GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL ÁREA DE ADMISIÓN, REGISTRO Y CONTROL ACADÉMICO DE LA UNIVERSIDAD VANCUR

JUAN CARLOS SILVA JARAMILLO

UOC UNIVERSITAT OBERTA DE CATALUNYA
MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TIC (MISTIC)
2014

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL ÁREA DE ADMISIÓN, REGISTRO Y CONTROL ACADÉMICO DE LA UNIVERSIDAD VANCUR

JUAN CARLOS SILVA JARAMILLO

Trabajo de Final de Máster

Profesor
Antonio José Segovia Henares
Máster Seguridad Información

UOC UNIVERSITAT OBERTA DE CATALUNYA
MÁSTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TIC (MISTIC)
2014

Este trabajo está dedicado a las personas que han creído, han sido pacientes y me han aconsejado:
Chela (mi mama), Karina, María Luisa y Soley (mis hermanas), y Kelly (mi novia)

En especial a Dios por mantenerme firme a pesar de los obstáculos

AGRADECIMIENTOS

Expreso mis agradecimientos a:

La Universidad UOC, en especial al programa de Máster Universitario MISTIC, por los conocimientos transmitidos a lo largo de la preparación académica y hacer profesionales con alto compromiso, responsabilidad y ética, para aplicarlos en el desempeño de la vida profesional y personal.

El Profesor Antonio José Segovia Henares, Máster en Seguridad de la Información, Docente del Máster Universitario MISTIC de la UOC, por sus valiosas aportaciones, apoyo y constante colaboración en el desarrollo de este trabajo.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Activo. Cualquier cosa que tenga valor para la organización.

Activo de Información. Datos o información propiedad de la organización que se almacena en cualquier tipo de medio y que es considerada por la misma como sensitiva o crítica para el cumplimiento de los objetivos.

Análisis de Riesgo. Uso sistemático de la información para identificar fuentes y para estimar el riesgo

Confidencialidad. La propiedad de que la información esté disponible y no se divulgue a personas, entidades o procesos no autorizados.

Disponibilidad. La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada

Enunciado de aplicabilidad. Documento que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de una organización.

Gestión del Riesgo. Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Información. Toda forma de conocimiento objetivo con representación física o lógica explícita.

Integridad. La propiedad de salvaguardar la exactitud e integridad de los activos.

Riesgo Residual. El riesgo remanente después del tratamiento del riesgo.

Seguridad de la Información. Preservación de la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información

Sistema de Gestión de la Seguridad de la Información (SGSI). Es parte del sistema gerencial general, su objetivo es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Sistema de Información. Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales

INTRODUCCION

El presente trabajo plantea el establecimiento de las bases para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Universidad de Vancur.

El SGSI, se fundamenta en la norma **NTC-ISO/IEC 27001,** esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del sistema de gestión de la seguridad de la información. También, adopta el modelo de procesos Planificar-Hacer-Verificar-Actuar (PDCA), que se aplica para estructurar todos los procesos del SGSI.

Algunos de los beneficios de la implementación de un SGSI, son:

- ✓ Reducción del riesgo de pérdida, robo o corrupción de información.
- ✓ Los clientes tienen acceso a la información a través medidas de seguridad.
- ✓ Los riesgos y sus controles son continuamente revisados.
- ✓ Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

La implementación de un SGSI es un proceso de continua mejora de la seguridad de la información, pero habitualmente empieza abarcando los procesos más críticos de la organización, para ir englobando áreas menos criticas en etapas posteriores; de ahí la razón de la puesta en marcha de un SGSI en el Área de Admisión, Registro y Control de la Universidad de Vancur, que define como alcance del SGSI las actividades relacionadas con los procesos de Admisión, Registro y Control, del Sistema de Información SIARC y del hardware que soporta este Sistema de información de la Universidad.

Los objetivos del Plan Director, definidos son:

- Definir la política de seguridad de información con el fin de crear concienciación de la dirección y los empleados en materia seguridad de la información que permita reducir incidentes de seguridad tales como: la desatención de escritorios, uso de claves, entre otros.
- Implementar medidas que mejoren la seguridad en el Sistema Informático SIARC, a modo de evitar y contrarrestar el fraude a través de accesos no autorizados, elevación de privilegios y otros tipos de ataques que lleguen afectar la integridad de la información.
- Reducir la posibilidad de interrupción del Sistema de Información SIARC ante el riesgo de presentarse contingencias como: incendios, caídas de energía, robo de equipos, sabotaje, entre otros.

Estos objetivos de plan director permitirán luego, establecer los proyectos que ayudaran a mitigar los riesgos al que están expuestos los activos de la dependencia luego de finalizar el análisis de riesgos.

El enfoque metodológico de esta investigación es cualitativo. La investigación cualitativa toma como misión "recolectar y analizar la información en todas las formas posibles, exceptuando la numérica. Tiende a centrarse en la exploración de un limitado pero detallado número de casos o ejemplos que se consideran interesantes o esclarecedores, y su meta es lograr `profundidad´ y no `amplitud´", indicado en el libro *Cómo se hace una investigación* de Blaxter (como se cita en Niño, 2011, p. 28). Los instrumentos de frecuente uso del enfoque cualitativo, son: preguntas, test, imágenes, textos, fotografías, talleres, sociogramas, reuniones, videos, grabaciones, documentos, etc.

El método seguido es el *Inductivo*. Siguiendo lo indicado por Méndez (2001), se eligió este procedimiento ya que permite cumplir con los objetivos y dar respuesta al problema que se identifico. Este método parte de la observación de fenómenos y situaciones particulares, aplicándose con mucha frecuencia en auditorias a organizaciones especificas, a modo de obtener explicaciones del fenómeno o situación analizada. Los resultados obtenidos pueden servir a posteriores investigaciones.

Finalmente, el trabajo se presenta con la siguiente estructura:

Capitulo Preliminar: NORMAS ISO 27001 e ISO 27002.
Capítulo I: SITUACIÓN ACTUAL
Capítulo II: SISTEMA DE GESTIÓN DOCUMENTAL
Capítulo III: ANALISIS DE RIESGOS
Capítulo IV: PLAN DE SEGURIDAD DE LA INFORMACIÓN
Capitulo V: AUDITORIA DE CUMPLIMIENTO

Capitulo Preliminar. NORMAS ISO 27001 e ISO 27002

1. NORMA ISO/IEC 27001

Es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Esta norma específica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). Para comenzar a hablar del origen de la norma ISO/IEC 27001, se debe referenciar la entidad de normalización británica, la British Standards Institution (BSI). Esta entidad emitió en 1995 la norma BS 7799.

La norma BS 7799 de BSI, tuvo como objeto proporcionar a cualquier empresa británica un conjunto de buenas prácticas para la gestión de la seguridad de su información. La norma BS 7799 estaba conformada por dos partes.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) 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 cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión. En 2005, con más de 1700 empresas certificadas en BS 7799-2, esta norma se publicó por ISO, con algunos cambios, como estándar ISO 27001. Al tiempo se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de ISO 27001:2005, BSI publicó la BS 7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Asimismo, ISO ha continuado, y continúa aún, desarrollando otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

2. ISO 27001:2013

Existen varios cambios con respecto a la versión 2005 en esta versión 2013. Entre ellos se destacan:

- Desaparece la sección "enfoque a procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras.
- Pasa de 102 requisitos a 130.
- Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114.
- Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube.
- Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de de identificar primero los activos, las amenazas y sus vulnerabilidades.

Una vez publicada la nueva norma, se ha abierto un periodo (se cree que es de dos años) durante el cual las organizaciones que deseen seguir certificadas deberán adecuar sus SGSI a la nueva versión. Esta actualización podrá consolidarse durante una auditoría de seguimiento, de re-certificación, o incluso mediante una auditoría extraordinaria si se considera oportuno.

Hay que destacar también que en la nueva versión el punto de partida es el análisis de riesgos, de forma que a partir de este análisis se determinan los controles que se necesitan, para después comparar esta lista con el anexo A para asegurar de que no se ha dejado ninguno aplicable;

3. NORMA ISO/IEC 27002

La ISO 27002 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management. Luego de una etapa de revisión y actualización

de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. Este estándar No es certificable.

El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995. ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar cuántos serán realmente los aplicables según sus propias necesidades.

4. Serie 27000

La seguridad de la información tiene asignada la serie 27000 dentro de los estándares ISO/IEC:

- ISO 27000: Publicada en mayo de 2009. Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.

- ISO/IEC 27001:2005 “Sistemas de Gestión de la Seguridad de la Información (SGSI)”. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSI’s deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799).

- ISO/IEC 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.

- ISO/IEC 27003: En fase de desarrollo; probable publicación en 2009. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. 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 27004: Publicada en diciembre de 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.

- ISO 27005: Publicada en junio de 2008. Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

- ISO 27006: Publicada en febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Capítulo I. SITUACIÓN ACTUAL

1. Contextualización

La Universidad Vancur, como universidad fomenta el acceso con equidad al sistema educativo colombiano, provee la mayor oferta de programas académicos, forma profesionales competentes y socialmente responsables. Estudia y enriquece el patrimonio cultural, natural y ambiental del país. Como tal lo asesora en los órdenes científico, tecnológico, cultural y artístico con autonomía académica e investigativa. La Universidad de Vancur cuenta con cinco sedes en el territorio colombiano, ofreciendo programas acorde a las necesidades de la economía regional.

La Universidad de Vancur desea mejorar sus niveles de seguridad de la información en el área de Admisión, registro y control; de este modo garantizar la disponibilidad, integridad y confidencialidad de la información.

1.1. Organigrama

El organigrama de la Universidad de Vancur y el área de Admisión, registro y control, demarcada con rojo, se muestra a continuación:

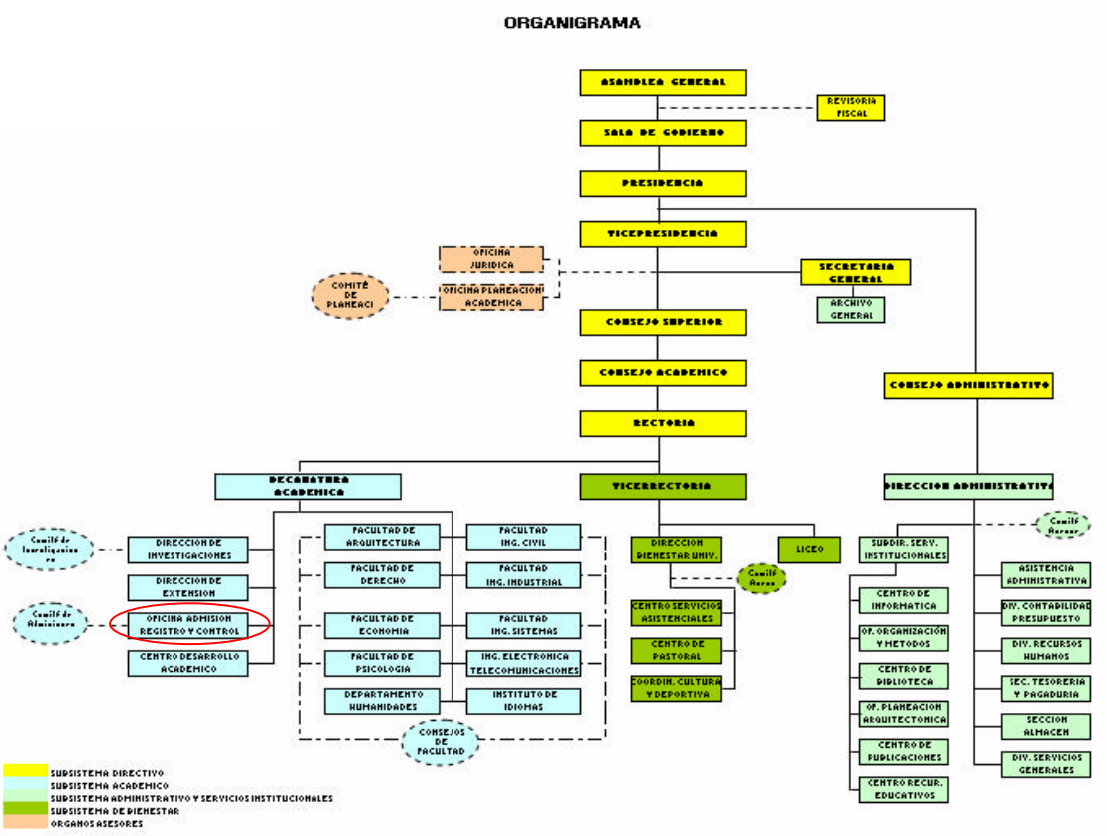

Figura 1. Organigrama Universidad Vancur

1.2. Área de Admisión, Registro y Control Académico

Admisiones como un grupo de apoyo de la Universidad de Vancur encargada de dirigir, coordinar, supervisar y controlar la ejecución de los planes, programas, políticas y reglamentación, formulada y adoptada en la institución en lo referente a los servicios de inscripción, admisión, matrícula, registro de información académica y control de estudiantes a través del uso y/o disposición de sistemas informáticos que ofrezcan información actualizada a quien lo requiera.

.

Figura 2. Organigrama de la oficina de Admisión, Registro y Control Académico

1.3. Funciones

Las funciones que se desarrollan en el área de Admisión, Registro y control son:

- Visar los Certificados de estudios, constancia de estudios y constancias de Orden de mérito.
- Llevar los registros de matrícula, actas de calificación y certificados de estudios.
- Apoyar la evaluación de las acciones de docencia de la Universidad.
- Realizar la matrícula de estudiantes de pregrado y post Grado en los dos Semestres Académicos.
- Elaborar y proponer el Calendario Académico.
- Consolidar los horarios de clases en coordinación con las Facultades.
- Racionalizar el uso de aulas y coordinar con las Oficinas correspondientes su adecuado mantenimiento y limpieza.
- Llevar el registro y control de egresados.

- Seleccionar de estudiantes que ocuparon los Primeros Puestos en el semestre académico concluido en estricto Orden Mérito y de acuerdo a su Reglamentación.
- Verificar los Registros de Notas con los asentados en Actas de los posibles egresados para su posterior certificación.
- Mantener el registro permanente de notas, planes de estudios, currículo y sílabos de cada una de las Facultades y escuela de Post Grado.
- Presentar el informe anual de las actividades realizadas.

Muchos de estos procesos se llevan a través del sistema informático SIARC (Sistema Informático de Admisión, Registro y Control) que reside en dos servidores de las oficinas de Admisión, registro y control. El sistema informático es administrado por el grupo de soporte informático y sistemas; este grupo tiene diversas funciones: realizar el mantenimiento del software en cuanto a la incorporación de nuevas y mejoradas funciones, administración y mantenimiento del servidor donde está alojado el sistema informático SIARC. En el segundo servidor se realizan las pruebas a las mejoras hechas a SIARC para luego ser puesto en marcha en el servidor principal.

El equipo técnico está encargado de manejar el SIARC, para generar los horarios académicos de cada programa durante el semestre y la asignación de aulas. Son los que gestionan los usuarios y contraseñas de docentes y administrativos de la universidad.

El área de registro Académico y archivo.
Registro académico colabora con los docentes si tienen dificultad en el momento de ingresar notas; además se encargan de los certificados de estudio, de llevar el control de egresados. Estas actividades se realizan en un modulo que se integra al SIARC.

Archivo y estadística, controla las actas de egresados y de aquellos que cumplen con la condición de grado; además de realizar cuando sean necesarias las estadísticas concernientes al ingreso de estudiantes, notas, entre otros.

1.4. Software

SIARC es un software desarrollado por el personal de soporte informático y sistemas, entregando diversas versiones ajustadas de acuerdo a los requerimientos expuesto por la universidad a lo largo de cuatro años. Este mismo personal se encargó del montaje del hardware necesario para el sistema de información que se desarrolló.

SIARC es una aplicación web desarrollada en ASP.NET y SQLSERVER como administrador de base de datos. El sistema operativo que está instalado en los servidores es Windows server 2008.

El Sistema de Información SIARC, integra los siguientes módulos:

- Generación de horarios para estudiantes y docentes, además de la asignación de aulas.
- Digitación de notas
- Modulo de inscripción, matricula, generación de certificados, este modulo es también accesible desde la web a través de la página de la Universidad Vancur.
- Gestión de contraseñas y roles, para docentes y administrativos.
- Reportes

1.5. Instalación física

El entorno donde se desarrollan las actividades del Área de Admisión, Registro y Control Académico es el siguiente:

Tabla 1. Instalación Física

Subgrupo	Ubicación	Descripción	Detalle
Espacio	oficinas	Despacho Director Admisión, registro y control	
		Despacho de secretario de Dirección	
		Despacho Director Admisión académica	
		Despacho Director de Desarrollo tecnológico	
		Despacho Director Registro académico	
		Registro académico Archivo y estadística	
	desarrollo	Área de soporte informático y sistemas	
Personal	Oficinas	Dirección	5
		Operaciones	6
	Desarrollo	Dirección	1
		Desarrollo Software y hardware	4
		Vigilante de acceso al área de admisión, Registro y control	1

1.6. Estado inicial de la seguridad:

- El grupo de soporte informático y sistemas, que está encargado del mantenimiento del Sistema de información SIARC (software hecho a la medida) no dispone de un plan de backups adecuado. Se realiza un respaldo antes de incorporar una nueva versión del Sistema de información SIARC en un disco duro externo. Superado el evento de actualización es descartada la copia de seguridad. En el servidor de desarrollo se realizan copias de seguridad cuando se comienza a trabajar en una nueva versión.
- Plan de mantenimiento del hardware no existe, cuando un equipo se avería es reparado y se cambia por una nueva pieza si es el caso.
- Los empleados del Área de Admisión, Registro y Control usan su usuario y contraseña para ingresar al SIARC, en los computadores usados no existen más controles de acceso.
- Seguridad en la instalación física, existe un control para la entrada y salida del Área de Admisión, Registro y Control llevado por una persona. El resto de puertas de las oficinas y sub-áreas son puertas normales y no hay control de entrada.
- No existe un Plan de continuidad para mantener o restaurar las operaciones del negocio en un tiempo razonable.
- Los equipos tienen reguladores de tensión, pero no existe un sistema ininterumpible de energía.

1.7. Alcance

Funcionamiento de un SGSI para las actividades relacionadas con los procesos de Admisión, Registro y Control, del Sistema de Información SIARC y del hardware que soporta este Sistema de información de la Universidad Vancur en su sede principal ubicada en Santa Marta.

2. Objetivos del Plan Director

- Definir la política de seguridad de información con el fin de crear concienciación de la dirección y los empleados en materia seguridad de la información que permita reducir incidentes de seguridad tales como: la desatención de escritorios, uso de claves, entre otros.
- Implementar medidas que mejoren la seguridad en el Sistema Informático SIARC, a modo de evitar y contrarrestar el fraude a través de accesos no autorizados, elevación de privilegios y otros tipos de ataques que lleguen afectar la integridad de la información.
- Reducir la posibilidad de interrupción del Sistema de Información SIARC ante el riesgo de presentarse contingencias como: incendios, caídas de energía, robo de equipos, sabotaje, entre otros.

3. Análisis Diferencial

Análisis diferencial con respecto a la **ISO/IEC 27001**.

No hay un SGSI implementado en la dependencia Admisión, Registro y Control Académico de la Universidad de Vancur.

Tabla 2. Análisis diferencial con respecto a la ISO/IEC 27001

Requerimientos	Comentario
Requerimientos de documentación	
Control de documentos	Existen documentos de roles y funciones operacionales de la dependencia, y la relación de los activos a su cargo. Los documentos requeridos por el SGSI no Existen, no se revisan ni se gestionan.
Control de registros	No se proporcionan evidencias de mantenerse registros del funcionamiento requeridos por el SGSI.
Responsabilidad de la Dirección	No se proporcionan evidencias del compromiso con la seguridad de la información.
Auditorías internas	No se realizan
Revisión por Dirección del SGSI	No se realizan. La dirección revisa la estadística generada por la dependencia. La Seguridad de la información ha estado a cargo del jefe de desarrollo tecnológico y este cuando es necesario solicita recursos para invertir en ese aspecto.
Mejoramiento del SGSI	No existen acciones de mejoramiento de SGSI, la dependencia no conoce los riesgos reales a los que están expuestos los activos.
Acción Correctiva	No existe un procedimiento establecido para eliminar las causa de no-conformidades
Acción Preventiva	No existe un documento donde se registre las no- conformidades potenciales y cómo prevenirlas

.

Tabla 3. Análisis diferencial con respecto a la **ISO/IEC 27002**

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
4.-Análisis de Riesgos	4.1- Análisis de Riesgo				X	
	4.2- Tratamiento del Riesgo				X	
5.-Política de seguridad	5.1.-Política de seguridad	5.1.1.-Documento de Política de Seguridad de la Información	¿Existe un documento de política de seguridad disponible para todos los usuarios?		X	El personal de soporte informático aplica los criterios de seguridad que considera adecuados.
		5.1.2.-Revisión de la Política de Seguridad de la Información	¿Se hacen revisiones regulares de la política de seguridad?		X	

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
6.-Seguridad en la compañía	6.1.-Organización interna	6.1.1.-Comité de Gestión para la Seguridad de la Información	¿Existe un comité de seguridad que trate las cuestiones de seguridad?		X	
		6.1.2-Coordinación de la Seguridad de la Información	¿Se coordinan las medidas de seguridad entre los distintos departamentos?		X	
		6.1.3-Asignación de responsabilidades sobre Seguridad de la Información	¿Están definidas las responsabilidades para proteger y controlar la información y los sistemas?		X	
		6.1.4-Proceso de autorización de recursos para el tratamiento de la información	¿Existe un proceso de autorización de la dirección para instalar nuevos equipos o aplicaciones?		X	
		6.1.5.-Acuerdos de confidencialidad	¿Firman los empleados un acuerdo de confidencialidad?		X	
		6.1.6.-Contactos con autoridades	¿Suele su empresa mantener contacto con autoridades especialistas de seguridad?		X	
		6.1.7.-Contactos con grupos de interés	¿Suele su empresa pertenecer a grupos de interés, foros, o asociaciones de seguridad externos?		X	
		6.1.8.-Revisión Independiente de la Seguridad de la Información	¿Se realizan revisiones independientes de la implantación de la seguridad?		X	Hasta ahora no se ha hecho ninguna.
7.-Gestión de activos	7.1.-Responsabilidad de los activos	7.1.1.-Inventario de activos	¿Existen y se mantienen actualizados inventarios de los activos del sistema de información?		X	Existe un inventario pero su actualización lo realizan cuando lo consideran oportuno.
		7.1.2-Propiedad de activos	¿Se han designado los propietarios de todos los activos del sistema de información?		X	
		7.1.3.-Uso aceptable de activos de información	¿Están definidos y documentados las reglas del uso aceptable de activos de sistemas de información?		X	
	7.2.-Clasificación de la información	7.2.1.-Guías de clasificación	¿Existe un esquema para clasificar la información y los sistemas en función de su confidencialidad o importancia?		X	
		7.2.2.-Marcado y tratamiento de la información	¿Existen procedimientos para identificar y usar la información, en base al esquema de clasificación?		X	
8.-Seguridad relativa al personal	8.1.-Previo a la contratación	8.1.1.-Perfiles y responsabilidad	¿Se incluyen en la definición del puesto de trabajo las responsabilidades de seguridad de cada cual?		X	
		8.1.2.-Revisión y verificación	¿Se verifica que son ciertos los datos aportados en el CV que aporta el personal, cuando solicita un puesto de trabajo?		X	
		8.1.3.-Términos y condiciones de la relación laboral	¿Están establecidas las responsabilidades relativas a la seguridad en los términos y condiciones del contrato de trabajo?		X	
	8.2.-Durante la contratación	8.2.1.-Gestión de responsabilidades	¿Se asegura que las responsabilidades de seguridad de cada cual son aplicadas?		X	
		8.2.2.-Educación y capacitación en seguridad de la información	¿Reciben los empleados y usuarios de terceras partes la formación apropiada, relativa a políticas y procedimientos?		X	
		8.2.3.-Procesos disciplinarios	¿Existe un proceso disciplinario para tratar las violaciones realizadas por los empleados, de las políticas y procedimientos de seguridad?	X		El proceso disciplinario que se aplica es el que está en el manual de funciones de cada cargo

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
	8.3.-A la finalización de la contratación	8.3.1.-Responsabilidades en la finalización	¿Están definidas y asignadas claramente las responsabilidades de los empleados y usuarios de terceras partes a la finalización de la contratación?		X	
		8.3.2.-Devolución de activos	¿Se asegura la devolución de todos los activos de la organización en posesión de los empleados y usuarios de terceras partes a la finalización de l a contratación, o acuerdo?		X	
		8.3.3.-Retirada de los derechos de acceso	¿Se asegura la retirada de los derechos de acceso de los empleados y usuarios de terceras partes a la finalización de la contratación o acuerdo?		X	Se trata de reflejar lo más rápido posible los cambios de los derechos de acceso a sistema de información una vez a terminado su contratación. Llegando a pasar 2 días.
9.-Seguridad física y del entorno	9.1.-Áreas seguras	9.1.1.-Perímetro de seguridad física	¿Existe un perímetro de seguridad para proteger las áreas donde están los sistemas?		X	El perímetro existe, pero no se controla quien entra o sale de él.
		9.1.2.-Controles físicos de accesos	¿Están las áreas de seguridad protegidas por controles de entrada, para permitir el acceso sólo al personal autorizado?		X	Las puertas de acceso a la dependencia son de seguridad. El resto de las puertas de las oficinas son normales de chapa y no hay ningún control de entrada.
		9.1.3.-Seguridad de oficinas, despachos y recursos	¿Están protegidos las oficinas y despachos que tienen algún requerimiento de seguridad especial?		X	
		9.1.4.-Protección ante amenazas externas y de entorno	¿Están protegidos las áreas de seguridad contra incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales u origen humano?		X	
		9.1.5.-El trabajo en las áreas de seguridad	¿Existen controles físicos especiales para trabajar en las áreas de seguridad?		X	
	9.2.-Seguridad de los equipos	9.2.1.-Localización y protección del Equipamiento	¿Están los equipos situados o protegidos para reducir las opciones de acceso no autorizado?	X		
		9.2.2.-Suministros	¿Están protegidos los equipos contra fallos de suministro (electricidad, agua, alcantarillado, calefacción, aire acondicionado) ?		X	Existe un regulador de tensión para proteger los equipos contra picos de tensión, pero no hay un SIE para cuando falle el suministro de energía
		9.2.3.-Seguridad del cableado	¿Están protegidos contra daños o escuchas los cables que transmitan datos o soporten servicios de información?		X	
		9.2.4.-Mantenimiento de equipos	¿Se mantienen los equipos en base a las recomendaciones del fabricante y/o procedimientos documentados?		X	El mantenimiento de los equipos no esta procedimentado,
		9.2.5.-Seguridad de equipos fuera de los locales de la Organización	¿Existen procedimientos de seguridad y que cubran la seguridad de los sistemas cuando se usan fuera de las premisas de la empresa?		X	No existe ninguna medida, y se sacan equipos, solo portátiles.
		9.2.6.-Seguridad en la reutilización o eliminación de equipos	¿Se borra la información de los equipos antes de reutilizarlos?	X		
		9.2.7.-Salida de propiedades	¿Se necesita una autorización para sacar de las oficinas equipos, información o software?		X	El control de software y de equipos portátiles no son controlados. Y en ocasiones se sacan sin autorización.
10.- Gestión de comunicaciones y operación	10.1.- Procedimientos operacionales y responsabilidad	10.1.1.-Documentación de procedimientos operativos	¿Están documentados y mantenidos los procedimientos operacionales?		X	
		10.1.2.-Gestión de cambios	¿Están controlados los cambios de los sistemas y aplicaciones?		X	
		10.1.3.-Segregación de Tareas	¿Están segregadas las tareas, para reducir la oportunidad de o malos usos de los sistemas?		X	

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
		10.1.4.-Separación de entornos de desarrollo, pruebas y operación	¿Están separadas las áreas de desarrollo y pruebas de las de los sistemas en operación?	X		Existe un servidor y equipos de pruebas
	10.2.-Gestión en el suministro de servicios (terceras partes)	10.2.1.-Prestación de servicios			X	
		10.2.2.-Monitorización y revisión de servicios de terceras partes			X	
		10.2.3.-Gestión de cambios			X	
	10.3..-Planificación y aceptación de sistemas	10.3.1.-Planificación de capacidades	¿Se controla la necesidad de aumentar la potencia eléctrica, y la capacidad de proceso y almacenamiento?		X	
		10.3.2.-Aceptación de Sistemas	¿Existen criterios de aceptación para nuevos sistemas, ampliaciones o nuevas versiones antes de aceptarlos?		X	No están bien definidos los criterios. La aplicación SIARC se le lleva un control de versiones y antes de ponerse en marcha debe tener la aceptación del director de departamento.
	10.4.-Protección contra software malicioso	10.4.1.-Control contra código malicioso	¿Existen procedimientos implantados para proteger a la empresa contra software malicioso?		X	Hay licencias de antivirus, que están instaladas en los ordenadores de la dependencia y en el servidor.
		10.4.2.-Control contra código móvil	¿Existen procedimientos implantados para proteger a la empresa contra código móvil?		x	
	10.5.-Copias de seguridad	10.5.1.-Copia de la información	¿Se hacen regularmente copias de seguridad?	X		Se hace una copia de seguridad cuando se considere necesario de la información del departamento de soporte informático.
	10.6.-Gestión de seguridad de red	10.6.1.-Controles de redes	¿Se ha implantado algún tipo de control para mantener la seguridad en la red?		X	Existe un firewall instalado
		10.6.2.-Seguridad en servicios de red	¿Están documentados los atributos de seguridad de todos los servicios de red?		X	
	10.7.-Seguridad y gestión de los soportes	10.7.1.-Gestión de soportes removibles	¿Hay procedimientos para gestionar soportes removibles con información como discos, CDs, informes impresos,...?		X	
		10.7.2.-Eliminación de soportes	¿Han desarrollado procedimientos para asegurar el archivo y la destrucción de los soportes informáticos?		X	
		10.7.3.-Procedimientos de utilización de la información	¿Existen procedimientos para manejar y almacenar la información, que la protejan de malos usos?		X	
		10.7.4.-Seguridad de la documentación de sistemas	¿Está la información y los documentos del sistema protegidos de accesos no autorizados?		X	
	10.8.-Intercambio de información	10.8.1.-Políticas y procedimientos para intercambio de información	¿Están documentadas las políticas, procedimientos y medidas para intercambio de información a través de todos los tipos formas de comunicación?		X	
		10.8.2.-Acuerdos para intercambio	¿Se han establecido acuerdos con otras empresas para intercambiar información o aplicaciones?	X		Con el ministerio de educación nacional
		10.8.3.-Seguridad de soportes en tránsito	¿Se toma alguna medida especial con los soportes en tránsito con información sensible?		X	
		10.8.4.-Seguridad de la mensajería electrónica	¿Existe una política para el uso del correo electrónico?		X	
		10.8.5.-Sistemas de información de negocio	¿Se han establecido políticas y directrices para controlar los riesgos de seguridad asociados con los sistemas dentro de las oficinas?		X	

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
	10.10.-Monitorización	10.10.1.-Auditoría de logs	¿Se mantienen durante un periodo de tiempo determinado los registros del sistema para su monitorización futuras del control de acceso?		X	
		10.10.2.-Revisión de uso de sistemas	¿Existen procedimientos para monitorizar el uso de servicios de proceso de información?		X	
		10.10.3.-Protección de logs	¿Está protegida contra sabotaje y accesos no autorizados los logs de sistemas de información		X	
		10.10.4.-Logs de administradores y operadores	¿Se registran y revisan regularmente las actividades de los administradores y operadores?		X	Se realiza cuando lo considerar necesario el departamento de Soporte informático
		10.10.5.-Logs de fallo del sistema	¿Se registran, analizan y aplican las acciones apropiadas a los fallos de sistemas?		X	
		10.10.6.-Sincronización de relojes	¿Están sincronizados todos los relojes de los ordenadores?		X	
11.-Control de acceso	11.1.-Requerimientos	11.1.1.-Política de control de accesos	¿Están documentados las reglas y los derechos de acceso de los usuarios y los grupos?		X	
	11.2.-Gestión de acceso de los usuarios	11.2.1.-Registro de usuarios	¿Quedan registrados los accesos de los usuarios a los servicios y sistemas?	X		
		11.2.2.-Gestión de privilegios	¿Está controlada la gestión de privilegios?	X		
		11.2.3.-Gestión de contraseñas de usuario	¿Existe un proceso para la gestión de passwords?		X	
		11.2.4.-Revisión de los derechos de acceso de los usuarios	¿Se revisan periódicamente los derechos de acceso de los usuarios?		X	
	11.3.-Responsabilidades de los usuarios	11.3.1.-Uso de contraseñas	¿Se indica a los usuarios que sigan buenas prácticas en la selección y uso de passwords?		X	
		11.3.2.-Equipamiento informático de usuario desatendido	¿Se solicita a los usuarios adoptar medidas de protección con los equipos desatendidos?		X	
		11.3.3.-Política de pantallas y mesas limpias	¿Existe una política de pantallas y mesas limpias para los entornos de trabajo (p.e. no dejar documentos sobre las mesas, o el ordenador sin salvapantallas, etc.)?		X	
	11.4.-Control de acceso de red	11.4.1.-Política de uso de los servicios de red	¿Está garantizado que los usuarios solo pueden acceder a los servicios para los que tienen autorización?	X		
		11.4.2.-Autenticación para conexiones externas	¿Están autenticadas las conexiones de los usuarios remotos?		X	
		11.4.3.-Identificación de equipos en la red	¿Se identifican automáticamente los terminales, para autenticar las conexiones a localizaciones específicas y a equipos portátiles?		X	La única autenticación es mediante logir y password.
		11.4.4.-Protección a puertos de diagnóstico remoto y configuración	¿Están controlados los accesos a los puertos de diagnóstico de los equipos del sistema?		X	
		11.4.5.-Segregación en las redes	¿Esta la red segmentada por grupos usuarios y servicios?		X	
		11.4.6.-Control de conexión a las redes	¿Está controlada la capacidad de conexión de los usuarios en redes compartidas?		X	

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
		11.4.7.-Control de enrutamiento en la red	¿Tienen controles que verifiquen las direcciones de origen y destino de las conexiones en las redes compartidas?		X	
	11.5.-Control de acceso al sistema operativo	11.5.1.-Procedimientos de log-on seguros	¿El acceso a los sistemas se realiza mediante un logon seguro?		X	
		11.5.2.-Identificación y autenticación de los usuarios	¿Tiene cada usuario un identificador único?		X	Los equipos de las oficinas no tienen usuarios a nivel del sistema operativo
		11.5.3.-Sistema de gestión de contraseñas	¿Tienen algún sistema de gestión de password que dé passwords difíciles de romper?		X	Existe un modulo generador de contraseñas pero nunca a sido probado el nivel de dificultad de los passwords generados
		11.5.4.-Utilización de utilidades del sistema	¿Están restringidos y controlados los programas de utilidades del sistema?		X	
		11.5.5.-Timeout de sesiones	¿Existen procedimientos y mecanismos para asegurar que se desconecten los terminales inactivos en localizaciones de riesgo?		X	
		11.5.6.-Limitación del tiempo de conexión	¿Existen restricciones en las horas a las que se pueden realizar conexiones a aplicaciones de alto riesgo, así como en su duración?		X	
	11.6.-Control de acceso a información y aplicaciones	11.6.1.-Restricción de acceso a la información	¿Está restringido el acceso a la información y funciones del sistema de aplicación?	x		
		11.6.2.-Aislamiento de sistemas sensibles	¿Están en un entorno aislado y dedicado los sistemas con información sensible?	x		
	11.7.-Portátiles y teletrabajo	11.7.1.-Informática móvil y comunicaciones	¿Existe una política y los controles para la protección contra el riesgo de trabajar con portátiles?		X	los desarrolladores se suelen llevar su portátil con los desarrollos que estén haciendo para continuar trabajando.
		11.7.2.-Teletrabajo	¿Existen políticas y procedimientos para autorizar y controlar las actividades de tele trabajo?		X	
	12.1.-Requisitos de seguridad de los sistemas	12.1.1..Análisis y espeificación de los requerimientos de seguridad	¿Se especifican los controles de seguridad necesarios para nuevos sistemas o mejoras de los actuales?		X	
	12.2.-Procesos correctos en aplicaciones	12.2.1.-Validación de los datos de entrada	¿Se validan los datos introducidos a las aplicaciones?	X		
		12.2.2.-Control del proceso interno	¿Existen chequeos de validación incorporados en el sistema para detectar corrupciones de los datos procesados?		X	
		12.2.3.-Integridad de mensajes	¿Se ha implantado algún sistema de autenticación de mensajes?		X	Los registros se almacenan en la base de datos incluyendo un código hash que se calcula en el momento de su inclusión.
		12.2.4.-Validación de los datos de salida	¿Se valida la salida de datos de la aplicación del sistema?		X	
12.- Compras, desarrollo y mantenimiento de sistemas	12.3.-Controles criptográficos	12.3.1.-Política de uso de los controles criptográficos	¿Existe una política de uso de controles de cifrado para la protección de la información?		X	
		12.3.2.-Gestión de claves	¿Se utiliza algún sistema de gestión de claves para soportar el uso de técnicas criptográficas?	X		
	12.4.-Seguridad de los archivos de sistema	12.4.1.-Control del software en explotación	¿Se aplica algún control para la implantar software en el sistema en operación?		X	
		12.4.2.-Protección de los datos de prueba del sistema	¿Están protegidos los datos de prueba?		X	
		12.4.3.-Control de acceso a la librería de programas fuente	¿Está controlado el acceso a las librerías de los programas fuente?		x	

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
	12.5.-Seguridad en los procesos de desarrollo y soporte	12.5.1.-Procedimientos de cambios operacionales	¿Existen procedimientos para el control de cambios?		X	
		12.5.2.-Revisión técnica de aplicaciones tras cambios del sistema operativo	¿Se revisan y aprueban los sistemas de aplicación cuando se producen cambios?	x		Cuando se hacen cambios en las aplicaciones se suelen probar.
		12.5.3.-Restricciones de cambios a los paquetes de software	¿Se desaconsejan las modificaciones de los paquetes de software?		x	Se realizan instalaciones ajenas a las labores a desarrollar en la dependencia.
		12.5.4.-Fugas de información	¿Se controla y chequea adquisición, uso y cambios de sw con referencia a posibles puertas traseras y códigos troyanos?		X	
		12.5.5.-Desarrollo externalizado	¿Se aplican controles para asegurar que el desarrollo subcontratado de software cumple con las medidas de seguridad necesarias?			
	12.6.-Gestión de vulnerabilidades técnicas	12.6.1.-Control de vulnerabilidades técnicas	¿Se obtiene información sobre vulnerabilidades técnicas de los sistemas de información, la exposición de la organización a tales vulnerabilidades y se toman las medidas apropiadas para tratar el riesgo asociado?		X	
13.-Gestión de incidentes de seguridad de la información	13.1.-Notificación de incidentes y amenazas	13.1.1.-Notificación de eventos de seguridad	¿Existe un canal a través del que se reporten los incidentes de seguridad?		X	Se reporta al departamento de soporte informático los fallos que se detectan en el software desarrollado.
		13.1.2.-Notificación de debilidades	¿Se solicita a los usuarios que comuniquen cualquier debilidad de seguridad o amenaza para el sistema?	X		
	13.2.-Gestión de incidentes y mejora	13.2.1.-Responsabilidad y procedimientos	¿Se han establecido procedimientos y responsabilidades, para la gestión de incidentes?		X	
		13.2.2.-Aprendiendo de los incidentes	¿Existen mecanismos funcionando, para realizar análisis del tipo, volumen y coste de los incidentes y fallos?		X	
		13.2.3.-Recolección de evidencias	Para apoyar una acción contra una persona u organización ¿Se mantienen las evidencias, conforme a las leyes y normas publicadas?		X	
14.-Plan de continuidad de negocio	14.1.-Gestión de la continuidad de negocio	14.1.1.-Inclusión de seguridad en el proceso de gestión de la continuidad del negocio	¿Existe un proceso establecido en la organización, para desarrollar y mantener la continuidad del negocio?		X	
		14.1.2.-Continuidad del negocio y análisis de riesgos	¿Existe un plan estratégico, basado en la valoración de riesgos, donde se detallen las acciones para la continuidad del negocio?		X	
		14.1.3.-Redacción e implantación de planes de continuidad incluida la seguridad de la información	¿Están desarrollados los planes de continuidad para mantener o restaurar las operaciones del negocio en un tiempo razonable?		X	
		14.1.4.-Marco de planificación de la continuidad del negocio	¿Existe un plan general de trabajo para asegurar que todos los planes son consistentes?		X	
		14.1.5.-Prueba, mantenimiento y reevaluación de los planes de continuidad	¿Se prueban regularmente los planes de continuidad de negocio para asegurar que son eficaces?		X	
15.-Conformidad legal	15.1.-Cumplimiento con los requisitos legales	15.1.1.-Identificación de la legislación aplicable	¿Están definidos y documentados, para cada sistema de información, todos los requisitos contractuales, reguladores y estatutarios?		X	
		15.1.2.-Derechos de propiedad intelectual	¿Hay procedimientos para asegurar el cumplimiento con las restricciones legales en el uso de material referente a los derechos de propiedad intelectual?		X	

Sección	Objetivo	Control	Cuestión	Si	No	Comentario
		15.1.3.-Salvaguarda de los registros de la organización	¿Están protegidos contra pérdida, destrucción y falsificación los registros importantes?		X	
		15.1.4.-Protección de datos de carácter personal y de la intimidad de las personas	¿Existen controles eficaces, para proteger la información personal en base a la legislación vigente?		X	
		15.1.5.-Evitar el mal uso de los recursos de tratamiento de información	¿Existe autorización de la dirección para usar el sistema para fines no relacionados con el negocio (usos personales)?		X	Los empleados utilizan el sistema para fines personales habitualmente, sobre todo el correo electrónico y la navegación Web.
		15.1.6.-Reglamentación de los controles de cifrado	¿Existen controles para asegurar el cumplimiento con los acuerdos nacionales para controlar el uso de cifrado?		X	
	15.2.-Cumplimiento con las políticas y normativas	15.2.1.-Cumplimiento con las políticas y normativas	¿Asegura la dirección que se siguen correctamente los procedimientos de seguridad, dentro de su área de responsabilidad?		X	
		15.2.2.-Comprobación de la conformidad técnica	¿Se chequean regularmente los sistemas de información para verificar el cumplimiento con los estándares de implantación de seguridad?		X	
	15.3.-Consideraciones de auditoria de sistemas de información	15.3.1.-Controles de Auditoría de sistemas de información	¿Están planificadas las auditorias de sistemas para reducir el riesgo de interrupciones en el proceso de negocio?		X	
		15.3.2.-Protección de las herramientas de auditoría de sistemas de Información	¿Esta protegido el acceso a las herramientas de auditoria del sistema?		X	

3.1. Resultados

El análisis diferencial muestra que el Área de Admisión, Registro y Control Académico carece de SGSI, evidencia de esto es el bajo cumplimiento de los requerimientos del estándar ISO 27001 y la ausencia de personal encargado de la Seguridad de la información como se muestra en el Organigrama de la dependencia. El estado de cumplimiento de los requerimientos del estándar ISO 27002 es bajo, un 13% de los controles esta implementado.

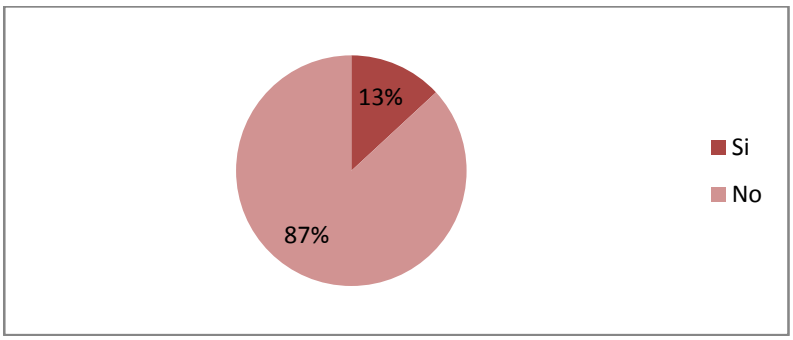

Figura 3. Estado inicial de implementación de controles de seguridad

La dependencia reconociendo la información critica que maneja en sus procesos y de la Universidad de Vancur, a modo de asegurar un entorno Seguro de la información inicia la implementación del SGSI.

La dependencia estableció como objetivos del Plan Director:

- Definir la política de seguridad de información
- Implementar medidas que mejoren la seguridad en el Sistema Informático SIARC, a modo de evitar y contrarrestar el fraude
- Reducir la posibilidad de interrupción del Sistema de Información SIARC ante el riesgo de presentarse contingencias

CAPITULO II. SISTEMA DE GESTION DOCUMENTAL

1. Esquema Documental

La ISO/IEC 27001 define cuales son los documentos necesarios para poder certificar el sistema, pero se centrará en siete de ellos a saber: Política de Seguridad, procedimiento de auditorías internas, gestión de indicadores, procedimiento revisión por dirección, gestión de roles y responsabilidades, metodología de análisis de riesgos y declaración de aplicabilidad.

1.1 Sistemática documental

Con la disposición de llevar una apropiada gestión documental, se definió las consideraciones a tener en cuenta al momento de crearse, actualizarse o revisarse un documento propio del SGSI del Área de Admisión, Registro y Control Académico.

1.1.1 Código del documento

Cada documento creado dentro del SGSI deberá tener un código que lo identifique de los demás documentos producidos. El código seguirá la siguiente estructura:

tipo de estándar. numero de estándar - versión, actualización, revisión

a continuacion se describe cada uno de los elementos del codigo documental.

Tipo de estandar. Indica la naturaleza del documento, este puede ser:

- **P**. Politica
- **Pro**. Procedimiento o Gestion
- **N**. Norma
- **Met**. Metodologia
- **Guia**. Declaracion o Guia
- **Man**. Manual o Instrucciones

Numero de estándar. Numero Consecutivo que permite diferenciar dentro del tipo de estándar.

Versión. Permite evidenciar la evolución del documento. Todo documento creado parte del número uno (1). Cuando se realizan cambios drásticos que

trasforma gran parte del contenido del documento, se deberá incrementar en uno el valor de la versión.

Actualización. Pequeños cambios en el contenido del documento. El valor inicial de la actualización es cero (0) y se irá incrementando en uno (1) a medida que se realicen nuevas actualizaciones

Revisión. Análisis del documento que verifica su valides y pertinencia dentro del SGSI. Su valor inicial es de uno (1). Cada vez que se realice una revisión se deberá incrementar en uno (1) su valor.

Estado del documento: Esta variable indica si el documento está en fase de borrador o preliminar (por aprobar), o por el contrario ha sido aceptado (aprobado). Sus dos estados posibles son: Por aprobar o Aprobado.

A continuación se listan los documentos definidos en el SGSI del Área de Admisión, Registro y Control Académico:

1.2. **Política de seguridad**. Normativa interna que cubre aspectos relativos al acceso de la información, uso de recursos de la organización, comportamiento en caso de incidentes de seguridad, entre otros.
Código del documento: **P.1-1.0.1**

1.3. **Procedimiento de auditorías internas**. Documento que incluye la planificación de las auditorías internas que se llevaran a cabo durante la vigencia de la certificación.
Código del documento: **Pro.1-1.0.1**

1.4. **Gestión de indicadores**. Indicadores que miden la eficacia de los controles de seguridad implantados.
Código del documento: **Pro.3-1.0.1**

1.5. **Procedimiento revisión por Dirección**. Define el procedimiento de revisión de las cuestiones más importantes en relación al SGSI por parte de la dirección.
Código del documento: **Pro.2-1.0.1**

1.6. **Norma de Gestión de roles y responsabilidades**. Conformación del comité de seguridad de las funciones y responsabilidades que cumplen.
Código del documento: **N.1-1.0.1**

1.7. **Metodología de análisis de riesgos**. Indica la sistemática para calcular el riesgo.
Código del documento: **Met.1-1.0.1**

1.8. **Declaración de aplicabilidad**. Documento que incluye todos los controles de seguridad establecidos en el Área de Admisión, Registro y Control Académico, además de la aplicabilidad y estado.
Código del documento: **Guia.1-1.0.1**

2. Resultados

- ✓ La definición de los documentos necesarios para el SGSI del Área de Admisión, Registro y Control Académico que pertenece a la fase de planificación. Estos documentos se convierten en la directriz en la gestión de la seguridad de la información en esta dependencia.

- ✓ Se definió la política de seguridad de la información para el área.

- ✓ Se estableció los mecanismos para la el Análisis de riesgos de los activos de la dependencia.

- ✓ Se realizó cambio en la estructura organizativa. Se vinculan nuevos agentes que intervienen en la seguridad de la información: El Responsable de Seguridad de la información. A cada agente que participa de los procesos de la dependencia se le establecieron responsabilidades en cuanto a la seguridad de la información (ver Figura 4).

- ✓ Se crea el comité de seguridad de la información que está conformado por: Representante de Dirección (Vicerrector administrativo), Jefe de Oficina Jurídica, Jefe de Admisión, Registro y Control Académico, Jefe de la Oficina de Sistemas, Jefe de Desarrollo Tecnológico, Responsable de seguridad de la información y el Asesor certificado en seguridad de la información.

Figura 4. Nueva estructura organizativa

CAPITULO III. ANALISIS DE RIESGOS

Todo proceso de análisis conlleva la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. Es así que muchas fuentes definen el análisis de riesgo como: Un proceso o secuencia de pasos que permiten identificar los riesgos a los que se encuentra sometida la empresa que se estudia. En este apartado se explicará el análisis que se realizó al Área de Admisión, Registro y Control Académico, con el objetivo de estudiar los riesgos a los que pueden estar sometidos los activos de esa dependencia.

El beneficio que le aporta este proceso a la Universidad de Vancur son: Conocer los elementos o activos que esta dependencia debe tratar de asegurar, de que o quien se debe proteger y cuáles serán las medidas adecuadas para contrarrestar los peligros a los que se exponen sus activos.

El proceso de análisis de riesgos, se inició al establecer el inventario de activos con los que cuenta la dependencia, luego se diseñó el árbol de dependencia de los activos, con el fin de identificar y valorar las dependencias entre ellos. Posterior a esto se definió la valoración de cada una de las dimensiones de seguridad con la cual se midió la criticidad de cada activo en las cinco dimensiones de seguridad. De este modo con la valoración de la criticidad de cada activo en las cinco dimensiones, se logra terminar el árbol de dependencias de los activos. Una vez se obtuvo toda la anterior información se logró diseñar la tabla de valoración de activos en donde se indica a demás de la estimación cualitativa se muestra la cuantitativa.

En el análisis de riesgo es necesario hacer la distinción entre los términos: Amenaza, vulnerabilidad, riesgo e impacto.

- ✓ ***Amenaza***. Son todas aquellas situaciones que pueden llegar a suceder en la dependencia y que podrían dañar los activos, provocando que estos no funcionen o que no puedan emplearse de modo correcto en la actividad de la dependencia.
- ✓ ***Vulnerabilidad***. Son las debilidades que presentan los activos y que son aprovechados por las amenazas para provocar un daño.
- ✓ **Riesgo**. Inseguridad a la que están expuestos los sistemas de información ya sean físicos (fuego, inundaciones, catástrofes naturales, etc.) o lógicos (virus, negación de servicio, etc.)
- ✓ ***Impacto***. Es la consecuencia que se produce en la dependencia cuando una amenaza aprovecha una vulnerabilidad para dañar un activo.

1. INVENTARIO DE ACTIVOS

La primera etapa en el análisis de riesgo es conocer los activos con que cuenta el Área de Admisión, Registro y Control Académico, en este caso, a través de entrevistas y de la observación se estableció los activos con los que cuenta esta dependencia. Luego para un mejor análisis se agruparon los activos de acuerdo con la metodología MAGERIT y de acuerdo a lo establecido por el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** que hace parte del esquema documental del SGSI del Área de Admisión, Registro y Control Académico.

Los grupos que se establecieron son: Instalaciones, Hardware, Aplicación, Datos, Red, Servicios, Equipamiento auxiliar y Personal. Las características que definen cada uno de estos grupos de activos se encuentran expresadas en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos**. Luego de aplicado este primer paso se obtuvo la lista de activos que se muestran en la Tabla 6 con su respectivo grupo o ámbito en las columnas de mismo nombre.

Para brindar una valoración de los activos de modo más preciso, se diseñó el árbol de jerarquías o dependencias entre activos. Esto permite identificar y valorar las dependencias entre activos; ya sean estos activos superiores o inferiores y de las necesidades de seguridad que se transmiten unos a otros.

La escala (ver Tabla 4) con la que se valorará cada una de las Dimensiones de seguridad de los activos, que son: Autenticación, Confidencialidad, Integridad, Disponibilidad y Auditoria o Trazabilidad (también conocidas como ACIDA), también se encuentra establecida en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos.** Luego de indicar el valor en cada una de las dimensiones de los activos (ver Tabla columna Aspectos críticos ACIDA), se pasó a completar el árbol de dependencias de activos y mostrar la valoración propia y acumulada de los activos que se apoyan en ellos (Ver Figura 5).

Tabla 4. Valoración dimensiones de seguridad

Valor		Criterio
10	Muy alto	Daño muy grave a la dependencia
7 -9	Alto	Daño grave a la dependencia
4 -6	Medio	Daño importante a la dependencia
1 -3	Bajo	Daño menor a la dependencia
0	Despreciable	Daño muy menor a la dependencia

En la Figura 5 se muestran las dependencias de los activos, en especial de aquellos que participan en tres de los servicios o procesos que realiza el Área de Admisión, Registro y Control Académico que son: Registro académico estudiantil, registro de notas e inscripción en línea a programas. Es de notar la importancia

que tienen los activos: Desde el superior “contraseña” hasta el activo inferior “Edificio del Área de Admisión” en el desarrollo de los procesos de negocio.

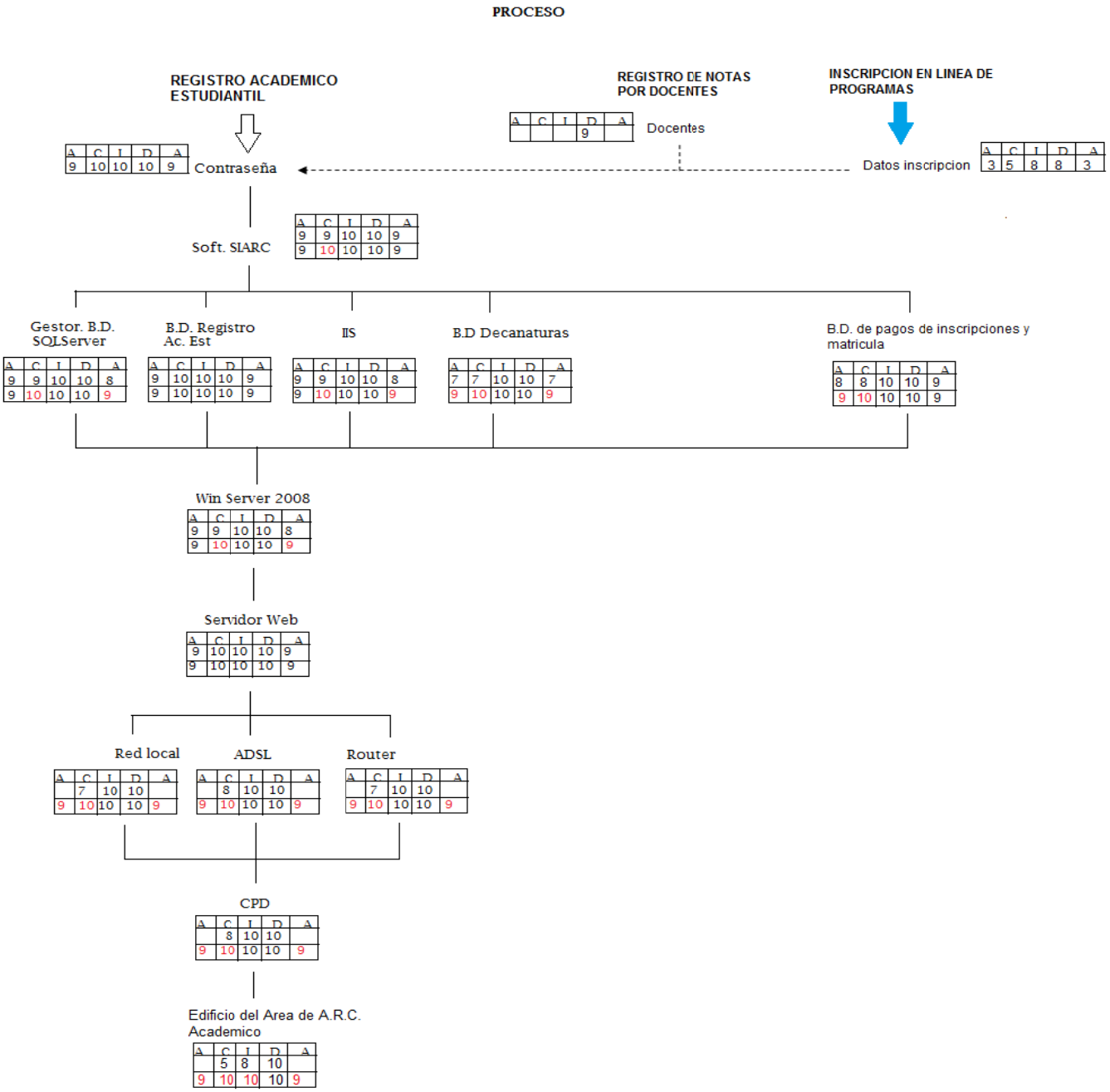

Figura 5. Dependencias entre activos

Conociendo los activos, los aspectos críticos que los afectan en cada una de las cinco dimensiones de seguridad y las dependencias que existen entre los activos, se procedió a valorar cada uno de los activos que posee el Área de Admisión, Registro y Control Académico. Para esto se definió la tabla de valoración de activos (Tabla 5), indicándose una escala cualitativa y una cuantitativa. Se concluye además con la siguiente tabla que el valor máximo de todos los activos que se analizan será de 200.000€.

Tabla 5. Escala de valoración de activos

Valoración	Rango	Valor
Muy Alta	>100.000	200.000€
Alta	50.000 < valor <= 100.000	75.000€
Media	10.000 < valor <= 50.000	30.000€
Bajo	5.000 < valor <= 10.000	7.000€
Muy Bajo	2.000 < valor <= 5.000	3.500€

La siguiente tabla muestra de forma resumida lo elaborado durante esta primera etapa del análisis de riesgo del Área de Admisión, Registro y Control Académico.

Tabla 6. Valoración de activos

Id	Ámbito	Activo	Valor	Aspectos Críticos				
				A	C	I	D	A
1	Instalaciones	Despacho Director Admisión, Registro y Control Académico	MUY BAJO		1	1	3	
2		Despacho jefe de admisión académica	MUY BAJO		1	1	3	
3		Despacho jefe del área de registro académico y archivo	MUY BAJO		1	1	3	
4		Despacho jefe desarrollo tecnológico	BAJO		3	3	5	
5		Área soporte informático y sistemas	MEDIO		2	8	8	
6		CPD del Área de Admisión, Registro y Control Académico	ALTO		8	10	10	
7		Área de archivo	ALTO		7	9	9	
8		Área de registro y control académico	BAJO		4	5	5	
9		Área técnica de admisión	BAJO		4	5	5	
10		Área de certificación académica	BAJO		4	5	5	
11		Edificio: Bloque del Área de admisión, registro y control académico	MUY ALTO		4	5	9	
12	Hardware	PCs desarrollo	MEDIO		9	8	8	
13		Portátiles de desarrollo	MEDIO		9	8	8	
14		PC entorno de pruebas	MEDIO		9	8	7	
15		Servidor desarrollo y prueba	ALTO		10	9	8	
16		Servidor web	ALTO	9	10	10	10	9
17		PC del Área de Archivo ayuda a la gestión de esta Área	MEDIO		8	8	6	
18		PCs de Registro y control académico	BAJO		3	2	2	

19		PCs de Certificación Académica	BAJO		3	4	3	
20		PCs de área técnica de admisión	BAJO		3	2	2	
21		PC de jefe desarrollo tecnológico	MEDIO		7	7	6	
22		PC de jefe del área de registro académico y archivo	BAJO		3	2	2	
23		PC de jefe de admisión académica	BAJO		3	2	2	
24		PC de Director Admisión, Registro y Control Académico	BAJO		3	2	2	
25		PC de secretaria de dirección	MUY BAJO		2	1	1	
26		Impresoras y servidor de impresión	BAJO		3	3	3	
56		Routers	ALTO		7	10	10	
27		Escáneres	MUY BAJO		4	1	1	
28	Software-Aplicación	SO Windows 7 con licencias	BAJO		3	8	8	
29		Gestor de B.D. SQLServer	MEDIO	9	9	10	10	8
30		Microsoft Visual Studio 2010 Asp.NET	BAJO		4	8	8	
31		Microsoft SourceSafe	BAJO		3	9	8	4
32		Software gestor de contraseña	MEDIO	9	9	10	10	8
33		Windows 2008 server	MEDIO	9	9	10	10	8
34		IIS 7.0	MEDIO	9	9	10	10	8
35		Antivirus	BAJO		8	8	8	
36		Servidor de correo electrónico	MUY BAJO	4	3	3	3	4
37		Desarrollo propio: Sistema informático SIARC	ALTO	9	9	10	10	9
	Datos	Hojas de vida docentes y del personal del área de admisión (físico y digital)	MEDIO	8	9	9	8	
		Código fuente aplicación SIARC	ALTO	9	9	10	10	9
		B.D. de pagos, inscripciones y matricula	ALTO	8	8	10	10	9
		Contraseñas de Estudiantes inscritos, matriculados y docentes	ALTO	9	10	10	10	9
		Resultados de pruebas al software de desarrollo	MEDIO		8	8	9	
		B.D. Registro Académico de estudiantes	ALTO	9	10	10	10	9
		B.D. Decanaturas, Programas, Pensum, Asignaturas.	BAJO	7	7	10	10	7
		B.D. Estudiantes inscriptos próximo periodo	BAJO	3	5	8	8	3
		B.D. Ganadores examen de admisión por programa académico	BAJO	4	6	9	8	3
		Inventario de activos del Área	BAJO		6	8	7	
	Media-Soporte de información	DVDs. Soporte de Software licenciado	MEDIO		6	9	9	
		Material impreso. Documentación física de estudiantes matriculados en las modalidad (presencial, Post grado y distancia)	MEDIO		8	9	9	
		Material impreso y digital. Actas de graduación de años anteriores	MEDIO		6	10	9	6
		Seguimiento y configuración de instalaciones	MEDIO		8	8	9	
		Configuración de equipos y sistemas	MEDIO		8	8	9	
		Backups, soporte en DVDs del servidor	ALTO		9	10	10	

		web y de Desarrollo						
		Material impreso: Algunos certificados	MUY BAJO		2	2	4	
55	Red	ADSL	ALTO		8	10	10	
57		Red local	ALTO		7	10	10	
58		Wifi red inalámbrica	BAJO		7	6	6	
59	Servicios	Registro académico Estudiantil	MEDIO	7	5	7	9	9
60		Registro Notas por Docentes	ALTO	10	8	9	9	9
61		Certificados	MEDIO	7	5	5	8	9
62		Inscripción en línea a programas académicos	MEDIO	8	3	4	9	7
63	Equipamiento auxiliar	Aire acondicionado	MEDIO		1	4	9	
64		Estabilizadores de tensión	MEDIO		1	4	10	
65		Cableado eléctrico	MEDIO		1	4	10	
66		Mobiliario: armarios, estantes.	MEDIO		1	4	9	
67	Personal	Vigilante de acceso al área de admisión, Registro y control	MEDIO				7	
68		Director Admisión, Registro y Control Académico	BAJO				5	
69		Jefe de admisión académica	BAJO				6	
70		Jefe del área de registro académico y archivo	BAJO				6	
71		Jefe desarrollo tecnológico	MEDIO				7	
72		Desarrolladores de Software SIARC	ALTO				8	
73		Técnicos Informáticos y de Red	ALTO				8	
74		Responsable de archivo	BAJO				5	
75		Responsables de registro y control académico	MEDIO				7	
76		Responsables técnicos de admisión Académica	MEDIO				7	
77		Responsable de certificación académica	BAJO				6	
78		Docentes	MEDIO				9	
79		Estudiantes pregrado, postgrados y a distancia	MEDIO				9	
80		Personas en proceso de inscripción y matricula	BAJO				6	

2. ANALISIS DE AMENAZAS

Durante esta etapa del análisis de riesgo, se identifican las amenazas a las que están expuestos los activos y que pueden afectar diferentes aspectos de la seguridad. Se habrá que indicar, además cual es la frecuencia con la que posiblemente se puede estar presentando cada amenaza y cuan vulnerable es el activo a la materialización de dicha amenaza. Para esto se utilizo el catalogo de amenazas que presenta la metodología MAGERIT. MAGERIT agrupa las amenazas en: desastres naturales, de origen industrial, errores y fallos no intencionados, y ataques intencionados.

Para el análisis de amenazas de los activos del Área de Admisión, Registro y Control Académico se agruparon nuevamente los activos en: Instalaciones, Hardware, Software, Datos, Media, Red, Servicios, Equipamiento auxiliar y Personal. Para cada grupo de activos se identificaron las amenazas a las que son vulnerables y se analizo el impacto que pueden sufrir en los cinco dimensiones de la seguridad del activo. Además a esto se estimo la frecuencia de materialización de dicha amenaza, de acuerdo a la tabla de frecuencia que se encuentra establecida en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos.** La Tabla 7 muestra el resultado del análisis de esta etapa.

Tabla 7. Activos y dimensiones de la seguridad

ACTIVO	FRECUENCIA Anual	A	C	I	D	T
[L] INSTALACIONES						
Despacho jefe desarrollo tecnológico			60%	30%	100%	
Área soporte informático y sistemas			60%	30%	100%	
CPD del Área de Admisión, Registro y Control Académico			60%	30%	100%	
Área de archivo			60%	30%	100%	
Edificio: Bloque del Área de admisión, registro y control académico			60%	30%	100%	
[N.7] FENOMENO SISMICO	1				60%	
[I.1] FUEGO	1				100%	
[I.2] DAÑOS POR AGUA	1				30%	
[E.19] FUGAS DE INFORMACION	12		10%			
[A.7] USO NO PREVISTO	1		30%	30%	60%	
[A.11] ACCESO NO AUTORIZADO	2		30%	10%		
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	2			30%		
[A.18] DESTRUCCION DE INFORMACION	2				60%	
[A.19] DIVULGACION DE INFORMACION	2		30%			
[A.26] ATAQUE DESTRUCCTIVO	1				60%	
[A.27] OCUPACION ENEMIGA	1		60%		100%	
[HW] HARDWARE		**A**	**C**	**I**	**D**	**T**
PCs desarrollo			60%	30%	100%	
Portátiles de desarrollo			60%	30%	100%	

PC entorno de pruebas			60%	30%	100%
Servidor desarrollo y prueba			60%	30%	100%
Servidor web			60%	30%	100%
PC del Área de Archivo ayuda a la gestión de esta Área			60%	30%	100%
PCs de Registro y control académico			60%	30%	100%
PCs de Certificación Académica			60%	30%	100%
PCs de área técnica de admisión			60%	30%	100%
PC de jefe desarrollo tecnológico			60%	30%	100%
Impresoras y servidor de impresión			60%	30%	100%
Routers			60%	30%	100%
[N.7] FENOMENO SISMICO	1				60%
[I.1] FUEGO	1				100%
[I.2] DAÑOS POR AGUA	1				60%
[I.3] CONTAMINACION MECANICA	4				30%
[I.5] AVERIA DE ORIGEN FISICO O LOGICO	12				60%
[I.6] CORTE DEL SUMINISTRO ELECTRICO	4				100%
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	2				60%
[E.2] ERRORES DEL ADMINISTRADOR	4		30%	10%	60%
[E.23] ERRORES DE MANTENIMIENTO/ ACTUALIZACION DE EQUIPOS HARDWARE	4				60%
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2				100%
[E.25] PERDIDA DE EQUIPOS	1		60%		100%
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	4		60%	30%	10%
[A.7] USO NO PREVISTO	1		30%	10%	60%
[A.11] ACCESO NO AUTORIZADO	12		60%	30%	
[A.23] MANIPULACION DE LOS EQUIPOS	2		60%		60%
[A.24] DENEGACION DE SERVICIO	2				100%
[A.25] ROBO	1		60%		100%
[A.26] ATAQUE DESTRUCCTIVO	1				100%
[SW] SOTFWARE - APLICACIONES INFORMATICAS		**A**	**C**	**I**	**D**	**T**
SO Windows 7 con licencias		60%	60%	60%	100%	
Gestor de B.D. SQLServer		60%	60%	60%	100%	
Microsoft Visual Studio 2010 Asp.NET		60%	60%	60%	100%	
Microsoft SourceSafe		60%	60%	60%	100%	
Software gestor de contraseña		60%	60%	60%	100%	
Windows 2008 server		60%	60%	60%	100%	
IIS 7.0		60%	60%	60%	100%	
Antivirus		60%	60%	60%	100%	
Servidor de correo electrónico		60%	60%	60%	100%	
Desarrollo propio: Sistema informático SIARC		60%	60%	60%	100%	
[I.5] AVERIA DE ORIGEN FISICO O LOGICO	12				100%	
[E.1] ERRORES DE LOS USUARIOS	12		30%	60%	10%	
[E.2] ERRORES DEL ADMINISTRADOR	12		30%	30%	60%	

[E.8] DIFUSION DE SOFTWARE DAÑINO	12		10%	30%	100%	
[E.9] ERRORES DE REENCAMINAMIENTO	2		10%			
[E.19] FUGAS DE INFORMACION	12		30%			
[E.20] VULNERABILIDADES DE LOS PROGRAMAS SOFTWARE	48		10%	60%	30%	
[E.21] ERRORES DE MANTENIMIENTO/ ACTUALIZACION DE PROGRAMAS SOFTWARE	12			60%	30%	
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	12	60%	60%	60%		
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	4		60%	30%	30%	
[A.7] USO NO PREVISTO	4		60%	30%	100%	
[A.8] DIFUSION DE SOFTWARE DAÑINO	4		30%	30%	100%	
[A.9] REENCAMINAMIENTO DE MENSAJES	2		30%			
[A.11] ACCESO NO AUTORIZADO	12		60%	60%		
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	4			60%		
[A.18] DESTRUCCION DE INFORMACION	4				60%	
[A.19] DIVULGACION DE INFORMACION	12		60%			
[A.22] MANIPULACION DE PROGRAMAS	4		60%	30%	30%	
[D] DATOS/ INFORMACION		**A**	**C**	**I**	**D**	**T**
Hojas de vida docentes y del personal del área de admisión (físico y digital)		60%	60%	60%	100%	100%
Código fuente aplicación SIARC		60%	60%	60%	100%	100%
B.D. de pagos, inscripciones y matricula		60%	60%	60%	100%	100%
Contraseñas de Estudiantes inscritos, matriculados y docentes		60%	60%	60%	100%	100%
Resultados de pruebas al software de desarrollo		60%	60%	60%	100%	100%
B.D. Registro Académico de estudiantes		60%	60%	60%	100%	100%
B.D. Decanaturas, Programas, Pensum, Asignaturas.		60%	60%	60%	100%	100%
B.D. Estudiantes inscriptos próximo periodo		60%	60%	60%	100%	100%
B.D. Ganadores examen de admisión por programa académico		60%	60%	60%	100%	100%
Inventario de activos del Área		60%	60%	60%	100%	100%
[E.1] ERRORES DE LOS USUARIOS	4		60%	30%	10%	
[E.2] ERRORES DEL ADMINISTRADOR	12		30%	30%	60%	
[E.3] ERRORES DE MONITORIZACION	12			60%		100%
[E.4] ERRORES DE CONFIGURACION	12			60%		
[E.15] ALTERACION ACCIDENTAL DE LA INFORMACION	4			30%		
[E.18] DESTRUCCION DE LA INFORMACION	2				100%	
[E.19] FUGAS DE INFORMACION	12		30%			
[A.3] MANIPULACION DE LOS REGISTRO DE ACTIVIDAD	4			60%		100%
[A.4] MANIPULACION DE LA CONFIGURACION	4		30%	60%	60%	
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	4	60%	60%	60%		

[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	4		60%	30%	30%	
[A.11] ACCESO NO AUTORIZADO	4		60%	60%		
[A.13] REPUDIO	12			30%		60%
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	4			60%		
[A.18] DESTRUCCION DE INFORMACION	2				60%	
[A.19] DIVULGACION DE INFORMACION	12		60%			
[MEDIA] SOPORTE DE INFORMACION		**A**	**C**	**I**	**D**	**T**
DVDs. Soporte de Software licenciado			100%	100%	100%	
Material impreso. Documentación física de estudiantes matriculados en las modalidad (presencial, Post grado y distancia)			100%	100%	100%	
Material impreso y digital. Actas de graduación de años anteriores			100%	100%	100%	
Seguimiento y configuración de instalaciones			100%	100%	100%	
Configuración de equipos y sistemas			100%	100%	100%	
Backups, soporte en DVDs del servidor web y de Desarrollo			100%	100%	100%	
Material impreso: Algunos certificados			100%	100%	100%	
[N.7] FENOMENO SISMICO	1				60%	
[I.1] FUEGO	1				100%	
[I.2] DAÑOS POR AGUA	1				60%	
[I.3] CONTAMINACION MECANICA	4				30%	
[I.6] CORTE DEL SUMINISTRO ELECTRICO	4				60%	
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	4				10%	
[I.10] DEGRADACION DE LOS SOPORTES DE ALMACENAMIENTO DE LA INFORMACION	12				60%	
[E.1] ERRORES DE LOS USUARIOS	12		60%	30%	10%	
[E.2] ERRORES DEL ADMINISTRADOR	12		30%	30%	60%	
[E.15] ALTERACION ACCIDENTAL DE LA INFORMACION	4			30%		
[E.18] DESTRUCCION DE LA INFORMACION	4				100%	
[E.19] FUGAS DE INFORMACION	12		30%			
[E.23] ERRORES DE MANTENIMIENTO/ ACTUALIZACION DE EQUIPOS HARDWARE	12				60%	
[E.25] PERDIDA DE EQUIPOS	2		100%		100%	
[A.7] USO NO PREVISTO	2		60%	30%	60%	
[A.11] ACCESO NO AUTORIZADO	2		60%	60%		
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	4			100%		
[A.18] DESTRUCCION DE INFORMACION	4			100%		
[A.19] DIVULGACION DE INFORMACION	12		100%			
[A.23] MANIPULACION DE LOS EQUIPOS	4		60%		60%	
[A.25] ROBO	2		100%		100%	
[A.26] ATAQUE DESTRUCCTIVO	1				60%	
[COM] REDES DE COMUNICACION		**A**	**C**	**I**	**D**	**T**

ADSL		60%	60%	100%	100%	
Red local		60%	60%	100%	100%	
Wifi red inalámbrica		60%	60%	100%	100%	
[I.8] FALLO DE SERVICIO DE COMUNICACIONES	2				100%	
[E.2] ERRORES DEL ADMINISTRADOR	12		60%	30%	100%	
[E.9] ERRORES DE REENCAMINAMIENTO	2		30%			
[E.15] ALTERACION ACCIDENTAL DE LA INFORMACION	2			30%		
[E.18] DESTRUCCION DE LA INFORMACION	4				100%	
[E.19] FUGAS DE INFORMACION	12		60%			
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	4				100%	
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	12	60%	60%	60%		
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	4		60%	30%	30%	
[A.7] USO NO PREVISTO	4		60%	60%	100%	
[A.9] REENCAMINAMIENTO DE MENSAJES	2		30%			
[A.11] ACCESO NO AUTORIZADO	12		60%	60%		
[A.12] ANALISIS DE TRAFICO	48		60%			
[A.14] INTERCEPTACION DE INFORMACION	12		60%			
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	4			100%		
[A.18] DESTRUCCION DE INFORMACION	2				100%	
[A.24] DENEGACION DE SERVICIO	4				100%	
[S] SERVICIOS		**A**	**C**	**I**	**D**	**T**
Registro académico Estudiantil		60%	60%	60%	100%	100%
Registro Notas por Docentes		60%	60%	60%	100%	100%
Certificados		60%	60%	60%	100%	100%
Inscripción en línea a programas académicos		60%	60%	60%	100%	100%
[E.1] ERRORES DE LOS USUARIOS	48		10%	30%	10%	
[E.2] ERRORES DEL ADMINISTRADOR	48		30%	60%	100%	
[E.9] ERRORES DE REENCAMINAMIENTO	2		30%			
[E.15] ALTERACION ACCIDENTAL DE LA INFORMACION	4			60%		
[E.18] DESTRUCCION DE LA INFORMACION	4				100%	
[E.19] FUGAS DE INFORMACION	12		30%			
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	12				100%	
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	48	60%	60%	60%		
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	12		60%	60%	60%	
[A.7] USO NO PREVISTO	4		60%	60%	60%	
[A.9] REENCAMINAMIENTO DE MENSAJES	2		30%			
[A.11] ACCESO NO AUTORIZADO	12		60%	60%		
[A.13] REPUDIO	48			30%		100%
[A.15] MODIFICACION DELIBERADA DE LA	12			60%		

INFORMACION						
[A.18] DESTRUCCION DE INFORMACION	4				100%	
[A.19] DIVULGACION DE INFORMACION	48		60%			
[A.24] DENEGACION DE SERVICIO	12				100%	
[AUX] EQUIPAMIENTO AUXILIAR		**A**	**C**	**I**	**D**	**T**
Aire acondicionado			30%	60%	100%	
Estabilizadores de tensión			30%	60%	100%	
Cableado eléctrico			30%	60%	100%	
Mobiliario: armarios, estantes.			30%	60%	100%	
[N.7] FENOMENO SISMICO	1				60%	
[I.1] FUEGO	1				100%	
[I.2] DAÑOS POR AGUA	1				60%	
[I.3] CONTAMINACION MECANICA	12				60%	
[I.5] AVERIA DE ORIGEN FISICO O LOGICO	48				60%	
[I.6] CORTE DEL SUMINISTRO ELECTRICO	4				100%	
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	4				60%	
[E.23] ERRORES DE MANTENIMIENTO/ ACTUALIZACION DE EQUIPOS HARDWARE	12				60%	
[E.25] PERDIDA DE EQUIPOS	2		10%		100%	
[A.7] USO NO PREVISTO	2		10%	30%	60%	
[A.11] ACCESO NO AUTORIZADO	2		30%	60%		
[A.23] MANIPULACION DE LOS EQUIPOS	4		30%		60%	
[A.25] ROBO	2		30%		100%	
[A.26] ATAQUE DESTRUCCTIVO	1				100%	
[P] PERSONAL		**A**	**C**	**I**	**D**	**T**
Vigilante de acceso al área de admisión, Registro y control			60%	60%	100%	
Director Admisión, Registro y Control Académico			60%	60%	100%	
Jefe de admisión académica			60%	60%	100%	
Jefe del área de registro académico y archivo			60%	60%	100%	
Jefe desarrollo tecnológico			60%	60%	100%	
Desarrolladores de Software SIARC			60%	60%	100%	
Técnicos Informáticos y de Red			60%	60%	100%	
Responsable de archivo			60%	60%	100%	
Responsables de registro y control académico			60%	60%	100%	
Responsables técnicos de admisión Académica			60%	60%	100%	
Responsable de certificación académica			60%	60%	100%	
Docentes			60%	60%	100%	
Estudiantes pregrado, postgrados y a distancia			60%	60%	100%	
Personas en proceso de inscripción y matricula			60%	60%	100%	
[E.7] DEFICIENCIAS EN LA ORGANIZACION	4				10%	
[E.19] FUGAS DE INFORMACION	12		30%			

[E.28] INDISPONIBILIDAD DEL PERSONAL	2			100%
[A.28] INDISPONIBILIDAD DEL PERSONAL	2			60%
[A.29] EXTORSION	1	60%	60%	60%
[A.30] INGENIERIA SOCIAL	2	60%	60%	60%

3. NIVEL DE RIESGO ACEPTABLE

En el análisis de Riesgo Intrínseco, Efectivo y Residual, se tomarán los datos obtenidos en el análisis de amenazas y de la Valoración de los activos del Área de Admisión, Registro y Control Académico. Para realizar estos análisis se debe contar con el nivel de Riesgo aceptado por la Dirección de la dependencia; es así que según lo establecido en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** los niveles de riesgo son lo mostrados en la Tabla8**.**

Tabla 8. Niveles de Riesgos

NIVEL DE RIESGO		
MA	Muy alto	>10.000,00 €
A	Alto	7.000,00 €
M	Medio	3.000,00 €
B	Bajo	1.000,00 €
N	Muy Bajo	200,00 €

La dirección también define el nivel de Riesgo Aceptable así como los **criterios de aceptación**:

- Durante la etapa de evaluación de riesgos se aceptan aquellos riesgos de nivel "Muy bajo", "Bajo" y "Medio", y no se aceptan los riesgos de nivel "Alto" y "Crítico" los cuales deben ser tratados.
- Durante la etapa de tratamiento de riesgos se aceptará el riesgo siempre y cuando el beneficio –costo sea negativo y no afecte la política de seguridad.

Definido el nivel de Riesgo Aceptable, se puede obtener los Riesgos Intrínseco, Efectivo y Residual, utilizando la información recopilada de los activos (su valoración, amenazas e impacto), utilizando la escala de Disminución del Impacto o la Frecuencia que está establecida en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** y conociendo los controles implementados en el Área de Admisión, Registro y Control Académico (ver Tabla 9).

Tabla 9. Controles implementados

Nº	Descripción
1	Extintores
2	Contratos de confidencialidad de plantilla

3	Documento disciplinario contra violaciones de seguridad
4	Mantenimiento del servidor de impresión
5	Mantenimiento de la climatización
6	Llaves de la puertas principal y de emergencia
7	llaves de acceso al CPD
8	Portero De la dependencia
9	Llaves del armario del Resp. Soft
10	Firewall 1
11	Firewall 2
12	politica de uso de los servicios de red
13	Revisión técnica de aplicaciones tras cambios del sistema operativo
14	gestion de claves
15	software de registro de actividad de usuarios
16	Copias de seguridad de datos
17	procedimiento de borrado de equipos
18	Antivirus
19	Software copias seguridad
20	Control de acceso
21	mantenimiento de servidores de aplicación

4. RIESGO INTRÍNSECO, EFECTIVO Y RESIDUAL

El Riesgo Intrínseco. Para este análisis se empleo la formula:

Riesgo = valorActivo * vulnerabilidad * Impacto

El Riesgo Efectivo. Para este análisis se empleo la formula:

Riesgo = valorActivo * vulnerabilidad * (1 – impactoReduccion) * Impacto

Riesgo Residual. Su cálculo se efectuó del siguiente modo:

RiesgoIntrinseco – RiesgoEfectivo.

5. CALCULO DEL RIESGO

Para el cálculo del riesgo se empleo la tabla que se encuentra definida en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** Anexo E.

Se paso a calcular primero el riesgo intrínseco al que están expuestos cada activo de acuerdo al tipo de activo al que pertenece. Es así, que por grupos se ubicaron

todos los activos de modo horizontal en la hoja de análisis y sus amenazas se listaron de modo vertical. Se debe recordar que las amenazas que se toman en cuenta en este análisis surgen del estudio previo que se realizo del análisis de amenazas y de la tabla 7 que resume sus resultados.

Existen Tipos de activos que agrupan muchos activos, convirtiendo el cálculo del riesgo en algo muy extenso; para evitar esto, se tomaron en cuenta aquellos que de acuerdo a la valoración que se hizo de ellos resultaron ser Alta y que además sea un activo critico para la misión de la dependencia. Aquí se apoyo en los resultados mostrados del análisis de activos de la tabla 6.

A modo de ilustración se agrego la hoja de análisis del Tipo de activos de Servicio que se muestran en la Tabla 10. Como es de apreciarse, este tipo de activos solo agrupó a cuatro de ellos y no se excluyo ninguno del análisis. Una vez se ubicaron los activos y las amenazas, se indico el valor de cada activo de acuerdo a la tabla 6 y a la escala de valoración de activos definido en la tabla 5. Es así que el activo Registro académico Estudiantil en la tabla 6 se valoró como MEDIO y de acuerdo a la escala de valoración los activos con valoración cualitativa MEDIO tiene una valoración cuantitativa de 30.000; de ese modo se indicó el valor de todos los activos (recuadros de color azul en Tabla 10).

Ahora por amenaza se colocó la frecuencia en que se presenta dicha amenaza, estos valores ya se habían obtenido en el análisis de las amenazas tabla 7. En la tabla 7 se puede verificar para el grupo de activos de Servicio la amenaza [E.1] ERRORES DE LOS USUARIOS obtuvo una valoración de 48 veces al año, es decir es probable que se presente esta amenaza 48 veces en un año. Este valor de 48 se ubicó en la casilla de frecuencia. Como se obtendrá el valor de riesgo intrínseco diario, todas las unidades en que se presentan las variables que participan de este cálculo se expresan por día. Luego la frecuencia 48 se divide entre 360 para obtener su valor diario, esto queda expresado en la casilla Frecuencia /360 de la Tabla 10.

El impacto o el porcentaje del daño que puede causar la amenaza se obtuvo de acuerdo a lo obtenido del análisis de amenazas que se resumen en la tabla 7. Si se observa la amenaza: [E.1] ERRORES DE LOS USUARIOS para el grupo de activos Servicios, se observa que la valoración del impacto en las cinco dimensiones de seguridad fue de: 10%, 30% y 10% para las dimensiones: confidencialidad, integridad y disponibilidad respectivamente. Estos tres porcentajes se promediaron para obtener el impacto de esa amenaza; de ese modo se obtuvo un 16.66% o 0.1666 que se muestra en la casilla impacto de la Tabla 10.

Teniendo cada uno de los valores de las variables que participan del cálculo del riesgo intrínseco y de acuerdo al documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** su fórmula es:

R. Intrínseco = valorActivo * vulnerabilidad * Impacto

Se tiene para el activo Registro académico Estudiantil un riesgo intrínseco de:

R. Intrínseco = 30000*0,133333333*0,166666667
R. Intrínseco =666,6666667

Como se muestra en el recuadro de color coral de la Tabla 10. Así se completo para cada amenaza el cálculo del riesgo intrínseco para el activo Registro académico Estudiantil y los demás activos del Tipo de activo Servicios.

Luego, para cada activo se sumo cada riesgo intrínseco obtenido en cada una de las amenazas, resultando el *riesgo intrínseco diario por activo*, como se muestra al final de la Tabla 10.Para el activo Registro académico Estudiantil el *riesgo intrínseco diario por activo* fue de15.866,67 €. Conociendo el riesgo intrínseco diario para cada activo, en el Tipo de activo de Servicio, se totalizaron para conocer el *Total riesgo intrínseco diario* para ese grupo de activos. Para el Tipo de activo Servicios el Total riesgo intrínseco diario fue de: 87.266,67 €.

Formulas:

*Riesgo intrínseco diario para activo = RiesgoIntrínsecoDelActivoParaAmenaza1 + RiesgoIntrínsecoDelActivoParaAmenaza2 + **…** + RiesgoIntrínsecoDelActivoParaAmenaza**N***

Total riesgo intrínseco diario = RiesgoIntrínsecoDiarioParaActivo1 + RiesgoIntrínsecoDiarioParaActivo2 + … +RiesgoIntrínsecoDiarioParaActivoN

De ese mismo modo se calculo el riesgo intrínseco para cada activo en cada grupo.

Tabla 10. Calculo del riesgo de los activos de servicios

				Registro académico Estudiantil		Registro Notas por Docentes		Certificados		Inscripción en línea a programas académicos	
				30000		75000		30000		30000	
[E.1] ERRORES DE LOS USUARIOS	48	0,133333333	0,166666667	666,6666667	90%	1666,666667	90%	666,6666667	90%	666,6666667	60%
				0,133333333	0,016666667	0,133333333	0,016666667	0,133333333	0,016666667	0,133333333	0,066666667
				66,66666667		166,6666667		66,66666667		266,6666667	
				600		1500		600		400	
[E.2] ERRORES DEL ADMINISTRADOR	48	0,133333333	0,633333333	2533,333333	90%	6333,333333	90%	2533,333333	90%	2533,333333	90%
				0,133333333	0,063333333	0,133333333	0,063333333	0,133333333	0,063333333	0,133333333	0,063333333
				253,3333333		633,3333333		253,3333333		253,3333333	
				2280		5700		2280		2280	
[E.9] ERRORES DE REENCAMINAMIENTO	2	0,005555556	0,3	50	60%	125	90%	50	60%	50	60%
				0,005555556	0,12	0,005555556	0,03	0,005555556	0,12	0,005555556	0,12
				20		12,5		20		20	
				30		112,5		30		30	
[E.15] ALTERACION ACCIDENTAL DE LA INFORMACION	4	0,011111111	0,6	200	90%	500	90%	200	90%	200	60%
				0,011111111	0,06	0,011111111	0,06	0,011111111	0,06	0,011111111	0,24
				20		50		20		80	
				180		450		180		120	

[E.18] DESTRUCCION DE LA INFORMACION	4	0,011111111	1	333,3333333	90%	833,3333333	90%	333,3333333	90%	333,3333333	60%
				0,011111111	0,1	0,011111111	0,1	0,011111111	0,1	0,011111111	0,4
				33,33333333		83,33333333		33,33333333		133,3333333	
				300		750		300		200	
[E.19] FUGAS DE INFORMACION	12	0,033333333	0,3	300	90%	750	90%	300	90%	300	90%
				0,033333333	0,03	0,033333333	0,03	0,033333333	0,03	0,033333333	0,03
				30		75		30		30	
				270		675		270		270	
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	12	0,033333333	1	1000	30%	2500	30%	1000	30%	1000	30%
				0,033333333	0,7	0,033333333	0,7	0,033333333	0,7	0,033333333	0,7
				700		1750		700		700	
				300		750		300		300	
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	48	0,133333333	0,6	2400	90%	6000	90%	2400	90%	2400	90%
				0,133333333	0,06	0,133333333	0,06	0,133333333	0,06	0,133333333	0,06
				240		600		240		240	
				2160		5400		2160		2160	
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	12	0,033333333	0,6	600	90%	1500	90%	600	90%	600	90%
				0,033333333	0,06	0,033333333	0,06	0,033333333	0,06	0,033333333	0,06
				60		150		60		60	
				540		1350		540		540	

[A.7] USO NO PREVISTO	4	0,011111111	0,6	200	90%	500	90%	200	90%	200	90%
				0,011111111	0,06	0,011111111	0,06	0,011111111	0,06	0,011111111	0,06
				20		50		20		20	
				180		450		180		180	
[A.9] REENCAMINAMIENTO DE MENSAJES	2	0,005555556	0,3	50	60%	125	90%	50	60%	50	60%
				0,005555556	0,12	0,005555556	0,03	0,005555556	0,12	0,005555556	0,12
				20		12,5		20		20	
				30		112,5		30		30	
[A.11] ACCESO NO AUTORIZADO	12	0,033333333	0,6	600	90%	1500	90%	600	90%	600	90%
				0,033333333	0,06	0,033333333	0,06	0,033333333	0,06	0,033333333	0,06
				60		150		60		60	
				540		1350		540		540	
[A.13] REPUDIO	48	0,133333333	0,65	2600	90%	6500	90%	2600	60%	2600	90%
				0,133333333	0,065	0,133333333	0,065	0,133333333	0,26	0,133333333	0,065
				260		650		1040		260	
				2340		5850		1560		2340	
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	12	0,033333333	0,6	600	90%	1500	90%	600	90%	600	60%
				0,033333333	0,06	0,033333333	0,06	0,033333333	0,06	0,033333333	0,24
				60		150		60		240	
				540		1350		540		360	
[A.18] DESTRUCCION DE INFORMACION	4	0,011111111	1	333,3333333	90%	833,3333333	90%	333,3333333	90%	333,3333333	90%
				0,011111111	0,1	0,011111111	0,1	0,011111111	0,1	0,011111111	0,1
				33,33333333		83,33333333		33,33333333		33,33333333	

				300		750		300		300	
[A.19] DIVULGACION DE INFORMACION	48	0,133333333	0,6	2400	90%	6000	90%	2400	90%	2400	60%
				0,133333333	0,06	0,133333333	0,06	0,133333333	0,06	0,133333333	0,24
				240		600		240		960	
				2160		5400		2160		1440	
[A.24] DENEGACION DE SERVICIO	12	0,033333333	1	1000	30%	2500	30%	1000	30%	1000	30%
				0,033333333	0,7	0,033333333	0,7	0,033333333	0,7	0,033333333	0,7
				700		1750		700		700	
				300		750		300		300	
					15.866,67		39.666,67		15.866,67		15.866,67
riesgo intrinseco diario por activo				€		€		€		€	
riesgo efectivo				2.816,67 €		6.966,67 €		3.596,67 €		4.076,67 €	
					13.050,00		32.700,00		12.270,00		11.790,00
riesgo residual				€		€		€		€	

Total riesgo intrinsico diario	87.266,67 €
Total Riesgo Efectivo	17.456,67 €
Total Riesgo Resdiual	69.810,00 €

Por grupo de activos se totalizo su riesgo intrínseco y es el mostrado en la Figura 6. Se aprecia que los grupos de activos que están por debajo del riesgo aceptado (7.000) son: locación y personal. Los más destacados por tener un alto riesgo intrínseco muy por encima del aceptado, son: servicios, datos y software.

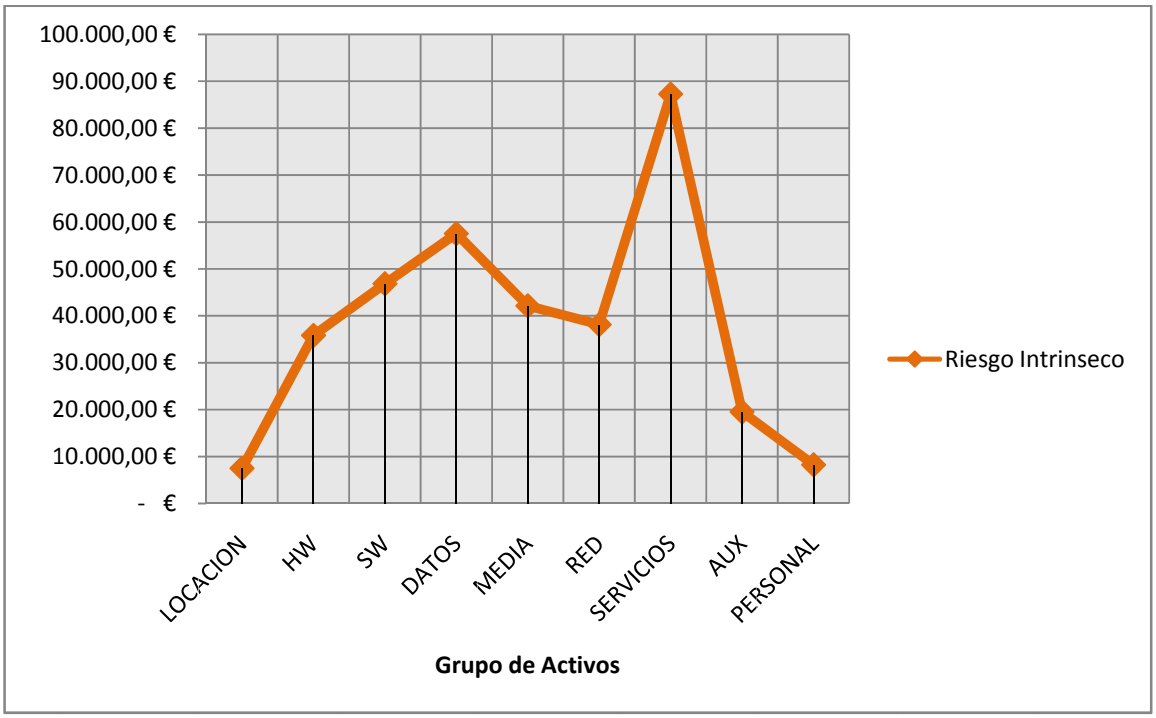

Figura 6. Riesgo intrínseco por grupos de activos

Las amenazas a las que más está expuesto el Área de Admisión, Registro y Control Académico, se destacan:A.19 Divulgación de información, E.2 Errores del administrador, I.5 Avería de origen físico o lógico, A.5 Suplantación de la identidad del usuario, A.13 Repudio y A.11 Acceso no autorizado. La Tabla 11 muestra de modo completo todas las amenazas que superaron el riesgo aceptable. La Figura7 muestra el riesgo intrínseco para todas las amenazas de la dependencia.

Tabla 11. Riesgo Intrínseco por Amenaza

AMENAZA	R. INTRINSECO
[A.19] DIVULGACION DE INFORMACION	32.383,33 €
[E.2] ERRORES DEL ADMINISTRADOR	28.888,89 €
[I.5] AVERIA DE ORIGEN FISICO O LOGICO	23.600,00 €
[A.5] SUPLANTACION DE LA IDENTIDAD DEL USUARIO	22.500,00 €
[A.13] REPUDIO	19.700,00 €
[A.11] ACCESO NO AUTORIZADO	19.663,89 €
[E.19] FUGAS DE INFORMACION	16.916,67 €
[A.12] ANALISIS DE TRAFICO	12.000,00 €
[A.15] MODIFICACION DELIBERADA DE LA INFORMACION	11.750,00 €

[E.1] ERRORES DE LOS USUARIOS	9.666,67 €
[E.3] ERRORES DE MONITORIZACION	9.600,00 €
[E.23] ERRORES DE MANTENIMIENTO/ ACTUALIZACION DE EQUIPOS HARDWARE	9.400,00 €
[A.24] DENEGACION DE SERVICIO	9.250,00 €
[E.24] CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	9.250,00 €
[A.18] DESTRUCCION DE INFORMACION	8.833,33 €
[E.20] VULNERABILIDADES DE LOS PROGRAMAS SOFTWARE	8.666,67 €
[E.18] DESTRUCCION DE LA INFORMACION	8.000,00 €
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	7.822,22 €
[E.4] ERRORES DE CONFIGURACION	7.200,00 €
[I.6] CORTE DEL SUMINISTRO ELECTRICO	7.000,00 €

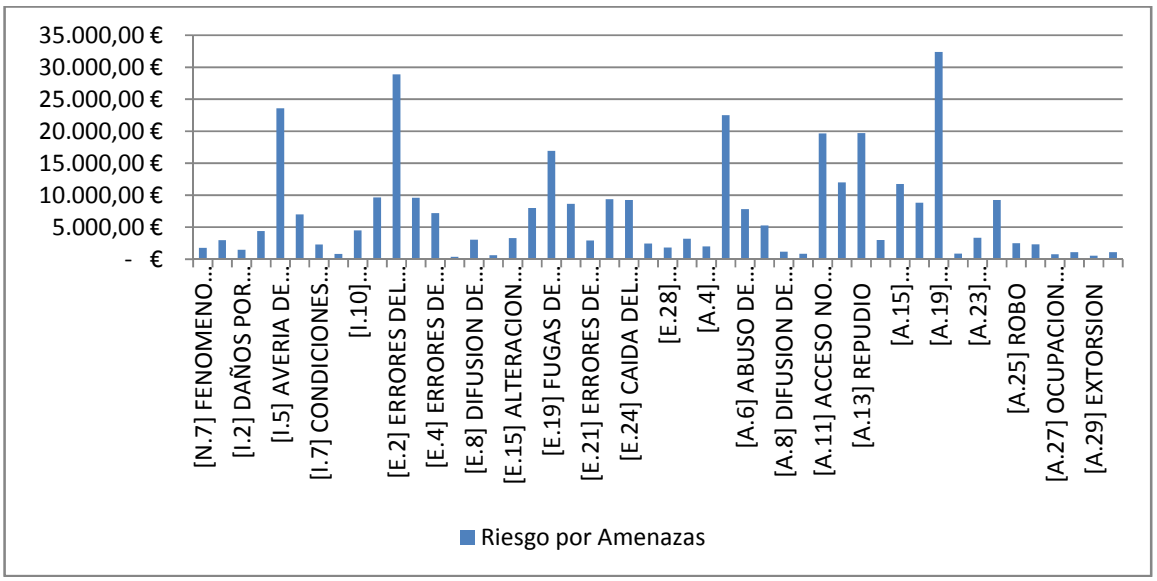

Figura 7. Riesgo Intrínseco por Amenazas

Analizando ahora los activos, los que presentan un nivel de riesgo muy por encima del aceptado, son: Registro Notas por Docentes, Red local, ADSL y Desarrollo propio: Sistema informático SIARC. Se encontraron 15 activos que superan el nivel de riesgo aceptado. La lista completa se muestra en la Tabla 12.

Tabla 12. Activos con Riesgo intrínseco superior al nivel aceptado

GRUPO	ACTIVO	R. INTRINSECO	TOTAL GRUPO
SERVICIOS	Registro Notas por Docentes	39.666,67 €	
	Registro académico Estudiantil	15.866,67 €	

	Certificados	15.866,67 €	
	Inscripción en línea a programas académicos	15.866,67 €	87.266,67 €
DATOS	B.D. de pagos, inscripciones y matricula	11.986,11 €	
	Contraseñas de Estudiantes inscritos, matriculados y docentes	11.986,11 €	
	B.D. Registro Académico de estudiantes	11.986,11 €	
	Código fuente aplicación SIARC	11.986,11 €	57.533,33 €
SOFTWARE	Desarrollo propio: Sistema informático SIARC	18.013,89 €	46.836,11 €
MEDIA	Backups, soporte en DVDs del servidor web y de Desarrollo	14.125,00 €	42.125,00 €
RED	Red local	19.070,44 €	
	ADSL	19.069,44 €	38.138,89 €
HARDWARE	Servidor desarrollo y prueba	7.166,67 €	
	Servidor web	7.166,67 €	
	Routers	7.166,67 €	35.833,33 €

La siguiente grafica muestra un esquema general del riesgo intrínseco de los activos del Área de Admisión, Registro y Control Académico.

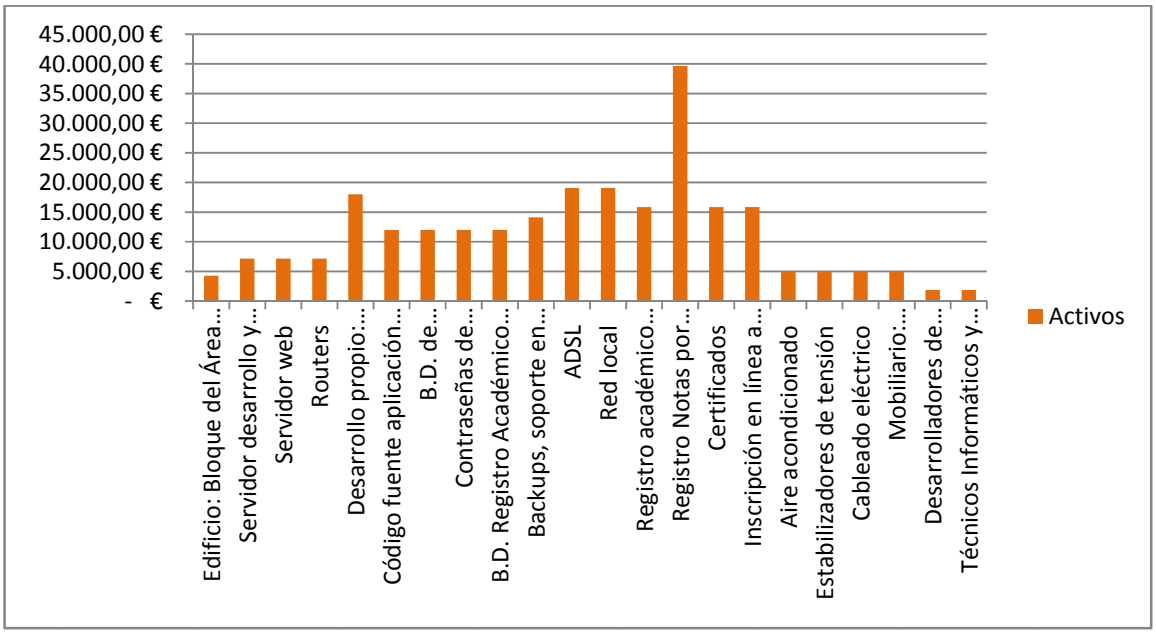

Figura 8. Riesgo Intrínseco de los Activos

5.1 Elección de salvaguardas

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos. La Tabla 13 resume los controles que fueron seleccionados.

Tabla 13. Salvaguardas

No.	Controles
1	Extintores
2	Contratos de confidencialidad de plantilla
3	Documento disciplinario contra violaciones de seguridad
4	Mantenimiento del servidor de impresión
5	Mantenimiento de la climatización
6	Llaves de la puertas principal y de emergencia
7	llaves de acceso al CPD
8	Portero De la dependencia
9	Llaves del armario del Resp. Soft
10	Firewall 1
11	Firewall 2
12	política de uso de los servicios de red
13	Revisión técnica de aplicaciones tras cambios del sistema operativo
14	gestión de claves
15	software de registro de actividad de usuarios
16	Copias de seguridad de datos
17	procedimiento de borrado de equipos
18	Antivirus
19	Software copias seguridad
20	Control de acceso
21	mantenimiento de servidores de aplicación
22	IDS Y IPS
23	Registros de actividades de auditoria
24	Documento de procedimiento de monitoreo de medios
25	perímetro de seguridad física
26	controles de entrada físicos
27	Sistema de detección de fuego
28	Procedimiento de trabajo en áreas seguras
29	Definición de áreas de acceso público y de entregas
30	Registros de actividades del administrados del sistema
31	Registros de fallas
32	Sincronización de reloj
33	política de control de acceso

34	gestión de acceso de usuarios
35	definición de responsabilidades de usuarios
36	política de seguridad de la información
37	gestión de activos
38	clasificación de la información
39	capacitaciones en seguridad de la información

Se eligieron controles de los dos grupos existentes. Por un lado los técnicos, tales como: copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o corta fuegos, y por otro los organizativos que son medidas organizativas tales como: la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios o los planes de capacitaciones.

La combinación de las medidas técnicas y organizativas consigue un nivel de seguridad razonable para el escenario de riesgo que se trataba de mitigar.

Una vez seleccionados los controles pertinentes, debe definirse los procedimientos para su implantación. Los controles de tipo organizativo pueden ser implantados mediante procedimientos, se deberá analizar la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Puede ser posible que varios controles puedan agruparse en un único procedimiento. El objetivo del procedimiento es contar con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

5.2 Riesgo Efectivo

Para el cálculo del riesgo se empleo la tabla que se encuentra definida en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** Anexo E.

Una vez decididas las acciones a tomar, se realizó un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando los controles y medidas que se decidieron implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo.

Se paso a calcular el riesgo efectivo, que es el riesgo al que quedan expuestos los activos luego de aplicarse los controles. Para este análisis se emplea la hoja de análisis indicando el porcentaje de disminución del impacto o frecuencia en la que se empleo como referencia la escala de porcentajes definida en el documento **Met.1-1.0.1 Metodología de Análisis de Riesgos**.

Si se observa la amenaza: [E.1] ERRORES DE LOS USUARIOS para el activo Registro académico estudiantil, y los controles seleccionados para contrarrestar

esta amenaza deberán tener una reducción del impacto o frecuencia en un 90%; este valor se coloca al lado derecho del riesgo intrínseco para el activo Registro académico estudiantil. Conociendo el índice de reducción del impacto o frecuencia (variable impactoReduccion) se puede calcular el Riesgo efectivo para la amenaza de ese activo.

Teniendo cada uno de los valores de las variables que participan del cálculo del riesgo efectivo y de acuerdo al documento **Met.1-1.0.1 Metodología de Análisis de Riesgos** su fórmula es:

PorcentajeReduccionDelImpacto = (1 – impactoReduccion) * Impacto
Riesgo = valorActivo * vulnerabilidad * **PorcentajeReduccionDelImpacto**

Se tiene para el activo Registro académico Estudiantil un riesgo efectivo de:

PorcentajeReduccionDelImpacto = (1- 0,9) * 0,166666667
PorcentajeReduccionDelImpacto = 0,016666667

Riesgo = 30000*0,133333333 * 0,016666667
Riesgo = 66,66

Como se muestra en el recuadro de color rosado de la Tabla 10. Así se completo para cada amenaza el cálculo del riesgo efectivo para el activo Registro académico Estudiantil y los demás activos del Tipo de activo Servicios.

Luego, para cada activo se sumo cada riesgo efectivo obtenido en cada una de las amenazas, resultando el *riesgo efectivo diario por activo*, como se muestra al final de la Tabla 10. Para el activo Registro académico Estudiantil el *riesgo efectivo diario por activo* fue de2.816,67 €. Conociendo el riesgo efectivo diario para cada activo, en el Tipo de activo de Servicio, se totalizaron para conocer el *Total riesgo efectivo diario* para ese grupo de activos. Para el Tipo de activo Servicios el Total riesgo efectivo diario fue de:17.456,67 €.

Formulas:

*Riesgo efectivo diario para activo = RiesgoEfectivoDelActivoParaAmenaza1 + RiesgoEfectivoDelActivoParaAmenaza2 + **…** + RiesgoEfectivoDelActivoParaAmenaza**N***

*Total riesgo efectivo diario = RiesgoEfectivoDiarioParaActivo1 + RiesgoEfectivoDiarioParaActivo2 + … +RiesgoEfectivoDiarioParaActivo**N***

De ese mismo modo se calculo el riesgo efectivo para cada activo en cada grupo.

5.3 Riesgo residual

Este riesgo controlado por los salvaguardas, empleo el mismo procedimiento de los cálculos de riesgos anteriores. Para el activo Registro académico estudiantil se calculo el riesgo residual por cada amenaza a la que estaba expuesto como se muestra en el recuadro de color verde de la Tabla 10. La fórmula que se empleo fue:

R. Residual = RiesgoIntrinseco – RiesgoEfectivo

Siguiendo con el ejemplo de la Tabla y del activo Registro academico estudiantil, se tiene que para la amenaza [E.1] ERRORES DE LOS USUARIOS, el riesgo residual es:

R. Residual = 666,66 – 66,66
R. Residual = 600

Luego, para cada activo se sumo cada riesgo residual obtenido en cada una de las amenazas, resultando el *riesgo residual diario por activo*, como se muestra al final de la Tabla 10. Para el activo Registro académico Estudiantil el *riesgo residual diario por activo* fue de 13.050 €. Conociendo el riesgo residual diario para cada activo, en el Tipo de activo de Servicio, se totalizaron para conocer el *Total riesgo residual diario* para ese grupo de activos. Para el Tipo de activo Servicios el Total riesgo residual diario fue de:69.810 €.

A continuación se realiza un análisis por tipo de activo de los Riesgos Intrínseco, Efectivo y Residual del Área de Admisión, Registro y Control Académico.

En los **activos de Locación** el Riesgo Intrínseco diario es de 7.486,11 €; se destaca el edificio del Bloque de Admisión, con un Riesgo Intrínseco de 4.277,78 €. Ningún activo sobrepasó el nivel de riesgo aceptable (que es de 7.000 €) se observa en la Figura9 que los controles implementados para los activos de Locación controlan un gran porcentaje del riesgo, de acuerdo a los niveles que se muestran de Riesgo Efectivo y Residual.

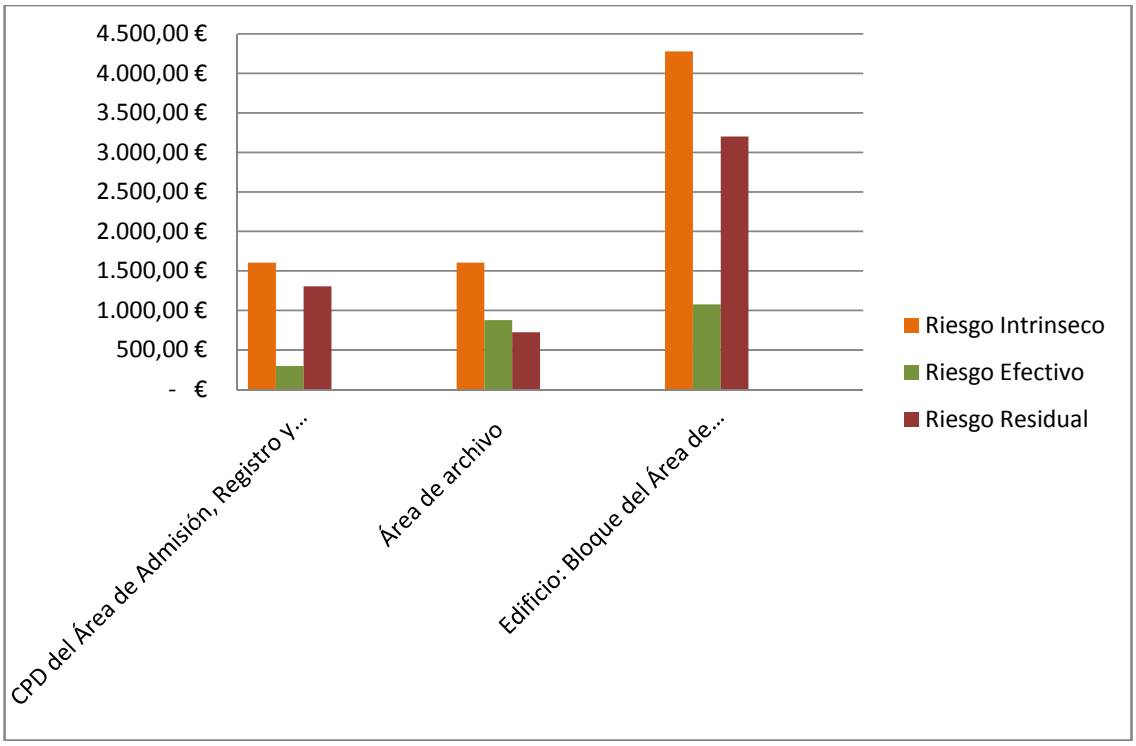

Figura 9. Activos del tipo locación

En los **activos de Hardware** el Riesgo Intrínseco diario es de35.833,33 €; se destacan los activos:
Servidor de Desarrollo y prueba, El Servidor web y los Routers con un Riesgo Intrínseco de7.166,67 € cada uno, sobrepasando el nivel de riesgo aceptable.

También se observa en la Figura 10que los controles implementados para los activos de Hardware reducen el riesgo intrínseco, de acuerdo a los niveles que se muestran de Riesgo Efectivo y Residual

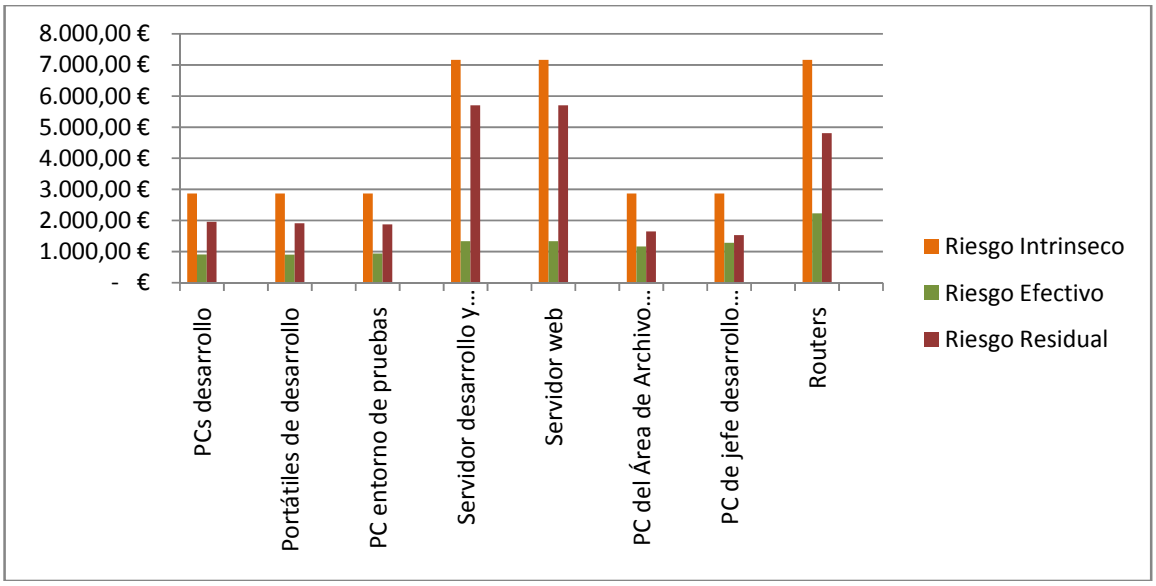

Figura10. Activos del tipo Hardware

En los **activos de Software** el Riesgo Intrínseco diario es de 46.836,11 €; se destacan los activos:
Gestor de BD SQLServer, Software Gestor de contraseñas, Windows 2008 server e IIS 7 con un Riesgo Intrínseco diario de 7.205,56 €, el Sistema Informático SIARC con 18.013,89 €, sobrepasando el nivel de riesgo aceptable.

También se observa en la Figura11 que los controles implementados para los activos de Software han evitado muchos Riesgos, de acuerdo a los niveles que se muestran de Riesgo Residual que sobre pasa al Riesgo Efectivo.

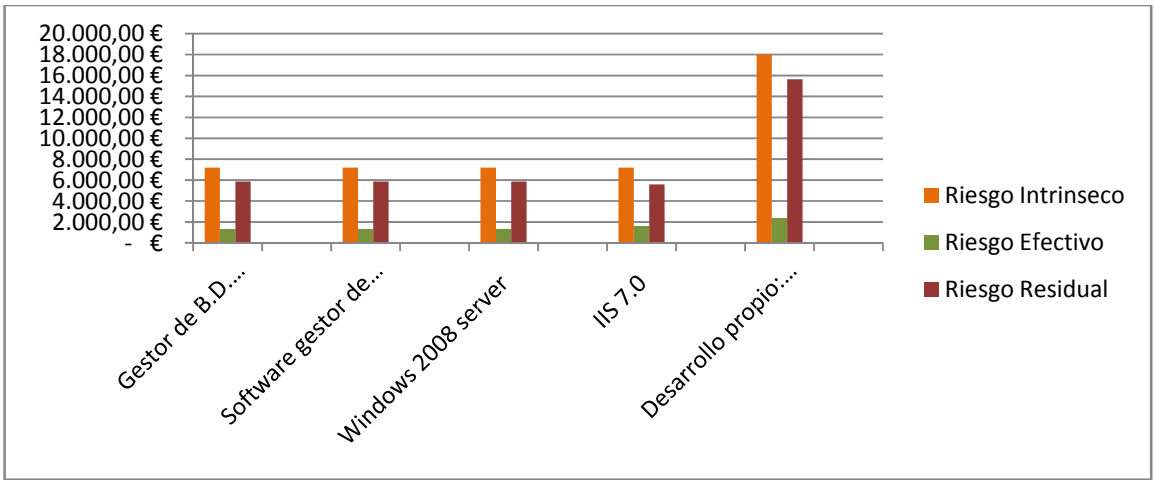

Figura11. Activos del tipo Software

En los **activos de Datos** el Riesgo Intrínseco diario es de 57.533,33 €; se destacan los activos:
Código fuente de aplicación SIARC, B.D de pagos e inscripciones, contraseñas de estudiantes y B.D. de registro académico de estudiantes con un Riesgo Intrínseco diario para cada activo de 11.986,11 €, sobrepasando el nivel de riesgo aceptable.

También se observa en la Figura12 que varios de los controles implementados para los activos de Datos han evitado muchos Riesgos, de acuerdo a los niveles que se muestran de Riesgo Residual que sobre pasa al Riesgo Efectivo.

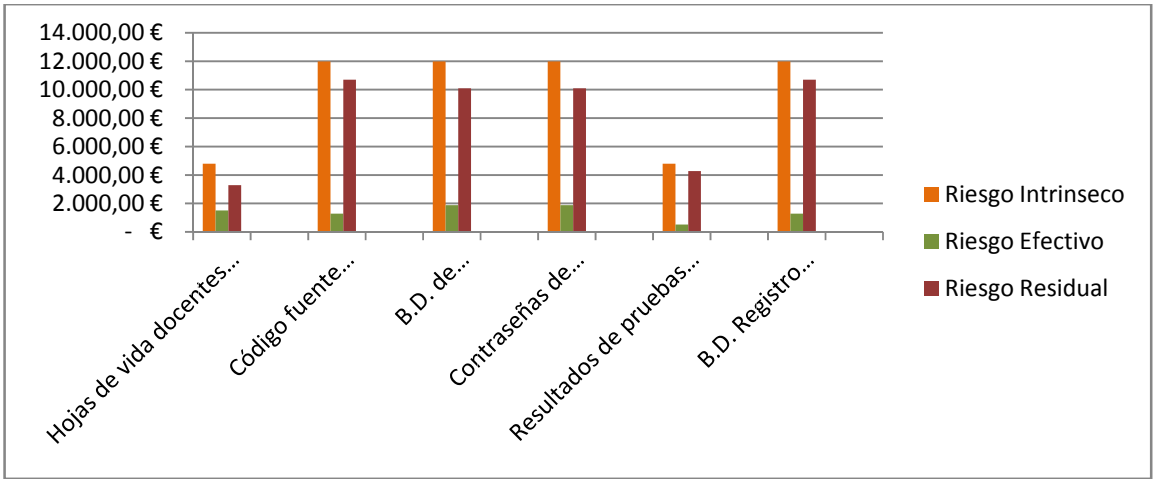

Figura12. Activos del tipo Datos

En los **activos de Soporte** el Riesgo Intrínseco diario es de 42.375,00 €; se destaca el activo: Backups soporte en DVD con un Riesgo Intrínseco diario de 14.125,00 €, sobrepasando el nivel de riesgo aceptable. En la Figura 13 se observa que los controles implementados para los activos de Soporte contrarrestan el riesgo intrínseco, de acuerdo a los niveles que se muestran de Riesgo Efectivo y Riesgo Residual.

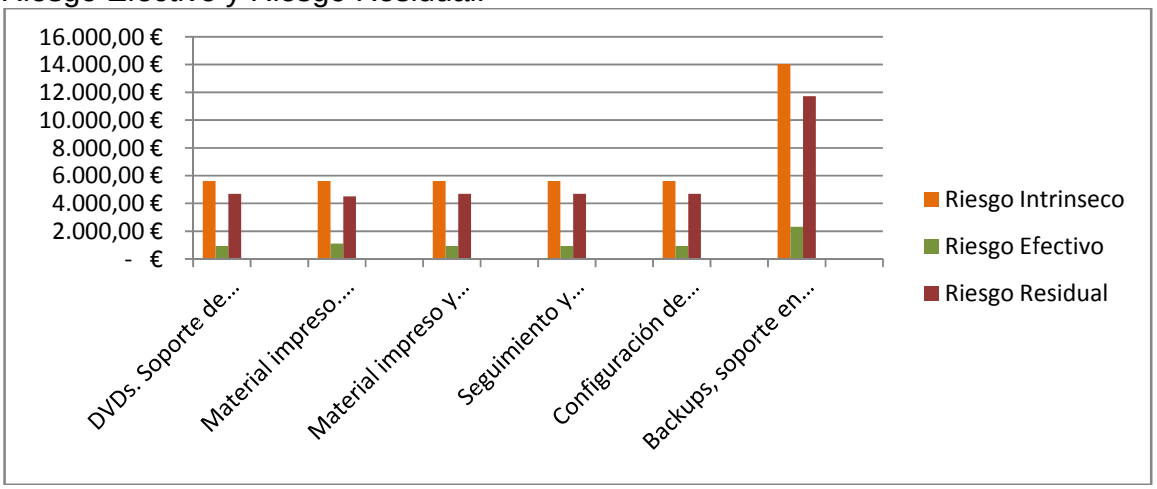

Figura 13. Activos del tipo Soporte

En los **activos de Red** el Riesgo Intrínseco diario es de 38.138,89 €; se destacan los activos: ADSL y Red local con un Riesgo Intrínseco diario de 19.069,44 € respectivamente, sobrepasando el nivel de riesgo aceptable.

En la Figura 14 se observa la influencia de los controles implementados para los activos de red y la relación con los Riesgos Efectivo y Residual.

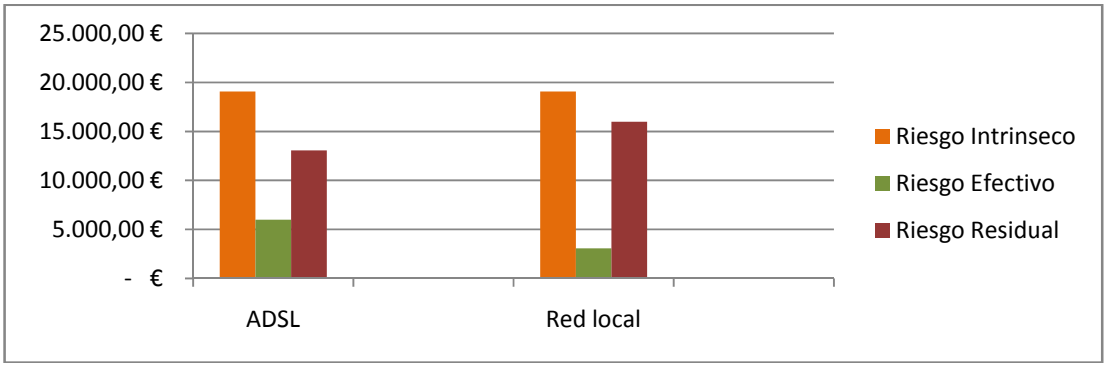

Figura 14. Activos del tipo Red

En los **activos de Servicios** el Riesgo Intrínseco diario es de 87.266,67 €; todos los activos de servicios sobrepasan el nivel de riesgo aceptable: Registro académico, certificados e inscripción en línea tienen un Riesgo Intrínseco diario de 15.866,67 €, mientras que para Registro de Notas por docentes es de 39.666,67 €.

En la Figura15 se observa en especial que los controles implementados para el activo Registro de Notas por docentes reducen altamente el riesgo Intrínseco pero sin embargo su riesgo efectivo llega a 6.966,67 €, se deberán aprobar revisiones posteriores que permitan vigilar el aumento o reducción del riesgo efectivo.

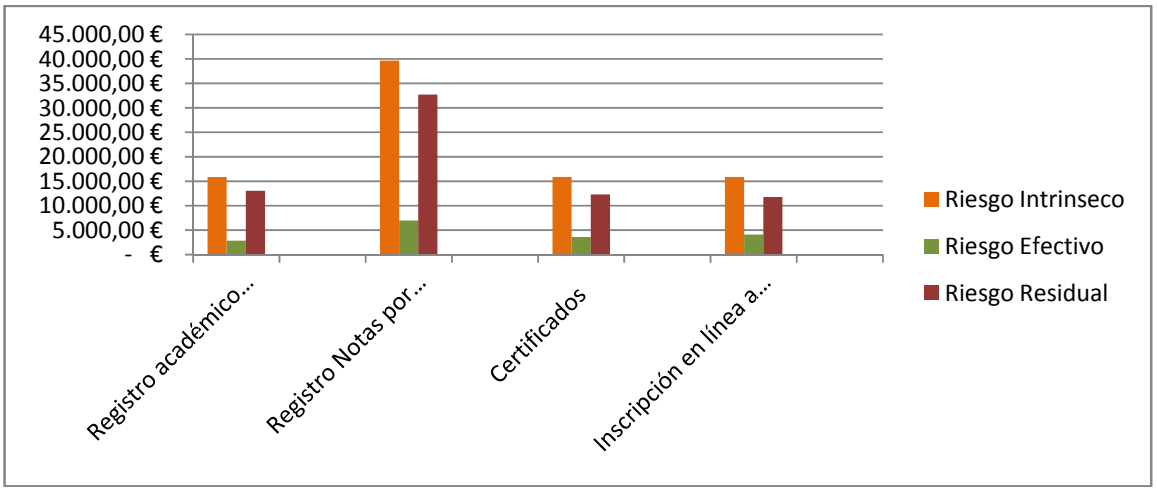

Figura 15. Activos del tipo Servicios

En los **activos Auxiliares** el Riesgo Intrínseco diario es de 19.522,22 €; ningún activo de este grupo sobrepasa el nivel de riesgo aceptable (verFigura16).

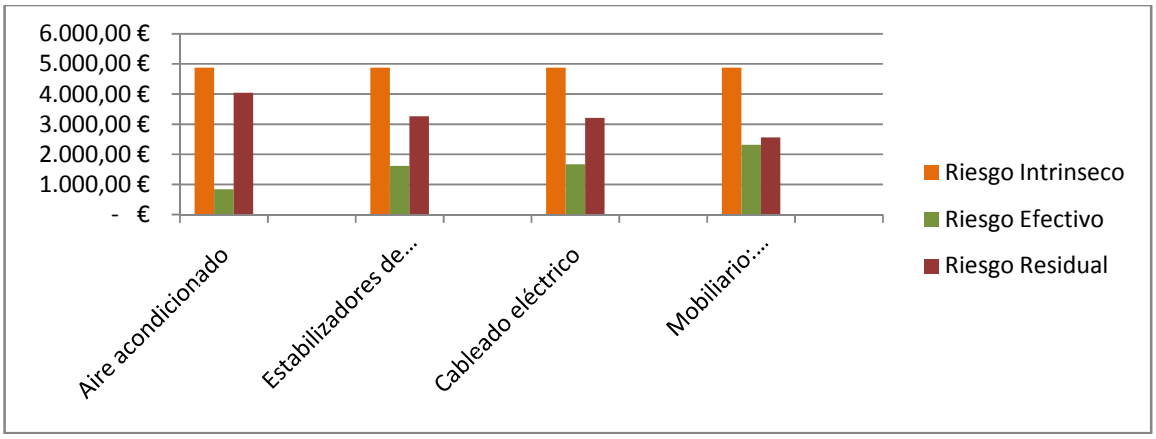

Figura 16. Activos del tipo Equipamiento Auxiliar

En los **activos de Personal** el Riesgo Intrínseco diario es de 8.250,00 €; ningún activo de este grupo sobrepasa el nivel de riesgo aceptable (ver Figura 17)

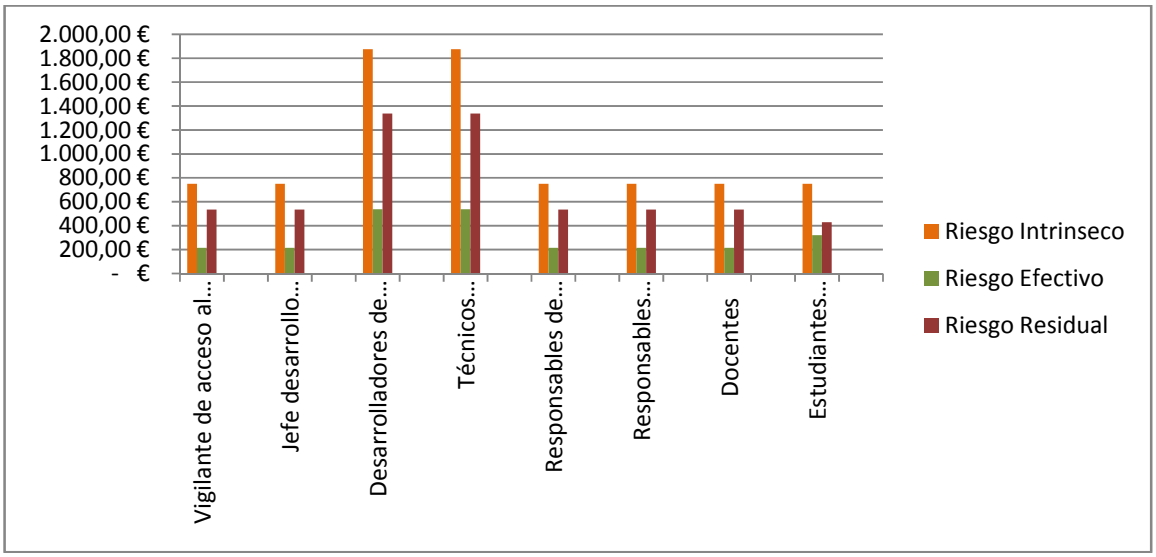

Figura 17. Activos del tipo Personal

6 RESULTADOS

Finalizada esta etapa se obtuvo un listado detallado de los activos relevantes a nivel de seguridad de la información en el Área de Admisión, Registro y Control Académico (ver Tabla 14), completándolo con una valoración cualitativa y cuantitativa, además del nivel de criticidad que representa cada activo para la dependencia desde las dimensiones ACIDA.

Tabla 14. Activos críticos del Área de Admisión, Registro y Control Académico

Grupo	Activo Critico
Locaciones	CPD del Área de Admisión, Registro y Control Académico
	Área de archivo
	Edificio: Bloque del Área de admisión, registro y control académico
Hardware	Servidor desarrollo y prueba
	Servidor web
Software	Desarrollo propio: Sistema informático SIARC
Datos	Código fuente aplicación SIARC
	B.D. de pagos, inscripciones y matricula
	Contraseñas de Estudiantes inscritos, matriculados y docentes
	B.D. Registro Académico de estudiantes
Media o soporte	Backups, soporte en DVDs del servidor web y de Desarrollo
Red	ADSL
	Red local
Servicios	Registro Notas por Docentes
Personal	Desarrolladores de Software SIARC
	Técnicos Informáticos y de Red

Se Realizó el estudio de las amenazas a que están expuestos los activos del Área de Admisión, Registro y Control Académico, la frecuencia con que se pueden presentar y el impacto que puede causar desde las dimensiones ACIDA.

Se evaluó el riesgo al que se estaría exponiendo cada activo de materializarse las amenazas identificadas para cada uno de ellos. Este dato permitirá priorizar el plan de acción para contrarrestar el Riesgo que sobrepaso el nivel aceptado.

Se obtuvieron varios activos con riesgo por encima del aceptado, destacándose: Registro de notas, ADSL, Red local, Sistema Informático SIARC, Registro académico, Certificados e Inscripción en línea (ver Figura 18).

A continuación se muestra una grafica que resumen el estado del Área de Admisión, Registro y Control Académico en control del Riesgo

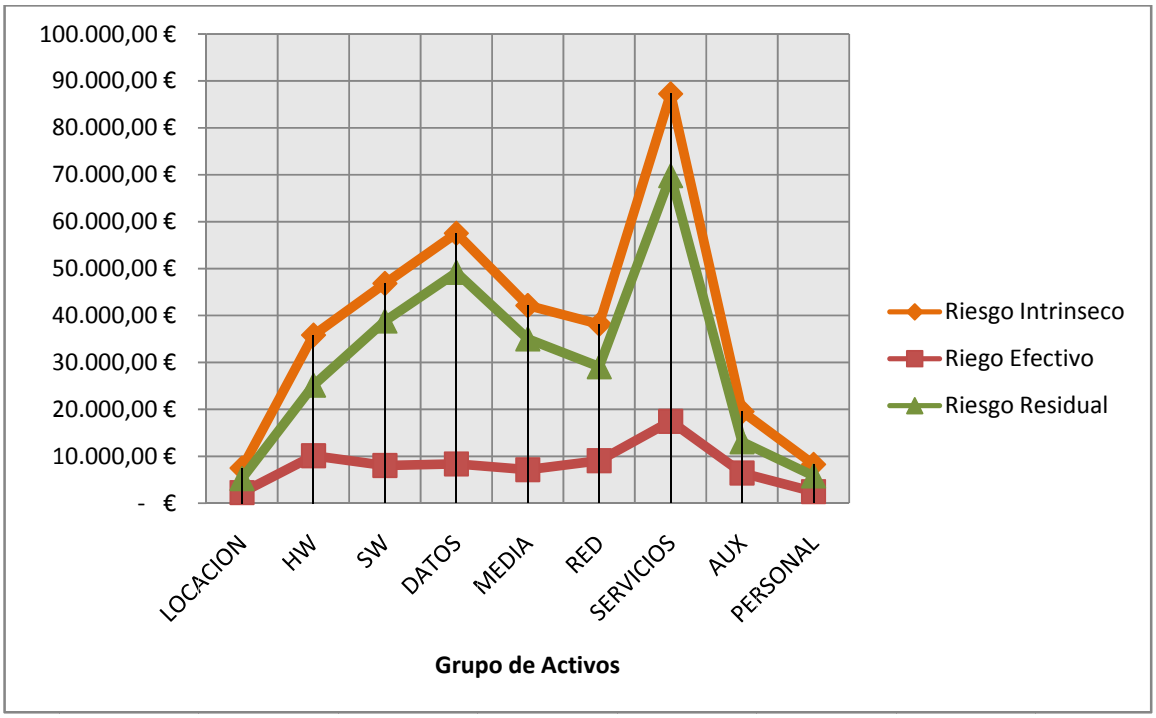

Figura 18. Riesgos Totales

CAPITULO IV. PLAN DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa de la Gestión de la seguridad de la información del Área de Admisión, Registro y Control Académico, se define que salvaguardas emplear, cómo y cuando se implementaran, y el presupuesto a ser utilizado para colocar en práctica los salvaguardas.

El Plan de seguridad de la información, también conocido como Plan Director de la seguridad de la información, agrupa las acciones que se seguirán para contrarrestar el riesgo identificado en proyectos; también, los prioriza con acciones a corto, mediano y largo plazo. El proyecto a corto plazo ubicará las acciones más urgentes dentro de las medidas planeadas; mientras que en el de largo plazo estarán las menos urgentes.

El Plan de Seguridad de la información deberá no solo definir proyectos, sino que estos deben contribuir a alcanzar los objetivos de seguridad definidos. Esto permitirá junto con el presupuesto y la planeación adecuada de acciones, ser aprobados por la Dirección de la dependencia.

1. PROPUESTAS DE PROYECTOS

Se plantearon tres proyectos que mejoraran el estado de la seguridad del Área de Admisión, Registro y Control Académico:

- **Proyecto 1.** Identificado como Proyecto de implementación inmediata, ya que son medidas de aplicación urgente para alcanzar un nivel básico de seguridad en varias dimensiones.
- **Proyecto 2.** Llamado: Proyecto a mediano plazo, integra el mayor número de controles buscando conseguir la seguridad en los sistemas de información.
- **Proyecto 3.** Denominado: Proyecto a largo plazo. Recoge un grupo reducido de controles y de mayor costo.

En cada proyecto se indican los criterios utilizados para seleccionar los controles, se listan los controles seleccionados en dos grupos: Organizativos y Técnicos. Luego se realiza una estimación del impacto que se espera tener con los controles seleccionados, así como del nivel de implementación que se alcanzaría. Se indica además que personas participaran del proyecto, la distribución de las actividades en el tiempo y el costo de implementación

La siguiente tabla resume la escala de tiempo de la implementación de cada uno de los proyectos. Se estima que para la culminación de cada proyecto tome un año; es así que la conclusión de todos ellos llevara tres años y tres meses, desde Mayo del 2014 hasta Agosto del 2017.

Tabla 15. Escala de tiempo de los proyectos

	2014	2015	2016	2017
Proyecto 1. Proyecto de implementación inmediata				
Inicia: Mayo 2014		Termina: Mayo 2015		
Proyecto 2. Proyecto a mediano plazo				
Inicia: Junio 2015		Termina: Junio 2016		
Proyecto 3. Proyecto a largo Plazo				
Inicia: Agosto 2016		Termina: Agosto 2017		
Convenciones				
Desarrollo de actividades de implementación del proyecto				
Puntos de control del proyecto				
Periodo de vacaciones				

A continuación se muestra con más detalles cada una de las propuestas

1.1 Proyecto 1. Proyecto de implementación inmediata

Este proyecto contribuye con el primer objetivo de seguridad definido en la **Capitulo I Titulo 2 Objetivos del plan director**. Busca crear concienciación de la dirección y los empleados en materia seguridad de la información que permita reducir incidentes de seguridad como: la desatención de escritorios, uso de claves y otros. Para ello se implementan Políticas y procedimientos necesarios para ayudar a generar conciencia y compromiso con la seguridad de la información del Área de Admisión, Registro y Control Académico; además de capacitaciones de buenas prácticas de seguridad.

Para seleccionar los controles adecuados a este proyecto se utilizo cuatro criterios, que son:

- Coste de la implementación y el mantenimiento del control
- Controles que ya existen y sólo hace falta modificarlos
- Aplicabilidad de acuerdo con los riesgos detectados
- Que incidan en el mayor numero de activos posibles

Los criterios de selección junto con el objetivo del Plan Director, condicionaron la selección de salvaguardas tanto del tipo organizativo como del Técnico en el corto plazo (primer año). Luego se definieron 44 actividades distribuidas en el tiempo

para la implementación de los controles organizativos y técnicos que fueron seleccionados. También se crearon tres puntos de control (cada 4 meses) que permitirán medir el nivel de cumplimiento de las actividades propuestas de este primer proyecto.

El impacto esperado de las medidas seleccionadas se basó en la evolución de las amenazas que fueron identificadas en el análisis de riesgo con respecto a los controles elegidos. De acuerdo a lo mostrado por el análisis de riesgo existen 20 amenazas que debe contrarrestar el Área de Admisión, Registro y Control Académico, con un riesgo intrínseco de 282.091,67 €. A cada una de estas amenazas se le definió los controles necesarios que podrían mermar el riesgo; luego se comparó con las medidas a implementarse en este proyecto midiendo el porcentaje de implementación que se lograría para cada control. Al final se promedia el porcentaje de implementación de los controles necesarios para mermar la amenaza. Este procedimiento se siguió con cada una de las 20 amenazas

La tabla completa con las amenazas e impactos esperados se muestra en el documento **Proyecto 1. Proyecto de implementación inmediata.** El impacto promedio que se logra es del 58%.

La implementación de las medidas propuestas afecta a varias amenazas reduciendo el riesgo de acuerdo al nivel de impacto esperado para cada amenaza. Lográndose un nivel de Protección de 136.340,51 €, una disminución del riesgo del 48% y la ubicación de 10 amenazas por debajo del nivel aceptado.
El promedio de mejora con respecto al estado anterior de la norma ISO/IEC 27002 es del 32%, solo la dimensión que no mejoraría con la implementación del proyecto es Gestión de continuidad.

Este primer proyecto necesitará una inversión de 20.248,00 € para su desarrollo.

1.2 Proyecto 2. Proyecto a mediano plazo

Este proyecto contribuye con el segundo objetivo de seguridad definido en la **Capitulo I Titulo 2 Objetivos del plan director**. Busca implementar medidas que mejoren la seguridad en el sistema informático SIARC que permita reducir incidentes de seguridad como: el fraude a través de accesos no autorizados y otros tipos de ataques que lleguen afectar la integridad de la información. Para ello se implementan Políticas, procedimientos y controles técnicos necesarios para ayudar a reducir la frecuencia y el impacto de accesos no autorizados; además de capacitaciones de buenas prácticas de seguridad.

Para seleccionar los controles adecuados a este proyecto se utilizo tres criterios, que son:

- Coste de la implementación y el mantenimiento del control
- Controles que ya existen y sólo hace falta modificarlos
- Aplicabilidad de acuerdo con los riesgos detectados

Los criterios de selección junto con el objetivo del Plan Director, condicionaron la selección de salvaguardas tanto del tipo organizativo como del Técnico en el mediano plazo (segundo año). Luego se definieron 50 actividades distribuidas en el tiempo para la implementación de los controles organizativos y técnicos que fueron seleccionados. También se crearon tres puntos de control (cada 4 meses) que permitirán medir el nivel de cumplimiento de las actividades propuestas de este segundo proyecto.

El impacto esperado de las medidas seleccionadas se basó de igual modo en el procedimiento explicado en el proyecto anterior.

La tabla completa con las amenazas e impactos esperados se muestra en el documento **Proyecto 2. Proyecto a mediano plazo.** El impacto promedio que se logra es del 91%.

La implementación de las medidas propuestas afecta a varias amenazas reduciendo el riesgo de acuerdo al nivel de impacto esperado para cada amenaza. Lográndose un nivel de Protección de 57.441,12 €, una disminución del riesgo del 20% y la ubicación de 9 amenazas por debajo del nivel aceptado.

El promedio de mejora con respecto al estado anterior de la norma ISO/IEC 27002 es del 89%, la dimensión de menor promedio de implementación es Gestión de continuidad con el 80%.

Este segundo proyecto necesitará una inversión de 51.960,00 € para su desarrollo.

1.3 Proyecto 3. Proyecto a largo Plazo

Este proyecto contribuye con el tercer objetivo de seguridad definido en la **Capitulo I Titulo 2 Objetivos del plan director**. Reducir la posibilidad de interrupción del Sistema de Información SIARC ante el riesgo de presentarse contingencias como: incendios, caídas de energía, robo de equipos, sabotaje, entre otros. Para ello se implementan Políticas, procedimientos y controles técnicos necesarios para ayudar a reducir la frecuencia y el impacto de interrupciones de origen industrial o natural.

Para seleccionar los controles adecuados a este proyecto se utilizo tres criterios, que son:

- Aplicabilidad de acuerdo con los riesgos detectados

Los criterios de selección junto con el objetivo del Plan Director, condicionaron la selección de salvaguardas tanto del tipo organizativo como del Técnico en el largo plazo (tercer año). Luego se definieron 25 actividades distribuidas en el tiempo para la implementación de los controles organizativos y técnicos que fueron seleccionados. También se crearon tres puntos de control (cada 4 meses) que permitirán medir el nivel de cumplimiento de las actividades propuestas de este tercer proyecto.

El impacto esperado de las medidas seleccionadas se basó de igual modo en el procedimiento explicado en los proyectos anteriores.

La tabla completa con las amenazas e impactos esperados se muestra en el documento **Proyecto 3. Proyecto a largo Plazo.** El impacto promedio que se logra es del 100%.

La implementación de las medidas propuestas logra un nivel de Protección de 1.897,50 €, una disminución del riesgo del 1% y la ubicación de todas las amenazas por debajo del nivel aceptado.

El promedio de mejora con respecto al estado anterior de la norma ISO/IEC 27002 es del 98%. Este tercer proyecto necesitará una inversión de 36.040,00 € para su desarrollo.

2. RESULTADOS

La aplicación del plan de seguridad de la información en el Área de Admisión, Registro y Control Académico requerirá de: tres años, invertir 108.248,00 € y la participación de todos los miembros que laboran en la dependencia para lograr reducir el riesgo, cuantificado en 282.091,67 €, a un 72% y evitar pérdidas de195.679,13 € al controlar las amenazas identificadas.

A continuación se resume las estadísticas de proyectos desarrollados en el plan de seguridad de la información y se indica de forma grafica la evolución de los diferentes dominios de la norma ISO/IEC 27002 Figura 19.

Tabla 16. Estadísticas de los proyectos desarrollados

		IMPACTO ESPERADO PROMEDIO	RIESGO RESIDUAL O NIVEL PROTEGIDO	DISMINUICION DEL RIESGO	INVERSION
ANALISIS DE RIESGO	282.091,67 €				
PROYECTO 1		58%	136.340,51 €	48%	20.248,00 €
PROYECTO 2		91%	57.441,12 €	20%	51.960,00 €
PROYECTO 3		100%	1.897,50 €	1%	36.040,00 €

TOTAL		195.679,13 €	72%	108.248,00 €

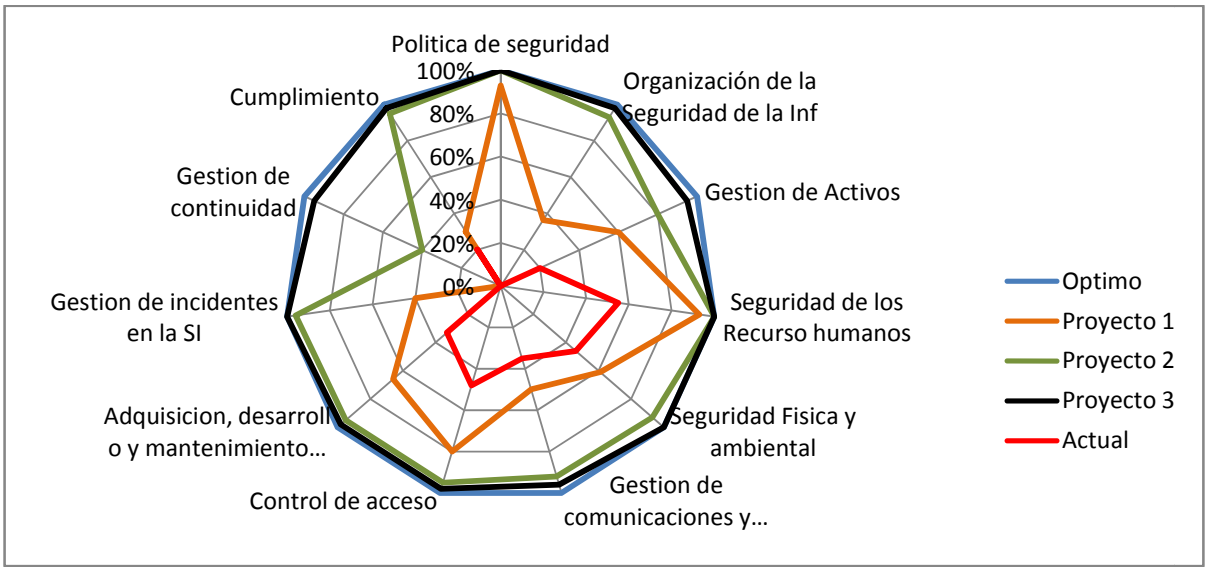

Figura 19. Evolución de los diferentes dominios de la norma ISO/IEC 27002

CAPITULO V. AUDITORIA DE CUMPLIMIENTO

En esta etapa de la Gestión de la seguridad de la información del Área de Admisión, Registro y Control Académico, se realiza una auditoria de cumplimiento con respecto a las normas ISO/IEC 27001 y 27002 con el fin de conocer que tanto ha avanzado la dependencia en cada uno de los aspectos que conforman las normas indicadas.

Una auditoria de cumplimiento es un proceso de revisión del cumplimiento de los requisitos de la norma que se tiene como referencia, en este caso serán la ISO/IEC 27001 y 27002; también se puede entender como el nivel de logro en el cumplimiento de los objetivos de cada aspecto de la norma. En las auditorias de cumplimiento se emplean modelos y escalas con el animo de unificar criterios al momento de evaluar cada aspecto de la norma, en este trabajo se utilizara el modelo de madurez de capacidades o CMM.

El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute). Este modelo consta de cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez. Los niveles son:

0 - Inexistente.
1 - Inicial.
2 - Repetible.
3 - Definido.
4 - Gestionado.
5 - Optimizado.

A continuación se muestra una tabla donde se explica cada uno de los niveles.

Tabla 17. Niveles de efectividad del modelo CMM

Valor CMM	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.

L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos
L6	N/A	No aplica	

1. Evaluación de madurez respecto a los controles definidos en la ISO/IEC 27001

Se tomaron como entrada los registros, documentos, procedimientos y políticas que evidencian el funcionamiento del SGSI como son: Análisis de riesgos, documento de aceptación del riesgo residual por Dirección, Plan de gestión de riesgo, política de seguridad de la información, declaración de aplicabilidad, entre otros. Cada requerimiento de la norma necesito confrontarse con las evidencias que al respecto había recopilado la dependencia, es así que al final se obtiene una valoración de acuerdo al nivel de cumplimiento evidenciado y siguiendo la escala del modelo CMM. A continuación se lista los requerimientos de la norma ISO/IEC 27001 junto con la valoración que obtuvo luego de su evaluación de madurez.

Tabla 18. Valoración del SGSI

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Observaciones
4	**SGSI**		
4.1	**Requerimientos Generales**		
4.1	La organización debe establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI documentado	100%	
4.2	**Establecer y Gestionar el SGSI**		
4.2.1	**Establecer el SGSI**		
4.2.1 (a)	Definir el alcance y los límites del SGSI	100%	
4.2.1 (b)	Definir una política de SGSI	100%	
4.2.1 (c)	Definir el enfoque de la evaluación de Riesgos	100%	
4.2.1 (d)	Identificar los riesgos	100%	
4.2.1 (e)	Analizar y evaluar los riesgos	100%	
4.2.1 (f)	Identificar y evaluar opciones para el tratamiento de riesgos	100%	
4.2.1 (g)	Seleccionar objetivos de control y controles para el tratamientos de riesgos	100%	
4.2.1 (h)	Obtener la aprobación por parte de la dirección de los riesgos residuales propuestos	100%	
4.2.1 (i)	Obtener la autorización de la Dirección para implementar y operar el SGSI	100%	

4.2.1 (j)	Preparar una Declaración de aplicabilidad	100%	
4.2.2	**Implementar el SGSI**		
4.2.2 (a)	Elaborar un plan de tratamiento de riesgos	100%	
4.2.2 (b)	Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados	100%	
4.2.2 (c)	Implementar los controles seleccionados en 4.2.1g para llegar a los objetivos de control	100%	
4.2.2 (d)	Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo estas mediciones van a ser utilizadas para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3c)	100%	
4.2.2 (e)	Implementar programas de formación y concienciación (ver 5.2.2)	95%	Se ha definido un proyecto para el programa de formación y concienciación que aún no ha cubierto todas las temáticas planteadas
4.2.2 (f)	Gestionar la operación del SGSI	100%	
4.2.2 (g)	Gestionar los recursos para el SGSI (ver 5.2)	100%	
4.2.2 (h)	Implementar procedimientos y otros controles capaces de permitir una rápida detección de eventos de seguridad y respuesta a incidentes de seguridad (ver 4.2.3[a])	100%	
4.2.3	**Monitorizar y Revisar el SGSI**		
4.2.3 (a)	Ejecutar procedimientos de monitorización y revisión y otros controles	95%	muchos controles no han sido revisados si cumplen con las políticas definidas
4.2.3 (b)	Llevar a cabo revisiones periódicas de la efectividad del SGSI	100%	
4.2.3 (c)	Medir la efectividad de los controles para verificar que se cumplen los requerimientos de seguridad	100%	
4.2.3 (d)	Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales y los niveles aceptables de riesgos identificados.	100%	
4.2.3 (e)	Llevar a cabo auditorías internas del SGSI de manera regular (ver 6)	100%	El plan de auditorías está definido y se cumple
4.2.3 (f)	Llevar a cabo una revisión por la dirección del SGSI de manera regular (ver 7.1)	100%	
4.2.3 (g)	Actualizar los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión	100%	
4.2.3 (h)	Registrar acciones y eventos que podrían tener impacto en la efectividad o el rendimiento del SGSI (ver 4.3.3)	100%	
4.2.4	**Mantener y mejorar el SGSI**		
4.2.4 (a)	Implementar las mejoras identificadas en el SGSI	100%	
4.2.4 (b)	Llevar a cabo las acciones correctivas y preventivas de acuerdo con 8.2 y 8.3	100%	
4.2.4 (c)	Comunicar las acciones y mejoras a todas las partes interesadas	100%	
4.2.4 (d)	Asegurar que las mejoras consiguen sus objetivos propuestos	100%	
4.3	**Requerimientos de Documentación**		
4.3.1	**Documentación General del SGSI**		
4.3.1 (a)	Documentar los procedimientos y objetivos de la política del SGSI (ver 4.2.1b)	100%	
4.3.1 (b)	Alcance del SGSI (ver 4.2.1A)	100%	
4.3.1 (c)	Procedimientos y controles de apoyo al SGSI	100%	

4.3.1 (d)	Descripción de la metodología de evaluación de Riesgos (ver 4.2.1c)	100%	
4.3.1 (e)	Informe de evaluación de Riesgos (ver desde el 4.2.1c al 4.2.1g)	100%	
4.3.1 (f)	Plan de Tratamiento de Riesgos (ver 4.2.2b)	100%	
4.3.1 (g)	Procedimientos necesitados por la organización para asegurar la planificación efectiva, la operación y el control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c)	100%	
4.3.1 (h)	Registros requeridos por este Estándar Internacional (ver 4.3.3)	100%	
4.3.1 (i)	Declaración de Aplicabilidad	100%	
4.3.2	**Control de Documentos**		
4.3.2	Los Documentos requeridos por el SGSI deberán ser protegidos y controlados. Un procedimiento documentado deberá ser establecido para definir las acciones de la dirección necesitadas para:		
4.3.2 (a)	Aprobar documentos para su adecuación antes de su emisión	100%	
4.3.2 (b)	Revisar y actualizar documentos cuando sea necesario y re-aprobar documentos.	100%	
4.3.2 (c)	Asegurar que los cambios y que los estados de revisión actual de los documentos están identificados	100%	
4.3.2 (d)	Asegurar que las versiones pertinentes de documentos aplicables están disponible y a punto para ser usados	100%	
4.3.2 (e)	Asegurar que los documentos permanecen legibles y fácilmente identificables	50%	el área de archivo lleva un esquema de etiquetado. Los demas lo desconocen
4.3.2 (f)	Asegurar que los documentos están disponibles para aquellos que lo necesiten y son transferidos, almacenados y en última instancia, eliminados de acuerdo a los procedimientos aplicables en base a su clasificación	100%	
4.3.2 (g)	Asegurar que los documentos de procedencia externa están identificados.	100%	
4.3.2 (h)	Asegurar que la distribución de los documentos está controlada.	100%	
4.3.2 (i)	Prevenir el uso no intencionado de documentos obsoletos.	50%	Los documentos están dentro de carpetas del servidor de ficheros. Las versiones obsoletas comparten carpetas con las versiones vigentes. Esto podría inducir a confusión. Está proyectada la implementación de un software de gestión documental que solucionará este tema.
4.3.2 (j)	Aplicar una identificación adecuada a los documentos si éstos son retenidos para cualquier propósito.	100%	
4.3.3	**Control de los Registros**		
4.3.3 (a)	Los registros deben establecerse y mantenerse para proporcionar evidencias de conformidad a los requerimientos y a la eficacia del SGSI	100%	
4.3.3 (b)	Los registros serán protegidos y controlados	100%	
4.3.3 (c)	El SGSI debe tener en cuenta los requisitos legales o reglamentarios y las obligaciones contractuales.	100%	
4.3.3 (d)	Los registros deben permanecer legibles, fácilmente identificables y recuperables.	100%	
4.3.3 (e)	Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de retención y desechado de los registros serán documentados e implementados.	100%	

4.3.3 (f)	Se mantendrán registros de los resultados del proceso, como se indica en el apartado 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.	100%	

Tabla 19. Gestión de la Responsabilidad

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
5	**Gestión de la Responsabilidad**		
5.1	**Compromiso de la dirección**		
5.1	La dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI por:	100%	
5.1 (a)	Establecer una política de SGSI	100%	
5.1 (b)	Asegurar de que se establecen los objetivos y los planes del ISMS	100%	
5.1 (c)	Establecer roles y responsabilidades para la seguridad de la información	100%	
5.1 (d)	Comunicar a la organización la importancia de satisfacer los objetivos de seguridad de la información y conforme a la política de seguridad de la información, sus responsabilidades en virtud de la ley así como la necesidad de la mejora continua	100%	
5.1 (e)	Proporcionar recursos suficientes para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI (ver 5.2.1)	100%	
5.1 (f)	Decidir los criterios de aceptación de riesgos y los niveles de riesgo aceptables	100%	
5.1 (g)	Asegurarse de que las auditorías internas del SGSI se llevan a cabo (ver 6)	100%	
5.1 (h)	La realización de revisiones por la dirección del SGSI (ver 7)	100%	
5.2	**Gestión de los recursos**		
5.2.1	**Provisión de Recursos**		
5.2.1	La organización deberá determinar y proveer los recursos necesarios para:		
5.2.1 (a)	Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI	100%	
5.2.1 (b)	Asegurar que los procedimientos de seguridad de la información son compatibles con los requerimientos del negocio	100%	
5.2.1 (c)	Identificar y abordar los requisitos legales y reglamentarios y las obligaciones contractuales de seguridad	100%	
5.2.1 (d)	Mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implementados	100%	
5.2.1 (e)	Llevar a cabo revisiones cuando sea necesario, y dar una respuesta adecuada a los resultados de estas revisiones	100%	
5.2.1 (f)	Cuando sea necesario, mejorar la eficacia del SGSI	100%	
5.2.2	**Formación, sensibilización y competencia**		
5.2.2	La organización debe asegurarse de que todo el personal al que se le asigna responsabilidades definidas en el SGSI sean competentes para desempeñar las tareas requeridas por:		
5.2.2 (a)	Determinar las competencias necesarias para el personal que realiza trabajo efectivo en el SGSI	100%	

5.2.2 (b)	Proporcionar formación o tomar otras acciones (por ejemplo, el empleo de personal competente) para satisfacer estas necesidades	95%	Se ha definido un proyecto para el programa de formación y concienciación que aún no ha cubierto todas las temáticas planteadas
5.2.2 (c)	Evaluar la efectividad de las acciones llevadas a cabo	100%	
5.2.2 (d)	El mantenimiento de los registros de educación, formación, habilidades, experiencia y calificaciones (véase 4.3.3)	100%	
5.2.2	La organización también debe asegurar que todo el personal pertinente es consciente de la relevancia e importancia de sus actividades de seguridad de la información y de cómo contribuyen al logro de los objetivos del SGSI.	95%	Se ha definido un proyecto para el programa de formación y concienciación que aún no ha cubierto todas las temáticas planteadas

Tabla 20. Auditoría Interna del SGSI

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
6	**Auditoría Interna del SGSI**		
6	La organización debe llevar a cabo auditorías internas del SGSI a intervalos planificados para determinar si los objetivos del control, controles, procesos y procedimientos de su SGSI:		
6 (a)	Cumplir con los requisitos de este Estándar Norma y la legislación o los reglamentos pertinentes	100%	
6 (b)	Cumplir con los requisitos de seguridad de la información identificados	100%	
6 (c)	Que está efectivamente implementado y mantenido	100%	
6 (d)	Desempeñe según lo esperado	100%	
6 (e)	Que sea planificado un programa de auditoría	100%	
6 (f)	La dirección responsable del área que esté siendo auditada debe asegurarse de que se toman acciones sin demora injustificada para eliminar las no conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones llevadas a cabo y el informe de resultados de la verificación (ver 8).	100%	

Tabla 21. Revisión por la dirección del SGSI

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
7	**Revisión por la dirección del SGSI**		
7.1	**General**		
7.1	La dirección revisará SGSI de la organización a intervalos planificados (por lo menos una vez al año) para asegurar su continua idoneidad, adecuación y eficacia	95%	No todos los aspectos han sido revisados
7.2 (a)	**Información para la Revisión**		

7.2	La información para una revisión incluirá:		
7.2 (a)	Resultados de Auditorías y revisiones del SGSI	100%	
7.2 (b)	Los comentarios de las partes interesadas	100%	
7.2 (c)	Técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el rendimiento y la eficacia del SGSI	100%	
7.2 (d)	Estado de las acciones preventivas y correctivas	100%	
7.2 (e)	Las vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgos anterior	100%	
7.2 (f)	Los resultados de las mediciones de la eficacia	100%	
7.2 (g)	Las acciones de seguimiento de revisiones previas de la dirección	95%	No todos los aspectos han sido revisados
7.2 (h)	Todos los cambios que podrían afectar al SGSI	100%	
7.2 (i)	Recomendaciones de mejora	100%	
7.3	**Resultados de la Revisión**		
7,3	El resultado de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con lo siguiente:		
7.3 (a)	Mejora de la eficacia del SGSI	100%	
7.3 (b)	Actualización del plan de tratamiento de riesgos y evaluación de riesgos	100%	
7.3 (c)	Modificación de los procedimientos y controles que la seguridad efecto la información, según sea necesario, para responder a eventos internos o externos que pueden influir en el SGSI	100%	
7.3 (d)	Necesidades de Recursos	100%	
7.3 (e)	Mejoras de cómo la efectividad de los controles está siendo medida	95%	No ha sido llevadas revisiones al respecto

Tabla 22. Mejora del SGSI

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
8	**Mejora del SGSI**		
8.1	**Mejora continua**		
8.1	La organización debe mejorar continuamente la eficacia del SGSI a través del uso de la política de seguridad de la información, los objetivos de seguridad de la información, resultados de las auditorías, el análisis de los eventos monitorizados, acciones correctivas y preventivas y la revisión por la dirección (véase 7).	100%	
8.2 (a)	**Acción Correctiva**		
8.2	La organización deberá tomar acciones para eliminar la causa de no conformidades con los requisitos del SGSI con el fin de prevenir la recurrencia de éstas. El procedimiento documentado de acciones correctivas debe definir requisitos para:		
8.2 (a)	Identificar las no conformidades	100%	
8.2 (b)	Determinar las causas de las no conformidades	100%	
8.2 (c)	Evaluar la necesidad de adoptar medidas para asegurar que las no conformidades no vuelvan a ocurrir	100%	
8.2 (d)	Determinar y aplicar las medidas correctivas necesarias	100%	
8.2 (e)	Registrar los resultados de las acciones tomadas (véase 4.3.3)	100%	

8.2 (f)	Revisar las acciones correctivas tomadas	95%	No todos los aspectos han sido revisados
8.3 (a)	**Acción Preventiva**		
8.3	La organización determinará acciones para eliminar las causas de no conformidades potenciales con los requisitos del SGSI con el fin de prevenir su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas a los efectos de los problemas potenciales. El procedimiento documentado para las acciones preventivas deben definir requisitos para:		
8.3 (a)	Identificar no conformidades potenciales y sus causas	100%	
8.3 (b)	Evaluar la necesidad de actuar para prevenir la ocurrencia de no conformidades	100%	
8.3 (c)	Determinar e implementar las acciones preventivas necesarias	100%	
8.3 (d)	Registrar los resultados de las acciones tomadas (véase 4.3.3)	100%	
8.3 (e)	Revisar las acciones preventivas tomadas	95%	No todos los aspectos han sido revisados
8,3	La organización debe identificar cambios en los riesgos y determinar las necesidades de acciones preventivas centrando la atención en los riesgos que han cambiado significativamente	100%	

A continuación se resumen los datos obtenidos luego de finalizarse la evaluación de madures de la norma ISO/IEC 27001 gestionada por el Área de Admisión, Registro y Control Académico.

Tabla 23. Niveles de madures con el numero de controles de la norma ISO/IEC 27001

Valor CMM	Efectividad	Significado	Número
L0	0%	Inexistente	0
L1	10%	Inicial / Ad-hoc	0
L2	50%	Reproducible, pero intuitivo	2
L3	90%	Proceso definido	0
L4	95%	Gestionado y medible	9
L5	100%	Optimizado	99
L6	N/A	No aplica	0

La siguiente Tabla agrupa los valores CMM en No conformidades Mayores y menores (las menores se pueden llamar oportunidades de mejora), y Controles

Ok. Las no conformidades mayores son los niveles L0 y L1, las no conformidades menores L2 y L3, y los controles Ok los niveles L4 y L5.

Tabla 24. Porcentaje de efectividad obtenida en cada dominio de la ISO/IEC 27001

Dominio	% de Efectividad	# NC Mayores	# NC Menores	Control OK
4.- SGSI	99%	0	2	54
5.- Gestión de la Responsabilidad	99%	0	0	20
6.- Auditoría Interna Del SGSI	100%	0	0	6
7.- Revisión por la Dirección del SGSI	98%	0	0	15
8.- Mejora del SGSI	99%	0	0	13

De acuerdo a lo obtenido en la evaluación de madurez en cada uno de los dominios de la norma ISO/IEC 27001 el promedio de efectividad es del 99%; además, solo se encuentran dos No Conformidades (NC) menores (u oportunidades de mejora) del dominio del SGSI, que son:

> **4.3.2 (e) Asegurar que los documentos permanecen legibles y fácilmente identificables**. Se encontró que el área de archivo lleva un esquema de etiquetado. El resto del Área lo desconocen.
>
> **4.3.2 (i) Prevenir el uso no intencionado de documentos obsoletos**. Los documentos están dentro de carpetas del servidor de ficheros. Las versiones obsoletas comparten carpetas con las versiones vigentes. Esto podría inducir a confusión. Está proyectada la implementación de un software de gestión documental que solucionará este tema.

Nueve de los componentes de la norma ISO 27001 fueron evaluados con un nivel CMM de L4 (95%) ya que no le han realizado revisiones del cumplimiento con respecto a las políticas de seguridad definidas por la dependencia.

A continuación se muestra el diagrama de radar, donde se aprecia cada uno de los aspectos que conforman la norma ISO/IEC 27001 y su nivel de madurez. Es de apreciar el nivel en cada uno de los aspectos de la norma cercanos al optimo (100%); de compararse con el estado inicial de implementación de esta misma norma es claro el gran avance al respecto, ya que en el inicio se contaba con muy pocos aspectos implementados y gestionados.

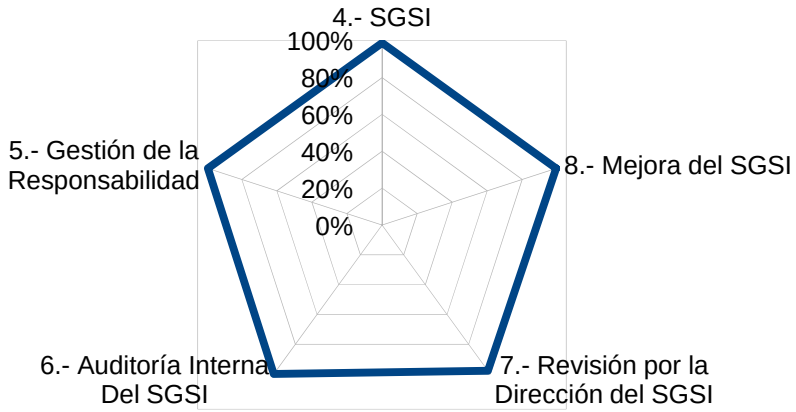

Figura 20. Grafico de radar del nivel de madures de la norma ISO/IEC 27001

El siguiente grafico resalta los niveles de cumplimiento en cada uno de los aspectos de la norma ISO/IEC 27001. Se aprecia la existencia de las dos No conformidades menores en el componente SGSI.

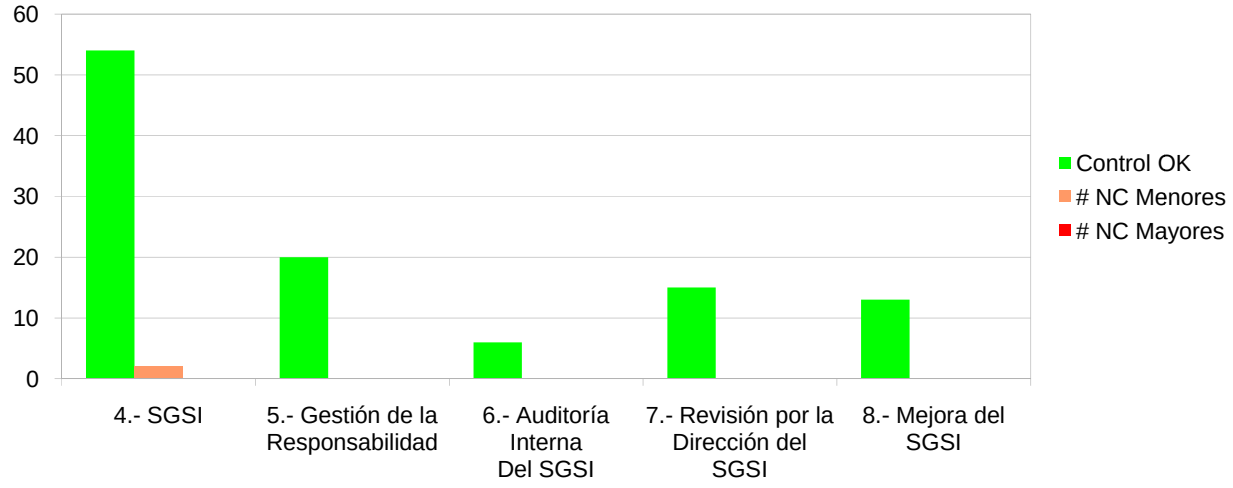

Figura 21. Grafico de barras niveles de cumplimiento de la norma ISO/IEC 27001

2. Evaluación de madurez respecto a los controles definidos en la ISO/IEC 27002

Se tomaron como entrada los registros, documentos, procedimientos y políticas que evidencian el funcionamiento del SGSI como son: Inspección visual de implementación de tecnologías, Logs, Revisiones anteriores, Análisis de riesgos, documento de aceptación del riesgo residual por Dirección, Plan de gestión de riesgo, política de seguridad de la información, declaración de aplicabilidad, entre otros. Cada requerimiento de la norma necesito confrontarse con las evidencias que al respecto había recopilado la dependencia, es así que al final se obtiene una valoración de acuerdo al nivel de cumplimiento evidenciado y siguiendo la escala del modelo CMM. A continuación se lista los dominios, objetivos de control y controles de la norma ISO/IEC 27002 junto con la valoración que obtuvo luego de su evaluación de madurez.

Tabla 25. Valoración de la Norma ISO/IEC 27002

Controles	valoración	observaciones
5.- Política de seguridad	100%	
5.1.-Política de seguridad de la información	100%	
5.1.1.-Documento de Política de Seguridad de la Información	100%	los procesos están bajo constante mejora
5.1.2.-Revisión de la Política de Seguridad de la Información	100%	los procesos están bajo constante mejora
6.- Organización de la seguridad de la información	90%	
6.1.-Organización interna	86%	
6.1.1.-Compromiso de la gerencia con la Seguridad de la Información	95%	Existen evidencias de los procesos liderados por la gerencia.
6.1.2-Coordinación de la Seguridad de la Información	100%	los procesos están bajo constante mejora
6.1.3-Asignación de responsabilidades sobre Seguridad de la Información	100%	los procesos están bajo constante mejora
6.1.4-Proceso de autorización de recursos para el tratamiento de la información	10%	No existe el procedimiento, pero se conoce de su importancia
6.1.5.-Acuerdos de confidencialidad	100%	los procesos están bajo constante mejora
6.1.6.-Contactos con autoridades	90%	No se sigue con indicadores numéricos y estadísticos su evolución
6.1.7.-Contactos con grupos de interés	90%	se mantienen contactos con grupos de interés, pero no se registra la incidencia de sus aportes
6.1.8.-Revisión Independiente de la Seguridad de la Información	100%	los procesos están bajo constante mejora
6.2.-Entidades externas	95%	
6.2.1.-Identificacion de riesgos relacionados con entidades externas	95%	se siguen con indicadores numéricos y estadísticos
6.2.2.-Tratamiento de la seguridad cuando se trabaja con clientes	95%	se siguen con indicadores numéricos y estadísticos
6.2.3.-Tratamiento de la seguridad en contratos con terceras personas	95%	No se han realizado revisiones a los contratos
7.- Gestión de Activos	83%	
7.1.-Responsabilidad de los activos	93%	
7.1.1.-Inventario de activos	95%	se siguen con indicadores numéricos y estadísticos, no se ha hecho revisiones periódicas de inclusión de nuevos activos
7.1.2-Propiedad de activos	95%	se siguen con indicadores numéricos y estadísticos

7.1.3.-Uso aceptable de activos de información	90%	no se sigue con indicadores numéricos y estadísticos
7.2.-Clasificación de la información	73%	
7.2.1.-Lineamientos de clasificación	95%	No se ha realizado revisiones
7.2.2.-Marcado y tratamiento de la información	50%	el área de archivo lleva un esquema de etiquetado
8.- Seguridad de los recursos humanos	96%	
8.1.-Previo a la contratación	97%	
8.1.1.-Roles y responsabilidad	95%	No se ha realizado revisiones
8.1.2.-Selección	100%	los procesos están bajo constante mejora
8.1.3.-Términos y condiciones de la relación laboral	95%	No se ha realizado revisiones
8.2.-Durante la contratación	98%	
8.2.1.-Gestión de responsabilidades	100%	
8.2.2.-Educación y capacitación en seguridad de la información	100%	
8.2.3.-Procesos disciplinarios	95%	No se ha realizado revisiones
8.3.-A la finalización de la contratación	92%	
8.3.1.-Responsabilidades en la finalización	90%	no se siguen con indicadores
8.3.2.-Devolución de activos	90%	no se siguen con indicadores
8.3.3.-Retirada de los derechos de acceso	95%	No se ha realizado revisiones
9.- Seguridad Física y Ambiental	93%	
9.1.-Áreas seguras	92%	
9.1.1.-Perímetro de seguridad física	90%	No se ha hecho seguimiento luego de las implementaciones
9.1.2.-Controles físicos de accesos	90%	No se ha hecho seguimiento luego de las implementaciones
9.1.3.-Seguridad de oficinas, despachos y recursos	90%	No se ha hecho seguimiento luego de las implementaciones
9.1.4.-Protección ante amenazas externas y de entorno	90%	No se ha hecho seguimiento luego de las implementaciones
9.1.5.-El trabajo en las áreas de seguridad	100%	
9.1.6.-Areas de Acceso público, entrega y carga	90%	No se ha hecho seguimiento luego de las implementaciones
9.2.-Seguridad de los equipos	94%	
9.2.1.-Localización y protección del Equipamiento	90%	No se ha hecho seguimiento luego de las implementaciones
9.2.2.-Servicios públicos	90%	No se ha hecho seguimiento luego de las implementaciones
9.2.3.-Seguridad del cableado	90%	No se ha hecho seguimiento luego de las implementaciones
9.2.4.-Mantenimiento de equipos	100%	
9.2.5.-Seguridad de equipos fuera de los locales de la Organización	90%	No se ha hecho seguimiento luego de las implementaciones
9.2.6.-Seguridad en la reutilización o eliminación de equipos	100%	
9.2.7.-Salida de propiedades	100%	
10.- Gestión de las comunicaciones y operaciones	91%	
10.1.-Procedimientos operacionales y responsabilidad	70%	
10.1.1.-Documentación de procedimientos operativos	10%	No existe el procedimiento pero se conoce de su importancia
10.1.2.-Gestión de cambios	90%	No se ha hecho seguimiento luego de las implementaciones

10.1.3.-Segregación de Tareas	90%	No se sigue con indicadores numéricos o estadísticos
10.1.4.-Separación de entornos de desarrollo, pruebas y operación	90%	No se ha hecho seguimiento luego de las implementaciones
10.2.-Gestión en el suministro de servicios (terceras partes)	88%	
10.2.1.-Prestación de servicios	90%	se han definido las condiciones de servicio y niveles de entrega pero no se llevan mediciones
10.2.2.-Monitorización y revisión de servicios de terceras partes	90%	el proceso esta implementado pero no se gestiona
10.2.3.-Gestión de cambios	50%	Existe con muchas deficiencias. Se hace teniendo en cuenta algunos procesos críticos
10.3..-Planificación y aceptación de sistemas	100%	
10.3.1.-Planificación de capacidades	100%	
10.3.2.-Aceptación de Sistemas	100%	
10.4.-Protección contra software malicioso	100%	
10.4.1.-Control contra código malicioso	100%	se realizan capacitaciones y está en constante mejora su procedimiento
10.4.2.-Control contra código móvil	100%	se realizan capacitaciones y está en constante mejora su procedimiento
10.5.-Copias de seguridad	95%	
10.5.1.-Copia de la información	95%	No se ha hecho una revisión de que se cumple con la política
10.6.-Gestión de seguridad de red	98%	
10.6.1.-Controles de redes	100%	
10.6.2.-Seguridad en servicios de red	95%	No se ha hecho una revisión de que se cumple con la política
10.7.-Seguridad y gestión de los soportes	96%	
10.7.1.-Gestión de soportes removibles	95%	No se ha hecho una revisión de que se cumple con la política
10.7.2.-Eliminación de soportes	95%	No se ha hecho una revisión de que se cumple con la política
10.7.3.-Procedimientos de utilización de la información	100%	se realizan capacitaciones y se verifica a intervalos el nivel de cumplimiento
10.7.4.-Seguridad de la documentación de sistemas	95%	Se realizan capacitaciones pero no se ha hecho una revisión de su cumplimiento
10.8.-Intercambio de información	84%	
10.8.1.- Procedimientos y Políticas de información y software	95%	Se realizan capacitaciones pero no se ha hecho una revisión de su cumplimiento
10.8.2.-Acuerdos para intercambio	95%	No se ha hecho una revisión de estos acuerdos
10.8.3.-Seguridad de soportes en tránsito	95%	No existe un análisis de los procesos llevados
10.8.4.-Seguridad de la mensajería electrónica	50%	No se han realizado capacitaciones al respecto para su manejo adecuado
10.8.5.-Sistemas de información de negocio	90%	No se ha realizado un seguimiento a la comunicación con los bancos
10.9.-Servicios de comercio electrónico	-1%	
10.9.1.- Comercio electrónico	-1%	no aplica
10.9.2.-Transacciones en línea	-1%	no aplica
10.9.3.-Informacion disponible públicamente	-1%	no aplica
10.10.-Monitorización	90%	
10.10.1.-Auditoría de logs	100%	
10.10.2.-Revisión de uso de sistemas	95%	No se revisan regularmente
10.10.3.-Protección de logs	95%	No se ha llevado un análisis de su eficacia

10.10.4.-Logs de administradores y operadores	100%	
10.10.5.-Logs de fallo del sistema	100%	
10.10.6.-Sincronización de relojes	50%	No todas las áreasestán sincronizadas
11.- Control de acceso	84%	
11.1.-Requerimientos comercial para el control de acceso	90%	
11.1.1.-Política de control de accesos	90%	no se ha realizado revisiones
11.2.-Gestión de acceso de los usuarios	100%	
11.2.1.-Inscripcion de usuario	100%	
11.2.2.-Gestión de privilegios	100%	
11.2.3.-Gestión de contraseñas de usuario	100%	
11.2.4.-Revisión de los derechos de acceso de los usuarios	100%	
11.3.-Responsabilidades de los usuarios	98%	
11.3.1.-Uso de contraseñas	100%	
11.3.2.-Equipamiento informático de usuario desatendido	100%	
11.3.3.-Política de pantallas y mesas limpias	95%	No se ha realizado revisiones
11.4.-Control de acceso de red	94%	
11.4.1.-Política de uso de los servicios de red	90%	
11.4.2.-Autenticación para conexiones externas	90%	no se han realizado pruebas posteriores a su implementación
11.4.3.-Identificación de equipos en la red	90%	no se han realizado pruebas posteriores a su implementación
11.4.4.-Protección a puertos de diagnóstico remoto y configuración	100%	
11.4.5.-Segregación en las redes	100%	
11.4.6.-Control de conexión a las redes	90%	no se han realizado pruebas de capacidad posteriores a su implementación
11.4.7.-Control de enrutamiento en la red	100%	
11.5.-Control de acceso al sistema operativo	98%	
11.5.1.-Procedimientos de registros en la terminal	95%	No se ha definido un periodo de revisión
11.5.2.-Identificación y autenticación de los usuarios	100%	
11.5.3.-Sistema de gestión de contraseñas	100%	
11.5.4.-Utilización de utilidades del sistema	90%	No se ha realizado un análisis de cumplimiento de todos los equipos
11.5.5.-Timeout de sesiones	100%	
11.5.6.-Limitación del tiempo de conexión	100%	
11.6.-Control de acceso a información y aplicaciones	100%	
11.6.1.-Restricción de acceso a la información	100%	
11.6.2.-Aislamiento de sistemas sensibles	100%	
11.7.-Portátiles y teletrabajo	10%	
11.7.1.-Informática móvil y comunicaciones	10%	No existe el procedimiento pero se conoce de su importancia
11.7.2.-Teletrabajo	10%	No existe el procedimiento pero se conoce de su importancia
12.-Adquisición, desarrollo y mantenimiento de los sistemas de información	99%	
12.1.-Requisitos de seguridad de los sistemas	100%	

12.1.1..Análisis y especificación de los requerimientos de seguridad	100%	
12.2.-Procesos correctos en aplicaciones	100%	
12.2.1.-Validación de los datos de entrada	100%	
12.2.2.-Control del proceso interno	100%	
12.2.3.-Integridad de mensajes	100%	
12.2.4.-Validación de los datos de salida	100%	
12.3.-Controles criptográficos	98%	
12.3.1.-Política de uso de los controles criptográficos	95%	No se ha hecho una revisión de que se cumple con la política
12.3.2.-Gestión de claves	100%	
12.4.-Seguridad de los archivos de sistema	100%	
12.4.1.-Control del software en explotación	100%	
12.4.2.-Protección de los datos de prueba del sistema	100%	
12.4.3.-Control de acceso a la librería de programas fuente	100%	
12.5.-Seguridad en los procesos de desarrollo y soporte	99%	
12.5.1.-Procedimientos de cambios operacionales	100%	
12.5.2.-Revisión técnica de aplicaciones tras cambios del sistema operativo	100%	
12.5.3.-Restricciones de cambios a los paquetes de software	100%	
12.5.4.-Fugas de información	95%	No se ha hecho una revisión de que se cumple con la política
12.5.5.-Desarrollo externalizado	-1%	
12.6.-Gestión de vulnerabilidades técnicas	100%	
12.6.1.-Control de vulnerabilidades técnicas	100%	
13.- Gestión de incidentes en la seguridad de la información	98%	
13.1.-Notificación de incidentes y amenazas	100%	
13.1.1.-Notificación de eventos de seguridad	100%	
13.1.2.-Notificación de debilidades	100%	
13.2.-Gestión de incidentes y mejora	95%	
13.2.1.-Responsabilidad y procedimientos	95%	No se ha hecho una revisión de que se cumple con la política
13.2.2.-Aprendiendo de los incidentes	100%	
13.2.3.-Recolección de evidencias	90%	No se llevan estadísticas ni medidas de los procedimientos realizados
14.- Gestión de la continuidad comercial	60%	
14.1.-Gestión de la continuidad de negocio	60%	
14.1.1.-Inclusión de seguridad en el proceso de gestión de la continuidad del negocio	90%	No se llevan estadísticas ni medidas de los procedimientos realizados
14.1.2.-Continuidad del negocio y análisis de riesgos	100%	
14.1.3.-Redacción e implantación de planes de continuidad incluida la seguridad de la información	10%	No se han implementado los planes de continuidad
14.1.4.-Marco de planificación de la continuidad del negocio	90%	Todos los participantes conocen del marco de referencia
14.1.5.-Prueba, mantenimiento y reevaluación de los planes de continuidad	10%	No se ha realizado aunque se conoce de su importancia
15.- Cumplimiento	97%	

15.1.-Cumplimiento con los requisitos legales	98%	
15.1.1.-Identificación de la legislación aplicable	100%	
15.1.2.-Derechos de propiedad intelectual	100%	
15.1.3.-Salvaguarda de los registros de la organización	95%	No se ha hecho una revisión de que se cumple con la política
15.1.4.-Protección de datos de carácter personal y de la intimidad de las personas	95%	No se ha hecho una revisión de que se cumple con la política
15.1.5.-Evitar el mal uso de los recursos de tratamiento de información	100%	
15.1.6.-Reglamentación de los controles de cifrado	95%	No se ha hecho una revisión de que se cumple con la política
15.2.-Cumplimiento con las políticas y normativas	98%	
15.2.1.-Cumplimiento con las políticas y normativas	95%	No se ha hecho una revisión de que se cumple con la política
15.2.2.-Comprobación de la conformidad técnica	100%	
15.3.-Consideraciones de auditoria de sistemas de información	95%	
15.3.1.-Controles de Auditoría de sistemas de información	95%	No se ha hecho una revisión de que se cumple con la política
15.3.2.-Protección de las herramientas de auditoría de sistemas de Información	95%	No se ha hecho una revisión de que se cumple con la política

A continuación se resumen los datos obtenidos luego de finalizarse la evaluación de madures de la norma ISO/IEC 27002 gestionada por el Área de Admisión, Registro y Control Académico.

.

Tabla 26. Niveles de madures con el numero de controles de la norma ISO/IEC 27002

Valor	Efectividad	Significado	Número
L0	0%	Inexistente	0
L1	10%	Inicial / Ad-hoc	6
L2	50%	Reproducible, pero intuitivo	4
L3	90%	Proceso definido	29
L4	95%	Gestionado y medible	32
L5	100%	Optimizado	59
L6	N/A	No aplica	4

El siguiente grafico muestra las proporciones en que están cada uno de los niveles en la escala de madurez CMM. El nivel optimizado de madurez alcanza el 44% de los controles, en cambio no hay controles en el nivel inexistente y tan solo un 4% en el inicial. Si se agrupa los niveles en: No conformidades Mayores (Inexistente e inicial), No conformidades Menores (Reproducible y Proceso definido) y Control Bueno (Gestionado y Optimizado) se obtendrían un: 4%, 25% y 68% respectivamente.

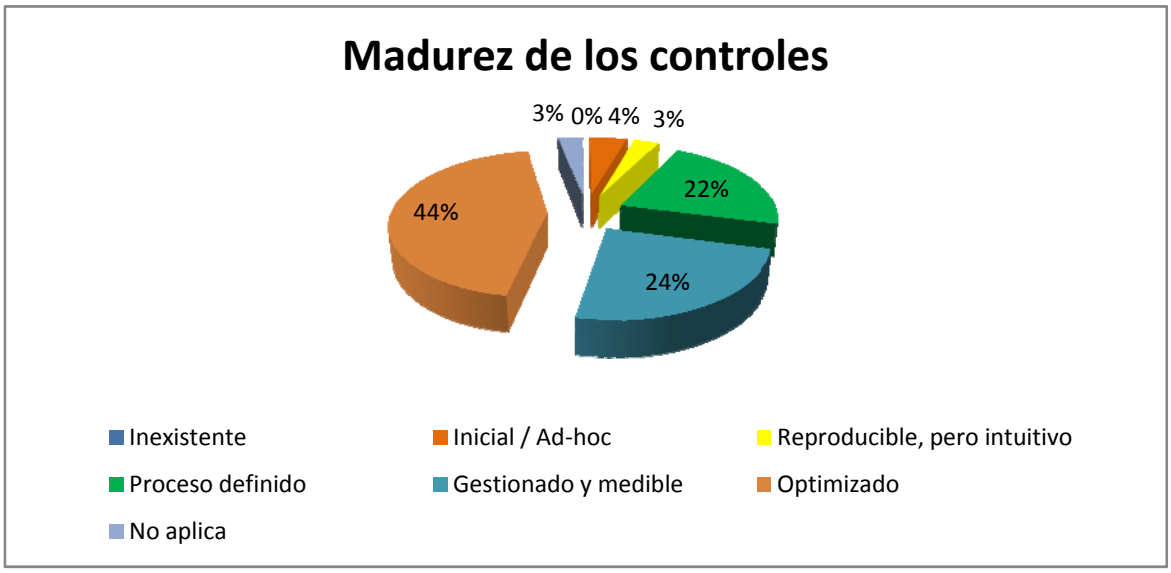

Figura 22. Madurez de los controles ISO/IEC 27002

De acuerdo a lo obtenido en la evaluación de madurez en cada uno de los dominios de la norma ISO/IEC 27002 el promedio de efectividad es del 90%; además, se encuentran seis No Conformidades (NC) Mayores y 33 Menores. Entre las No Conformidades Mayores, que sería el 4% de los controles que se sitúan en ese nivel, están:

6.1.4-Proceso de autorización de recursos para el tratamiento de la información.
10.1.1.-Documentación de procedimientos operativos
11.7.1.-Informática móvil y comunicaciones
11.7.2.-Teletrabajo
14.1.3.-Redacción e implantación de planes de continuidad incluida la seguridad de la información
14.1.5.-Prueba, mantenimiento y reevaluación de los planes de continuidad
En cada uno de estos controles No existe evidencia de la puesta en marcha del procedimiento, pero se conoce de su importancia

En las No conformidades Menores, que es el 25% de los controles que se sitúan en ese nivel, se debe destacar: la falta de evidencias de llevarse mediciones que

verifiquen el cumplimiento con respecto a la política de seguridad del Área de Admisión, Registro y Control Académico.

Se puede distinguir en la siguiente tabla el dominio al que pertenecen las No conformidades Mayores y menores, además de los controles Ok y los que no aplican. El dominio con mayor efectividad es Política de seguridad, el de menos efectividad es Gestión de la continuidad comercial.

Tabla 27. Porcentaje de efectividad obtenida en cada dominio de la ISO/IEC 27002

Dominio	% de Efectividad	# NC Mayores	# NC Menores	Control OK	N/A
5.- Política de seguridad	100%	0	0	2	0
6.- Organización de la SI	90%	1	2	8	0
7.- Gestión de Activos	83%	0	2	3	0
8.- Seguridad de los recursos humanos	96%	0	2	7	0
9.- Seguridad Física y Ambiental	93%	0	9	4	0
10.- Gestión de las comunicaciones y operaciones	91%	1	9	19	3
11.- Control de acceso	84%	2	6	17	0
12.-Adquisición, desarrollo y mantenimiento de SI	99%	0	0	16	1
13.- Gestión de incidentes en la SI	98%	0	1	4	0
14.- Gestión de la continuidad comercial	60%	2	2	1	0
15.- Cumplimiento	97%	0	0	10	0
Total		6	33	91	4
Total controles		134			

A continuación se muestra el diagrama de radar, donde se aprecia cada uno de los aspectos que conforman la norma ISO/IEC 27002 y su nivel de madurez. Es de apreciar el nivel en varias de las dimensiones de la norma cercanos al 90%; de compararse con el estado inicial de implementación de esta misma norma es claro el gran avance al respecto, ya que en el inicio se contaba con muy pocos aspectos implementados y gestionados.

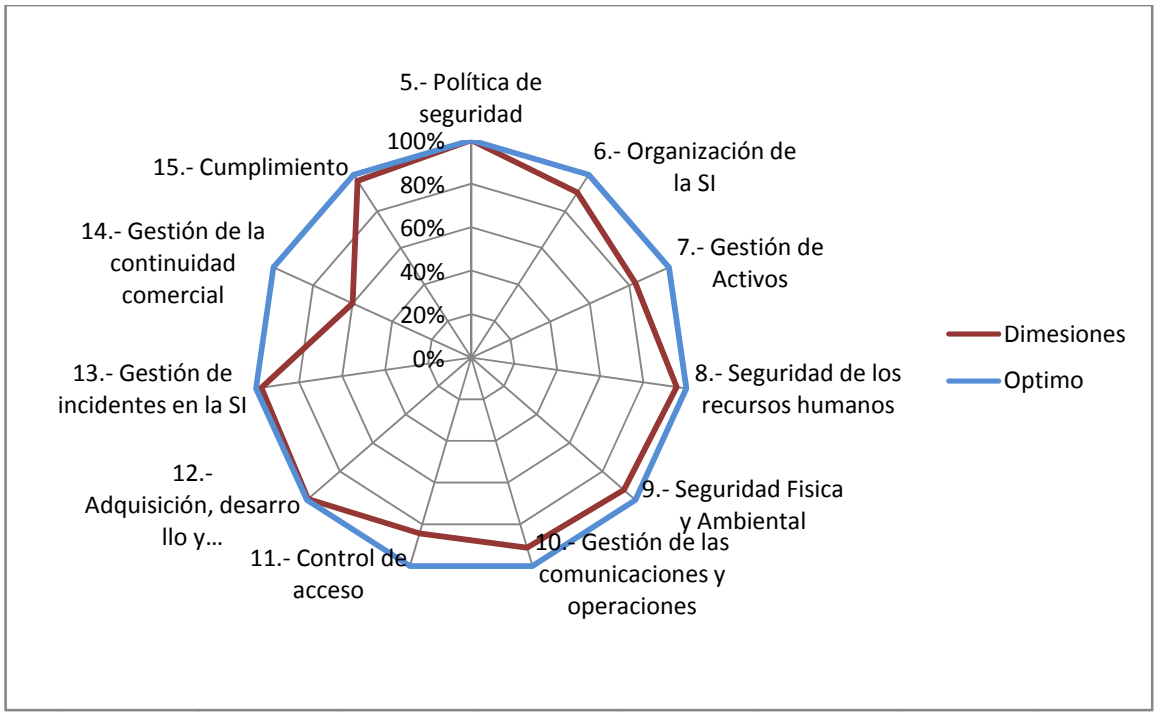

Figura 23. Grafico de Radar del nivel de madurez de la norma ISO/IEC 27002

El siguiente grafico resalta los niveles de cumplimiento en cada uno de los aspectos de la norma ISO/IEC 27002. Se aprecia la existencia de las No conformidades Mayores en las dimensiones: Organización de la SI, Gestión de las comunicaciones y operaciones, Control de acceso y Gestión de la Continuidad.

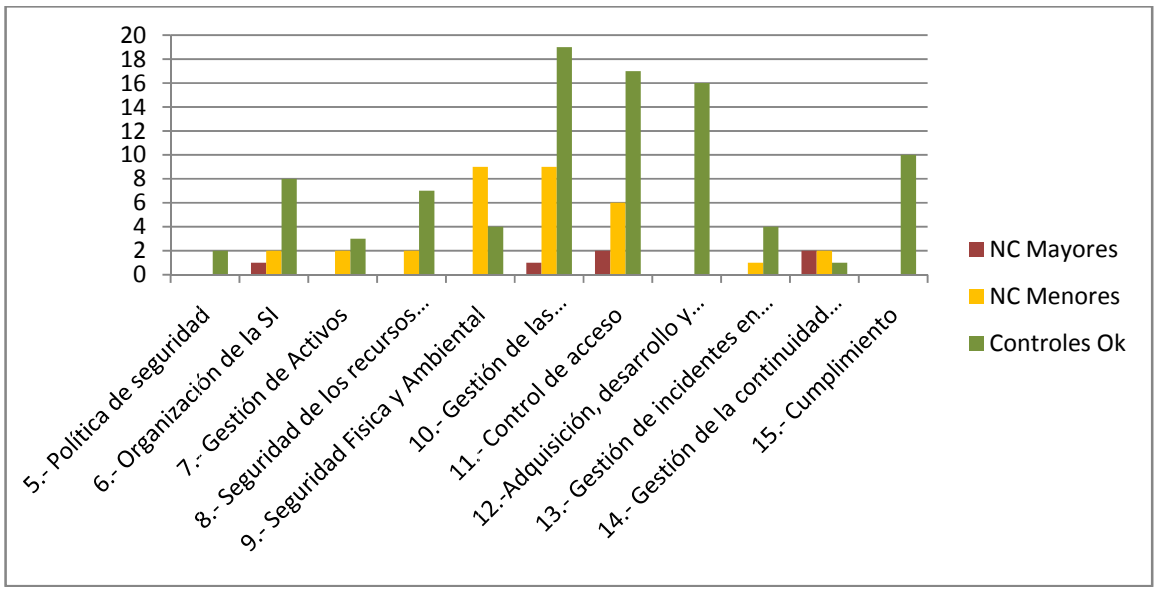

Figura 24. Grafico de barras niveles de cumplimiento de la norma ISO/IEC 27002

. Formato de informe de Auditoría Interna

UNIVERSIDAD UV DE VANCUVER	**Formato de informe de Auditoría Interno**	Versión 1 Pág.1 de 2

1. DATOS DE LA AUDITORIA INTERNA	
Auditoria No.	00010
Norma de Referencia	ISO/IEC 27001
Periodo de Auditoria	Finalización de la implementación de los proyectos
Lugar de la Auditoria	Área de Admisión, Registro y Control Académico de la Universidad de Vancur
Equipo Auditor	

2. ALCANCE DE LA AUDITORIA INTERNA

Auditoria del PDCA de referencia ISO/IEC 27001 del Sistema de Gestión de Seguridad de la Información del Área de Admisión, Registro y Control Académico

2.1. Exclusiones reportadas

Ninguna

3. OBJETIVOS DE LA AUDITORIA INTERNA

- ✓ Determinar el grado en el cual el SGSI del Área de Admisión, Registro y Control Académico de la Universidad de Vancur cumple con los requisitos de la norma ISO/IEC 27001

4. DEFINICIONES

NO CONFORMIDAD: Incumplimiento de un requisito de la norma ISO/IEC 27001 y pone en riesgo la efectividad del SGSI
OBSERVACION: Es una falla aislada o esporádica en el contenido o incumplimiento de los documentos del SGSI, o cualquier incumplimiento en un requisito de la norma de referencia que no llega a afectar de manera critica al SGSI.
OPORTUNIDAD DE MEJORA: Acción recomendada de un requisito de la norma ISO/IEC 27001

5. FORTALEZAS Y DEBILIDADES

FORTALEZAS	DEBILIDADES
El gran avance con respecto al estado inicial de implementación de esta misma norma. La participación esmerada de la dirección de la dependencia por cumplir con la Seguridad de la información	Algunos ítems del PDCA de la norma ISO/IEC 27001 no han sido revisados aun por su responsable su nivel de cumplimiento con las políticas establecidas.

6. RESULTADOS DE LA AUDITORIA INTERNA

6.1. No conformidades

Se hallaron **0** No Conformidades (NC) durante la auditoría interna. Las No Conformidades se resumen en el siguiente cuadro.

Proceso	Descripción	Responsable	Auditor

6.2. Observaciones Y Oportunidades De Mejora

Las Observaciones (OBS) y Oportunidades de Mejora (OM) identificadas durante la auditoría interna se detallan a continuación:

Observaciones:

4.3.2 (e) Asegurar que los documentos permanecen legibles y fácilmente identificables. Se encontró que el área de archivo lleva un esquema de etiquetado. El resto del Área lo desconocen.

4.3.2 (i) Prevenir el uso no intencionado de documentos obsoletos. Los documentos están dentro de carpetas del servidor de ficheros. Las versiones obsoletas comparten carpetas con las versiones vigentes. Esto podría inducir a confusión. Está proyectada la implementación de un software de gestión documental que solucionará este tema.

Oportunidades de Mejora:

Nueve de los componentes de la norma ISO 27001 fueron evaluados con un nivel CMM de L4 (95%) ya que no le han realizado revisiones del

cumplimiento con respecto a las políticas de seguridad definidas por la dependencia, como son:

5.2.2 (b) Proporcionar formación o tomar otras acciones (por ejemplo, el empleo de personal competente) para satisfacer estas necesidades.

Se ha definido un proyecto para el programa de formación y concienciación que aún no ha cubierto todas las temáticas planteadas

Los siguientes ítems no han sido revisados si cumplen con las políticas definidas:

4.2.2 (e) Implementar programas de formación y concienciación.

4.2.3 (a). Ejecutar procedimientos de monitorización y revisión y otros controles.

7.1 La dirección revisará SGSI de la organización a intervalos planificados para asegurar su continua idoneidad, adecuación y eficacia

7.2 (g) Las acciones de seguimiento de revisiones previas de la dirección

7.3 (e) Mejoras de cómo la efectividad de los controles está siendo medida

8.2 (f) Revisar las acciones correctivas tomadas

8.3 (e) Revisar las acciones preventivas tomadas

7. CONCLUSIONES DE LA AUDITORIA INTERNA

El nivel en cada uno de los aspectos de la norma son cercanos al optimo (100%); de compararse con el estado inicial de implementación de esta misma norma es claro el gran avance al respecto, ya que en el inicio se contaba con muy pocos aspectos implementados y gestionados.

No se encontraron No conformidades

Se realizaron dos observaciones: Para asegurar que los documentos permanecen legibles y fácilmente identificables, y de prevenir el uso no intencionado de documentos obsoletos.

En las Oportunidades de mejora: Aun no se han realizado revisiones del cumplimiento con respecto a las políticas de seguridad definidas por la dependencia

CONCLUSIONES

La Gestión de la seguridad de la información es un sistema de procesos que se plantean desde el análisis de riesgos y además se encuentra alineado con la misión de la empresa., que permite luego desarrollar planes de seguridad que reducirán el riesgo a un nivel esperado. Es un sistema que debe permanecer en constante mejora.

REFERENCIAS

CONSUEGRA, José. Plan director de seguridad de la información. [En línea]. 2013. Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/22961/16/jconsuegraTFM0613Presentacion.pdf

DONDERS, Eric. Un Modelo Electrónico y una Metodología de un SGSI para PYMES e-SGSI. [En línea]. 2010. Disponible en:http://es.scribd.com/doc/46528565/Un-Modelo-Electronico-y-una-Metodologia-de%C2%A0un-SGSI-para-PYMES-e-SGSI

ENJUTO, José. Planes de tratamiento de riesgos. En: Seguridad y gestión. [En línea]. 2006. Disponible en:http://secugest.blogspot.com/2006/11/planes-de-tratamiento-de-riesgos.html

INTECO-CERT. Plan de tratamiento del riesgo. [En línea]. 2010.Disponible en: http://es.scribd.com/doc/33892096/47/PLAN-DE-TRATAMIENTO-DEL-RIESGO

KOSUTIC, Dejan. Consejos sobre la evaluación de riesgos para empresas pequeñas. [En línea]. 2010. Disponible en: http://blog.iso27001standard.com/es/2010/04/02/consejos-sobre-la-evaluacion-de-riesgos-para-empresas-pequenas/

MANUAL DE SEGURIDAD de información. [En línea]. V1, 2013. Disponible en: http://contratos.ecopetrol.com.co/Anexos%20de%20Procesos/50033457/ANEXO%2013%20MANUAL%20DE%20SEGURIDAD%20DE%20INFORMACION.pdf

Méndez, C. (2001). Metodología: Diseño y desarrollo del proceso de investigación. Bogotá: McGRAW-HILL

MORAN, Eric. Niveles de aceptación de riesgos versus criterios de aceptación del riesgo. [En línea]. 2012. Disponible en:http://www.ericmorana-sgsi-27001.com/2012/10/niveles-de-riesgo-aceptable-versus.html

Niño, V. M. (2011). Metodologia de la investigacion: Diseño y ejecucion. Bogota: Ediciones de la U.

OBRA SOCIAL de los empleados públicos de Catamarca. Controles criptográficos. [En línea]. 2014. Disponible en:http://www.osep-catamarca.gov.ar/web/index.php?option=com_content&view=article&id=102&Itemid=93

PEREZ, M. T. Soluciones administrativas y técnicas para proteger los recursos computacionales de personal interno- insiders. [En línea]. 2007. Disponible en: http://www.web.facpya.uanl.mx/rev_in/Revistas/4.2/A7.pdf

ROLES Y RESPONSABILIDADES de Seguridad de la Información. [En línea]. V1, 2010. Disponible en: http://www.ecopetrol.com.co/documentos/64203_Anexo_15._ECP-DTI-G-11_Roles_y_Responsabilidades_de_Seguridad_de_la_Informaci%C3%B3n_2010-v-1%5B1%5D.pdf

UNIVERSIDAD TECNOLOGICA Nacional Rectorado. Políticas de seguridad de la información. [En línea]. 2009. Disponible en: http://www.utn.edu.ar/download.aspx?idFile=14736