunque se encuentran en armarios, la seguridad que brindan los armarios de cableado no es la adecuada.

Routers: La configuración, mantenimiento y disponibilidad del routers Cisco 1900 depende del proveedor Emtel, ya que se tiene en comodato de acuerdo al contrato adquirido actualmente por ellos.

Firewalls: Se tienen actualmente 3 Firewalls o UTM (Equipos Unificados contra Amenazas) marca Fortinet modelos 200B, 80C y 60B respectivamente, 2 están en uso y uno de reserva. Estos equipos son muy confiables por la seguridad parametrizable que tienen y son muy completos por la cantidad de módulos de seguridad que incorporan como antispam, Firewall con políticas fácilmente configurables, antivirus Web, Filtrado Web, monitor del estado de memoria y CPU del equipo, así como monitor de tráfico In/Out por interfaz o zona y un Sistema IPS pre configurado bastante eficiente además de un administrador de ancho de banda por interfaz entre otras funcionalidades.

Antivirus: La institución actualmente paga un licenciamiento anual por el sistema de protección antivirus de ESET en su versión 5.0.22 para empresas, un servidor de políticas y de actualizaciones para clientes así como el derecho a usar la consola de administración.

Desempeño de la Red: La disponibilidad y desempeño de la red está sujeta a la misma confiabilidad de los equipos de red en sí. Como medida de prevención se tienen en stock 2 Switches de 48 puertos administrables 10/100/1000, y 2 Switches de 24 puertos 10/100/1000. En algunos sitios aún se tienen instalados Switches 10/100 lo que no da un buen rendimiento en esos equipos con relación a los demás. Se puede crear un cuello de botella en ocasiones entre la sede alterna (Bicentenario-Casa Obando) y la sede principal (Encarnación) en periodos de matrículas donde se accede a los sistemas de información académica y se realizan consultas y procesos con alto consumo de ancho de banda y las capacidades del firewall de esa sede no es la suficiente para atender estas solicitudes simultaneas además del tráfico normal existente (Internet, Servicios Internos de red, Video-Vigilancia IP, Telefonía IP entre otros).

Topología de Red: Nuestra topología de red se puede definir entre una mezcla de topología en árbol y topología en estrella. En árbol teniendo en cuenta que desde

la sede principal se derivan todos los servicios y conexiones hacia las otras subredes y Switches además de la conexión hacia las dos sedes alternas a través del canal de interconexión por fibra.

Planos, Conexiones y Diseño: La sede encarnación por ser una edificación antigua no tiene planos de red, existen algunos planos eléctricos pero están desactualizados. De la sede Bicentenario se tienen todos los planos eléctricos de voz y datos. Estamos en proceso de actualización de la diagramación lógica y diseño de las redes y subredes en las diferentes sedes. Se tiene la distribución lógica y diseño del direccionamiento de red en la LAN de cada sede. En cuanto a conexiones y cableado se cuenta casi con el 90% de la red de datos con cable Cat 6 y la interconexión con la sede alterna además de la conexión con la red académica Renata y RUP se hace por fibra óptica con velocidades de 30Mbps y 50Mbps respectivamente.

- B. Con respecto a las medidas que se deben tener en cuenta en las organizaciones mediante el filtrado de diversos protocolos en los routers de acceso.

Pregunta: Que medidas internas concretas utilizan en la empresa u organización, para lograr este objetivo planteado?

R./

En el router no sabemos qué medidas se tengan porque dependen directamente del proveedor, lo que si tenemos filtrado a nivel de servicios, puertos y protocolos se maneja en los equipos UTM mencionados tanto de entrada como de salida, con políticas bien definidas de acuerdo al servicio prestado.

Aquí se observa un ejemplo de la política creada en el UTM Fortigate 200B.

The screenshot shows the 'Editar Política' (Edit Policy) configuration page in FortiGate. The policy is named 'JUNO Mapso' and is applied to the 'all' interface. The configuration includes the following details:

- Zona/Interfaz Origen:** (Zona) INTERNET
- Dirección Origen:** all
- Zona/Interfaz Destino:** (Zona) INTERCONEXION SERVIDORES
- Dirección Destino:** JUNO Mapso
- Horario:** always
- Servicio:**
 - HTTP
 - CNS
 - POP3
 - SMTP
 - IMAP
 - ACCEPT

Acción:

- Registrar Tráfico Permitido
- Habilitar web cache
- Habilitar NAT
 - Utilizar Dirección de Interfaz Destino
 - Uso dinámica de IP Pool
 - Utilizar Tabla Central de NAT
- Habilitar Política Basada en Identidad
- Resolver nombres de usuario mediante Agente FSSO
- UTM
 - Habilitar Antivirus
 - Habilitar Filtrado Web
 - Habilitar Control de Aplicaciones
 - Habilitar IPS
 - Habilitar Filtrado Email

Additional configuration options visible include 'Entrega de paquetes' (set to 'Entrada'), 'Default Action' (set to 'default'), and 'Protect HTTP Server' (set to 'protect_http_server').

- C. Con respecto a que gran parte de los ataques que se producen son debidos a la obtención de las claves empleando un programa de sniffing en una red Ethernet.

Preguntas:

- Cual estrategia tienen planteada en su empresa para contrarrestar estos ataques a la seguridad?
R./ No existe estrategia como tal, solo se tienen las políticas configuradas en el firewall de acuerdo a servicios, protocolos y puertos desde internet, hacia internet y entre zonas, que permiten en cierto grado minimizar este tipo de amenaza, además por la funcionalidad de protección de servidores http o de correo mediante el IPS.
- Que estrategias utilizan para descongestionar el tráfico y para permitir una mayor descongestión del tráfico interno.
R./ Se tiene segmentada la red, el diseño del direccionamiento y el subneting de acuerdo al número de equipos por segmento además de la creación de VLANs mejoran el rendimiento de la red y eliminan tráfico innecesario, también está configurado NAT para equipos de uso administrativo y docente y el servicio Proxy para todos los equipos de salas de cómputo; para agilizar las búsquedas de recursos compartidos y equipos en red se tiene configurado un servidor Wins.
- En la empresa se han presentado ataques informáticos? De que clase? Por favor describirlos a detalle.

Hubo un ataque hace 4 años aproximadamente donde se comprometió la seguridad, configuración e información del servidor web y de correo en ese entonces, al parecer se aprovechó un agujero de seguridad en un framework de programación utilizado y abrió un puerto ftp embebido con privilegios por consola, hicieron escalada de privilegios y afectaron la interfaz gráfica, algunos servicios y archivos y obtuvieron la clave de acceso al motor mysql, esto se dio por desconocimiento en aspectos de seguridad y la falta de un escenario de pruebas para no comprometer directamente el servidor de producción y primero haber probado el aplicativo y funcionalidades del mismo.

- Que mecanismos y que servicios de seguridad se usa en la empresa?

R. / UTM con los módulos de filtrado, protección y análisis de tráfico, Sistema de protección Antivirus, Firewall personal por equipo (Administrativos), segmentación de red y diseño del direccionamiento con subneting. En la parte física se tienen 30 cámaras IP, sistemas de alarmas en salas de cómputo, laboratorios, cuartos de servidores y centros de cableado.

- D. Con respecto a la Ubicación Del IDS En Una Organización. Mecanismos de Seguridad

Pregunta: Existen principalmente tres zonas en las que podríamos poner un sensor – Si lo tienen en que zona está ubicado, si no donde lo ubicarían.

R. / El UTM incorpora un sistema IPS y este se encuentra activo en dos zonas actualmente, la primera es a la entrada del canal de Internet e Interconexión con la sede alterna y lo tenemos activo en la zona DMZ.

E. Con respecto a los tipos de amenazas humanas. Los actos humanos que pueden afectar la seguridad de un sistema son variados, entre los más comunes e importantes están:

Curiosos, Intrusos remunerados, Personal enterado, Terroristas, Robo, Sabotaje, Fraude.

Pregunta:Cuál de estos tipos de amenaza se ha presentado en su organización?

R./ Los IPS en sus logs de corta duración, generalmente informan de intentos de ataque a los servidores, al parecer según los ataques que se previenen vienen de herramientas de scanning y sniffing, creemos que pueden ser personas Curiosas o Personas entrenadas.

F. Con respecto a la Implementación de plan de seguridad Para la implementación del Plan de Seguridad para cualquier organización, se debe tender en cuenta principalmente aquellas herramientas que nos permitirán tener una información confiable mediante archivos de trazas o logísticos de todos los intentos de conexión que se han producido sobre un sistema, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Pregunta: Describa el Plan de Seguridad Implementado en la organización

R./ Actualmente la Institución No tiene un plan de seguridad implementado.

Dentro de las recomendaciones hechas, se sugiere comenzar con un estudio de análisis de riesgos para evaluar el nivel de seguridad actual en la Institución, según los resultados obtenidos generar un marco de trabajo que permita establecer la adopción de controles para los riesgos encontrados, diseñar políticas de seguridad y aprobar en un futuro la implantación de un Sistema de Gestión de Seguridad de la Información.

14.4 Anexo D: Catalogo De Salvaguardas

Protecciones Generales u Horizontales

H Protecciones Generales.

H.IA Identificación y autenticación.

H.AC Control de acceso lógico.

H.ST Segregación de tareas.

H.IR Gestión de incidencias.

H.tools Herramientas de seguridad.

H.tools.AV Herramienta contra código dañino.

H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión.

H.tools.CC Herramienta de chequeo de configuración.

H.tools.VA Herramienta de análisis de vulnerabilidades H.tools.TM Herramienta de monitorización de tráfico.

H.tools.DLP DLP: Herramienta de monitorización de contenidos.

H.tools.LA Herramienta para análisis de logs.

H.tools.HP Honey net / honey pot.

H.tools.SFV Verificación de las funciones de seguridad.

H.VM Gestión de vulnerabilidades.

H.AU Registro y auditoría.

Protección de los Datos / Información

D Protección de la Información

D.A Copias de seguridad de los datos (backup)

D.I Aseguramiento de la integridad

D.C Cifrado de la información

D.DS Uso de firmas electrónicas

D.TS Uso de servicios de fechado electrónico (time stamping)

Protección de las Claves Criptográficas

K Gestión de claves criptográficas

K.IC Gestión de claves de cifra de información

K.DS Gestión de claves de firma de información

K.disk Gestión de claves para contenedores criptográficos

K.comms Gestión de claves de comunicaciones

K.509 Gestión de certificados

Protección de los Servicios

S Protección de los Servicios

S.A Aseguramiento de la disponibilidad

S.start Aceptación y puesta en operación

S.SC Se aplican perfiles de seguridad
S.op Explotación
S.CM Gestión de cambios (mejoras y sustituciones)
S.end Terminación
S.www Protección de servicios y aplicaciones web
S.email Protección del correo electrónico
S.dir Protección del directorio
S.dns Protección del servidor de nombres de dominio (DNS)
S.TW Teletrabajo S.voip Voz sobre IP

Protección de las Aplicaciones (Software)
SW Protección de las Aplicaciones Informáticas
SW.A Copias de seguridad (backup)
SW.start Puesta en producción
SW.SC Se aplican perfiles de seguridad
SW.op Explotación / Producción
SW.CM Cambios (actualizaciones y mantenimiento)
SW.end Terminación

Protección de los Equipos (Hardware)
HW Protección de los Equipos Informáticos
HW.start Puesta en producción
HW.SC Se aplican perfiles de seguridad
HW.A Aseguramiento de la disponibilidad
HW.op Operación
HW.CM Cambios (actualizaciones y mantenimiento)
HW.end Terminación
HW.PCD Informática móvil
HW.print Reproducción de documentos
HW.pabx Protección de la centralita telefónica (PABX)

Protección de las Comunicaciones
COM Protección de las Comunicaciones
COM.start Entrada en servicio
COM.SC Se aplican perfiles de seguridad
COM.A Aseguramiento de la disponibilidad
COM.aut Autenticación del canal
COM.I Protección de la integridad de los datos intercambiados
COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op Operación
COM.CM Cambios (actualizaciones y mantenimiento)
COM.end Terminación
COM.internet Internet: uso de ? acceso a
COM.wifi Seguridad Wireless (WiFi)
COM.mobile Telefonía móvil

COM.DS Segregación de las redes en dominios

Protección en los Puntos de Interconexión con otros Sistemas

IP Puntos de interconexión: conexiones entre zonas de confianza

IP.SPP Sistema de protección perimetral IP.BS Protección de los equipos de frontera

Protección De Los Soportes De Información

MP Protección de los Soportes de Información

MP.A Aseguramiento de la disponibilidad

MP.IC Protección criptográfica del contenido

MP.clean Limpieza de contenidos

MP.end Destrucción de soportes

Protección De Los Elementos Auxiliares

AUX Elementos Auxiliares

AUX.A Aseguramiento de la disponibilidad

AUX.start Instalación

AUX.power Suministro eléctrico

AUX.AC Climatización

AUX.wires Protección del cableado

Seguridad Física – Protección De Las Instalaciones

L Protección de las Instalaciones

L.design Diseño

L.depth Defensa en profundidad

L.AC Control de los accesos físicos

L.A Aseguramiento de la disponibilidad

L.end Terminación

Salvaguardas Relativas Al Personal

Son aquellas que se refieren a las personas que tienen relación con el sistema de información.

PS Gestión del Personal

PS.AT Formación y concienciación

PS.A Aseguramiento de la disponibilidad

Salvaguardas De Tipo Organizativo

Son aquellas que se refieren al buen gobierno de la seguridad.

G Organización

G.RM Gestión de riesgos

G.plan Planificación de la seguridad

G.exam Inspecciones de seguridad

Continuidad De Operaciones

Prevención y reacción frente a desastres.

BC Continuidad del negocio

BC.BIA Análisis de impacto (BIA)

BC.DRP Plan de Recuperación de Desastres (DRP)

Externalización

Es cada vez más flexible la frontera entre los servicios de seguridad prestados internamente y los servicios contratados a terceras partes. En estos casos es fundamental cerrar los aspectos de relación contractual:

SLA: nivel de servicio, si la disponibilidad es un valor

NDA: compromiso de secreto, si la confidencialidad es un valor

Identificación y calificación del personal encargado

Procedimientos de escalado y resolución de incidencias

Procedimiento de terminación (duración en el tiempo de las responsabilidades asumidas)

Asunción de responsabilidades y penalizaciones por incumplimiento

E Relaciones Externas

E.1 Acuerdos para intercambio de información y software

E.2 Acceso externo

E.3 Servicios proporcionados por otras organizaciones

E.4 Personal subcontratado

Adquisición Y Desarrollo

NEW Adquisición / desarrollo

NEW.S Servicios: Adquisición o desarrollo

NEW.SW Aplicaciones: Adquisición o desarrollo

NEW.HW Equipos: Adquisición o desarrollo

NEW.COM Comunicaciones: Adquisición o contratación

NEW.MP Soportes de Información: Adquisición

NEW.C Productos certificados o acreditados

14.5 Anexo E: Valoración De Riesgos

Tabla 32: Valoración de Riesgos

SISTEMAS DE COMUNICACIONES											
Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles
		A	M	B	L	M	C				
R1	Sistema telefónica IP no funciona adecuadamente		X			X		Aceptarlo	No hace parte del core del negocio, es contratado con el ISP	Preventivo	N/A. Sin embargo se recomienda realizar las actividades y controles: ISO 27001: 10.3 Planificación y Aceptación del Sistema. En su defecto posible montaje de sistema VoIP propio.
R2	Interrupciones frecuentes a sistemas de comunicación como chat institucional o algún servicio dependiente de estas tecnologías.			X	X			Aceptarlo	El servicio es provisto de manera gratuita por un agente externo - google.	N/A.	N/A.
HARDWARE											
Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles
		A	M	B	L	M	C				
R3	Falta de mantenimiento correctivo		X			X		Establecer un control y planeación periódica	Establecer planes de mantenimiento efectivos por semestre o por mes y monitorearlos.	Correctivo	ISO 27001: 9.2.4 Mantenimiento de equipos.
R4	Instalación de equipos de cómputo		X				X	Establecer un control	Acordar que se sugieran consejos para instalar de	Correctivo	ISO 27001: 9.2.4

manera incorrecta								forma correcta los equipos y de igual forma generar un procedimiento único a seguir.	Mantenimiento de equipos.
-------------------	--	--	--	--	--	--	--	--	---------------------------

ADMINISTRACION DE INFORMACION

Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles
		A	M	B	L	M	C				
R5	Perdida de información de respaldo			X		X		Establecer un control	Integrar una herramienta para ejecutar copias de la información crítica y la implantación de un sistema de gestión documental como Nexus.	Correctivo y Preventivo	ISO 27001: 10.5.1 Respaldo de la información
R6	Daño de la información por incorrecto almacenamiento		X				X	Establecer un control	Establecer parámetros efectivos para la administración, manejo y almacenamiento.	Correctivo y Preventivo	ISO 27001: 10.5.1 Respaldo de la información

DISPOSITIVOS DE RED

Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles
		A	M	B	L	M	C				
R7	Falta de documentación para la administración y configuración de los dispositivos activos de red como Switches, Routers y Firewalls o UTMs			X		X		Establecer un control	Generar documentación para la administración de los dispositivos de red por parte del administrador de los mismos.	Correctivo	ISO 27001: 10.1.1 Procedimientos operativos documentados

R8	Falta de procedimientos que indique como restaurar la interconexión entre sedes			X		X			Establecer un control	Definir una política de recuperación de desastres o un plan alternativo de operación	Preventivo y correctivo	ISO 27001: 10.1.1 Procedimientos operativos documentados ISO 27001: 14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información
----	---	--	--	---	--	---	--	--	-----------------------	--	-------------------------	--

SEGURIDAD FISICA

Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles
		A	M	B	L	M	C				
R9	El sistema de cámaras de seguridad IP no funciona correctamente			X		X		Establecer un control	Se debe hacer un monitoreo constante al sistema, consola de administración y al servidor de almacenamiento.	Preventivo	ISO 27001: 9.1.1 Perímetro de seguridad física
R10	Se identifican puntos muertos en el sistema de seguridad		X			X		Establecer un control	Implementación de cámaras de seguridad en los puntos muertos con movimiento 180 grados.	Preventivo	ISO 27001: 9.1.1 Perímetro de seguridad física

INSTALACIONES ELECTRICAS

Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles
		A	M	B	L	M	C				
R11	No existe conexión de polo a tierra en algunas dependencias sede Encarnación		X			X		Establecer un control	Contratar una empresa especializada en instalaciones eléctricas y	Preventivo y correctivo	ISO 27001: 9.2.2 Servicios de soporte
R12	No existe instalación de		X			X		Establecer un control	mantenimiento para las	Preventivo y correctivo	

	sistema eléctrico regulado en algunos puntos sedes Encarnación – Casa Obando									adecuaciones necesarias en el circuito eléctrico y/o sistemas de respaldo.		
R13	UPS en mal estado o mal funcionamiento por falta de mantenimiento			X			X		Establecer un control		Correctivo	
SISTEMAS DE INFORMACION Y SOFTWARE DE PROTECCION												
Riesgo/Valoración		Probabilidad			Impacto			Tratamiento	Observaciones	Tipo de control	Controles	
		A	M	B	L	M	C					
R14	No existen planes alternos en caso de falla de las aplicaciones utilizadas en la institución que permita recuperar un sistema a su normalidad.			X			X	Establecer un control	Implementar una herramienta de respaldos y restauración de planes de contingencia	Correctivo	ISO 27001: 14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información.	
R15	Se cuenta con un sistema centralizado de antivirus pero no está configurado adecuadamente.		X				X	Establecer un control	Se debe efectuar por medio de la consola todo el proceso de configuración de acuerdo a las políticas y controles sugeridos	Preventivo y correctivo	ISO 27001: 10.4 Protección contra código móvil y malicioso	
R16	No se cuenta con la documentación de los usuarios y perfiles de acceso a las diferentes aplicaciones web o sistemas de información como SIAG.			X			X	Establecer un control	Generar la documentación respectiva de roles y responsabilidades dentro de las aplicaciones.	Correctivo	ISO 27001: 11.2.2 Gestión de privilegios	

Fuente: Esta Investigación

Matriz De Riesgos

Tabla 33: Matriz de Riesgos

	Leve	Moderado	Catastrófico
Alto			
Medio		R1, R3, R10, R11, R12	R4, R6, R15
Bajo	R2	R7, R8, R9, R13, R16	R5, R14

Riesgos Identificados

Probabilidad Baja – Impacto Leve

R2: Servicios de chat.

Probabilidad Baja – Impacto Moderado

R7: Falta de documentación para la administración y configuración de los dispositivos activos de red como Switches, Routers y Firewalls o UTM's.

R8: Falta de procedimientos que indique como restaurar la interconexión entre sedes.

R9: El sistema de cámaras de seguridad IP no funciona correctamente.

R13: UPS en mal estado o mal funcionamiento.

R16: No se cuenta con la documentación de los usuarios y perfiles de acceso a las diferentes aplicaciones web o sistemas de información como SIAG.

Probabilidad Media – Impacto Moderado

R1: Sistema de telefonía IP no funciona adecuadamente.

R3: Falta de mantenimiento correctivo.

R10: Se identifican puntos muertos en el sistema de seguridad.

R11: No existe conexión de polo a tierra.

R12: No existe instalación de sistema eléctrico regulado.

Los siguientes riesgos serán controlados directamente por la institución.

Probabilidad Baja – Impacto Catastrófico

R5: Pérdida de información de respaldo.

R14: No existen planes alternos en caso de falla de las aplicaciones utilizadas en la institución que permita recuperar un sistema a su normalidad.

Probabilidad Media – Impacto Catastrófico

R4: Instalación de equipos de cómputo de manera incorrecta.


R6: Daño de la información por incorrecto almacenamiento.

R15: Se cuenta con un sistema centralizado de antivirus pero no está configurado adecuadamente.

En resumen, el informe técnico y los datos aquí expuestos reflejan que existen riesgos, amenazas y vulnerabilidades en todo sentido, especialmente en el

tratamiento de la información y los sistemas que administran la misma al interior de la Institución Universitaria Colegio Mayor del Cauca, es de vital importancia asumir una postura consiente de que se deben iniciar procesos, esfuerzos y planes que lleven a la implementación de un Sistema de seguridad de la información (SGSI) apoyándose en las normas actuales vigentes ya mencionadas que apliquen en el país, buscando mantener en cierto grado un nivel de seguridad de la información aceptable..

14.6 Anexo D: Propuesta; Formato de Política De Seguridad

Numero documento	005	POLÍTICA PARA LA ADMINISTRACIÓN DE SERVIDORES			
Fecha de elaboración	28/03/14				
Fecha actualización		Área:	Elaborado por:	Aprobado por:	
		TIC	JJPR & MCC		

Introducción


En redes locales los servidores facilitan el acceso a la red y sus recursos de una manera apropiada y eficaz además de segura, partiendo claro esta del buen manejo, mantenimiento y administración que se efectúe sobre los mismos. De igual manera se debe garantizar a los usuarios la integridad, la confiabilidad y la disponibilidad de la información.

Finalidad

La finalidad de la política para la administración de servidores se basa en la descripción de los requerimientos y acciones mínimas a tener presentes para tratar y eliminar virus de cómputo además de prevenir sus variantes.

Definiciones:


Recursos Informáticos : Cualquier tipo de información, recursos en línea, medios de almacenamiento magnético y todas las actividades relacionadas a información computacional, incluyendo cualquier dispositivo capaz de recibir correos,

Numero documento	005	POLÍTICA PARA LA ADMINISTRACIÓN DE SERVIDORES			
Fecha de elaboración	28/03/14				
Fecha actualización	Área:	Elaborado por:	Aprobado por:		
	TIC	JJPR & MCC			

mensajes instantáneos, navegación en la Web, con capacidad de recepción, almacenamiento, manejo, o transmisión electrónica de datos, no limitada servidores, computadores personales, portátiles, computadores manuales, asistentes personales portátiles (PDA), sistemas de procesamiento distribuido, redes inalámbricas, recursos de telecomunicación, ambientes de redes, equipos de fax e impresoras.

Servidor: En informática, un servidor es una computador especializado que, formando parte de una red, provee servicios a otros computadores normales denominadas clientes también puede ser una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un computador y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un solo computador cumpla simultáneamente las funciones de cliente y de servidor.

Servidor Antivirus: En informática, un servidor antivirus es un computador con características hardware apropiadas de servidor que, formando parte de una red, provee servicios a otros computadores denominados clientes, se encarga de actualizar su base de datos de definiciones de virus y actualizar a sus clientes,


Numero documento	005	POLÍTICA PARA LA ADMINISTRACIÓN DE SERVIDORES			
Fecha de elaboración	28/03/14				
Fecha actualización	Área:	Elaborado por:	Aprobado por:		
	TIC	JJPR & MCC			

además monitorea el estado de los mismos e incluso se pueden programar tareas específicas en ellos.

Servidor Web: Un servidor web es un programa o aplicación diseñado para transferir hipertextos, páginas web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música. El programa implementa el protocolo HTTP (HyperText Transfer Protocol) que pertenece a la capa de aplicación del modelo OSI. El término también se emplea para referirse al servidor físico que ejecuta dicho servicio.

Servidor de Correo: Un servidor de correo es una aplicación informática cuya función es parecida al Correo postal solo que en este caso los correos (otras veces llamados mensajes) que circulan, lo hacen a través de redes de transmisión de datos y a diferencia del correo postal, por este medio solo se pueden enviar adjuntos de archivos de cualquier extensión y no paquetes o encomiendas al viajar la información en formato electrónico.

Servidor DNS: Domain Name System / Service (o DNS, en español: sistema de nombre de dominio) es un servicio de nomenclatura jerárquica para computadores, servicios o cualquier recurso conectado a internet o a una red privada. Este sistema asocia información variada con nombres de dominios

Numero documento	005	POLÍTICA PARA LA ADMINISTRACIÓN DE SERVIDORES			
Fecha de elaboración	28/05/14				
Fecha actualización		Área:	Elaborado por:	Aprobado por:	
		TIC	JJPR & MCC		

asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

UTM: Unified Threat Management (Tratamiento Unificado contra amenazas), dispositivo que permite la gestión unificada de amenazas. Generalmente integra Firewall (Sistema Cortafuegos), Antivirus, Antiespías, Detección de Intrusos, Administración de ancho de banda, Filtrado Web o de navegación de usuarios entre otras.

Políticas Para La Administración De Servidores

- Se debe garantizar que el sitio físico donde se instalarán los servidores y equipos adicionales para su funcionamiento sea el adecuado.
- Si es un servidor nuevo se deben considerar algunos de los pasos generales antes de la adecuación del mismo:
 - ✓ Instalación del sistema operativo adecuado e idóneo según el servicio que prestará dicho equipo.
 - ✓ Si es un sistema operativo de tipo comercial se debe instalar el licenciado por la institución.

Numero documento	005	POLÍTICA PARA LA ADMINISTRACIÓN DE SERVIDORES			
Fecha de elaboración	28/03/14				
Fecha actualización		Área:	Elaborado por:	Aprobado por:	
		TIC	JJPR & MCC		

- ✓ Se deberán aplicar los respectivos parches de seguridad y actualización correspondientes al sistema instalado y un sistema de protección o antivirus.
 - ✓ Se deberá configurar el acceso red de acuerdo a las los servicios prestados; esta configuración va de la mano con la política de configuración y administración de sistemas firewall-UTM.
 - ✓ Se deberá generar un documento actualizable con los parámetros de seguridad, configuraciones de servicios en ellos aplicados, logs de auditoría.
- Se deben actualizar constantemente parches de seguridad, de aplicación o de actualización de componentes o servicios, para garantizar la estabilidad de los servidores.
 - Es aconsejable hacer un mantenimiento físico o hardware de los servidores por lo menos una vez al año.
 - Se debe monitorear constantemente el estado de los servicios y aplicaciones que cada uno de los servidores presta.

Alcance

Esta Política aplica a los encargados directos del mantenimiento y administración de los servidores con los que cuenta la institución.

Sanciones Disciplinarias

La violación de esta política puede resultar en acciones disciplinarias que puede ocasionar llamado de atención a los empleados y contratistas o consultores. Adicionalmente los encargados están sujetos a perder el acceso a los privilegios de uso de equipos tecnológicos institucionales, e iniciar un proceso disciplinario por poner en riesgo los servicios, información y equipos de carácter institucional.