Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Trabajo de Final de Máster

Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013

Autor: Rodolfo Xavier Bojorque Chasi

Director: Antonio José Segovia Henares

Memoria
Septiembre 2014 – Enero 2015

AGRADECIMIENTOS

Agradezco a Dios por su infinita providencia, compañero fiel e inseparable en las frías madrugadas y fines de semana.

De manera especial agradezco a mi esposa Daysi por todas las horas de matrimonio y hogar que le he robado debido a los estudios, sin ella no hubiera sido posible el nivel de dedicación y preparación.

A mis hijos Matías y Eimi por haber integrado en su rutina la comprensión de que papá está estudiando.

A la Universidad Politécnica Salesiana del Ecuador, a través de su Rector el Padre Javier Herrán y su Vicerrector Docente el Licenciado Fernando Pesantez, a quienes aprecio y admiro como autoridades pero sobre todo como amigos; sin su apoyo no hubiese sido posible estudiar.

A mi tutor del TFM y consultor de la asignatura de SGSI, Antonio José Segovia Henares, por su don de consejo, comprensión, ayuda y motivación. En todo momento sentí su apoyo y aliento hacia el trabajo realizado.

También deseo agradecer a todos los consultores de las diferentes asignaturas, a pesar de la distancia siempre estuve acompañado mediante sus consejos y recomendaciones.

Finalmente agradezco a todas las personas que me brindaron apoyo a lo largo de este camino, a mi Madre Loli, siempre pendiente de cualquier necesidad; a mi cuñado y a la vez amigo Miguel y a los compañeros del Máster que me permitieron tener un crecimiento profesional.

DEDICATORIA

Dedico este trabajo a mi familia, sobre todo a mi esposa Daysi, su apoyo incondicional y total desprendimiento me permitió coordinar el tiempo de trabajo, estudio y sobre todo de familia, gracias a ella mis hijos Matías y Eimi han podido desarrollarse en un ambiente cálido de hogar.

RESUMEN

Actualmente la información es un activo esencial para las diferentes organizaciones, en el Ecuador empresas de toda índole han comenzado a realizar diferentes tipos de inversiones para protegerla, sin embargo, no siempre la inversión va a la par de la seguridad, pues la mayoría de las soluciones suelen ser iniciativa Ad-hoc que no responden a la realidad, políticas, misión y visión de las organizaciones, en este sentido es fundamental comprender a la seguridad de la información como un sistema donde per se la globalidad de la solución es siempre mayor a la suma de las soluciones de sus partes.

Los Sistemas de Gestión de Seguridad de la Información (SGSI), permiten articular normas internacionalmente reconocidas para crear, implementar, operar, monitorear, mantener y mejorar la seguridad de la información con las políticas, misión y visión organizacional.

El presente Trabajo Final de Master consiste en la implementación de un SGSI basado en la norma ISO/IEC 27001:2013 para la UPS, que en los últimos años ha realizado cuantiosas inversiones en seguridad sin obtener beneficios acordes a la inversión.

ABSTRACT

Nowadays information is an essential asset to organizations, in Ecuador, different enterprises have begun to make different inversions for protect their information; however, inversion does not represent security, in the most of cases, the solutions are Ad-hoc initiatives that no response to actuality, policies, mission and vision of organizations, in this sense it is fundamentality understand to information security as a system, where the whole solution is more than the sum of the parts.

The Information Security Management System (ISMS) permits to articulate recognized international standards to create, implement, operate, monitor, maintain, and improve the security information to organizational policies, mission and vision.

The issue for this Final Master Work an ISMS implementation based in ISO/IEC 27001:2013 for the UPS, in the last years the UPS has made considerable inversions in security without benefits according to the inversion.

ÍNDICE

Contenidos:

0 CAPÍTULO 1: SITUACIÓN ACTUAL

0.1 INTRODUCCIÓN AL PROYECTO

La empresa seleccionada es la UPS, Institución de Educación Superior con 20 años de vida institucional, tiene su matriz en la ciudad de Cuenca, con sedes en las ciudades de Quito y Guayaquil, este centro de estudios superiores acoge 22.000 estudiantes, en el cual trabajan más de 1.100 profesores y 300 miembros como personal administrativo[1]. Dentro del sistema de educación superior ecuatoriano la UPS está cataloga como Universidad Cofinanciada, lo cual significa que a parte de sus ingresos particulares recibe fondos públicos, su accionar se encuentra regulado por la Ley Orgánica de Educación Superior (LOES) y su estatuto.

En la actualidad el organismo que regula la educación superior del Ecuador es el CES (Consejo de Educación Superior) quienes a partir de la LOES han definido los reglamentos, políticas y normas del quehacer académico universitario. Todo el trabajo de las universidades ecuatorianas es auditado por el CEAACES (Consejo de Evaluación, Aseguramiento y Acreditación de la Calidad de la Educación Superior).

Los dos entes gubernamentales mantienen un monitoreo y supervisión constante del proceso académico, mediante la solicitud de datos e informes de diversa índole, razón por la cual la universidad en su plan estratégico, denominado "Carta de Navegación" 2014-2018"[2], define los diferentes objetivos estratégicos, de los cuales resaltamos el 4.2.

> *"Los estudiantes y docentes de las UPS disponen de accesibilidad a las TIC"*

Y el objetivo estratégico 5.6.

> "*Las dependencias universitarias tienen acceso a información relevante, consistente, congruente y oportuna a través de las tecnologías de la información y comunicación.*"

El plan estratégico define los siguientes indicadores/métricas para cumplir con los objetivos, en lo referente a accesibilidad el 4.2.1 y 4.2.2 con sus respectivos resultados/metas.

> ***4.2.1***
> *Indicador: Ancho de banda de Internet comercial por estudiante (Kbps/estudiante).*
> *Meta: Al 2018, la UPS cuenta con al menos 60 Kbps por estudiante.*

> ***4.2.2***
> *Indicador: Disponibilidad del servicio de Internet.*
> *Meta: Al 2018, la disponibilidad del servicio de Internet comercial es de al menos un 99,9% en los campus de la UPS.*

Sobre seguridad citamos los indicadores 5.6.3 y el 5.6.4

> ***5.6.3***
> *Indicador: Grado de vulnerabilidad de las Tecnologías de la Información y Comunicación de la UPS.*

[1] Tomado de UPS en Cifras 2014 http://www.ups.edu.ec/documents/10184/25094/2014+UPS+en+cifras/e3c99930-78e3-4e8f-857b-670020f7fba1?version=1.1

[2] Carta de Navegación 2014-2018 http://www.ups.edu.ec/documents/10184/20982/Carta+de+navegaci%C3%B3n+2014-2018/d31d2ceb-d6f4-494f-86f8-0456e084a1f0?version=1.4

Meta: Al 2018, el grado de vulnerabilidad de las Tecnologías de la Información y Comunicación de la UPS es de mínimo impacto.

5.6.4
Indicador: Disponibilidad de los servicios de información de la UPS
Meta: Al 2015, la disponibilidad de los servicios de información de la UPS es de al menos un 99,9%.

En resumen el proceso principal de UPS es la gestión académica, cuya operatividad se soporta en la conectividad que brindan las tecnologías de la Información para acceder a los sistemas de información garantizando la confidencialidad, integridad y disponibilidad.

0.2 ENFOQUE

Los servicios de tecnologías de la información como los sistemas de información se encuentran centralizados en la matriz en el Departamento de Tecnologías de la Información y de la Comunicación, la figura 0.1 nos permite observar el organigrama del departamento a nivel nacional.

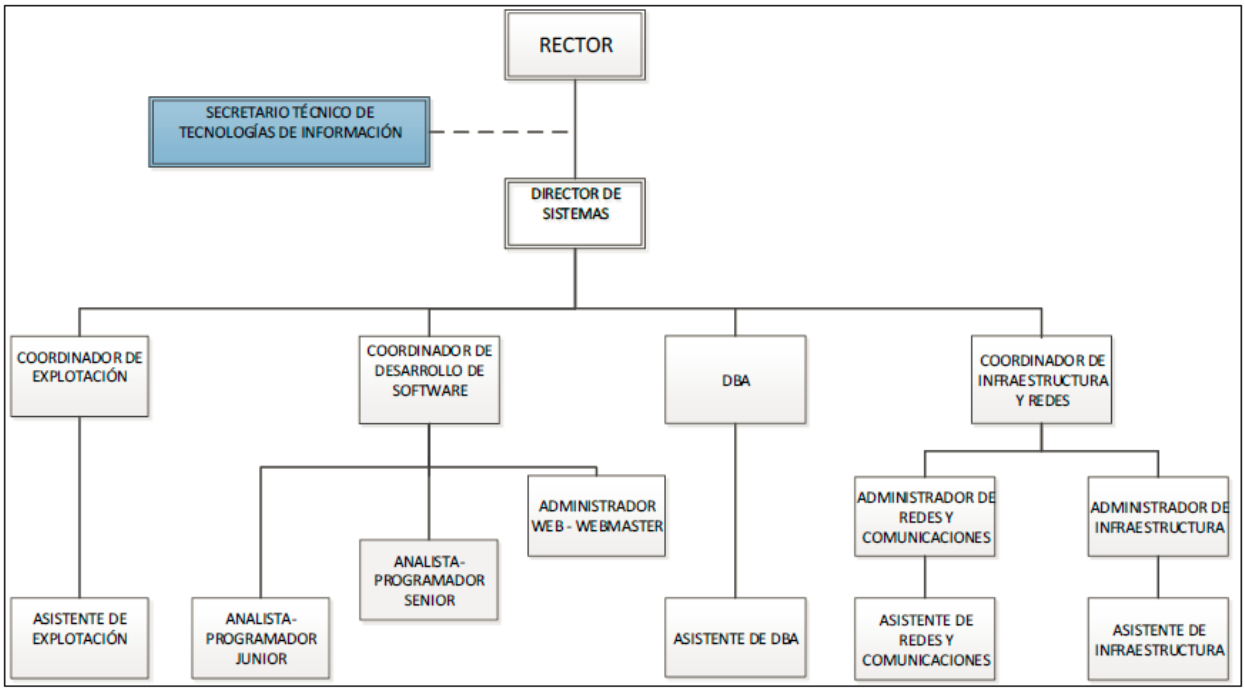


Figura 0.1. Organigrama Nacional del Departamento de TI.
Imagen tomada del documento Descriptivo de Cargos Tecnologías de la Información

La universidad no tiene implantado un Sistema de Gestión de la Seguridad de la Información (SGSI), sin embargo, el documento Descriptivo de Cargos enumera diferentes responsabilidades referentes a la seguridad, a continuación listamos los cargos, su objetivo general y las responsabilidades que tienen relación directa con la seguridad de la información.

- Secretario Técnico de Tecnologías de la Información
  Objetivo general del cargo:
  Coordinar la planificación, organización, administración y control de los servicios y proyectos de TI realizados en la Universidad Politécnica Salesiana.
  Responsabilidad 8: Participar en la planificación de la seguridad informática, planes de contingencia y aceptación de riesgos, conjuntamente con las Direcciones Técnicas de Sede, Coordinaciones y Dirección de Sistemas.
  Responsabilidad 12: Implementar los controles de seguridad del portal.
- DBA
  Objetivo general del cargo:

Garantizar la disponibilidad, integridad y confidencialidad de los sistemas de gestión de base de datos de la UPS.
Responsabilidad 6: Proponer el plan de seguridad y auditoria de los sistemas de gestión de base de datos de la UPS.
Responsabilidad 7: Ejecutar el plan de seguridad y auditoria de los sistemas de gestión de base de datos de la UPS aprobado.

- Asistente del DBA

  Objetivo general del cargo:
  Brindar soporte para el correcto funcionamiento de los sistemas de gestión de base de datos de la UPS.
  Responsabilidad 4: Dar soporte en la ejecución del plan de seguridad y auditoria de los sistemas de gestión de base de datos de la UPS aprobado.
- Coordinador de Infraestructura y redes

  Objetivo general del cargo:
  Planificar, definir, realizar, coordinar y supervisar la operatividad de la infraestructura de servidores, telecomunicaciones y redes en toda la UPS.
  Responsabilidad 11: Participar en la planificación de las seguridades físicas y lógicas de los sistemas informáticos, evaluación de riesgos y elaboración de planes de contingencia y aceptación de riesgos en el ámbito de su responsabilidad.
- Administrador de redes y comunicaciones

  Objetivo general del cargo:
  Garantizar el correcto funcionamiento de la red, comunicaciones y seguridad informática de la red convergente de la UPS.
  Responsabilidad 2: Proponer el plan de seguridad de la red convergente de la UPS en coordinación con la Dirección de Sistemas, Secretaría Técnica de Tecnologías de la Información y Directores Técnicos de TI.
  Responsabilidad 3: Ejecutar el plan de seguridad aprobado de la red convergente de la UPS.
  Responsabilidad 7: Instalar, administrar, documentar y monitorear la seguridad de la infraestructura de red y comunicaciones.
- Asistente de redes y comunicaciones

  Objetivo general del cargo:
  Brindar soporte para el correcto funcionamiento de la red, comunicaciones y seguridad informática relacionada a la red convergente de la UPS.
  Responsabilidad 4: Dar soporte en la documentación y monitoreo de la seguridad de la red convergente de la UPS.
- Administrador de infraestructura

  Objetivo general del cargo:
  Garantizar el correcto funcionamiento de la Infraestructura de Servidores y datos dentro de la Universidad Politécnica Salesiana.
  Responsabilidad 9: Implementar seguridades a nivel de sistemas operativos
- Asistente de infraestructura

  Objetivo general del cargo:
  Brindar soporte para el correcto funcionamiento de la Infraestructura de Servidores y datos dentro de la Universidad Politécnica Salesiana.
  Responsabilidad 7: Documentar los niveles de seguridades implementados en los sistemas operativos

Con fines operativos en las respectivas sedes se utiliza el organigrama de la figura 0.2.

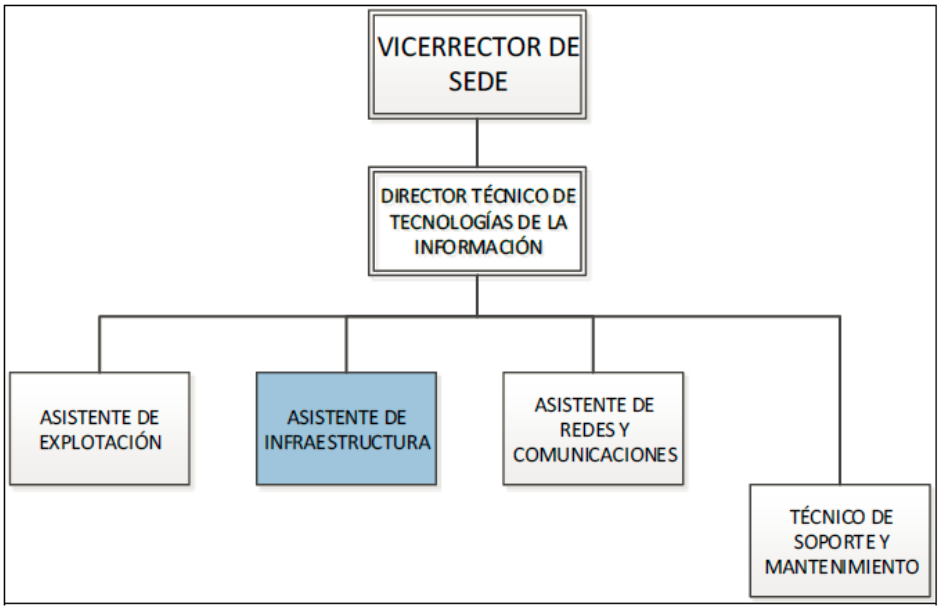


Figura 0.2. Organigrama de Sede.
Imagen tomada del documento Descriptivo de Cargos Tecnologías de la Información

En las sedes existe un asistente para cada una de las áreas del Departamento de Tecnologías de la Información (explotación, infraestructura, y redes y comunicaciones) con las mismas funciones del organigrama nacional.

En resumen, la seguridad es concebida como procesos aislados de cada dependencia del Departamento de Tecnologías de la Información, incluso muchos cargos tienen la responsabilidad de ser auditores de sus propias funciones. Situación que da cuenta de una seguridad de la información desarticulad sin políticas de alto nivel aprobadas por la dirección sobre seguridad.

0.3 ALCANCE

0.3.1 PROCESOS Y SERVICIOS

Los sistemas de información que dan soporte al proceso académico, incluyendo los procesos de las áreas de recursos humanos y financiero, según la declaración de aplicabilidad vigente.

La información deberá ser protegida independientemente de si es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. El hecho de que determinada información esté disponible fuera del alcance no significa que no se le aplicarán las medidas de seguridad; esto solamente implica que la responsabilidad por la aplicación de las medidas de seguridad será transferida a un tercero que administre esa información.

0.3.2 UBICACIONES

Sede Matriz, compuesta por el campus El Vecino y el edificio del Rectorado que se encuentra dentro del mismo campus. Los Centros de Procesamiento de Datos de Quito y Guayaquil.

0.3.3 REDES E INFRAESTRUCTURA DE TI

Red de comunicación LAN que incluirá, la zona desmilitarizada, la red cableada del área administrativa, red inalámbrica de acceso a la comunidad universitaria y todos los dispositivos que la conforman.
Red de comunicación WAN que incluiría los enlaces de datos hacia las sedes Quito y Guayaquil.
Centro de datos principal ubicado en la matriz, incluyendo toda su infraestructura, todos los equipos de procesamiento de datos de la matriz, tanto del personal administrativo como de los laboratorios.

0.3.4 EXCLUSIONES

Se excluye los equipos y dispositivos móviles particulares que se conecten a la red inalámbrica.
Se excluyen las redes LAN de las sedes Quito y Guayaquil debido a que son extensiones operativas del Departamento de Tecnologías de la Información, de igual manera los equipos de procesamiento de datos del personal docente y/o administrativo como de los laboratorios de las sedes referenciadas.

0.4 OBJETIVOS DE SEGURIDAD

Acorde a la política institucional definida en su plan estratégico los objetivos del plan director son:

0.4.1.1 Brindar una alta disponibilidad de los sistemas informáticos tanto en conexiones internas y/o externas.

0.4.1.2 Garantizar la integridad de la información académica según la normativa estipulada en el Reglamento de Régimen Académico del CES y el Reglamento de Evaluación y Acreditación de Programas y Carreras del CEAACES.

0.4.1.3 Asegurar la confidencialidad de la información según su nivel de seguridad, independientemente de su naturaleza (papel, digital) y que sea procesada, trasmitida, almacenada.

0.4.1.4 Implementar un SGSI acorde a la norma ISO/IEC 27001:2013 alineado con el Plan Estratégico 2014-2018.

0.5 ANÁLISIS DIFERENCIAL

Para el análisis diferencial se utilizan métricas basadas en el modelo de madurez de COBIT (Control Objectives for Information and related Technology) y CMM (Capability Maturity Model). La tabla 0.1 presenta el significado para cada estado.

Estado	Significado
? Desconocido	Todavía no ha sido chequeado
No existente	Falta completa de política reconocible, proceso, control, etc.
Inicial	Desarrollo apenas iniciado y requerirá un significante trabajo para completar los requerimientos.
Limitado	Progresando de manera correcta pero todavía no completado
Definido	Desarrollo más o menos completo aunque el detalle es deficiente y/o todavía no se ha implementado y respaldado activamente por la Dirección
Gestionado	Desarrollo está completo, el proceso/control ha sido implementado y recientemente comenzó a operar
Optimizado	El requerimiento es completamente satisfactorio, está operando plenamente como era de esperar, está iniciando el monitoreo y mejora activamente, y existe evidencia substancial para probar todo a los auditores
No aplicable	Este requerimiento no es aplicable a la organización. Nota: Todos los requerimientos en el cuerpo de ISO/IEC 27001 son mandatorios, si el SGSI

Tabla 0.1. Modelo de Madurez, utilizada para el análisis diferencial

En el anexo 01, se puede encontrar el análisis diferencial de la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013 con respecto a la universidad, la figura 0.3 permite apreciar el estado de implementación de

la norma ISO/IEC 27001, es importante resaltar que el estado de la norma en diferentes puntos alcanza como máximo el estado de “Definido”.

En la figura 0.4 se aprecia el estado de madurez de los diferentes controles, es importante encontrarnos con el 9% de controles con el estado de madurez de “Gestionado”, además el 46% del total de controles están o han sobrepasado el estado “Inicial”, lo cual ratifica que la universidad se encuentra con una seguridad desarticulada.

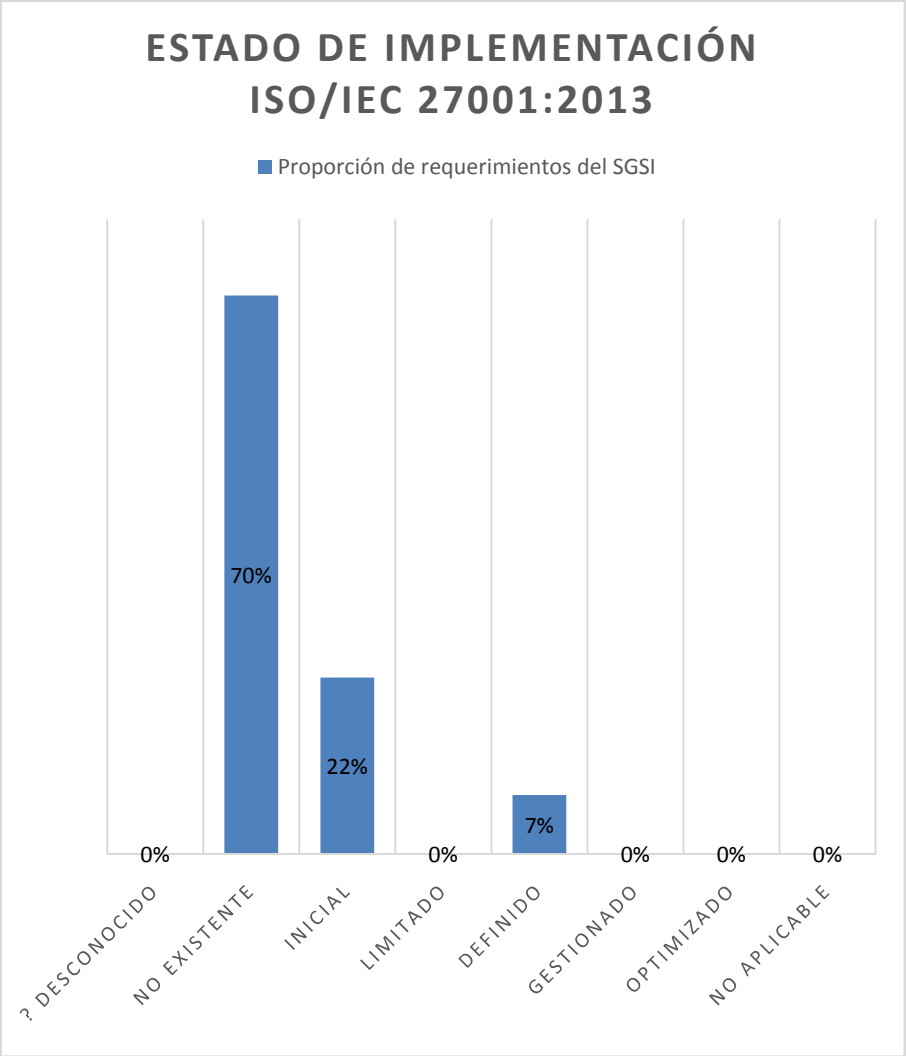


Figura 0.3. Estado de implementación del SGSI

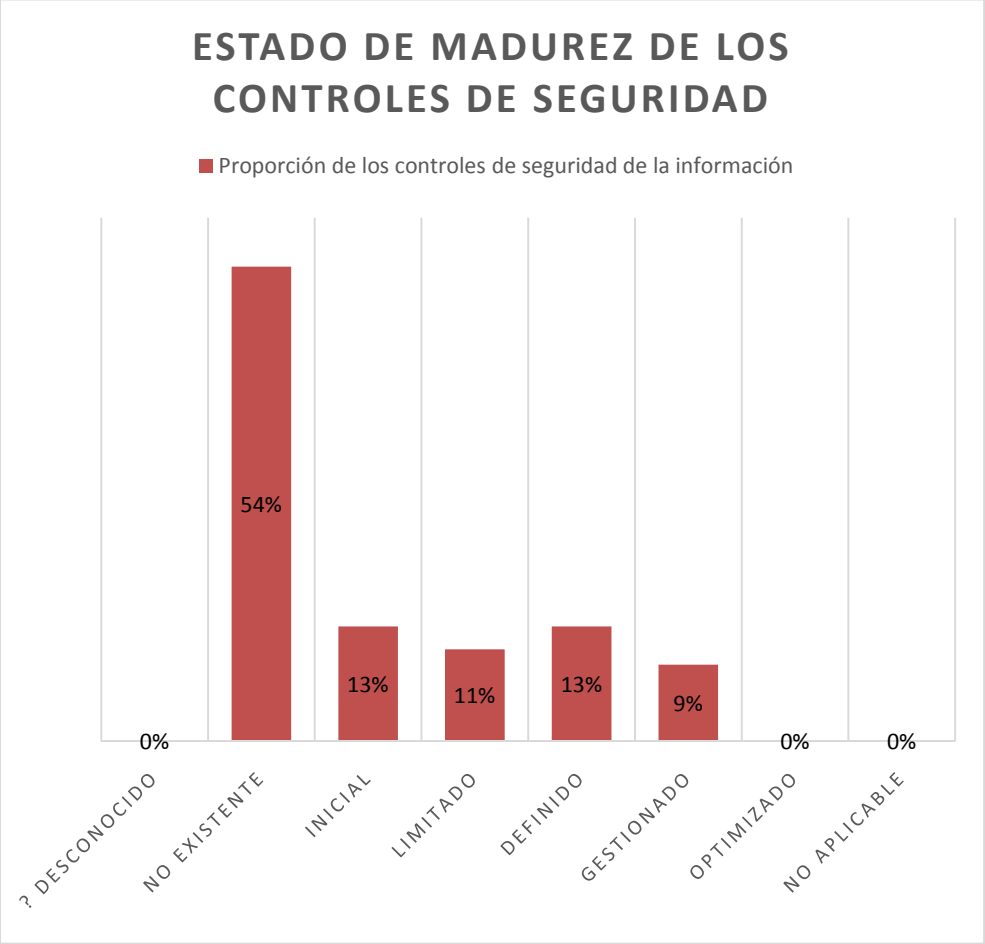


Figura 0.4. Estado de madurez de los controles

Finalmente la tabla 0.2, permite apreciar la proporción de controles según el estado de madurez

Estado	Significado	Proporción de requerimientos del SGSI	Madurez de los controles de seguridad de la información
? Desconocido	Todavía no ha sido chequeado	**0%**	**0%**
No existente	Falta completa de política reconocible, proceso, control, etc.	**70%**	**54%**
Inicial	Desarrollo apenas iniciado y requerirá un significante trabajo para completar los requerimientos.	**22%**	**13%**
Limitado	Progresando de manera correcta pero todavía no completado	**0%**	**11%**
Definido	Desarrollo más o menos completo aunque el detalle es deficiente y/o todavía no se ha implementado y respaldado activamente por la Dirección	**7%**	**13%**

Gestionado	El requerimiento es completamente satisfactorio, está operando plenamente como era de esperar, está iniciando el monitoreo y mejora activamente, y existe evidencia substancial para probar todo a los auditores	**0%**	**9%**
No aplicable	Este requerimiento no es aplicable a la organización. Nota: Todos los requerimientos en el cuerpo de ISO/IEC 27001 son mandatorios, si el SGSI	**0%**	**0%**

Tabla 0.2. Resumen de análisis diferencial

1 CAPÍTULO 2: SISTEMA DE GESTIÓN DOCUMENTAL

1.1 DEFINICIÓN DE LA GESTIÓN DOCUMENTAL

Esta sección tiene la finalidad de normalizar la estructura, forma, presentación, control, gestión, difusión y registro de la documentación generada en el SGSI de la UPS, para alcanzar los siguientes objetivos:

- Transmitir una imagen única.
- Producir documentación homogénea y con calidad.
- Facilitar la lectura o consulta de la documentación.
- Identificar claramente la documentación.
- Asegurar la utilización de las últimas ediciones.
- Disponer de un archivo único para acceder a la documentación.

El ámbito de la presente gestión documental alcanza:

- Documentación del Sistema de Gestión de Seguridad de la Información
- Documentación de Actividades Técnicas.
- Normativa Interna.
- Documentación de Origen Externo.

1.1.1 CODIFICACIÓN DE LA DOCUMENTACIÓN

Todos los documentos del SGSI mantendrán el siguiente esquema: SGSI-XX-YYYY donde:

- SGSI: son las siglas que identificarán siempre al documento como perteneciente al Sistema de Gestión de Seguridad de la Información.
- XX: son dos siglas que identificaran el tipo de documento de acuerdo a:
  - PO: Política de Seguridad
  - NO: Norma
  - PR: Procedimiento
  - IT: Instructivo Técnico
  - MM: Manual
- YYYY: Máximo cuatro siglas que permiten identificar el alcance del documento, por lo general se utilizará las iniciales del nombre del documento, por ejemplo si el documento se denomina “Política de Seguridad de la Información” se puede utilizar “PSI”.

1.1.2 ESTRUCTURA DEL DOCUMENTO

Todo documento deberá tener la siguiente estructura:

- Encabezado que indique claramente el logo de la universidad, el tipo de documento, el título del documento y la versión del mismo según la tabla 1.1:

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	Tipo de Documento	Código:
	Título del documento	Versión X.X

Tabla 1.1 Encabezado de todo documento del SGSI

- Pie de página que debe contener el número actual de página y el total de páginas del documento.
- La primera página debe mostrar el título del documento y la información de la última versión según la tabla 1.2.

Código:	
Versión:	X.X
Fecha de la versión:	10 de Octubre de 2014
Creado por:	Ing. Rodolfo Xavier Bojorque Chasi
Aprobado por:	
Nivel de confidencialidad:	Interno

Tabla 1.2 Información para primera página de documentación

- La segunda Hoja debe contener el historial de modificaciones según la tabla 1.3 y el índice de contenidos

Fecha	Versión	Creado por	Descripción de la modificación
10/Oct/2014	0.1	Rodolfo Bojorque	Creación del Documento
12/Oct/2014	0.2	Rodolfo Bojorque	Actualización

Tabla 1.3 Control de modificaciones

- El desarrollo del documento siempre tendrá como primer punto una introducción que defina antecedentes, necesidades e importancia del documento, como segundo punto los objetivos del documento y como tercer punto el alcance del mismo.

1.1.3 CONFIDENCIALIDAD

De acuerdo a las políticas de clasificación de la información, los documentos están sometidos a ciertas restricciones en su utilización, pueden considerarse de nivel público, interno y confidencial. Dicha clasificación debe quedar claramente establecida en el control de documentación detallado en el Tabla 1.1.

1.1.4 DIFUSIÓN

Para difundir la información se debe tener en cuenta su confidencialidad de acuerdo a la política de clasificación de la información.

A continuación se detallan las condiciones para difundir la documentación generada por la UPS.

Publicación
La documentación referente al Sistema de Gestión de Seguridad de la Información se publicará, una vez aprobada, para ello la UPS mediante la Secretaría Técnica de Comunicación y Publicaciones iniciará el proceso de difusión respectivo considerando el nivel de confidencialidad de la información.

Para información pública del Sistema de Gestión de Seguridad de la Información se publicará los documentos en la respectiva sección de la página web institucional, se notificará a todos los docentes y personal administrativo mediante el correo electrónico, todos los receptores deberán emitir el acuse de recibo y la aceptación de los términos de la política. Adicionalmente se imprimirá el documento de las políticas que reposará en cada departamento o unidad de la UPS.

Para información interna del Sistema de Gestión de Seguridad de la Información se notificará a los respectivos destinatarios mediante un comunicado de correo electrónico, todos los receptores deberán notificar acuse de recibo, declarar haber leído el documento y aceptar los términos de la misma.
En caso de considerarse necesario, el Responsable de Seguridad de la Información en coordinación con el Procurador asistirán en la firma de acuerdos de confidencialidad en los casos pertinentes.

La información confidencial no se publicará de ninguna manera y será responsabilidad absoluta de su propietario.

Archivo
Los documentos originales firmados del Sistema de Gestión de Seguridad de la Información serán custodiados de acuerdo a las directrices determinadas por la Secretaría Técnica de Gestión Documental
En el caso de los documentos de carácter técnico y documentación externar de carácter técnica, es responsabilidad de cada Jefe/Director/Coordinador departamental asegurar que la información esté disponible y accesible en las ubicaciones necesarias, realizándose, si fuese necesario, una distribución controlada de los mismos.

1.2 POLÍTICA DE SEGURIDAD

1.2.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.2.1.1 Introducción

El Consejo Superior de la UPS ha decidido adoptar un conjunto de medidas para proteger los activos estratégicos de la institución. Entre estos activos se encuentra la información, los documentos, las plataformas y los sistemas de información que permiten su tratamiento, almacenamiento, comunicación y explotación, fundamentales para el desarrollo de las actividades académico-administrativas y futuro de la institución.
Entre los objetivos estratégicos de la UPS reflejados en la Carta de Navegación 2014-2018, la seguridad de la información es un medio eficaz desde el cual:

> *3.4 La comunidad universitaria está debidamente informada de las políticas institucionales que implementa la UPS.*
> *4.1 Los estudiantes y docentes de la UPS disponen de accesibilidad a las TIC*
> *5.2 Los usuarios de la UPS se benefician de servicios de calidad a través de la aplicación del modelo de gestión con base en la unificación y sistematización.*
> *5.6 Las dependencias universitarias tienen acceso a información relevante, consistente, congruente y oportuna a través de las tecnologías de la información y comunicación*
> *5.8 La UPS desarrolla una gestión económica-financiera, que facilita la toma de decisiones y el cumplimiento de los objetivos institucionales, en el marco de la normativa vigente*
> *5.9 La comunidad universitaria de la UPS cuenta con información gestionada y conservada eficientemente*

Para poder asumir estos objetivos, es necesario que dentro de la universidad se garantice la consecución de unos niveles de confidencialidad, disponibilidad e integridad de los activos de información de un modo efectivo y medible.

1.2.1.2 Objetivos

La política de seguridad de la información persigue los siguientes objetivos:

- Crear un marco referencial para asegurar una protección efectiva de la información de la Universidad Politécnica Salesiana.
- Establecer las expectativas de la universidad en relación al correcto uso que el personal haga de los recursos de información de la UPS, así como de las medidas que se deben adoptar para la protección de estos recursos.
- Infundir a todo el personal de la UPS, la conciencia de la necesidad de la seguridad de la información y la comprensión de sus responsabilidades individuales.

- Especificar las medidas esenciales de seguridad de la información que la UPS debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad y disponibilidad de la información, con lo que se podrían ocasionar las siguientes consecuencias:
    - Pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.).
    - Pérdida de imagen institucional.
    - Pérdida de credibilidad ante los entes reguladores de la educación superior ecuatoriana
    - Falta de disponibilidad de los diferentes servicios de TI (redes, acceso a internet, sistemas de información)

Proporcionar a todo el personal de la UPS una herramienta que facilite la toma de decisiones apropiadas relacionadas con los mecanismos o soluciones de seguridad de la información.

1.2.1.3 Alcance

Esta política se aplica a todo el personal docente, administrativo o de servicio, así como a todo activo de información que la UPS posea actualmente o en el futuro, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger activos de información que se encuentren en otros formatos.

La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

Cualquier sistema que se encuentre ejecutándose en un computador o dispositivo que se encuentre conectado a las redes universitarias y a todos los sistemas de información suministrados por la UPS.

Todas las partes externas que prestan servicios a la UPS en materia de instalaciones de procesamiento de información y actividades de negocio.

1.2.1.4 Política

- La información debe ser protegida por sus responsables y usuarios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en los conceptos de seguridad de la información y en base al valor que le otorgue su propietario.
- Por cada uno de los niveles de clasificación establecidos en la Política de Clasificación de la Información, se definirán controles de seguridad para la confidencialidad, integridad y disponibilidad de la información. Estos controles quedarán documentados en normativas asociadas al presente documento.
- Todo aquello que no está expresamente permitido está prohibido, siendo necesario exponer la situación en conflicto para que se otorgue autorización explícita a aquello que se necesita o utiliza. Esto implica la deshabilitación de todo aquello que no sea necesario.
- La información y las tecnologías de información asociadas deben ser usadas sólo para propósitos relacionados con las distintas funciones universitarias y autorizados por los supervisores y propietarios, debiéndose aplicar criterios de buen uso cuando no exista una política o normativa explícita para su utilización.
- Todo recurso tecnológico, procedimiento académico-administrativo y, en general, las actividades realizadas en el entorno de trabajo tecnológico deberán proveer de algún mecanismo o procedimiento confiable mediante el cual sea posible identificar e individualizar inequívocamente a un usuario. Del mismo modo deberá registrar las actividades de un determinado usuario en un período de tiempo señalado. Este registro deberá ser almacenado y podrá ser consultado en caso de ser requerido. El tiempo, condiciones y lugar de almacenaje será definido claramente para cada caso particular.

- Cuando sea estrictamente necesario proporcionar información “Confidencial” o de “Uso Interno” a terceros, se deberán suscribir acuerdos de confidencialidad con el tercero. Adicionalmente se definirán controles específicos, los que estarán establecidos en la Normativa correspondiente.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- La información es un activo vital, por lo que todo acceso, uso y procesamiento, deberá ser consistente con las políticas y estándares emitidos por la universidad.
- Los supervisores deben procurar que todo el personal reciba una formación en materia de seguridad, consistente con sus necesidades y rol dentro de la universidad.
- El personal tiene la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política. Los supervisores deberán analizar cada caso reportándolos al Departamento de Tecnologías de la Información, de manera que se adopten las medidas correspondientes para evitar su repetición.
- La UPS se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan.
- Toda la información creada o procesada por la universidad debe ser considerada como de “Uso Interno”, a menos que el propietario de la información considere otro nivel de clasificación, pudiendo ser “Confidencial” o “Pública”.
- Está absolutamente prohibido al personal de la UPS divulgar cualquier información de clasificación “Confidencial” o “Uso Interno”, salvo que sea explícitamente autorizado por el propietario de la información, quien deberá hacerse responsable de esta divulgación.
- La UPS se reserva el derecho de tomar medidas administrativas en contra del personal que no dé cumplimiento a lo dispuesto en la presente política y en su documentación de referencia.
- La presente política es el marco de referencia de seguridad de los sistemas de información para la UPS. Para garantizar la consecución de los objetivos de seguridad establecidos, se ha desarrollado un cuerpo normativo en el que se detallan las medidas técnicas, organizativas y de gestión necesarias para garantizar el cumplimiento de las directrices establecidas en la presente política.
- El incumplimiento de esta política por parte del personal docente, administrativo o de servicio de la UPS y de las normativas que la desarrollan podrá comportar la apertura de procedimientos disciplinarios.

Anualmente, o ante un cambio relevante en los Sistemas de Información, el responsable de seguridad deberá realizar una revisión y o adecuación de la Política de Seguridad a la realidad de la Compañía.

1.2.2 POLÍTICA DE ALTO NIVEL

El UPS, consciente de la importancia que la seguridad en el tratamiento de la información tiene para toda la institución, sus estudiantes, docentes, personal administrativo y de servicio; los proveedores y en general todas las instituciones con las que se mantiene relación, ha considerado fundamental establecer el tipo de tratamiento que debe darse a la información de la que es propietaria o depositaria, durante todo su ciclo de vida y con el fin de garantizar su confidencialidad, integridad y disponibilidad, y cumpliendo escrupulosamente con todos los requerimientos legales que sean de aplicación en cada momento.

El objetivo prioritario de esta política es disponer de un sistema eficiente y eficaz para la gestión de la seguridad de la información, y como consecuencia de ello obtener el más alto nivel de garantía en su tratamiento dentro de la UPS y que redunde en una mejora continua en nuestra relación interna y externa, logrando con ello que nuestros destinatarios perciban el compromiso de la UPS con respecto a la seguridad y a la satisfacción de los servicios ofrecidos.

Para lograr estos objetivos, la UPS se compromete a facilitar, por todos los medios a su alcance y de forma proporcional a los riesgos detectados, los recursos necesarios para que la institución disponga de un entorno alineado con los objetivos de la Carta de Navegación 2014-2018 y los objetivos de seguridad plasmados en toda la documentación desarrollada a partir de esta política. Esta política y toda la documentación relacionada serán distribuidas por canales adecuados y en base a la necesidad del conocimiento a todos las partes interesadas.
Todas las partes implicadas se comprometen a cumplir y a hacer cumplir todos los principios de seguridad que se ha establecido, garantizando la protección de la información en todo momento; y evitando y colaborando a que la seguridad de la información sea mantenida de forma permanente.

La UPS cuenta con la colaboración de todo su personal y asume la responsabilidad de motivar y formar adecuadamente a todos ellos. Quienes están en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política.

Las actividades deliberadas contra los objetivos de esta política serán tratadas de acuerdo a la legislación y a la relación contractual existente en cada momento.

Esta política de seguridad entra en vigor el día de su publicación y será revisada anualmente por el Responsable de Seguridad de la Información y el Consejo Superior.

Dr. XXXXXXXXXXX
Rector
Cuenca, a XX de XXXX de 2014

1.2.3 Política de Clasificación de la Información

1.2.3.1 Introducción

Para el tratamiento efectivo de activos de información, la UPS definirá una clasificación de criticidad de acuerdo a las políticas de la organización, esto permitirá implementar los diferentes controles de acuerdo a la criticidad del activo y facilitará a los propietarios su clasificación y gestión de privilegios.

1.2.3.2 Objetivos

- Difundir la visión y la importancia de los diferentes activos de información de la UPS según su criticidad.
- Definir los niveles de criticidad de la información que se almacena, circula, digitaliza, comunica, transmite mediante cualquier medio en la UPS.

1.2.3.3 Alcance

Todos los activos de información, incluso aquellos nuevos que se generarán con posterioridad a la publicación de la presente política.

1.2.3.4 Clasificación de la Información

Información Pública: Es información cuyo acceso es libre, su divulgación no supone un perjuicio para la universidad y no requiere medidas de protección para su confidencialidad.

Información Interna: Es información cuyo acceso está restringido a los trabajadores de la UPS, previa autorización del respectivo propietario. Su divulgación a personal no autorizado o externos a la universidad puede comportar un incumplimiento grave de carácter legal, acuerdo de confidencialidad u otro.

Información Confidencial: Es información de importancia estratégica para la universidad, cuyo acceso está restringido, controlado y solamente los propietarios de la información tienen acceso a ella, únicamente los propietarios pueden autorizar su divulgación parcial o total. Su divulgación sin autorización puede comportar pérdidas económicas elevadas o desprestigio grave para la universidad.

Para clasificar la información el Comité de Seguridad de la Información designará los respectivos propietarios de información, cuyas responsabilidades se detallan en el documento Organización de la Seguridad de la Información.

Etiquetado de Información

Para la correcta implantación de la política toda la información digital o impresa deberá establecer claramente en una zona reconocible su nivel de clasificación, para la información clasificada como confidencial cada propietario deberá implementar las medidas que considere pertinentes de acuerdo a la realidad de su departamento, unidad y/o coordinación.

1.2.4 Política de Control de Acceso

1.2.4.1 Introducción

Para garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información se define la siguiente política de control de acceso.

1.2.4.2 Objetivos

- Asegurar los activos de información.
- Impedir el acceso no autorizado.

1.2.4.3 Alcance

Todos los sistemas de información de la universidad, los futuros desarrollos, bases de datos, servicios e infraestructura.

Todo personal docente, administrativo o de servicio que requiera acceder a activos de información, áreas de acceso restringido

Estudiantes que utilizan los diferentes servicios de TI de la universidad

1.2.4.4 Política

Todos los recursos de tecnologías de la información, activos y sistemas de información de la UPS deberán ser accedidos y utilizados mediante el respectivo control de acceso, para ello la universidad ha dividido el control de acceso en físico y lógico.

1.2.4.5 Control de acceso físico

Para la implementación del control de acceso físico la universidad utilizará la siguiente clasificación de zonas, estas áreas cubren un espacio físico determinado y el Comité de Seguridad de la Información establecerá los respectivos responsables en los casos que amerite.

Zonas Públicas: Son áreas que no requieren ningún tipo de vigilancia, están abiertas al público en general.

Zonas Privadas: Son áreas a las que únicamente tiene acceso el personal y los estudiantes, el acceso a dichas áreas deberá estar monitoreado por videovigilancia.

Zonas restringidas: Son áreas a las que únicamente se puede tener acceso con la respectiva autorización, para el ingreso a zonas restringidas siempre se deberá llevar la respectiva identificación. Para cada zona restringida se designará un responsable quien deberá velar para que la política se cumpla y autorizar el acceso a su área de visitas y/o personal externo.

Toda visita o personal externo deberá estar siempre acompañado de la manera que el responsable de cada área considere necesaria, para ello el responsable de área deberá llevar un control de acceso con la identificación, día y hora y la identidad del personal que ha autorizado dicho acceso.

1.2.4.6 Control de acceso lógico

Usuarios

Los usuarios que por motivos de su trabajo o actividad requieren acceder a los diferentes sistemas de información y servicios de TI deberán contar con un identificador único para acceder a todos los servicios. La Secretaría Técnica de Recursos Humanos definirá el identificador de cada actor en coordinación con la Secretaría Técnica de Tecnologías de la Información y Comunicación para la gestión de alta y baja de usuarios.

En el caso de los sistemas de información cada propietario de la información deberá autorizar los diferentes accesos del usuario y los privilegios de acceso.

Contraseñas

Todos los sistemas y servicios deben autenticar a los usuarios para ello deben utilizar contraseñas seguras basadas en la siguiente regla:

- Mínimo 8 caracteres

- Debe estar conformada por lo menos con una letra minúscula, mayúscula, número y signo de puntuación
- Las contraseñas caducan cada seis meses

1.2.4.7 Acceso a los sistemas de información institucionales

Para acceder a un sistema informático siempre se necesitará la autorización del propietario de la información. Dicha autorización debe ser adjuntada con el respectivo grado de privilegio para cada activo. La coordinación de explotación se encargará de gestionar y garantizar que todos los accesos sean únicamente los solicitados

1.2.4.8 Acceso a la red inalámbrica

El objetivo de la red inalámbrica es brindar conectividad a internet a los usuarios, para acceder a la red inalámbrica se requiere una autenticación univoca por usuario, dicha autenticación será válida únicamente para un dispositivo a la vez.

La universidad garantiza el acceso libre a todo tipo de información que se encuentre en la red con fines académicos en beneficio de garantizar la democratización del conocimiento.
El usuario de la red inalámbrica acepta incondicionalmente que para efectos de calidad del servicio la universidad puede monitorizar sus acciones garantizando el derecho a la privacidad.

El mal uso de la red como apropiación excesiva del ancho de banda, acceso a sitios peligrosos, pornográficos y/o utilización de herramientas de penetración, escaneo de puertos y/o exploits conllevará la suspensión por una hora del servicio, en caso de reincidencia, el servicio se suspenderá durante dos días y en caso de volver a reincidir el servicio se suspenderá definitivamente y se notificará inmediatamente al Responsable de Seguridad para brindar soporte y seguimiento a la incidencia.

Acceso a sistemas operativos:
El acceso a terminales de escritorio y estaciones de trabajo se lo realizará mediante el servicio de directorio corporativo, donde se gestionará las credenciales y privilegios que el usuario tendrá para el equipo, por ningún concepto, usuario alguno tendrá privilegios de administrador sobre el equipo.

Los propietarios de equipos portátiles tendrán un usuario adicional para acceder al sistema operativo fuera de la red de la universidad.

1.2.5 Política de Uso de Correo Electrónico

1.2.5.1 Introducción

El correo electrónico es una herramienta de comunicación institucional, se lo utilizará solo con fines relacionados a las actividades académico-laborales en la universidad. Para ello todos los docentes, personal administrativo y estudiantes contarán con su cuenta personal. Las autoridades y cargos de dirección de unidades-departamentos tendrán una cuenta corporativa.

1.2.5.2 Objetivos

- Definir el uso correcto del correo electrónico personal e institucional
- Proteger los activos de información que se encuentren en las cuentas de correo electrónico, sean personales o institucionales
- Garantizar la privacidad de la información

1.2.5.3 Alcance

Todos los usuarios del servicio de correo electrónico de la universidad y todas las cuentas personales e institucionales

1.2.5.4 Política

Las cuentas de correo electrónico personales son de propiedad exclusiva de la UPS, el usuario es consiente y acepta que como tal, la UPS puede requerir el acceso a la misma mediante las vías permitidas por la ley. Se considera cuenta personal toda aquella que identifica a la persona como tal, por ejemplo, juanperez@ups.edu.ec

Las cuentas de correo electrónico institucionales también son propiedad exclusiva de la UPS, y como tal puede acceder a las mismas sin previo aviso ni autorización, siempre en coordinación entre la Secretaría Técnica de Recursos Humanos y la Secretaría Técnica de Tecnologías de la Información. Se consideran cuentas institucionales toda aquella que identifica una unidad, departamento, comisión, etc. de la UPS, por ejemplo, rectorado@ups.edu.ec

Está permitido

- Utilizar el correo electrónico para actividades institucionales, académicas, investigativas, se considera válido incluso el envío de correos masivos con comunicados, informaciones, etc. siempre y cuando sean institucionales.
- Utilizar el correo electrónico con fines personales siempre y cuando no incumpla alguna de las prohibiciones detalladas en esta política.
- Registrar la cuenta de correo electrónico en sitios externos a los de la UPS siempre y cuando los fines sean institucionales o académicos.

Está prohibido

- Enviar correos masivos o cadenas de correo electrónico con fines políticos, publicitarios, religiosos, sexuales, discriminatorios o de cualquier índole ajena a los intereses de la universidad.
- Enviar datos personales por correo electrónico con el fin de asegurar la privacidad de todos los usuarios, por lo tanto cualquier solicitud de datos personales por correo electrónico está prohibida.
- Enviar información clasificada como confidencial por correo electrónico, sea en su contenido o como archivo adjunto.

Todos los usuarios son responsables de notificar inmediatamente al Responsable de Seguridad de la Información el incumplimiento de esta política por parte de cualquier usuario.

La UPS se reserva el derecho de revocación de acceso para los siguientes casos:

- Cuentas que se consideran como origen de correo no deseado (Spam).
- Cuentas personales de usuarios dados de baja.
- Cuentas que propaguen software malicioso (malware, virus).

Los usuarios de cuentas revocadas serán oficialmente comunicados por el Responsable de Seguridad de la Información para gestionar el incidente.

1.2.6 Política de Desarrollo Seguro

1.2.6.1 Introducción

La UPS cuenta con un equipo de desarrollo de proyectos de software, seguir buenas prácticas de seguridad en todo el ciclo de vida de desarrollo del software (SDLC) permite evitar y mitigar vulnerabilidades y fallos en la programación.

1.2.6.2 Objetivos

- Desarrollar software seguro.
- Mitigar las vulnerabilidades en los desarrollos internos.
- Establecer planes de continuidad.

1.2.6.3 Alcance

Todos los integrantes del equipo de desarrollo de aplicaciones, explotación, el DBA y el Coordinador de Desarrollo de Software.
Todos los sistema de información que se encuentran en producción, desarrollo y todos los futuros proyectos.

1.2.6.4 Política

Para cada fase del desarrollo: Análisis, especificación de requerimientos, diseño, construcción, pruebas y producción se establecerán controles que garanticen la implementación de código seguro.

Se debe contar con diferentes bases de datos, una para desarrollo y otra para pruebas, en los dos casos se deberá garantizar la confidencialidad de la información, para ello el DBA disociará los datos para garantizar la confidencialidad y privacidad de la información.

Las aplicaciones que utilicen tecnología Web antes de salir a producción deben ser sometidas a pruebas de penetración y escaneo de vulnerabilidades.

Los códigos fuentes deberán estar almacenados en un repositorio en un área de acceso restringido, el nivel de clasificación de este activo siempre será confidencial.

1.2.7 Política de Gestión de Incidentes

1.2.7.1 Introducción

Los incidentes de seguridad serán comunicados a través de canales de información definidos y autorizados por la dirección. Todo el personal académico, administrativo y estudiantes son responsables de reportar cualquier incidente de seguridad.

1.2.7.2 Objetivos

- Garantizar la operatividad del negocio.
- Responder de manera pertinente y eficaz ante incidentes de seguridad.

1.2.7.3 Alcance

Todo el Sistema de Gestión de Seguridad de la Información.
Todo el personal docente, administrativo, estudiantes.

1.2.7.4 Política

Toda detección de un supuesto incidente de seguridad será comunicado inmediatamente al Responsable de Seguridad de la Información, quien dependiendo del caso activará los diferentes planes de continuidad o elevará al Comité de Seguridad de la Información la incidencia.

Se definirá un proceso que permita documentar, cuantificar y monitorear el impacto de un incidente de seguridad, con la finalidad de evaluarlo y tratar de minimizarlo, en un proceso de mejora continua.

En caso de tratarse de un incidente crítico el Procurador (representante legal de la universidad) conjuntamente con el Responsable de Seguridad de la Información iniciarán los procesos disciplinarios o legales correspondientes.

1.3 Organización de la Seguridad de la Información

La organización de la seguridad de la información permite identificar los diferentes roles y responsabilidades de todos los actores en la seguridad de la información, para el detalle nos podemos referir al anexo 02 Organización de la Seguridad de la Información.

1.4 Procedimiento de Auditorías Internas

Las auditorías internas son una garantía de ejecución del ciclo PDCA. Tienen gran importancia en el proceso de mejora continua y podemos encontrar su detalle en el anexo 03 Procedimiento de Auditorías Internas.

1.5 Gestión de Indicadores

La gestión de indicadores le permitirá a la UPS contar con parámetros para la toma de decisiones referentes al SGSI, en el anexo 04 Gestión de Indicadores se describe los detalles para la implementación de indicadores.

1.6 Procedimiento de Revisión por la Dirección

La Dirección debe revisar periódicamente el estado del SGSI, el anexo 05 Procedimiento de Revisión por la Dirección tiene como finalidad entregar pautas y directrices a la dirección para establecer el grado de pertinencia del SGSI.

1.7 Metodología de Análisis de Riesgos

La Metodología de análisis de riesgos permitirá establecer a la UPS un análisis y gestión de riesgos acorde a las necesidades institucionales, en el anexo 06 Metodología de Análisis de Riesgos se detalla la metodología.

1.8 Declaración de Aplicabilidad

La Declaración de Aplicabilidad es un documento que describe los controles de la ISO/IEC 27002:20013 que son objetivos, relevantes y aplicables al SGSI de la UPS.

Tipo	Apartado	Aplicación	Justificación
Dominio	5. POLÍTICAS DE SEGURIDAD		
Objetivo	5.1 Directrices de la Dirección en seguridad de la información		
Control	5.1.1 Conjunto de políticas para la seguridad de la información	SI	Debe existir un conjunto de políticas de seguridad de la información, aprobados por la dirección, publicados y comunicados.
Control	5.1.2 Revisión de las políticas para la seguridad de la información	SI	Las políticas deben ser evaluadas por los diferentes propietarios y cada año someterlas a aprobación del Comité de Dirección, la política ecuatoriana está en proceso de transición con leyes y reglamentos que afecta directamente a la UPS.
Dominio	6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN		
Objetivo	6.1 Organización interna		
Control	6.1.1 Asignación de responsabilidades para la seguridad de la información.	SI	El comité de dirección debe aprobar la Organización de la Seguridad de la Información, ahí se definen todas las responsabilidades para la seguridad de la información.
Control	6.1.2 Segregación de tareas.	SI	Las diferentes tareas deben ser segregadas.
Control	6.1.3 Contacto con las autoridades.	SI	Se debe definir los procedimientos adecuados para mantener la comunicación con las autoridades para la gestión de incidencias.

Control	6.1.4 Contacto con grupos de interés especial.	SI	Es necesario mantener contacto con grupos de seguridad y capacitaciones en seguridad de la información.
Control	6.1.5 Seguridad de la información en la gestión de proyectos.	SI	Se debe gestionar como proyecto la seguridad de la información.
Objetivo	6.2 Dispositivos para movilidad y teletrabajo.		
Control	6.2.1 Política de uso de dispositivos para movilidad.	SI	Se utilizará políticas y medidas de seguridad para manejar dispositivos móviles.
Control	6.2.2 Teletrabajo.	SI	Se utilizará políticas y medidas de seguridad para el teletrabajo, por lo general la universidad realiza sesiones con las otras sedes mediante videoconferencia y a determinados usuarios se les facilita conexiones VPN.
Dominio	7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS		
Objetivo	7.1 Antes de la contratación		
Control	7.1.1 Investigación de antecedentes.	SI	Toda contratación se realiza mediante concurso público de méritos y oposición.
Control	7.1.2 Términos y condiciones de contratación.	SI	Todos los trabajadores conocerán los términos referentes a políticas de la seguridad de la información y firmarán acuerdos de no divulgación.
Objetivo	7.2 Durante la contratación		
Control	7.2.1 Responsabilidades de gestión.	SI	Todos los trabajadores conocerán su rol con el sistema de gestión de seguridad de la información.
Control	7.2.2 Concienciación, educación y capacitación en seguridad de la información	SI	Existen proyecto de capacitación y concienciación sobre la seguridad para todo el personal de la universidad.
Control	7.2.3 Proceso disciplinario.	SI	Se necesita procesos disciplinarios definidos para las faltas de seguridad de la información.
Objetivo	7.3 Cese o cambio de puesto de trabajo.		
Control	7.3.1 Cese o cambio de puesto de trabajo.	SI	Recursos Humanos y el Departamento de Tecnologías de la Información deberán coordinar las diferentes acciones al cese de actividad de un trabajador.
Dominio	8. GESTIÓN DE ACTIVOS.		
Objetivo	8.1 Responsabilidad sobre los activos.		
Control	8.1.1 Inventario de activos.	SI	Todos los activos de información, procesos y servicios deben ser inventariados.
Control	8.1.2 Propiedad de los activos.	SI	Todo activo debe tener un propietario asignado.
Control	8.1.3 Uso aceptable de los activos.	SI	Se necesita políticas y normas para uso aceptable de activos.

Control	8.1.4 Devolución de activos.	SI	Se debe implementar controles para la devolución de activos.
Objetivo	8.2 Clasificación de la información.		
Control	8.2.1 Directrices de clasificación.	SI	La información se clasificará mediante directrices establecidas en la Política de Activos de Información.
Control	8.2.2 Etiquetado y manipulado de la información.	SI	Toda la información debe ser etiquetada bajo la Política de Activos de Información.
Control	8.2.3 Manipulación de activos.	SI	Los activos tienen reglas para su manejo de acuerdo al nivel de clasificación.
Objetivo	8.3 Manejo de los soportes de almacenamiento.		
Control	8.3.1 Gestión de soportes extraíbles.	SI	Deben existir normas sobre los soportes extraíbles de acuerdo a la necesidad organizacional.
Control	8.3.2 Eliminación de soportes.	SI	La eliminación de soportes debe basarse en procedimientos formales.
Control	8.3.3 Soportes físicos en tránsito.	SI	Para el traslado de soportes físicos de información se necesita reglas de seguridad.
Dominio	9. CONTROL DE ACCESOS.		
Objetivo	9.1 Requisitos de negocio para el control de accesos.		
Control	9.1.1 Política de control de accesos.	SI	Todos el personal requiere seguir la Política de Control de Acceso aprobada por la dirección.
Control	9.1.2 Control de acceso a las redes y servicios asociados.	SI	Existe una política de acceso a las redes organizacionales.
Objetivo	9.2 Gestión de acceso de usuario.		
Control	9.2.1 Gestión de altas/bajas en el registro de usuarios.	SI	Se debe gestionar un proceso formal de altas y bajas de usuarios.
Control	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	SI	Es necesario gestionar el proceso de autorización de acceso a los recursos del SGSI.
Control	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	SI	Todos los sistemas de información necesitan privilegios de acceso a información de los usuarios.
Control	9.2.4 Gestión de información confidencial de autenticación de usuarios.	SI	Toda clave o dispositivo de acceso es personal e intransferible.
Control	9.2.5 Revisión de los derechos de acceso de los usuarios.	SI	Periódicamente se debe revisar los derechos de acceso de los usuarios.
Control	9.2.6 Retirada o adaptación de los derechos de acceso	SI	Todos los accesos deben ser suspendidos a los usuarios que terminan su relación laboral con la universidad.
Objetivo	9.3 Responsabilidades del usuario.		
Control	9.3.1 Uso de información confidencial para la autenticación.	SI	Todos los usuarios son responsables de la confidencialidad de sus claves de acceso.

Objetivo	9.4 Control de acceso a sistemas y aplicaciones.		
Control	9.4.1 Restricción del acceso a la información.	SI	El Sistema Nacional Académico, Sistema Nacional Financiero, Sistema Nacional de Recursos Humanos, correo electrónico y ambientes virtuales de aprendizaje deben gestionar los accesos según privilegios y autorizaciones de uso.
Control	9.4.2 Procedimientos seguros de inicio de sesión.	SI	Uso de contraseñas y comunicaciones cifradas donde la Política de Control de Acceso lo determine necesario.
Control	9.4.3 Gestión de contraseñas de usuario.	SI	Los usuarios deben utilizar contraseñas fuertes, un sistema debe apoyarlos en la elección de una clave fuerte.
Control	9.4.4 Uso de herramientas de administración de sistemas.	SI	Los sistemas críticos son fuertemente restringidos y controlados.
Control	9.4.5 Control de acceso al código fuente de los programas	SI	El repositorio de códigos fuentes necesita autenticación.
Dominio	10. CIFRADO.		
Objetivo	10.1 Controles criptográficos.		
Control	10.1.1 Política de uso de los controles criptográficos.	SI	Existen redes VPN, por lo que la política es necesaria.
Control	10.1.2 Gestión de claves.	SI	Ninguna clave debe guardarse en texto plano y se debe utilizar criptografía para protegerlas.
Dominio	11. SEGURIDAD FÍSICA Y AMBIENTAL.		
Objetivo	11.1 Áreas seguras.		
Control	11.1.1 Perímetro de seguridad física.	SI	Existe la necesidad de perímetros en el centro de procesamiento de datos y diferentes área de acceso restringido.
Control	11.1.2 Controles físicos de entrada.	SI	Ingreso al parqueadero mediante tarjeta magnética, control de acceso mediante tarjeta magnética al CDP.
Control	11.1.3 Seguridad de oficinas, despachos y recursos.	SI	Videovigilancia en todas las zonas internas.
Control	11.1.4 Protección contra las amenazas externas y ambientales.	SI	La matriz y las sedes se encuentran en zonas susceptibles de inundación y terremotos.
Control	11.1.5 El trabajo en áreas seguras.	SI	Se debe definir los procedimientos de trabajo en áreas seguras.
Control	11.1.6 Áreas de acceso público, carga y descarga.	SI	Los proveedores deben utilizar áreas carga y descarga.
Objetivo	11.2 Seguridad de los equipos.		
Control	11.2.1 Emplazamiento y protección de equipos.	SI	Los equipos y activos deben llevar salvaguardas de acuerdo a la Política de Activos de Información.

Control	11.2.2 Instalaciones de suministro.	SI	La protección eléctrica y continuidad de suministro se debe garantizar a nivel de los servicios críticos.
Control	11.2.3 Seguridad del cableado.	SI	Uso de cableado estructurado en todos los edificios para evitar intercepciones, interferencia y daños.
Control	11.2.4 Mantenimiento de los equipos.	SI	Los equipos deben ser sometidos a mantenimientos periódicos para garantizar su disponibilidad e integridad.
Control	11.2.5 Salida de activos fuera de las dependencias de la empresa.	SI	Todos los activos deben tener medidas según su clasificación para salir de la universidad.
Control	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	SI	Según el nivel de clasificación de la información que contiene cada equipo se debe definir las salvaguardas necesarias.
Control	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	SI	Todos los equipos que se vayan a reutilizar deben ser sometidos a procesos de revisión y borrado para evitar filtraciones de información confidencial.
Control	11.2.8 Equipo informático de usuario desatendido.	SI	Debe existir controles para los equipos desatendidos.
Control	11.2.9 Política de puesto de trabajo despejado y de pantalla limpia.	SI	Es necesario una política de uso correcto de equipos.
Dominio	12. SEGURIDAD EN LA OPERATIVA.		
Objetivo	12.1 Responsabilidades y procedimientos de operación.		
Control	12.1.1 Documentación de procedimientos de operación.	SI	Todo proceso debe estar documentado.
Control	12.1.2 Gestión de cambios.	SI	En el desarrollo de software existe un detallado sistema de control de cambios.
Control	12.1.3 Gestión de capacidades.	SI	El rendimiento del equipo y su capacidad debe ser monitoreada para garantizar un alto rendimiento.
Control	12.1.4 Separación de entornos de desarrollo, prueba y producción.	SI	Existe el área de desarrollo, pruebas y producción.
Objetivo	12.2 Protección contra código malicioso.		
Control	12.2.1 Controles contra el código malicioso.	SI	Uso de antivirus y actualizaciones automáticas en un servidor centralizado.
Objetivo	12.3 Copias de seguridad.		
Control	12.3.1 Copias de seguridad de la información.	SI	Existen backups de la base de datos diarios, mediante cintas.
Objetivo	12.4 Registro de actividad y supervisión.		
Control	12.4.1 Registro y gestión de eventos de actividad.	SI	Los servicios críticos están sometidos a monitoreo constante.
Control	12.4.2 Protección de los registros de información.	SI	Los logs de los diferentes servicios y aplicaciones deben ser protegidos.

Control	12.4.3 Registros de actividad del administrador y operador del sistema.	SI	Los logs se gestionan en todos los equipos críticos.
Control	12.4.4 Sincronización de relojes.	SI	Se utiliza NTP para sincronizar toda la infraestructura y para registrar todas las transacciones de los usuarios.
Objetivo	12.5 Control del software en explotación.		
Control	12.5.1 Instalación del software en sistemas en producción.	SI	Los equipos en producción son controlados por explotación.
Objetivo	12.6 Gestión de la vulnerabilidad técnica.		
Control	12.6.1 Gestión de las vulnerabilidades técnicas.	SI	Todas las vulnerabilidades deben ser gestionadas.
Control	12.6.2 Restricciones en la instalación de software.	SI	Debe existir un conjunto de reglas para instalación de software.
Objetivo	12.7 Consideraciones de las auditorías de los sistemas de información.		
Control	12.7.1 Controles de auditoría de los sistemas de información.	SI	Es necesario planear auditorías periódicas.
Dominio	13. SEGURIDAD EN LAS TELECOMUNICACIONES.		
Objetivo	13.1 Gestión de la seguridad en las redes.		
Control	13.1.1 Controles de red.	SI	El acceso a las redes internas de la universidad debe ser autorizado y controlado.
Control	13.1.2 Mecanismos de seguridad asociados a servicios en red.	SI	Los diferentes servicios de red deben ser autorizados.
Control	13.1.3 Segregación de redes.	SI	Las redes deberán estar claramente segmentadas.
Objetivo	13.2 Intercambio de información con partes externas.		
Control	13.2.1 Políticas y procedimientos de intercambio de información.	SI	Verificar procedimientos regulados por los entes de control de la educación superior del Ecuador.
Control	13.2.2 Acuerdos de intercambio.	SI	Existen acuerdos con Microsoft y Amazon.
Control	13.2.3 Mensajería electrónica.	SI	La universidad tiene un sistema de correo electrónico.
Control	13.2.4 Acuerdos de confidencialidad y secreto	SI	Todas las partes externas firman acuerdos de confidencialidad.
Dominio	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		
Objetivo	14.1 Requisitos de seguridad de los sistemas de información.		
Control	14.1.1 Análisis y especificación de los requisitos de seguridad.	SI	La seguridad está implementada en todo el SDLC.

Control	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	SI	Se utiliza comunicaciones cifradas en redes públicas.
Control	14.1.3 Protección de las transacciones por redes telemáticas.	SI	Todas las transacciones deben ser seguras.
Objetivo	14.2 Seguridad en los procesos de desarrollo y soporte.		
Control	14.2.1 Política de desarrollo seguro de software.	SI	Se requiere una política de desarrollo aprobado por la dirección.
Control	14.2.2 Procedimientos de control de cambios en los sistemas.	SI	Todo cambio es documentado y se le da el seguimiento posterior.
Control	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	SI	Soporte se encargará de verificar que no existen incompatibilidades de hardware o software.
Control	14.2.4 Restricciones a los cambios en los paquetes de software.	SI	Todos los paquetes de software deben tener un control de cambios.
Control	14.2.5 Uso de principios de ingeniería en protección de sistemas.	SI	Se debe utilizar principios de ingeniería para seguridad de sistemas.
Control	14.2.6 Seguridad en entornos de desarrollo.	SI	Los entornos de desarrollo deben garantizar la seguridad de la información.
Control	14.2.7 Externalización del desarrollo de software.	SI	Los desarrolladores externos deben firmar acuerdos de confidencialidad.
Control	14.2.8 Pruebas de seguridad de los sistemas.	SI	Es necesario probar la seguridad de los sistemas de información.
Control	14.2.9 Pruebas de aceptación.	SI	Se debe establecer criterios para testear el software.
Objetivo	14.3 Datos de prueba.		
Control	14.3.1 Protección de los datos utilizados en pruebas.	SI	Los datos para pruebas siguen estrictas políticas de confidencialidad.
Dominio	15. RELACIONES CON SUMINISTRADORES.		
Objetivo	15.1 Seguridad de la información en las relaciones con suministradores.		
Control	15.1.1 Política de seguridad de la información para suministradores.	SI	Debe existir políticas para Desarrollo Externo aprobadas por la dirección.
Control	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	SI	Los proveedores deben realizar contratos que contemplen el riesgo y sean parte de la gestión del mismo.
Control	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	SI	Se debe negociar cadenas de suministro con los proveedores.
Objetivo	15.2 Gestión de la prestación del servicio por suministradores.		

Control	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	SI	Se debe monitorizar los diferentes servicios de terceros, conectividad, ancho de banda.
Control	15.2.2 Gestión de cambios en los servicios prestados por terceros.	SI	Se debe firmar contratos que contemplen cualquier cambio en la calidad de servicio de los proveedores.
Dominio	16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.		
Objetivo	16.1 Gestión de incidentes de seguridad de la información y mejoras.		
Control	16.1.1 Responsabilidades y procedimientos.	SI	La política debe definir todos los roles en la gestión de incidentes.
Control	16.1.2 Notificación de los eventos de seguridad de la información.	SI	La Política de Gestión de Incidentes determina los procedimientos de notificación.
Control	16.1.3 Notificación de puntos débiles de la seguridad.	SI	Existen procedimientos claros de comunicación de puntos débiles.
Control	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	SI	Se debe gestionar el riesgo para evaluar los diferentes eventos de seguridad.
Control	16.1.5 Respuesta a los incidentes de seguridad.	SI	Se necesita procedimientos de respuesta a incidentes de seguridad.
Control	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	SI	Se debe analizar los incidentes para retroalimentar el aprendizaje de los mismos.
Control	16.1.7 Recopilación de evidencias.	SI	Debe existir procedimientos de recolección de evidencias.
Dominio	17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DELA CONTINUIDAD DEL NEGOCIO.		
Objetivo	17.1 Continuidad de la seguridad de la información.		
Control	17.1.1 Planificación de la continuidad de la seguridad de la información.	SI	Debe existir un Plan de Continuidad de la Seguridad de la Información.
Control	17.1.2 Implantación de la continuidad de la seguridad de la información.	SI	La universidad debe proveer de procedimientos y controles que aseguren el nivel de continuidad de seguridad de la información.
Control	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Se debe evaluar y revisar periódicamente los planes de continuidad de la seguridad de la información.
Objetivo	17.2 Redundancias.		
Control	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	SI	Los servidores e infraestructura crítica implementan redundancias a nivel físico y lógico.
Dominio	18. CUMPLIMIENTO.		

Objetivo	18.1 Cumplimiento de los requisitos legales y contractuales.		
Control	18.1.1 Identificación de la legislación aplicable.	SI	Todos los controles deben estar identificados y documentados.
Control	18.1.2 Derechos de propiedad intelectual (DPI).	SI	Todo desarrollo, configuración y documentación es propiedad intelectual de la UPS
Control	18.1.3 Protección de los registros de la organización.	SI	Toda la información académica y financiera debe ser protegida contra perdida, destrucción y falsificación.
Control	18.1.4 Protección de datos y privacidad de la información personal.	SI	En Ecuador no existe legislación sobre los datos personales, pero es una tendencia mundial y es muy conveniente considerar parámetros mínimos de privacidad.
Control	18.1.5 Regulación de los controles criptográficos.	SI	La universidad al tener sus propios servidores, intercambia información con terceros por lo que utiliza encriptación bajo las normas y regulaciones vigentes.
Objetivo	18.2 Revisiones de la seguridad de la información.		
Control	18.2.1 Revisión independiente de la seguridad de la información.	SI	Es necesario un equipo de Auditoría Interna.
Control	18.2.2 Cumplimiento de las políticas y normas de seguridad.	SI	Se debe implementar la mejora contínua mediante auditorías internas.
Control	18.2.3 Comprobación del cumplimiento.	SI	Se debe evaluar y comprobar el estado de cumplimiento mediante auditorías internas.

2 CAPÍTULO 3: ANÁLISIS DE RIESGOS

De acuerdo al anexo 06 Metodología de Análisis de Riesgos se procedió a caracterizar los activos de la UPS. Es importante identificar las salvaguardas que tiene implementadas la UPS, para disminuir la frecuencia del impacto de las diferentes amenazas.

2.1 INVENTARIO DE ACTIVOS

Se ha caracterizado los activos según MAGERIT, utilizando la clasificación del punto 7 del anexo 06. A cada activo se le ha asignado su respectivo propietario quien ha proporcionado el valor del mismo para la organización.

Código activo	Denominación	Descripción	Caracterización	Propietario	Observación
I-001	Información académica	Información acerca de estudiantes y docentes, datos personales de los mismos, calificaciones, distributivos, horarios.	[inf] Información	Vicerrector Docente	[essential] Activo esencial para la UPS
I-02	Información Talento Humano	Información de contratos laborales, sueldo, nóminas, datos personales del personal.	[inf] Información	Secretario Técnico de Recursos Humanos	[essential] Activo esencial para la UPS
I-003	Información financiera	Información de balances, cuentas, presupuestos, etc.	[inf] Información	Secretario Técnico de Finanzas	[essential] Activo esencial para la UPS
S-001	Sistema Nacional Académico (SNA)	Sistema de información para el control de: • Inscripciones • Matrículas • Calificaciones • Paracademicos • Resoluciones • Bienestar Estudiantil • Interface financiera • Evaluación Docente • Trabajos de grado	[service] Servicio	Vicerrector Docente	[essential] Activo esencial para la UPS
S-002	Sistema Nacional de Recursos Humanos	Sistema de información para el control de: • Nómina • Distributivos • Contratos • Acciones de personal • Remuneraciones	[service] Servicio	Secretario Técnico de Recursos Humanos	[essential] Activo esencial para la UPS
S-003	Sistema Nacional Financiero	Sistema de información para el control de: • Activos fijos • Adquisiciones • Clientes • Conciliación bancaria • Contabilidad • Control pagos • Facturación • Flujo Caja • Inventarios	[service] Servicio	Secretario Técnico de Finanzas	[essential] Activo esencial para la UPS
S-004	AVAC	Servicio de Ambientes Virtuales de Aprendizaje Cooperativo: • Toma de evaluaciones • Envío de trabajos • Material docente • Foros académicos • Chats académicos	[service] Servicio	Vicerrector Docente	[essential] Activo esencial para la UPS

		• Material Docente			
D-001	Datos del SNA, SIGAC y SQUAD	Base de Datos ORACLE Standar Edition 11g VER 11.2.0.2	[D] Datos	DBA	[essential] Activo esencial para la UPS
D-002	Datos del AVAC	Base de Datos MySQL Server 5.0.77	[D] Datos	Docentes	
D-003	Datos institucionales	Ficheros de reglamentos, normas, leyes, resoluciones de los diferentes órganos universitarios	[D] Datos	DBA	Ficheros [file] Datos de Gestión interna [int]
D-004	Código Fuentes	Códigos fuente de los sitemas internos (SNA, SQUAD, SIGAC) y aplicaciones desarrolladas internamente	[D] Datos	Coordinador de Explotación	[source]
D-005	Backups	Copias de respaldo	[D] Datos		Backups [backup]
D-006	Logs	Registros de los diferentes servidores	[D] Datos	Coordinador de Infraestructura y Redes / Coordinador de red	[logs]
K-001	Certificados de clave pública X509	Claves de firmas digitales de autoridades, claves de VPN, certificados de HTTPS	[K] Claves criptográficas	Responsable de Seguridad de la Información	
S-005	Internet	Servicio contratado al Proveedor CEDIA con soporte técnico de TELCONET.	[S] Servicios Generales	Director de Departamento de TIC	
S-006	Correo electrónico	Correo con dominio institucional ups.edu.ec, Este servicio es externo proporcionado por Microsoft	[S] Servicios Generales	Director de Departamento de TIC	[email]
S-007	Portal Web	Es un espacio de difusión e Imagen Institucional al mundo, en la promoción de sus publicaciones, eventos y noticias.	[S] Servicios Generales	Secretario Técnico de Comunicación	[www]
S-008	Proxy	Servicio de proxy para distribuir el internet en toda la universidad	[S] Servicios Generales	Administrador de Redes y Comunicaciones	
S-009	Almacenamiento de Ficheros	Servidor de Ficheros Windows Server 2008 R2 Enterprise (virtualizado)	[S] Servicios Generales	Coordinador de Infraestructura y Redes	[file]
S-010	Servicio de gestión de identidades	Servidor CAS	[S] Servicios Generales	Coordinador de Infraestructura y Redes	[CAS]
S-011	Servicios Web Docentes	Muestra al docente diferentes recursos disponibles por la Universidad en la Web	[S] Servicios Generales	Vicerrector Docente	
S-012	Servicios Web Estudiantes	Muestra al estudiante diferentes recursos disponibles por la Universidad en la Web	[S] Servicios Generales	Vicerrector Docente	
S-013	Servicio de Antivirus	Aplicación F-Secure centralizada	[S] Servicios Generales	Responsable de Seguridad de la Información	[av] Antivirus
S-014	Sistema de Gestión Documental	Servidor Quipux	[S] Servicios Generales	Secretario Técnico de Gestión Documental	
S-015	Servicio de Directorio	Servidor de Active Directory	[S] Servicios Generales	Administrador de Redes y Comunicaciones	[dir] Servidor de Directorio
S-016	Telefonía IP	Servicio de telefonía Interna/externa entre los campus de la Universidad	[S] Servicios Generales	Administrador de Redes y Comunicaciones	
S-017	Enlaces WAN	Servicios contratados a terceros (CNT y TELCONET) que garantiza conectividad entre las diferentes Sedes de la UPS. Situación que permite el acceso a la información que reside en la ciudad de Cuenca	[S] Servicios Generales	Director de Departamento de TIC	
S-018	Videoconferencia	Permite el desarrollo de reuniones virtuales en diferentes áreas geográficas, promoviendo la comunicación interna/externa de la comunidad universitaria	[S] Servicios Generales	Administrador de Redes y Comunicaciones	
S-019	WIFI	Permite la conectividad en todos los campus	[S] Servicios	Administrador	

		y acceso a internet	Generales	de Redes y Comunicaciones	
S-020	Repositorio Digital Académico	Servidor D-Space, que permite la gestión de tesis, revistas, e-books.	[S] Servicios Generales	Dirección de bibliotecas	
S-021	Pagos en línea	Aplicación externa gestionada por VISA	[S] Servicios Generales	Director de Departamento de TIC	
S-022	Servicio de copias de seguridad	Servidor IBM-Tivoli que permite respaldar la información.	[S] Servicios Generales	DBA	
SW-001	Sistemas Operativos de Servidor	• GNU/Linux Centos5.8 Centos5.7 Centos5.6 Centos5.5 Centos5.3 • Red Hat Enterprise Linux Server 5.7 • IBM AIX 5.3 • Windows Server Enterprise 2008 R2 X64 • Windows Server Enterprise 2003 R2 X64	[SW] Software	Coordinador de Infraestructura y Redes	[os] Sistema Operativo
SW-002	Sistemas Operativos usuarios	Sistemas operativos instalado en todos los equipos de docentes y personal administrativo: • Windows Profesional 7 • Windows Profesional 8 • Windows Profesional 8.1	[SW] Software	Director de Departamento de TIC	[os] Sistema Operativo
SW-003	Antivirus	F-Secure	[SW] Software	Director de Departamento de TIC	
SW-004	Ofimática	Utilitarios como Microsoft Office, Microsoft Visio, Microsoft Project	[SW] Software	Director de Departamento de TIC	
SW-005	Software Académico	Aplicaciones y programas de carácter académico para todas las carreras de Grado y programas de Posgrado que se instala en los diferentes laboratorios de la UPS	[SW] Software	Director de Departamento de TIC	[acad_sw]
SW-006	Sistema Gestor de Base de Datos	Oracle Standar Edition 11g VER 11.2.0.2	[SW] Software	Director de Departamento de TIC	[dbms]
SW-007	Software de Desarrollo	JAVA, JSP, JPA 2.0 (Hibernate 3), JSF 2.0, JS, CSS, WebServices (Axis), RICHFACES, Oracle forms 10G, Oracle reports 10G, PHP, EJB 3.1	[SW] Software	Coordinador de Desarrollo de Software	[des_sw]
HW-001	Servidores DataCenter Matriz Cuenca	• Servidor BLADE HS21 • Servidor BLADE HS22 • IBM System x3500 M3 • IBM X3550 M2 INTEL XEON 2.4 GHZ, 8GB RAM HD 500 GB • IBM X3550 M2 INTEL XEON 2.4 GHZ, 48GB RAM HD 1TB GB SERVER VMWARE ESXI 5.0 • Intel_Xeon3.00GHz/500GB/2GB/NA • Intel_Xeon3.00GHz/500GB/4GB/NA • Intel_Xeon3.00GHz/2TB/8GB/NA • Intel_Xeon3.00GHz/2TB/16GB/NA • IBM-Tivoli (Robot de copias de seguridad) • Quad Core Xeon E5410 Processor2x6MB Cache/ 750G/ 4G/ Dell PowerEdge2950 • Dual core XEON/ 75 G, 75 G/ 2 Gb/ Dell PowerEdge 2850 • Intel Xeon_E5530_2.40GHz/24Gb System x3500	[HW] Hardware	Coordinador de Infraestructura y Redes	
HW-002	Servidores CDP Quito campus El Giron	• Servidor BLADE HS21 • Servidor BLADE HS22 • Intel_Xeon3.60GHz/2X136,72GB/4GB/NA	[HW] Hardware	Director de TIC (Quito)	

		DL-380G4 • Intel Xeon_X5650_2,67GHz/2TB/8GB/ DL-380G7 • Intel_Xeon3.00GHz/500GB/2GB/NA • Intel_Xeon3.00GHz/2X34,14GB/2GB/NA • Intel_DualCore3.0GHz/160GB/4GB/NA • Intel_PIV 3.0GB/160GB/2GB/ • Intel_Core2Duo2.6GHz/320GB/2GB/NA • Quad Core Xeon E5410 Processor2x6MB Cache/ 750G/ 4G/ Dell PowerEdge2950 • Dual core XEON/ 75 G, 75 G/ 2 Gb/ Dell PowerEdge 2850 • Intel Xeon_E5530_2.40GHz/24Gb System x3500			
HW-003	Servidores CDP Quito campus Kennedy	• IBM X3500 M2 INTEL XEON 2.4 GHZ, 2GB RAM HD 250GB • INTEL XEON PIV 3 GHZ (2 PROCESADORES), 2GB RAM, 2 DISCO • INTEL PENTIUM D 3.4 GHZ, 3 GB RAM, 1 HD 250 GB	[HW] Hardware	Director de TIC (Quito)	
HW-004	Servidores CDP Quito campus Sur	• IBM X3550 M2 INTEL XEON 2.4 GHZ, 8GB RAM HD 500 GB • IBM X3550 M2 INTEL XEON 2.4 GHZ, 48GB RAM HD 500 GB SERVER VMWARE ESXI 5.0	[HW] Hardware	Director de TIC (Quito)	
HW-005	Servidores CDP Guayaquil	• HS21 Blade Server • IBM BladeCenter HS22 • IBM System x3500 M3 • HP Proliant ML150 G6	[HW] Hardware	Director de TIC (Guayaquil)	
HW-006	Telefonía IP	Cuenca: • (3) Intel Celeron 3.20GHz/149,05GB/2GB Quito campus El Girón: • (3) Intel Celeron 3.20GHz/149,05GB/2GB Quito campus Kennedy: • (2) Intel Celeron 3.20GHz/149,05GB/2GB Quito campus Sur: • (1) Intel Celeron 3.20GHz/149,05GB/2GB Guayaquil: • (2) Intel Celeron 3.20GHz/149,05GB/2GB	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-007	Videoconferencia	Infraestructura Polycom Cuenca: • Servidor Polycom • 4 Salas equipadas Quito campus El Girón: • 6 Salas equipadas Quito campus Kennedy: • 1 Sala equipada Quito campus Sur: • 1 Sala equipada Guayaquil: • 2 Salas equipadas	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-008	PC-Administrativos	500 Equipos	[HW] Hardware	Coordinador de Soporte Técnico	
HW-009	PC-Portátiles Docentes	1200 Equipos, los docentes reciben siempre un equipo portátil	[HW] Hardware	Coordinador de Soporte Técnico	
HW-010	PC-Desarrollo	30 Equipos portátiles	[HW] Hardware	Coordinador de Desarrollo de Software	
HW-011	PC-Portátiles Administrativos	200 portátiles. Las autoridades, directores departamentales y coordinadores reciben un equipo portátil	[HW] Hardware	Coordinador de Soporte Técnico	
HW-012	Red WAN	CISCO 6509-E (redundancia de equipo)	[HW] Hardware	Coordinador de	

		Switch core		Infraestructura y Redes	
HW-013	Backbone LAN	Cada sede cuenta con chasis y switches: • CISCO Catalyst 6500 Series • Catalyst 3560 E (equipo con redundancia)	[HW] Hardware	Coordinador de Infraestructura y Redes	
HW-014	Firewall	CISCO ASA (Equipo con redundancia)	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-015	Router WAN	CISCO 3845	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-016	LAN Cuenca	Conjunto de switches, routers y el respectivo cableado para la sede Cuenca	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-017	LAN Quito	Conjunto de switches, routers y el respectivo cableado para la sede Quito	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-018	LAN Guayaquil	Conjunto de switches, routers y el respectivo cableado para la sede Guayaquil	[HW] Hardware	Administrador de Redes y Comunicaciones	
HW-019	Impresoras	400 impresoras a nivel nacional	[HW] Hardware	Coordinador de Soporte Técnico	
COM-001	Teléfonos IP	Equipos CISCO para telefonía IP	[COM] Redes de comunicaciones	Coordinador de Soporte Técnico	
COM-002	WIFI	Access Point para dar conectividad WIFI	[COM] Redes de comunicaciones	Administrador de Redes y Comunicaciones	
COM-003	WAN	Enlaces dedicados redundantes que mantienen la conectividad de las tres sedes	[COM] Redes de comunicaciones	Coordinador de Infraestructura y Redes	
COM-004	LAN Cuenca	Configuraciones de los diferentes equipos red, estructura, VLANS, etc. de la sede Cuenca	[COM] Redes de comunicaciones	Administrador de Redes y Comunicaciones	
COM-005	LAN Quito	Configuraciones de los diferentes equipos red, estructura, VLANS, etc. de la sede Quito	[COM] Redes de comunicaciones	Administrador de Redes y Comunicaciones	
COM-006	LAN Guayaquil	Configuraciones de los diferentes equipos red, estructura, VLANS, etc. de la sede Guayaquil	[COM] Redes de comunicaciones	Administrador de Redes y Comunicaciones	
COM-007	VPN	Configuraciones y Software para realizar conexiones VPN	[COM] Redes de comunicaciones	Administrador de Redes y Comunicaciones	
M-001	Backups	Cintas magnéticas de respaldos de: bases de datos institucional, servidor de archivos, configuraciones de servidores, plataforma virtual, fuentes y ejecutables, configuraciones de proxy, CAS, datos del portal institucional, configuraciones de Quipux, base de datos Quipux, base de datos de Biblioteca	[M] Media	Asistente de DBA	[backup]
M-002	Documentación Administrativa UPS	Documentación Interna de la UPS impresa en papel: Contratos, facturas, currículos, etc.	[M] Media	Secretaría General	[printed]
M-003	Documentación Académica UPS	Documentación académica de la UPS impresa en papel: Record académicos, carpetas personales de estudiantes, actas de los diferentes Consejos.	[M] Media	Secretaría de Campus	[printed]
M-004	Documentación Técnica	Manuales de usuarios, procedimientos, configuraciones	[M] Media	Director de Departamento TIC	[printed]
AUX-001	Generadores Eléctricos	Generador eléctrico en Cuenca y Guayaquil	[AUX] Equipamiento Auxiliar	Coordinador de Soporte Técnico	
AUX-002	Destructores de papel	Existen 200 Destructoras de papel en Cuenca, Quito y Guayaquil	[AUX] Equipamiento Auxiliar	Coordinador de Soporte Técnico	
L-001	Sede Matriz	Edificios: Cornelio Merchán, Mario Ritzini,	[L] Instalaciones	Vicerrector de	

		Guillermo Mensi, Rectorado		Sede	
L-002	Sede Quito	Edificios: Bloque A, Bloque B, Kennedy, Sur	[L] Instalaciones	Vicerrector de Sede	
L-003	Sede Guayaquil	Edificios: Domingo Comín, La Joya, Centenario	[L] Instalaciones	Vicerrector de Sede	
L-004	Data Center Cuenca	Centro de procesamiento de datos Cuenca	[L] Instalaciones	Director de TIC	
L-005	CDP Quito	Centro de procesamiento de datos Quito	[L] Instalaciones	Director de TIC	
L-006	CDP Guayaquil	Centro de procesamiento de datos Guayaquil	[L] Instalaciones	Director de TIC	
P-001	Dirección	Rector, Vicerrector Docente, Vicerrector Académico General, Vicerrectores de Sede, Secretarías Técnicas	[P] Personal	Rector	
P-002	Director de TIC	Director del Departamental de Tecnologías de la Información y Comunicación	[P] Personal	Dirección	
P-003	Departamento de TIC	Coordinador de Infraestructura y Redes Administrador de Redes y Comunicaciones DBA Coordinador de Desarrollo de Software	[P] Personal	Director de TIC	
P-004	Personal de Desarrollo	Programadores Junior Programadores Senior	[P] Personal	Coordinador de Desarrollo de Software	
P-005	Usuarios Internos	Personal Administrativo	[P] Personal	Dirección	
P-006	Docentes	Personal Académico	[P] Personal	Vicerrector Docente	
P-007	Estudiantes	Estudiantes de la Universidad	[P] Personal	Vicerrector de Sede	

Tabla 2.1 Identificación de activos

2.2 VALORACIÓN DE LOS ACTIVOS

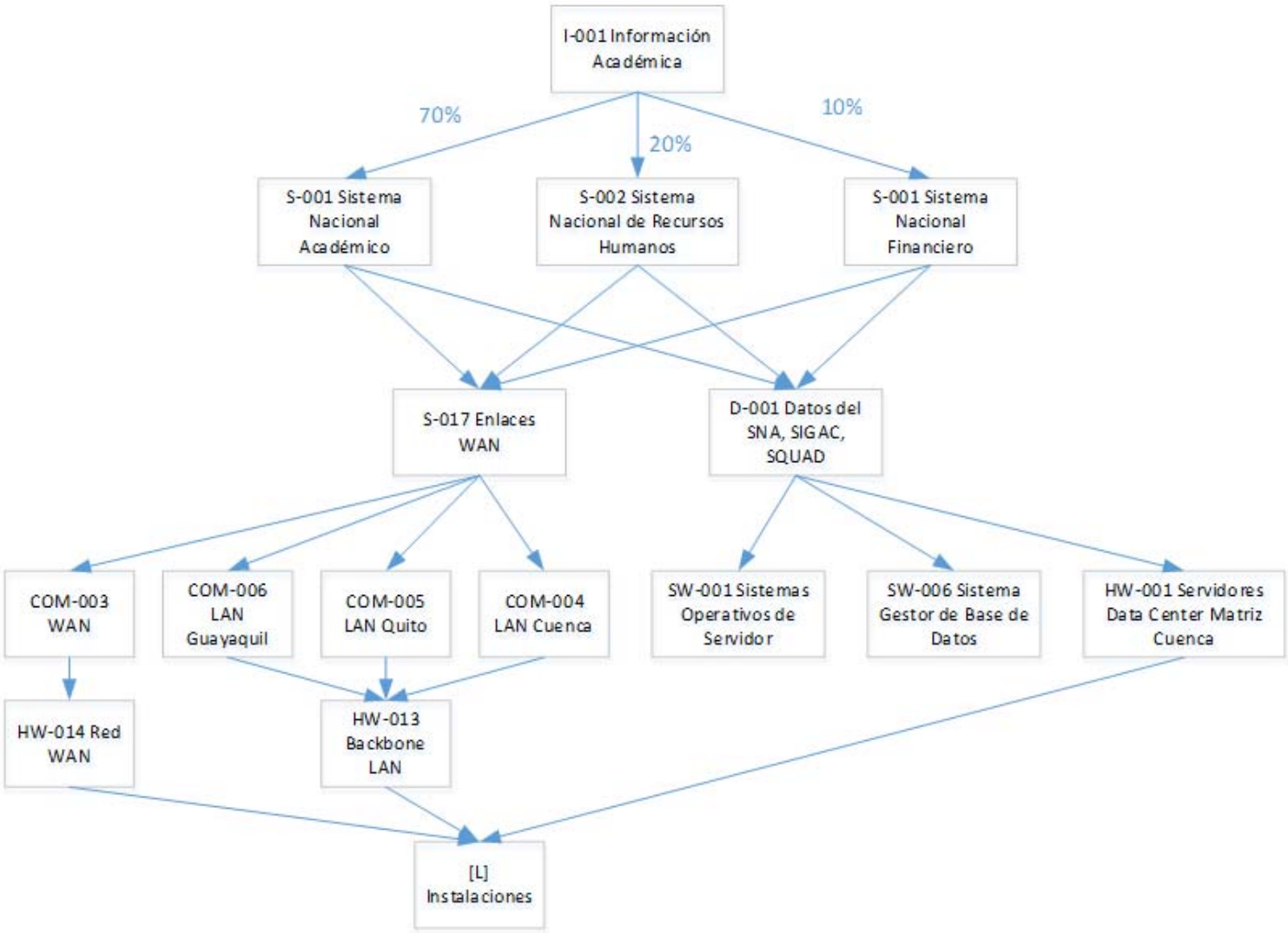
A los activos se les asignó una valoración basada principalmente en su valor económico o costo de reposición y se consideró la relación de los activos esenciales (información [inf], servicios [service] y la base de datos [D]) que por su naturaleza no tienen una valoración económica fácil de cuantificar porque dependen de aspectos intangibles.

2.2.1 ANÁLISIS DE DEPENDENCIAS DE ACTIVOS

La UPS cuenta con cinco activos esenciales, los cuales son el soporte de todo el negocio, estas características conllevan a que se realice un análisis de dependencia de cada uno de estos activos esenciales.

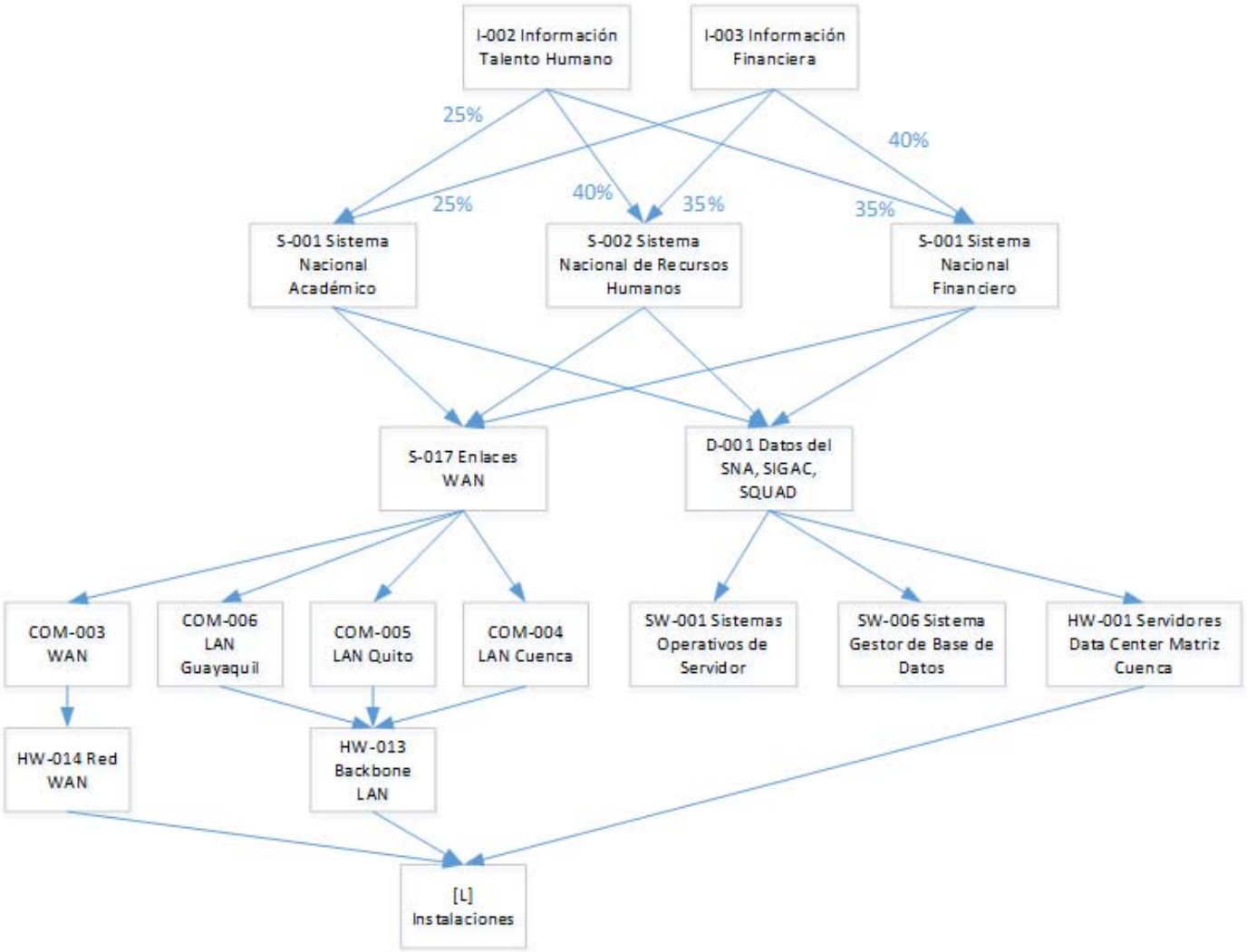
2.2.1.1 Dependencias del activo I-001

La información académica es el principal activo de la UPS, el negocio de la universidad gira en torno a la información académica. Los organismos de control de la educación superior ecuatoriana requieren de esta información para procesos de evaluación y acreditación.



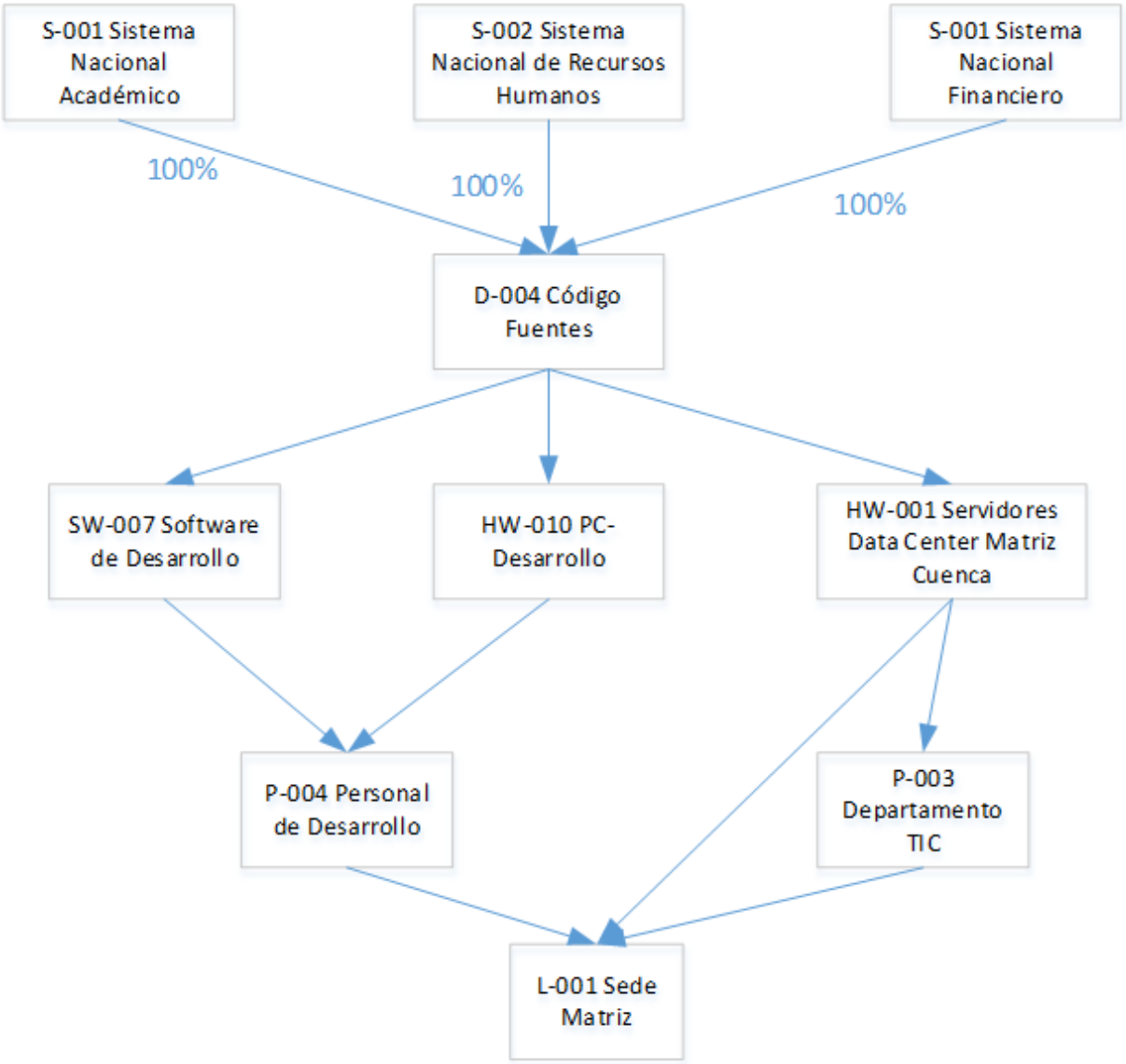
2.2.1.2 Dependencias del activo I-002 e I-003

No menos importantes es la información del Talento Humano y Financiera, se realiza el árbol de dependencias simultáneo de estos dos activos porque son la información que complementa a la información académica, existe una estrecha relación entre academia-talento humano-finanzas que permiten la gestión eficiente de toda la universidad.



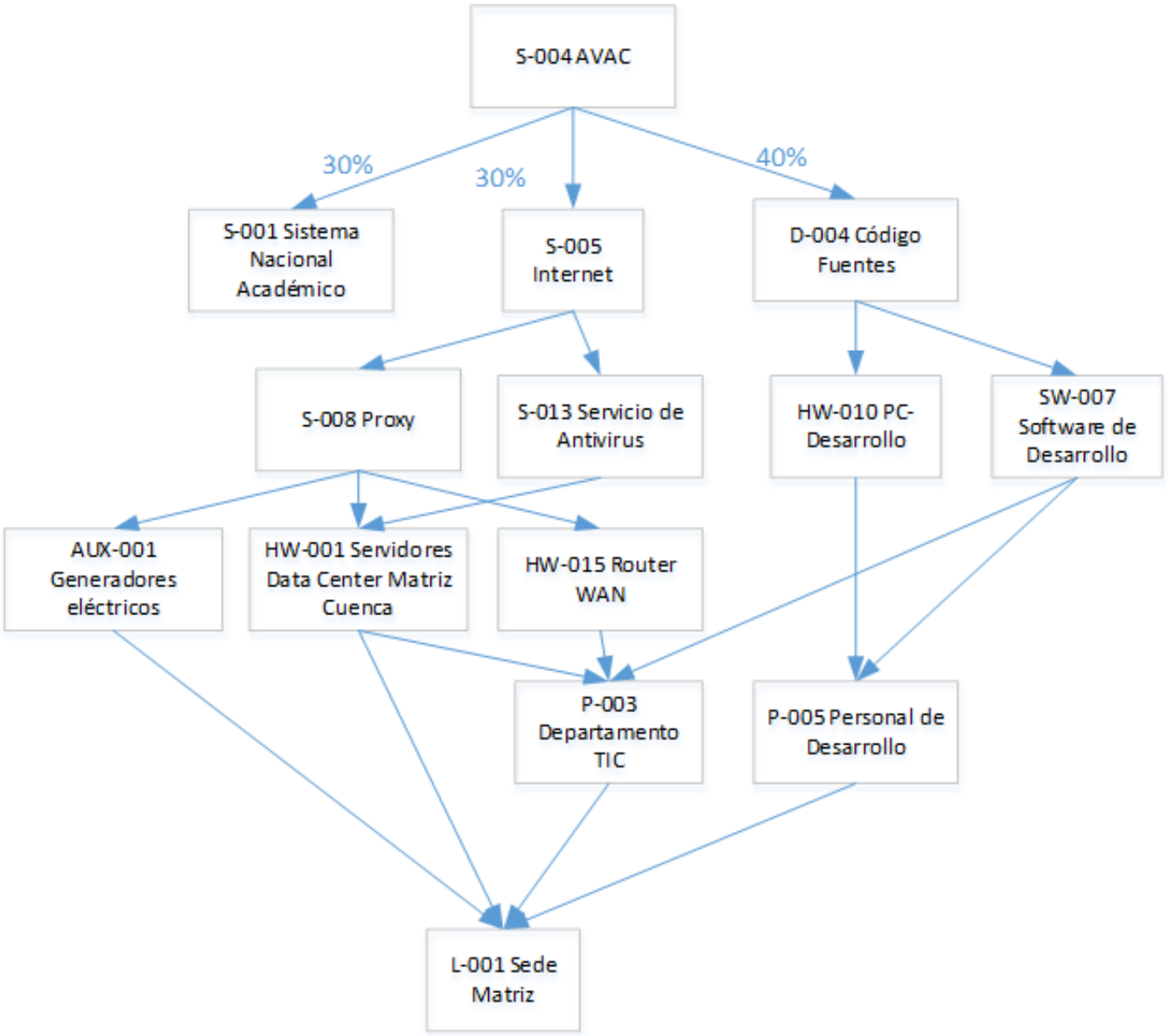
2.2.1.3 Dependencias del activo S-001, S-002, S003

Los tres sistemas (académico, recursos humanos y financiero) son el soporte de toda la información, todas las actividades de la universidad se registran gracias a estos sistemas de información.



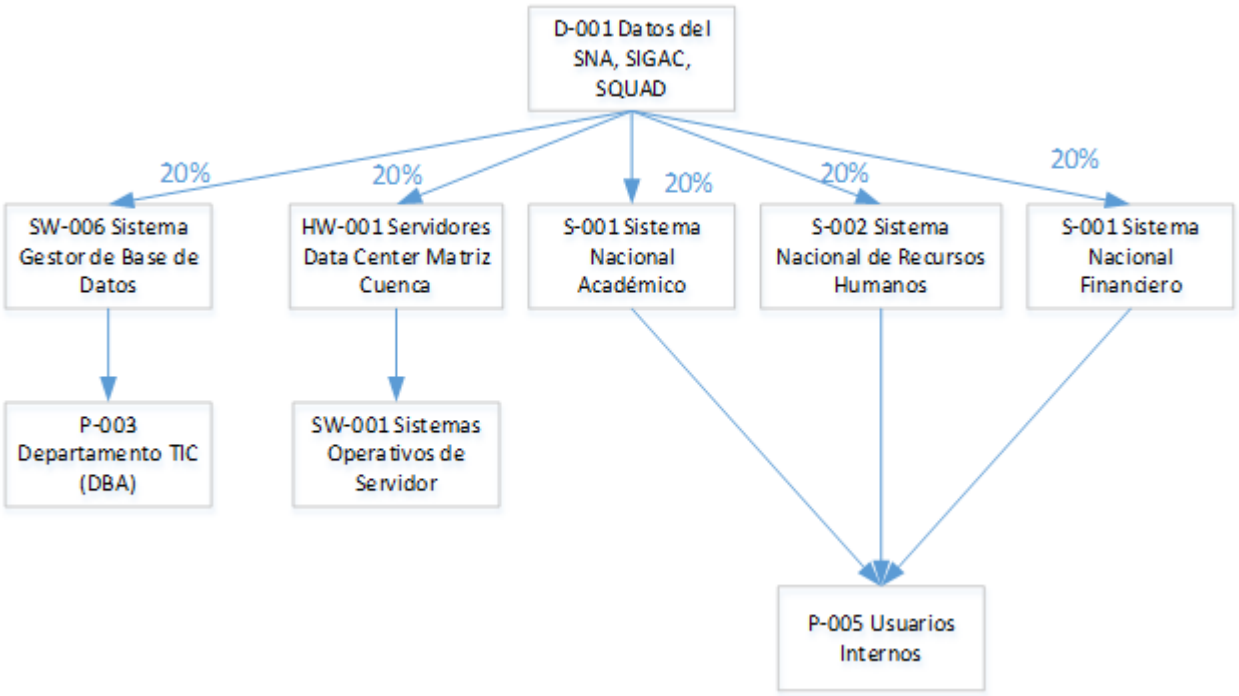
2.2.1.4 Dependencias del activo S-004

Las aulas virtuales de aprendizaje garantizan el desarrollo de la academia, es un servicio permite el trabajo diarios e interacción entre docentes y estudiantes.



2.2.1.5 Dependencias del activo D-001

La base de datos institucional, almacena y recopila todos los registros que se generan en los sistemas principales, al mismo tiempo necesita una infraestructura de hardware y software para poder brindar las prestaciones que requiere la universidad



2.3 TABLA RESUMEN DE VALORACIÓN

Para la valoración de activos se ha determinado la tabla 2.2 según el anexo 06 Metodología y Análisis de Riesgo

Valoración de activos		
Descripción	**Abreviatura**	**Valor**
Muy alto	MA	500.000,00 USD
Alto	A	300.000,00 USD
Medio	M	100.000,00 USD
Bajo	B	10.000,00 USD
Muy bajo	MB	1.000,00 USD

Tabla 2.2 Valoración de activos

Dicha valoración debe ser completada con el impacto relacionado a cada dimensión del activo.

Caracterización	Código activo	Denominación	Valoración cualitativa	Valoración cuantitativa	Autenticidad [A]	Confidencialidad [C]	Integridad [I]	Disponibilidad [D]	Trazabilidad [T]
[inf] Información	I-001	Información académica	MA	500.000,00 USD	2	4	9	6	2
[inf] Información	I-002	Información Talento Humano	MA	500.000,00 USD	2	6	9	4	2
[inf] Información	I-003	Información financiera	MA	500.000,00 USD	2	6	9	4	2
[service] Servicio	S-001	Sistema Nacional Académico (SNA)	MA	500.000,00 USD	4	4	6	8	2
[service] Servicio	S-002	Sistema Nacional de Recursos Humanos	MA	500.000,00 USD	4	4	6	6	2
[service] Servicio	S-003	Sistema Nacional Financiero	MA	500.000,00 USD	4	8	6	6	2
[service] Servicio	S-004	AVAC	MA	500.000,00 USD	2	0	2	8	0
[D] Datos	D-001	Datos del SNA, SIGAC y SQUAD	MA	500.000,00 USD	6	6	9	9	2
[D] Datos	D-002	Datos del AVAC	A	300.000,00 USD	1	2	4	6	1
[D] Datos	D-003	Datos institucionales	M	100.000,00 USD	2	4	4	4	0
[D] Datos	D-004	Código Fuentes	M	100.000,00 USD	2	8	8	4	0
[D] Datos	D-005	Backups	B	10.000,00 USD	2	8	6	2	2
[D] Datos	D-006	Logs	B	10.000,00 USD	2	2	6	2	8
[K] Claves criptográficas	K-001	Certificados de clave pública X509	M	100.000,00 USD	9	9	8	2	2
[S] Servicios Generales	S-005	Internet	A	300.000,00 USD	0	0	0	8	2
[S] Servicios Generales	S-006	Correo electrónico	M	100.000,00 USD	6	6	2	6	0
[S] Servicios Generales	S-007	Portal Web	B	10.000,00 USD	2	2	4	4	0
[S] Servicios Generales	S-008	Proxy	B	10.000,00 USD	0	0	0	4	4
[S] Servicios Generales	S-009	Almacenamiento de Ficheros	MB	1.000,00 USD	4	4	6	4	2
[S] Servicios Generales	S-010	Servicio de gestión de identidades	M	100.000,00 USD	6	8	4	8	0
[S] Servicios Generales	S-011	Servicios Web Docentes	B	10.000,00 USD	4	4	4	4	0
[S] Servicios Generales	S-012	Servicios Web Estudiantes	B	10.000,00 USD	4	4	4	4	0
[S] Servicios Generales	S-013	Servicio de Antivirus	B	10.000,00 USD	0	0	9	6	0
[S] Servicios Generales	S-014	Sistema de Gestión Documental	B	10.000,00 USD	9	6	8	2	4
[S] Servicios Generales	S-015	Servicio de Directorio	B	10.000,00 USD	4	8	4	4	4
[S] Servicios Generales	S-016	Telefonía IP	M	100.000,00 USD	2	8	2	6	0
[S] Servicios Generales	S-017	Enlaces WAN	A	300.000,00 USD	0	9	6	8	0
[S] Servicios Generales	S-018	Videoconferencia	B	10.000,00 USD	0	4	0	6	0
[S] Servicios Generales	S-019	WIFI	M	100.000,00 USD	0	0	0	6	0
[S] Servicios Generales	S-020	Repositorio Digital Académico	B	10.000,00 USD	6	2	6	4	0

[S] Servicios Generales	S-021	Pagos en línea	A	300.000,00 USD	8	8	8	8	8
[S] Servicios Generales	S-022	Servicio de copias de seguridad	B	10.000,00 USD	4	4	6	4	0
[SW] Software	SW-001	Sistemas Operativos de Servidor	B	10.000,00 USD	4	2	8	8	6
[SW] Software	SW-002	Sistemas Operativos usuarios	B	10.000,00 USD	1	2	2	6	1
[SW] Software	SW-003	Antivirus	M	100.000,00 USD	0	0	2	4	0
[SW] Software	SW-004	Ofimática	M	100.000,00 USD	0	0	2	4	0
[SW] Software	SW-005	Software Académico	A	300.000,00 USD	0	2	2	8	0
[SW] Software	SW-006	Sistema Gestor de Base de Datos	A	300.000,00 USD	8	8	8	8	8
[SW] Software	SW-007	Software de Desarrollo	MB	1.000,00 USD	0	8	2	4	0
[HW] Hardware	HW-001	Servidores DataCenter Matriz Cuenca	MA	500.000,00 USD	2	4	8	9	2
[HW] Hardware	HW-002	Servidores CDP Quito campus El Giron	A	300.000,00 USD	2	4	8	6	2
[HW] Hardware	HW-003	Servidores CDP Quito campus Kennedy	A	300.000,00 USD	2	4	8	6	2
[HW] Hardware	HW-004	Servidores CDP Quito campus Sur	A	300.000,00 USD	2	4	8	6	2
[HW] Hardware	HW-005	Servidores CDP Guayaquil	MA	500.000,00 USD	2	4	8	6	2
[HW] Hardware	HW-006	Telefonía IP	A	300.000,00 USD	0	2	2	6	0
[HW] Hardware	HW-007	Videoconferencia	A	300.000,00 USD	0	2	4	4	0
[HW] Hardware	HW-008	PC-Administrativos	B	10.000,00 USD	0	4	1	6	0
[HW] Hardware	HW-009	PC-Portátiles Docentes	M	100.000,00 USD	0	2	2	2	0
[HW] Hardware	HW-010	PC-Desarrollo	B	10.000,00 USD	0	4	4	4	0
[HW] Hardware	HW-011	PC-Portátiles Administrativos	B	10.000,00 USD	0	6	2	6	0
[HW] Hardware	HW-012	Red WAN	A	300.000,00 USD	2	2	2	9	2
[HW] Hardware	HW-013	Backbone LAN	A	300.000,00 USD	2	2	2	9	2
[HW] Hardware	HW-014	Firewall	M	100.000,00 USD	2	2	2	8	2
[HW] Hardware	HW-015	Router WAN	B	10.000,00 USD	2	2	2	8	2
[HW] Hardware	HW-016	LAN Cuenca	A	300.000,00 USD	2	2	2	6	2
[HW] Hardware	HW-017	LAN Quito	A	300.000,00 USD	2	2	2	6	2
[HW] Hardware	HW-018	LAN Guayaquil	A	300.000,00 USD	2	2	2	6	2
[HW] Hardware	HW-019	Impresoras	B	10.000,00 USD	0	2	1	2	0
[COM] Redes de comunicaciones	COM-001	Teléfonos IP	M	100.000,00 USD	0	2	2	6	0
[COM] Redes de comunicaciones	COM-002	WIFI	M	100.000,00 USD	0	0	2	6	0
[COM] Redes de comunicaciones	COM-003	WAN	A	300.000,00 USD	4	4	2	9	4
[COM] Redes de comunicaciones	COM-004	LAN Cuenca	M	100.000,00 USD	4	4	2	9	4
[COM] Redes de comunicaciones	COM-005	LAN Quito	M	100.000,00 USD	4	4	2	9	4

[COM] Redes de comunicaciones	COM-006	LAN Guayaquil	M	100.000,00 USD	4	4	2	9	4
[COM] Redes de comunicaciones	COM-007	VPN	B	10.000,00 USD	4	9	2	6	4
[M] Media	M-001	Backups	MB	1.000,00 USD	2	2	6	2	2
[M] Media	M-002	Documentación Administrativa UPS	B	10.000,00 USD	4	4	2	2	0
[M] Media	M-003	Documentación Académica UPS	M	100.000,00 USD	4	2	6	2	0
[M] Media	M-004	Documentación Técnica	B	10.000,00 USD	4	2	4	4	0
[AUX] Equipamiento Auxiliar	AUX-001	Generadores Eléctricos	A	300.000,00 USD	0	0	4	4	0
[AUX] Equipamiento Auxiliar	AUX-002	Destructores de papel	B	10.000,00 USD	0	4	0	2	0
[L] Instalaciones	L-001	Sede Matriz	MA	500.000,00 USD	0	4	4	4	0
[L] Instalaciones	L-002	Sede Quito	MA	500.000,00 USD	0	4	4	4	0
[L] Instalaciones	L-003	Sede Guayaquil	MA	500.000,00 USD	0	4	4	4	0
[L] Instalaciones	L-004	Data Center Cuenca	A	300.000,00 USD	0	6	4	6	0
[L] Instalaciones	L-005	CDP Quito	M	100.000,00 USD	0	6	4	6	0
[L] Instalaciones	L-006	CDP Guayaquil	M	100.000,00 USD	0	6	4	6	0
[P] Personal	P-001	Dirección	B	10.000,00 USD	0	6	4	6	0
[P] Personal	P-002	Director de TIC	B	10.000,00 USD	0	8	6	7	0
[P] Personal	P-003	Departamento de TIC	M	100.000,00 USD	0	8	6	9	0
[P] Personal	P-004	Personal de Desarrollo	MB	1.000,00 USD	0	4	4	4	0
[P] Personal	P-005	Usuarios Internos	B	10.000,00 USD	0	6	4	4	0
[P] Personal	P-006	Docentes	B	10.000,00 USD	0	2	4	6	0
[P] Personal	P-007	Estudiantes	B	10.000,00 USD	0	2	2	6	0

Tabla 2.3 Valoración de activos

2.4 ANÁLISIS DE AMENAZAS

Para la clasificación de amenazas se utilizó el catálogo expuesto en la tabla 4 del anexo 06 Metodología y Análisis de Riesgos, a continuación se puede apreciar la incidencia de cada amenaza sobre las dimensiones de los diferente activos, Magerit define claramente la dimensión que es afectada por cada amenaza.

En la clasificación de activos se destaca los activos [inf] y [service] como los esenciales de la UPS.

Código	Amenaza	Dimensiones					Activos según la clasificación del punto 2.3											
		A	C	I	D	T	[inf]	[service]	[D]	[k]	[S]	[SW]	[HW]	[COM]	[M]	[AUX]	[L]	[P]
[N.1]	Fuego				x								x		x	x	x	
[N.2]	Daños por agua				x								x		x	x	x	
[N.3]	Desastres naturales				x								x		x	x	x	
[I.1]	Fuego				x								x		x	x	x	
[I.2]	Daños por agua				x								x		x	x	x	
[I.3]	Contaminación mecánica				x								x		x	x		
[I.4]	Contaminación electromagnética				x								x		x	x		
[I.5]	Avería de origen físico o lógico				x							x	x		x	x		
[I.6]	Corte del suministro eléctrico				x								x		x	x		
[I.7]	Condiciones inadecuadas de temperatura o humedad				x								x		x	x		
[I.8]	Fallo de servicios de comunicaciones				x									x				
[I.9]	Interrupción de otros servicios y suministros esenciales				x		x		x									
[I.10]	Degradación de los soportes de almacenamiento de la información				x										x			
[I.11]	Emanaciones electromagnéticas				x								x		x	x	x	
[E.1]	Errores de los usuarios		x	x	x		x	x	x	x	x	x			x			
[E.2]	Errores del administrador		x	x	x		x	x	x	x	x	x	x	x	x			
[E.3]	Errores de monitorización (log)			x		x	x		x									
[E.4]	Errores de configuración			x			x		x									
[E.7]	Deficiencias en la organización				x													x

[E.8]	Difusión de software dañino		x	x	x							x							
[E.9]	Errores de re-encaminamiento		x					x			x	x		x					
[E.10]	Errores de secuencia			x				x			x	x		x					
[E.14]	Escapes de información		x				x		x										
[E.15]	Alteración accidental de la información			x			x	x	x		x	x		x	x		x		
[E.18]	Destrucción de información				x		x	x	x		x	x		x	x				
[E.19]	Fugas de información		x				x	x	x	x	x	x			x			x	
[E.20]	Vulnerabilidades de los programas (software)		x	x	x							x							
[E.21]	Errores de mantenimiento / actualización de programas (software)			x	x							x							
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)				x								x		x	x			
[E.24]	Caída del sistema por agotamiento de recursos				x							x	x	x					
[E.25]	Pérdida de equipos		x		x								x		x	x			
[E.28]	Indisponibilidad del personal				x													x	
[A.3]	Manipulación de los registros de actividad (log)			x		x	x		x										
[A.4]	Manipulación de la configuración	x	x	x			x		x										
[A.5]	Suplantación de la identidad del usuario	x	x	x			x	x	x	x	x	x		x					
[A.6]	Abuso de privilegios de acceso		x	x	x		x	x	x	x	x	x	x	x					
[A.7]	Uso no previsto		x	x	x		x	x	x		x	x	x	x	x	x			
[A.8]	Difusión de software dañino		x	x	x							x							
[A.9]	Re-encaminamiento		x					x			x	x		x					

	de mensajes																		
[A.10]	Alteración de secuencia			x				x			x	x		x					
[A.11]	Acceso no autorizado		x	x			x	x	x	x	x	x	x	x	x	x	x		
[A.12]	Análisis de tráfico		x											x					
[A.13]	Repudio			x		x	x	x	x		x								
[A.14]	Interceptación de información (escucha)		x											x					
[A.15]	Modificación deliberada de la información			x			x	x	x	x	x	x	x	x	x				
[A.18]	Destrucción de información				x		x	x	x	x	x	x		x	x				
[A.19]	Divulgación de información		x				x	x	x	x	x	x		x	x				
[A.22]	Manipulación de programas		x	x	x							x							
[A.23]	Manipulación de los equipos		x		x								x		x	x			
[A.24]	Denegación de servicio				x			x			x	x	x	x					
[A.25]	Robo		x		x		x		x				x		x	x			
[A.26]	Ataque destructivo				x								x		x	x	x		
[A.27]	Ocupación enemiga		x		x												x		
[A.28]	Indisponibilidad del personal				x													x	
[A.29]	Extorsión		x	x	x													x	
[A.30]	Ingeniería social (picaresca)		x	x	x													x	

Tabla 2.4 Identificación de amenazas

En el anexo 07 *Análisis de Riesgos*, en su hoja *activos-amenazas* se puede apreciar la relación de las diferentes amenazas con cada una de las dimensiones de los activos.

2.5 IMPACTO POTENCIAL Y RESIDUAL

Con la valoración de activos, la caracterización de amenazas y su afección a cada dimensión se procedió a realizar el impacto potencial. El análisis completo se encuentra en el anexo 07 *Análisis de Riesgos* en su hoja *impacto*, a continuación se presenta un resumen para apreciar únicamente las amenazas que tienen un impacto muy alto, alto y medio.

Código Activo	Activo	Código Amenaza	Amenaza	Frecuencia	Valor. Freq	Valor Impacto	Impacto
I-002	Información Talento Humano	[A.19]	Divulgación de información	MA	1	300.000,00 USD	MA
I-003	Información financiera	[A.19]	Divulgación de información	MA	1	300.000,00 USD	MA
S-001	Sistema Nacional Académico (SNA)	[E.1]	Errores de los usuarios	MA	1	300.000,00 USD	MA
S-003	Sistema Nacional Financiero	[E.1]	Errores de los usuarios	MA	1	300.000,00 USD	MA
I-001	Información académica	[A.6]	Abuso de privilegios de acceso	MA	1	225.000,00 USD	A
I-002	Información Talento Humano	[A.6]	Abuso de privilegios de acceso	MA	1	225.000,00 USD	A
I-003	Información financiera	[A.6]	Abuso de privilegios de acceso	MA	1	225.000,00 USD	A
S-002	Sistema Nacional de Recursos Humanos	[E.1]	Errores de los usuarios	MA	1	225.000,00 USD	A
I-001	Información académica	[A.19]	Divulgación de información	MA	1	200.000,00 USD	A
D-004	Código Fuentes	[A.6]	Abuso de privilegios de acceso	MA	1	80.000,00 USD	M
I-001	Información académica	[E.15]	Alteración accidental de la información	A	0,14246575	64.109,59 USD	M
I-001	Información académica	[A.7]	Uso no previsto	A	0,14246575	64.109,59 USD	M
I-002	Información Talento Humano	[E.15]	Alteración accidental de la información	A	0,14246575	64.109,59 USD	M
I-002	Información Talento Humano	[A.7]	Uso no previsto	A	0,14246575	64.109,59 USD	M
I-003	Información financiera	[E.15]	Alteración accidental de la información	A	0,14246575	64.109,59 USD	M
I-003	Información financiera	[A.7]	Uso no previsto	A	0,14246575	64.109,59 USD	M
COM-002	WIFI	[A.6]	Abuso de privilegios de acceso	MA	1	60.000,00 USD	M
S-001	Sistema Nacional Académico (SNA)	[A.6]	Abuso de privilegios de acceso	A	0,14246575	56.986,30 USD	M
S-001	Sistema Nacional Académico (SNA)	[A.24]	Denegación de servicio	A	0,14246575	56.986,30 USD	M
S-003	Sistema Nacional Financiero	[A.6]	Abuso de privilegios de acceso	A	0,14246575	56.986,30 USD	M
S-003	Sistema Nacional Financiero	[A.19]	Divulgación de información	A	0,14246575	56.986,30 USD	M
S-004	AVAC	[E.1]	Errores de los usuarios	A	0,14246575	56.986,30 USD	M
S-004	AVAC	[E.18]	Destrucción de información	A	0,14246575	56.986,30 USD	M
I-002	Información Talento Humano	[E.19]	Fugas de información	A	0,14246575	42.739,73 USD	M
I-003	Información financiera	[E.19]	Fugas de información	A	0,14246575	42.739,73 USD	M
S-001	Sistema Nacional Académico (SNA)	[E.15]	Alteración accidental de la información	A	0,14246575	42.739,73 USD	M
S-002	Sistema Nacional de Recursos Humanos	[E.15]	Alteración accidental de la información	A	0,14246575	42.739,73 USD	M
S-002	Sistema Nacional de	[A.6]	Abuso de privilegios	A	0,14246575	42.739,73 USD	M

	Recursos Humanos		de acceso				
S-002	Sistema Nacional de Recursos Humanos	[A.24]	Denegación de servicio	A	0,14246575	42.739,73 USD	M
S-003	Sistema Nacional Financiero	[E.15]	Alteración accidental de la información	A	0,14246575	42.739,73 USD	M
S-003	Sistema Nacional Financiero	[A.24]	Denegación de servicio	A	0,14246575	42.739,73 USD	M
SW-005	Software Académico	[E.20]	Vulnerabilidades de los programas (software)	A	0,14246575	34.191,78 USD	M
SW-005	Software Académico	[E.21]	Errores de mantenimiento / actualización de programas (software)	A	0,14246575	34.191,78 USD	M
I-001	Información académica	[E.1]	Errores de los usuarios	A	0,14246575	32.054,79 USD	M
I-001	Información académica	[A.11]	Acceso no autorizado	A	0,14246575	32.054,79 USD	M
I-002	Información Talento Humano	[E.1]	Errores de los usuarios	A	0,14246575	32.054,79 USD	M
I-002	Información Talento Humano	[A.11]	Acceso no autorizado	A	0,14246575	32.054,79 USD	M
I-003	Información financiera	[E.1]	Errores de los usuarios	A	0,14246575	32.054,79 USD	M
I-003	Información financiera	[A.11]	Acceso no autorizado	A	0,14246575	32.054,79 USD	M
I-001	Información académica	[E.19]	Fugas de información	A	0,14246575	28.493,15 USD	M
S-001	Sistema Nacional Académico (SNA)	[A.19]	Divulgación de información	A	0,14246575	28.493,15 USD	M
S-002	Sistema Nacional de Recursos Humanos	[A.19]	Divulgación de información	A	0,14246575	28.493,15 USD	M
HW-009	PC-Portátiles Docentes	[A.7]	Uso no previsto	MA	1	20.000,00 USD	M
COM-002	WIFI	[A.11]	Acceso no autorizado	MA	1	20.000,00 USD	M
D-001	Datos del SNA, SIGAC y SQUAD	[A.6]	Abuso de privilegios de acceso	M	0,03287671	14.794,52 USD	M
S-001	Sistema Nacional Académico (SNA)	[A.7]	Uso no previsto	M	0,03287671	13.150,68 USD	M
S-003	Sistema Nacional Financiero	[E.19]	Fugas de información	M	0,03287671	13.150,68 USD	M
S-003	Sistema Nacional Financiero	[A.7]	Uso no previsto	M	0,03287671	13.150,68 USD	M
D-004	Código Fuentes	[A.25]	Robo	A	0,14246575	11.397,26 USD	M
S-016	Telefonía IP	[A.7]	Uso no previsto	A	0,14246575	11.397,26 USD	M

Tabla 2.5 Amenazas principales según el impacto

2.6 NIVEL DE RIESGO

En el anexo 07 *Análisis de Riesgos* se puede apreciar los diferentes niveles de riesgo para cada activo según sus amenazas, a continuación se presenta a manera de resumen la comparación del impacto con la probabilidad.

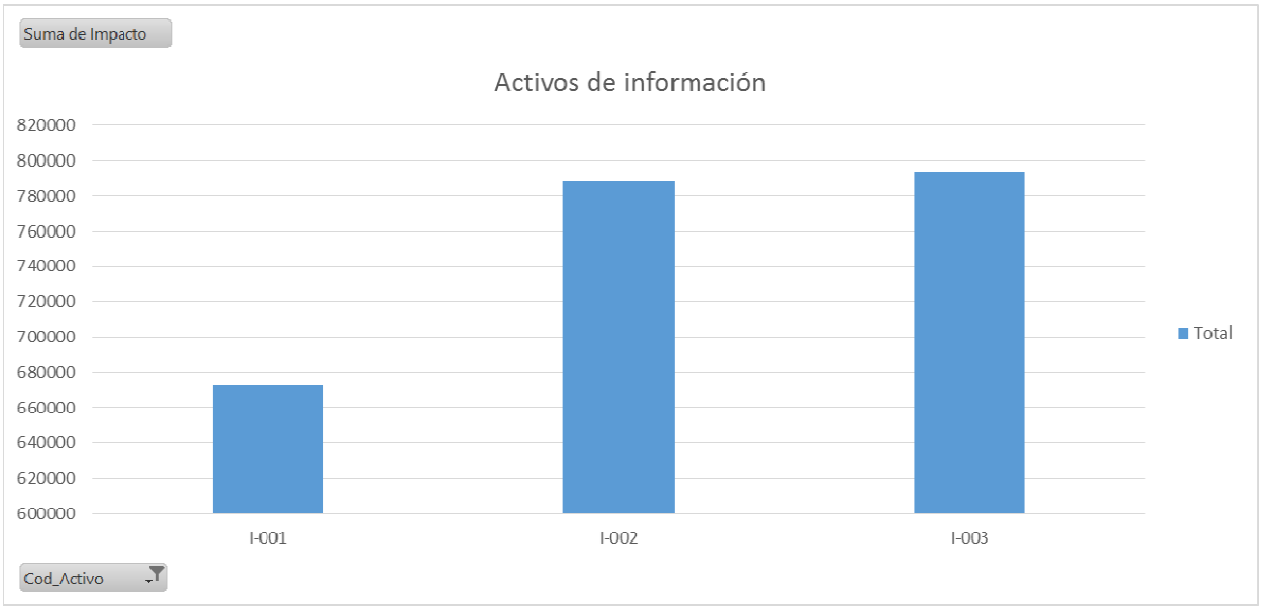
		Frecuencia/probabilidad				
		MA	**A**	**B**	**M**	**MB**
Impacto	**MA**	4				
	A	5				
	B	9	7	13	29	47
	M	4	33		4	
	MB		12	27	39	1277
	NA (no aplica)	2				55

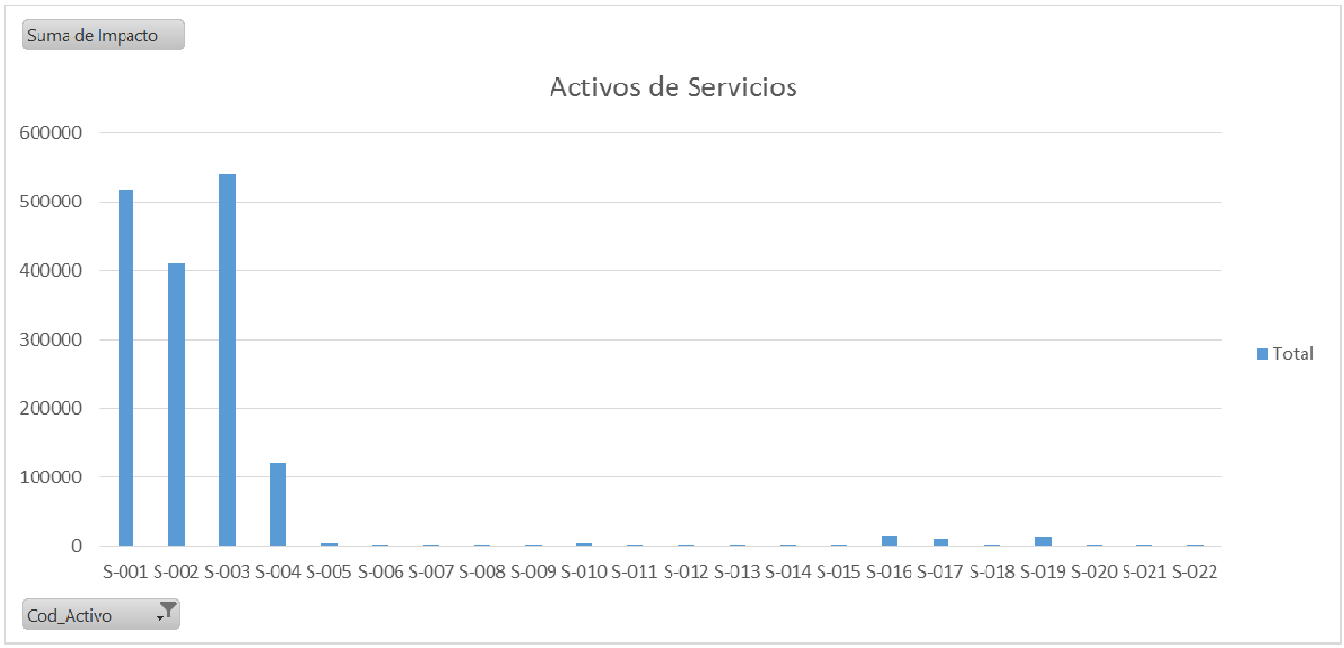
Tabla 2.5 Valoración del riesgo

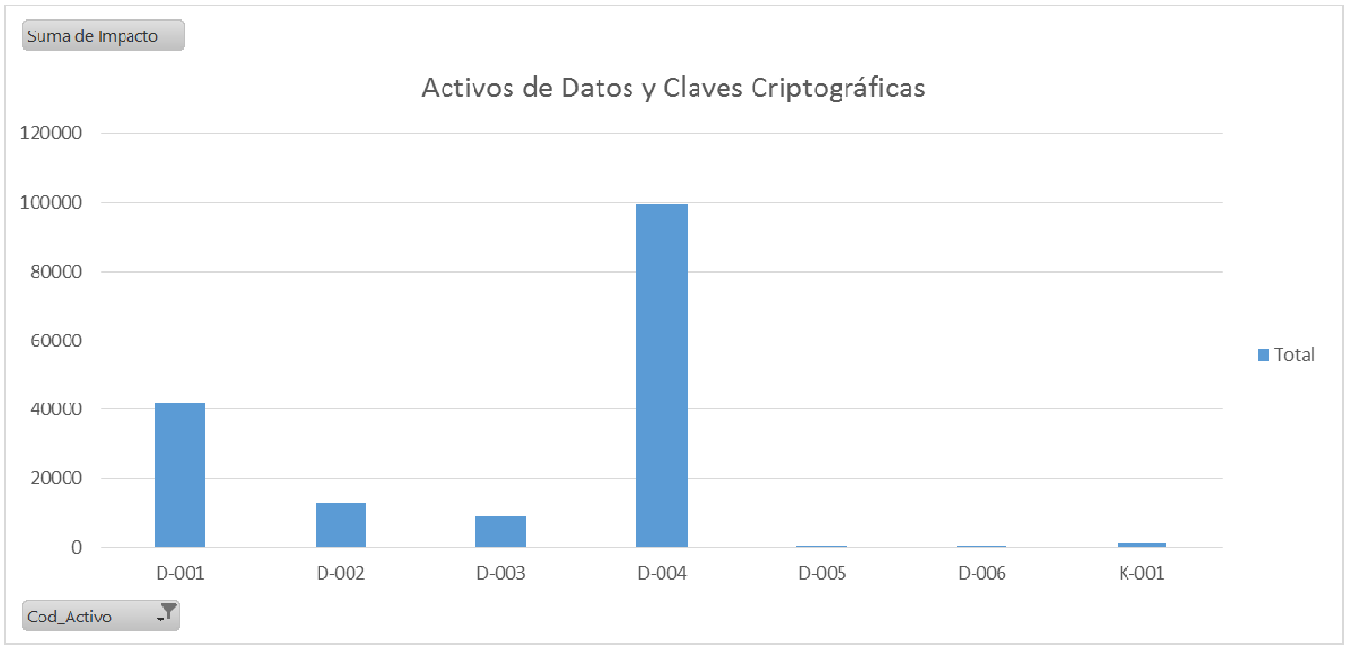
Existen 4 amenazas de impacto muy alto y frecuencia muy alta que son las que deberían ser tratadas de manera prioritaria.

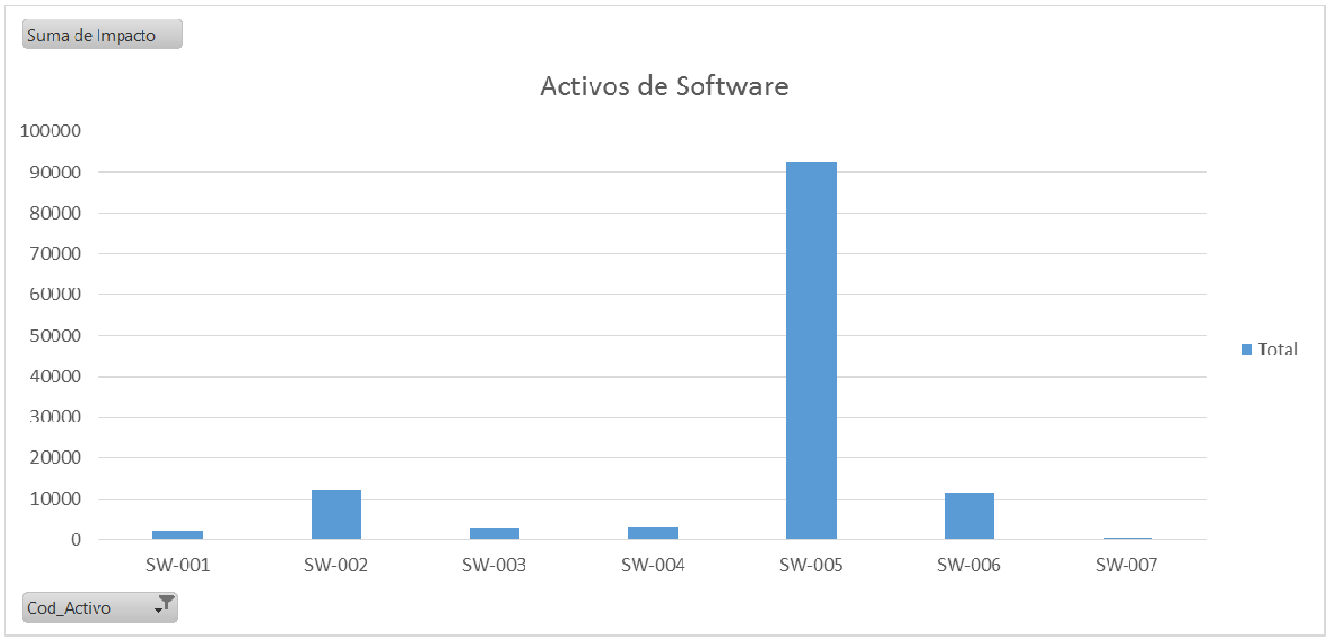
Gracias a las salvaguardas que tiene implementadas la universidad podemos apreciar que existen 1355 amenazas con impacto muy bajo.

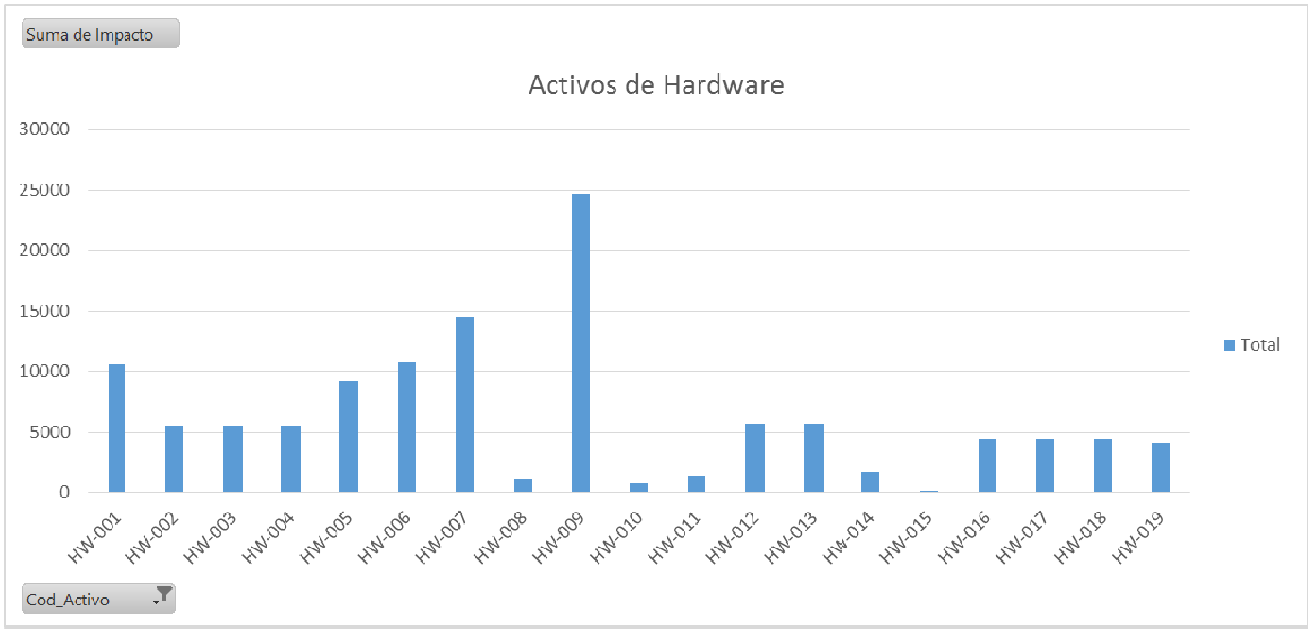
Las gráficas nos permiten apreciar el impacto acumulado para todos los tipos de activos

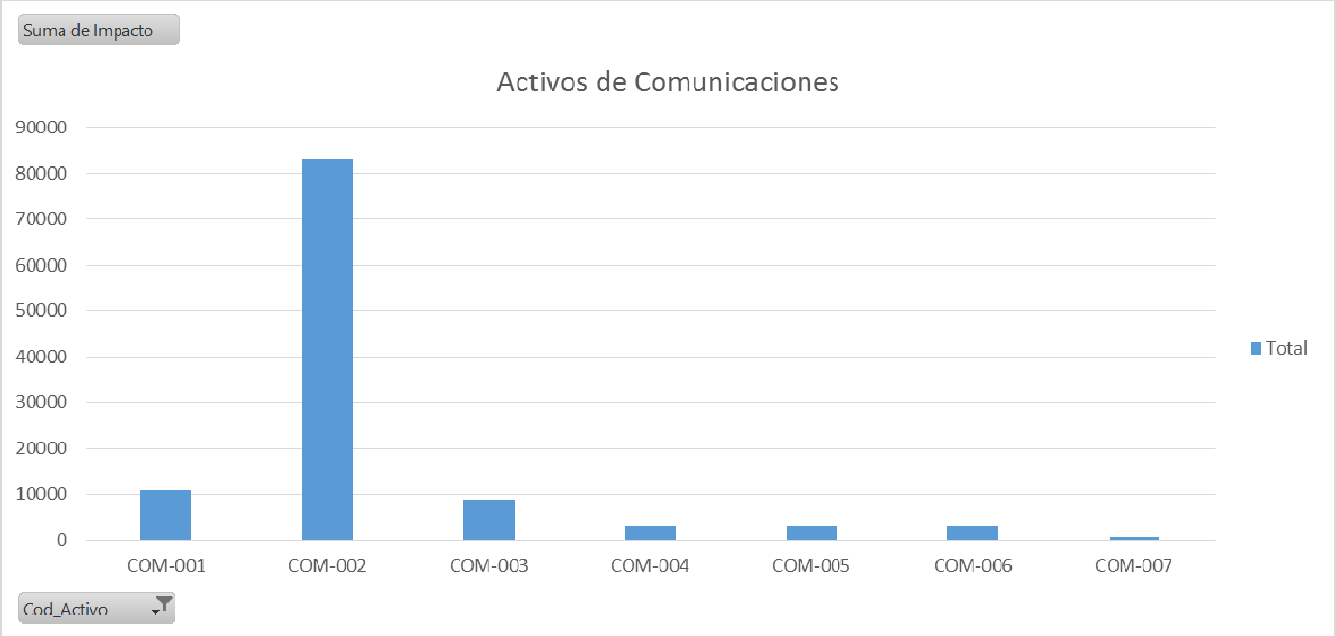


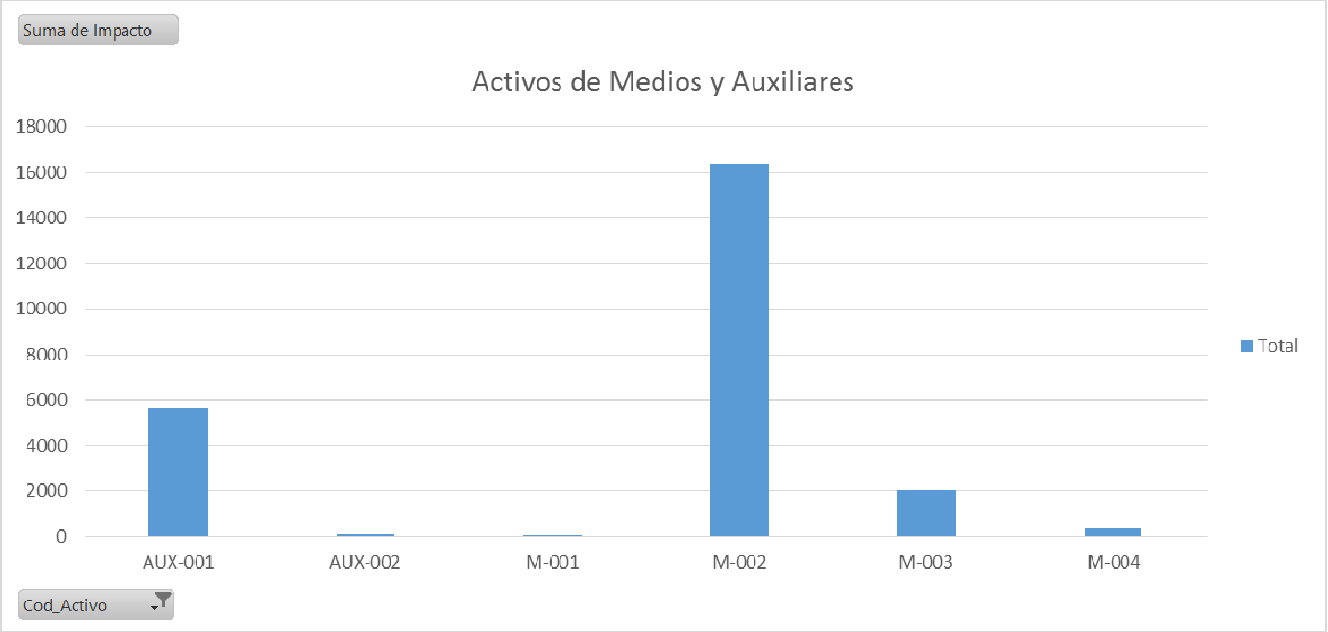

Suma de Impacto
Activos de Servicios
600000
500000
400000
300000
200000
100000
0
S-001 S-002 S-003 S-004 S-005 S-006 S-007 S-008 S-009 S-010 S-011 S-012 S-013 S-014 S-015 S-016 S-017 S-018 S-019 S-020 S-021 S-022
Total
Cod_Activo

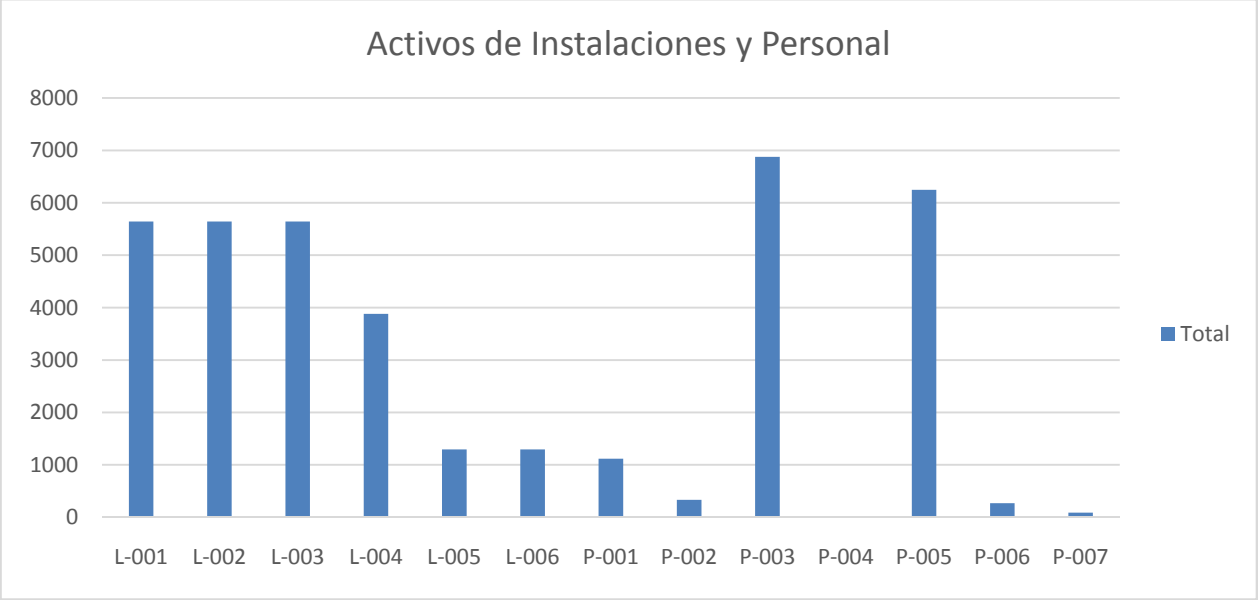

Suma de Impacto
Activos de Datos y Claves Criptográficas
120000
100000
80000
60000
40000
20000
0
D-001 D-002 D-003 D-004 D-005 D-006 K-001
Total
Cod_Activo


Suma de Impacto
Activos de Software
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
SW-001
SW-002
SW-003
SW-004
SW-005
SW-006
SW-007
Total
Cod_Activo


Suma de Impacto
Activos de Hardware
30000
25000
20000
15000
10000
5000
0
HW-001
HW-002
HW-003
HW-004
HW-005
HW-006
HW-007
HW-008
HW-009
HW-010
HW-011
HW-012
HW-013
HW-014
HW-015
HW-016
HW-017
HW-018
HW-019
Total
Cod_Activo


Suma de Impacto
Activos de Comunicaciones
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
COM-001
COM-002
COM-003
COM-004
COM-005
COM-006
COM-007
Total
Cod_Activo


Suma de Impacto
Activos de Medios y Auxiliares
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
AUX-001
AUX-002
M-001
M-002
M-003
M-004
Total
Cod_Activo


Activos de Instalaciones y Personal
8000
7000
6000
5000
4000
3000
2000
1000
0
L-001
L-002
L-003
L-004
L-005
L-006
P-001
P-002
P-003
P-004
P-005
P-006
P-007
Total

3 CAPÍTULO 4: PROPUESTAS DE PROYECTOS

3.1 PROPUESTAS

Luego de conocer el análisis de riesgos, la UPS establece su umbral en el nivel de aceptación para aquellos cuyo impacto está determinado como Bajo, sin importar la frecuencia de ocurrencia, puesto que representa un valor que es fácilmente asumible por la organización.

En este contexto nos encontramos ante cincuenta riesgos de categoría media, alta y muy alta(tabla 2.5), a continuación se podrá observar una serie de análisis con la finalidad de establecer la mejor estrategia en la implementación de un plan de tratamiento del riesgo.

Primeramente se identifica que activos concretos y que amenazas concretas son las que están ocurriendo, mediante este análisis se determina que los cincuenta riesgos se distribuyen en trece activos según la tabla 3.1 y doce amenazas según la tabla 3.2.

Código Activo	Activo
I-002	Información Talento Humano
I-003	Información financiera
S-001	Sistema Nacional Académico (SNA)
S-003	Sistema Nacional Financiero
I-001	Información académica
S-002	Sistema Nacional de Recursos Humanos
D-004	Código Fuentes
COM-002	WIFI
S-004	AVAC
SW-005	Software Académico
HW-009	PC-Portátiles Docentes
D-001	Datos del SNA, SIGAC y SQUAD
S-016	Telefonía IP

Tabla 3.1 Activos cuya clasificación de riesgo es media, alta y muy alta

Cod_Amenaza	Amenaza
[A.19]	Divulgación de información
[E.1]	Errores de los usuarios
[A.6]	Abuso de privilegios de acceso
[E.15]	Alteración accidental de la información
[A.7]	Uso no previsto
[A.24]	Denegación de servicio
[E.18]	Destrucción de información
[E.19]	Fugas de información
[E.20]	Vulnerabilidades de los programas (software)
[E.21]	Errores de mantenimiento / actualización de programas (software)
[A.11]	Acceso no autorizado
[A.25]	Robo

Tabla 3.2 Amenazas cuya incidencia en los activos tiene una clasificación de riesgo media, alta y muy alta

Si tratamos la amenaza de divulgación de la información podemos abarcar seis riesgos, dos de ellos de impacto muy alto, uno de impacto alto y tres de impacto medio según la tabla 3.3.

Cod_Activo	Activo	Cod_Amenaza	Amenaza	Impacto
I-002	Información Talento Humano	[A.19]	Divulgación de información	MA
I-003	Información financiera	[A.19]	Divulgación de información	MA
I-001	Información académica	[A.19]	Divulgación de información	A
S-003	Sistema Nacional Financiero	[A.19]	Divulgación de información	M
S-001	Sistema Nacional Académico (SNA)	[A.19]	Divulgación de información	M
S-002	Sistema Nacional de Recursos Humanos	[A.19]	Divulgación de información	M

Tabla 3.3 Riesgos caracterizados por la amenaza de divulgación de la información [A.19].

Seguidamente, se realiza el mismo análisis con la amenaza de errores de los usuarios, el resultado se expresa en dos riesgos de impacto muy alto, uno de impacto alto y cuatro de impacto medio, según la tabla 3.4.

Cod_Activo	Activo	Cod_Amenaza	Amenaza	Impacto
S-001	Sistema Nacional Académico (SNA)	[E.1]	Errores de los usuarios	MA
S-003	Sistema Nacional Financiero	[E.1]	Errores de los usuarios	MA
S-002	Sistema Nacional de Recursos Humanos	[E.1]	Errores de los usuarios	A
S-004	AVAC	[E.1]	Errores de los usuarios	M
I-001	Información académica	[E.1]	Errores de los usuarios	M
I-002	Información Talento Humano	[E.1]	Errores de los usuarios	M
I-003	Información financiera	[E.1]	Errores de los usuarios	M

Tabla 3.4 Riesgos caracterizados por la amenaza de errores de los usuarios [E.1]

Al cruzar la información de la tabla 3.3 y de la tabla 3.4, se determina que tanto la divulgación de la información y los errores de los usuarios se producen en los activos esenciales de información académica, financiera y talento humano; y en los servicios esenciales que son los sistemas nacionales (académico, financiero y de recursos humanos) en conclusión la primera y más importante estrategia del plan debe ser mitigar el riesgo en estos activos tratando dichas amenazas, debido que cubren la totalidad de riesgos de nivel muy alto, dos de los cinco riesgos de nivel alto y siete de los 41 riesgos de nivel medio. La estrategia se basará en que la dirección de la UPS apruebe en la brevedad posible la nueva estructura de organización de la seguridad para que las políticas puedan ser aprobadas e implementadas inmediatamente.

Al analizar los riesgos mediante la tabla 3.5 se determina que los activos esenciales tienen veintitrés riesgos provocados de manera intencional por los usuarios y 18 riesgos provocados por errores no intencionales, lo cual determina la segunda estrategia del plan de tratamiento del riesgo que consiste en protegernos de manera legal mediante políticas y normas de los errores intencionales de los usuarios.

	[A.11]	[A.19]	[A.24]	[A.25]	[A.6]	[A.7]	[E.1]	[E.15]	[E.18]	[E.19]	[E.20]	[E.21]	Total general
COM-002	1				1								2
D-001					1								1
D-004				1	1								2
HW-009						1							1
I-001	1	1			1	1	1	1		1			7
I-002	1	1			1	1	1	1		1			7
I-003	1	1			1	1	1	1		1			7
S-001		1	1		1	1	1	1					6
S-002		1	1		1		1	1					5
S-003		1	1		1	1	1	1		1			7
S-004							1		1				2
S-016						1							1
SW-005											1	1	2
Total general	**4**	**6**	**3**	**1**	**9**	**7**	**7**	**6**	**1**	**4**	**1**	**1**	**50**

Tabla 3.5 Riesgos de nivel medio, alto y muy alto; según los activos y amenazas

La tercera estrategia buscará articular los diferentes controles Ad-hoc implementados en la UPS para que puedan mitigar los errores no intencionales como los intencionales de los usuarios, además de implementar los controles faltantes según la declaración de aplicabilidad, con esto se espera priorizar activos como D-001, COM-002, D-004, HW-009, S-016 y SW-005.

La cuarta estrategia del plan de tratamiento del riesgo es la concienciación de todo el personal de la UPS, comunicarles las políticas, las responsabilidades de cada uno y las implicaciones que puede tener la pérdida de confidencialidad, integridad y disponibilidad de la información.

Finalmente la última estrategia es la implementación de un Plan de Continuidad del Negocio.

3.2 Plan de Tratamiento del Riesgo

El plan de tratamiento del riesgo se divide en 6 proyectos, derivados de las diferentes estrategias de tratamiento del riesgo, cabe destacar que la UPS debe arrancar desde cero con la implementación del SGSI.

3.2.1 Proyecto 1: Estructuración de la organización de la seguridad de la información

La estructura actual de la UPS no da soporte a la implementación del SGSI, problemas en la estructuración de los cargos del departamento como ser auditores de sus propias responsabilidades hacen evidente la necesidad de contar con un experto en Seguridad de la Información y un Auditor Interno; para ello la UPS a nivel de dirección debe brindar todo el apoyo tanto para contratación del nuevo personal como para la restructuración del actual descriptor de cargos del Departamento de Tecnologías de la Información.

3.2.1.1 Objetivos

Contar con una estructura de organización de la seguridad de la información.

Mejorar el dominio 6 de la norma ISO/IEC 27002:2013 “Aspectos organizativos de la seguridad de la información”.

3.2.1.2 Duración

Para este proyecto se estima una duración de un mes

3.2.1.3 Activos dentro del alcance del proyecto:

Según la tabla 3.6 se listan los activos que están dentro del alcance de este proyecto, además se puede apreciar las amenazas que el proyecto busca mitigar con la creación de la estructura de la organización de la seguridad de la información.

Activos	Amenazas		
	[E.2]	[E.4]	[E.7]
Almacenamiento de Ficheros	X.		
Antivirus	X.		
AVAC	X.		
Backbone LAN	X.		
Backups	X.	X.	
Código Fuentes	X.	X.	
Correo electrónico	X.		
Datos del AVAC	X.	X.	
Datos del SNA, SIGAC y SQUAD	X.	X.	
Datos institucionales	X.	X.	
Departamento de TIC			X.
Dirección			X.
Director de TIC			X.
Docentes			X.
Documentación Académica UPS	X.		
Documentación Administrativa UPS	X.		
Documentación Técnica	X.		
Enlaces WAN	X.		
Estudiantes			X.
Firewall	X.		
Impresoras	X.		
Información académica	X.	X.	
Información financiera	X.	X.	
Información Talento Humano	X.	X.	
Internet	X.		
LAN Cuenca	X.		
LAN Guayaquil	X.		
LAN Quito	X.		
Logs	X.	X.	
Ofimática	X.		
Pagos en línea	X.		
PC-Administrativos	X.		
PC-Desarrollo	X.		
PC-Portátiles Administrativos	X.		
PC-Portátiles Docentes	X.		
Personal de Desarrollo			X.
Portal Web	X.		
Proxy	X.		
Red WAN	X.		
Repositorio Digital Académico	X.		
Router WAN	X.		

Servicio de Antivirus	X.		
Servicio de copias de seguridad	X.		
Servicio de Directorio	X.		
Servicio de gestión de identidades	X.		
Servicios Web Docentes	X.		
Servicios Web Estudiantes	X.		
Servidores CDP Guayaquil	X.		
Servidores CDP Quito campus El Giron	X.		
Servidores CDP Quito campus Kennedy	X.		
Servidores CDP Quito campus Sur	X.		
Servidores DataCenter Matriz Cuenca	X.		
Sistema de Gestión Documental	X.		
Sistema Gestor de Base de Datos	X.		
Sistema Nacional Académico (SNA)	X.		
Sistema Nacional de Recursos Humanos	X.		
Sistema Nacional Financiero	X.		
Sistemas Operativos de Servidor	X.		
Sistemas Operativos usuarios	X.		
Software Académico	X.		
Software de Desarrollo	X.		
Telefonía IP	X.		
Teléfonos IP	X.		
Usuarios Internos			X.
Videoconferencia	X.		
VPN	X.		
WAN	X.		
WIFI	X.		

Tabla 3.6 Activos implicados en el proyecto 1 frente a las amenazas que el proyecto busca mitigar

3.2.1.4 Planificación

Es necesario realizar las siguientes tareas:

1) Reunión con la Dirección: En esta reunión se planteará la problemática de la seguridad de la información al Rector de la Universidad quien estará asesorado por el Secretario Técnico de Tecnologías de la Información y Comunicación, el resultado principal de esta reunión es que el Rector coloque en el orden del día del Consejo Superior de la UPS la creación de los nuevos cargos y la redefinición del Descriptor de Cargos del Departamento de Tecnologías de la Información y Comunicación.
   El tiempo estimado para esta reunión es de un día.
   El responsable de llevar a cabo esta tarea es el actual Secretario Técnico de Tecnologías de la Información y Comunicación.

2) Actualización del descriptor de cargos del departamento de TI: En Consejo Superior como máximo organismo universitario deberá aprobar la nueva estructura.
   El tiempo estimado es de un día.
   La responsabilidad de esta actividad recae en el Rector de la UPS, quien invitará al exclusivamente para este punto al Secretario Técnico de Tecnologías de la Información y Comunicación.

3) Llamamiento público a concurso de méritos y oposición: El departamento de Talento Humano convocará mediante la prensa a concurso público para el cargo de Responsable de Seguridad de la Información y Auditor Interno.

Para esta tarea se estima la duración de una semana para receptar la documentación de los diferentes candidatos
El responsable de esta actividad es la Secretaría Técnica de Gestión del Talento Humano

4) Entrevistas: Para esta tarea se definirá un equipo consultor, liderado por el Secretario Técnico de Tecnologías de la Información.
Se estima un tiempo de una semana para esta actividad.
Los responsables son el Equipo Consultor y el Secretario Técnico de Gestión del Talento Humano.

5) Evaluación: Para esta tarea se contratará una consultoría, que elaborará la evaluación para el concurso.
El tiempo estimado de evaluación es de un día.
La responsabilidad de esta tarea es de la Consultoría.

6) Contratación: El proyecto concluye con la contratación de los dos nuevos cargos.
Tiempo estimado 1 día.
Responsable: Secretario Técnico de Gestión del Talento Humano.

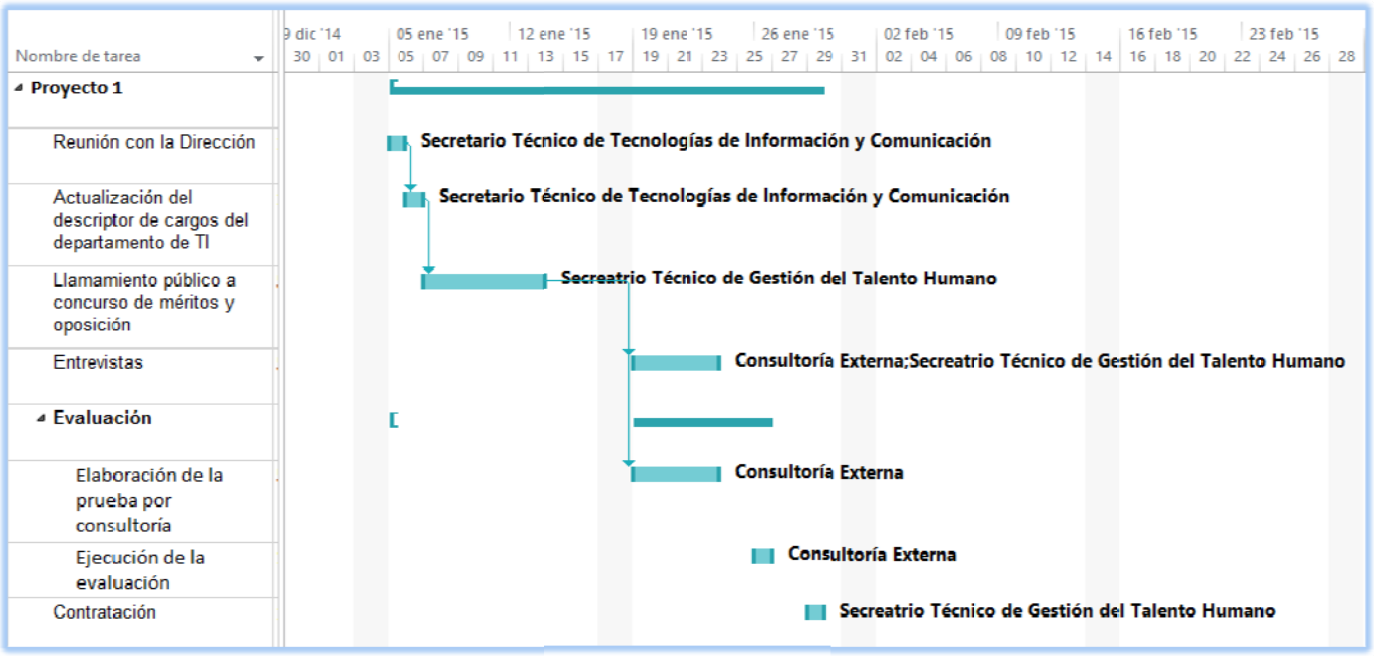


Figura 3.1 Diagrama de Gantt de la planificación del proyecto 1

3.2.1.5 Presupuesto:

Rubro	Cantidad	Valor unidad	Subtotal
Horas de personal	80	15,00 USD	1.200,00 USD
Contratación consultoría	1	4.000,00 USD	4.000,00 USD
Publicación prensa	1	1.200,00 USD	1.200,00 USD
		Total	6.400,00 USD

Tabla 3.7 Presupuesto del proyecto 1

3.2.2 PROYECTO 2: DEFINICIÓN, APROBACIÓN Y DIFUSIÓN INMEDIATA DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

En la UPS no existe concienciación sobre la seguridad de la información tanto a nivel directivo, estratégico como operacional, las diferentes propuesta son de tipo Ad-hoc para sectores específicos del

departamento de Tecnologías de la Información y Comunicación que han sido implementadas por iniciativa del personal del departamento.

3.2.2.1 Objetivos

Alcanzar por lo menos el nivel de madurez de “Gestionado” en el dominio 5 de la norma ISO/IEC 27002:2013 “Políticas de Seguridad”.
Alcanzar por lo menos el nivel de madurez de “Definido” en el domino 7 de la norma ISO/IEC 27002:2013 “Seguridad ligada a los recursos humanos”.

3.2.2.2 Duración

Para este proyecto se estima una duración de tres meses

3.2.2.3 Activos dentro del alcance de este proyecto:

Según la tabla 3.6 podemos apreciar los activos que estarán dentro del alcance de este proyecto, según las amenazas que tienen implicación directa con el proyecto.

Activos	Amenazas							
	[A.10]	[A.11]	[A.14]	[A.19]	[A.6]	[A.8]	[E.15]	[E.8]
Almacenamiento de Ficheros	X.	X.		X.	X.		X.	
Antivirus	X.	X.		X.	X.	X.	X.	X.
AVAC	X.	X.		X.	X.		X.	
Backbone LAN		X.			X.			
Backups		X.		X.	X.		X.	
CDP Guayaquil		X.					X.	
CDP Quito		X.					X.	
Certificados de clave pública X509		X.		X.	X.			
Código Fuentes		X.		X.	X.		X.	
Correo electrónico	X.	X.		X.	X.		X.	
Data Center Cuenca		X.					X.	
Datos del AVAC		X.		X.	X.		X.	
Datos del SNA, SIGAC y SQUAD		X.		X.	X.		X.	
Datos institucionales		X.		X.	X.		X.	
Destructores de papel		X.						
Documentación Académica UPS		X.		X.			X.	
Documentación Administrativa UPS		X.		X.			X.	
Documentación Técnica		X.		X.			X.	
Enlaces WAN	X.	X.		X.	X.		X.	
Firewall		X.			X.			
Generadores Eléctricos		X.						
Impresoras		X.			X.			
Información académica		X.		X.	X.		X.	
Información financiera		X.		X.	X.		X.	
Información Talento Humano		X.		X.	X.		X.	
Internet	X.	X.		X.	X.		X.	
LAN Cuenca	X.	X.	X.	X.	X.		X.	
LAN Guayaquil	X.	X.	X.	X.	X.		X.	
LAN Quito	X.	X.	X.	X.	X.		X.	
Logs		X.		X.	X.		X.	
Ofimática	X.	X.		X.	X.	X.	X.	X.
Pagos en línea	X.	X.		X.	X.		X.	

PC-Administrativos		X.			X.			
PC-Desarrollo		X.			X.			
PC-Portátiles Administrativos		X.			X.			
PC-Portátiles Docentes		X.			X.			
Portal Web	X.	X.		X.	X.		X.	
Proxy	X.	X.		X.	X.		X.	
Red WAN		X.			X.			
Repositorio Digital Académico	X.	X.		X.	X.		X.	
Router WAN		X.			X.			
Sede Guayaquil		X.					X.	
Sede Matriz		X.					X.	
Sede Quito		X.					X.	
Servicio de Antivirus	X.	X.		X.	X.		X.	
Servicio de copias de seguridad	X.	X.		X.	X.		X.	
Servicio de Directorio	X.	X.		X.	X.		X.	
Servicio de gestión de identidades	X.	X.		X.	X.		X.	
Servicios Web Docentes	X.	X.		X.	X.		X.	
Servicios Web Estudiantes	X.	X.		X.	X.		X.	
Servidores CDP Guayaquil		X.			X.			
Servidores CDP Quito campus El Giron		X.			X.			
Servidores CDP Quito campus Kennedy		X.			X.			
Servidores CDP Quito campus Sur		X.			X.			
Servidores DataCenter Matriz Cuenca		X.			X.			
Sistema de Gestión Documental	X.	X.		X.	X.		X.	
Sistema Gestor de Base de Datos	X.	X.		X.	X.	X.	X.	X.
Sistema Nacional Académico (SNA)	X.	X.		X.	X.		X.	
Sistema Nacional de Recursos Humanos	X.	X.		X.	X.		X.	
Sistema Nacional Financiero	X.	X.		X.	X.		X.	
Sistemas Operativos de Servidor	X.	X.		X.	X.	X.	X.	X.
Sistemas Operativos usuarios	X.	X.		X.	X.	X.	X.	X.
Software Académico	X.	X.		X.	X.	X.	X.	X.
Software de Desarrollo	X.	X.		X.	X.	X.	X.	X.
Telefonía IP	X.	X.		X.	X.		X.	
Teléfonos IP	X.	X.	X.	X.	X.		X.	
Videoconferencia	X.	X.		X.	X.		X.	
VPN	X.	X.	X.	X.	X.		X.	
WAN	X.	X.	X.	X.	X.		X.	
WIFI	X.	X.	X.	X.	X.		X.	

Tabla 3.8 Activos implicados en el proyecto 2 frente a las amenazas que el proyecto busca mitigar

3.2.2.4 Planificación

Para la realización del proyecto se efectivizarán las siguientes tareas:

1) Creación de las políticas faltantes: Se debe complementar políticas para:
   Política de Criptografía
   Política de Dispositivos móviles
   Política de manejo de activos
   Para esta tarea se estima un tiempo de dos semanas.

Quien liderará la realización de las diferentes políticas será el Responsable de Seguridad de la Información y existirá a corresponsabilidad de cada Coordinador de las diferentes áreas del Departamento de Tecnologías de Seguridad de la Información

2) Reunión de aprobación con la dirección: Una vez elaboradas las políticas estas deben ser puestas a conocimiento del Comité de Seguridad quienes las elevarán a conocimiento del Comité de Dirección.
Para esta tarea se estima un tiempo de tres días.
Los responsables de la actividad son el Comité de Seguridad de la Información.

3) Difusión de las políticas. Las políticas deben difundirse y comunicarse inmediatamente a todo el personal de la compañía, para ello se seguirá la sistemática de difusión.
Para esta tarea se estima el tiempo de un mes, debido a que se debe comunicar a cerca de 22.000 estudiantes, 1.100 docentes y 300 administrativos.
El Responsable de Seguridad de la Información liderará un equipo de comunicación y difusión.

4) Firmas de acuerdo de confidencialidad: La parte más delicada es la firma de los diferentes acuerdos de confidencialidad y aceptación de las políticas
Para esta tarea se estima un tiempo de dos semanas
Los responsables serán el Responsable de Seguridad de la Información conjuntamente con el Procurador

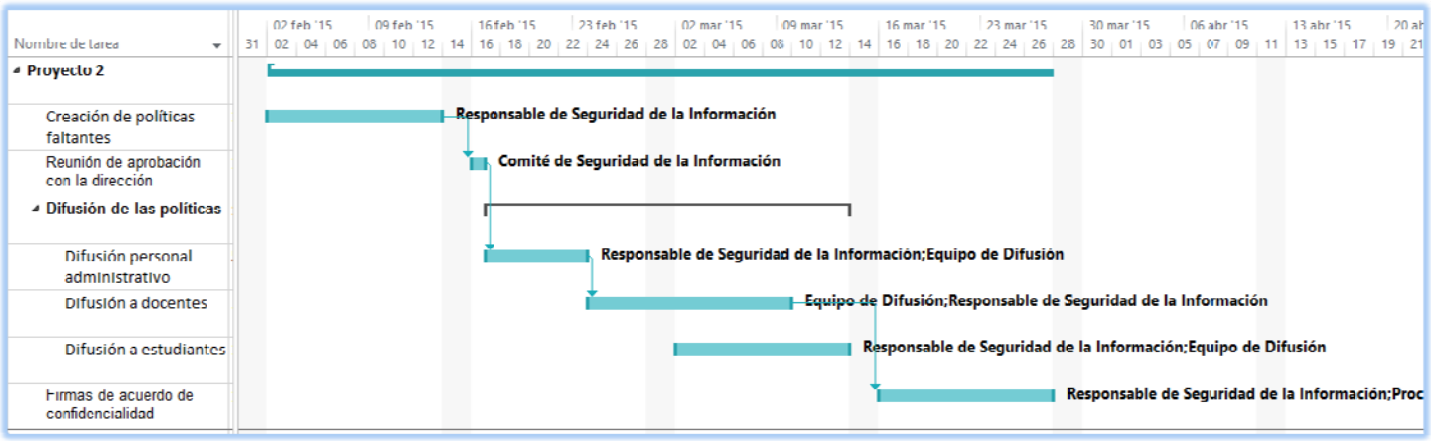


Figura 3.2 Diagrama de Gantt de la planificación del proyecto 2

3.2.2.5 Presupuesto:

Rubro	Cantidad	Valor unidad	subtotal
Horas para creación de las políticas	80	15,00 USD	1.200,00 USD
Material de difusión (imprenta)	1	2.500,00 USD	2.500,00 USD
Horas para difusión de las políticas	150	8,00 USD	1.200,00 USD
Horas de procuraduría	80	15,00 USD	1.200,00 USD
		Total	6.100,00 USD

Tabla 3.9 Presupuesto del proyecto 2

3.2.3 PROYECTO 3: ARTICULACIÓN DE LOS CONTROLES EXISTENTES CON LA POLÍTICA DEL SGSI

Actualmente el departamento de Tecnologías de la Información y Comunicación ha implementado una infinidad de controles, todos están desarticulados y responden a iniciativas Ad-hoc de los integrantes del departamento, buscar la sinergia entre la política y estos controles es prioritario para la UPS.
Es importante destacar que la articulación de controles o salvaguardas puede implicar la modificación, eliminación de los controles actuales o la agregación de nuevos controles a los existentes.

3.2.3.1 Objetivos

Alcanzar por lo menos el estado de madurez de "Definido" según la norma ISO/IEC 27002:2013 para los dominios:

Adquisición, desarrollo y mantenimiento de los sistemas de información.
Relación con suministradores.
Gestión de incidentes en la seguridad de la información.
Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
Seguridad en la operativa.
Seguridad física y ambiental.
Cifrado.

3.2.3.2 Duración

Para este proyecto se estima la duración de tres meses, puede arrancar en paralelo con el proyecto 2.

3.2.3.3 Activos dentro del alcance del proyecto

Los activos implicados son todos aquellos sobre los cuales recae alguna salvaguarda, del total de 84 activos sobre 63 existe alguna salvaguarda; en total existen 33 salvaguardas/controles que mitigan 371 riesgos, en el documento Análisis de Riesgo anexo se puede apreciar las diferentes salvaguardas para cada activo.

3.2.3.4 Planificación

Se requiere realizar las siguientes tareas:

1) Reunión con el Departamento de TI: En esta reunión se pretende sintetizar el alcance de este proyecto, implicar a los diferentes actores y comprometerlos en la ejecución del proyecto. El responsable de esta actividad será el Responsable de Seguridad de la Información.
   La duración de esta reunión es de un día.
   La actividad se llevará a cabo por el Responsable de Seguridad de la Información.

2) Revisión de documentación y controles del departamento de TI: Esta actividad se dividirá en cuatro fases que se trabajarán en paralelo en el transcurso de dos semanas, la responsabilidad global de la actividad es del Responsable de Seguridad de la Información.

   a. Revisión de controles de infraestructura, el responsable es el Coordinador de Infraestructura.
   b. Revisión de controles de redes y comunicaciones, el responsable es el Coordinador de Redes y Comunicaciones.
   c. Revisión de controles de desarrollo de software, el responsable es el Coordinador de Desarrollo de Software.
   d. Revisión de controles de explotación y soporte técnico, el responsable el Coordinador de explotación.

3) Análisis y depuración de controles Ad-hoc: Una vez revisados los diferentes controles se procederá a articularlos de acuerdo a las políticas, para esta fase se realizará un reunión general de un día de duración y se trabajará en la articulación en el periodo de dos semanas.
   Los responsables serán los diferentes coordinadores del departamento de Tecnologías de la Información y Comunicación y el Responsable de Seguridad de la Información.

4) Desarrollo de los controles faltantes: Se dará prioridad a cumplir los diferentes controles de las políticas, que todavía faltasen según la Declaración de Aplicabilidad. Para esta tarea se estima una duración de dos meses.

   La responsabilidad de esta actividad es del Responsable de Seguridad de la Información, quien requerirá, según sea el caso, de cualquier responsable de las diferentes áreas del Departamento de Tecnologías de la Información y Comunicación.

5) El personal del Departamento de Tecnologías de la información contará con un presupuesto de 20.000 dólares para capacitación en temas específicos para dar cumplimiento a la tarea 4. Dicho presupuesto lo deberá justificar el Responsable de Seguridad de las Tecnologías de la información.

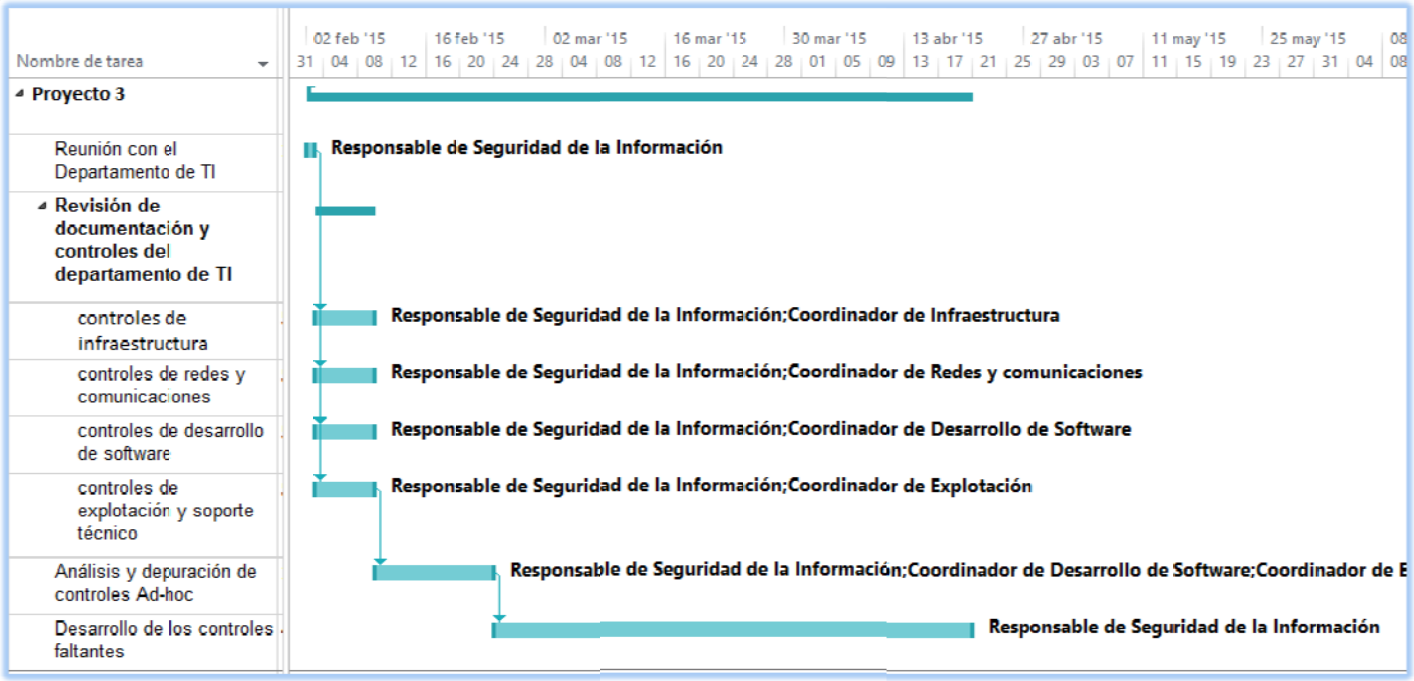


Figura 3.3 Diagrama de Gantt de la planificación del proyecto 3

3.2.3.5 Presupuesto

Rubro	Cantidad	Valor unidad	Subtotal
Horas de personal técnico de TI	800	8,00 USD	6.400,00 USD
Horas de coordinadores del departamento de TI	100	15,00 USD	1.500,00 USD
Horas de consultoría de seguridad de la información	100	25,00 USD	2.500,00 USD
Capacitación Personal de TI	1	20.000,00 USD	20.000,00 USD
		Total	30.400,00 USD

Tabla 3.10 Presupuesto del proyecto 3

3.2.4 PROYECTO 4: PLAN DE CONCIENCIACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Es fundamental establecer un plan de concienciación, este proyecto solo puede ser ejecutado una vez que se hayan realizado todos los proyectos anteriores.

3.2.4.1 Objetivo

Alcanzar el nivel de madurez por lo menos de “Gestionado” en los dominios de la ISO/IEC 27002:2013:

Cumplimiento
Gestión de Incidentes en la seguridad de la información
Seguridad ligada a los recursos humanos

3.2.4.2 Duración

Para este proyecto se estima una duración de un mes, incluida la evaluación.

3.2.4.3 Planificación

1) Reunión de planificación con el Comité de Dirección. La duración de esta actividad es de un día.
   El responsable de esta actividad es el Comité de Seguridad de la Información, quienes elevarán al Comité de Dirección la propuesta.

2) Desarrollo de las capacitaciones generales: Se desea en el periodo de un mes realizar una capacitación sistemática a todos los estudiantes, docentes y administrativos en las siguientes temáticas:
   Capacitación de Seguridad de la Información e implicaciones legales.
   Capacitación Ingeniería Social.
   Los responsables de ejecutar la capacitación será un equipo consultor contratado por la UPS.

3) Capacitaciones específicas: Según las necesidades institucionales se realizarán capacitaciones en las siguientes áreas:
   Capacitación del cuerpo legal de la universidad
   Capacitación del departamento financiero y de recursos humanos
   Capacitación de los docentes en propiedad intelectual
   Los responsables de ejecutar la capacitación será un equipo consultor contratado por la UPS.

4) Evaluación: Esta tarea permitirá valorar la eficacia de cada una de las capacitaciones.
   Para garantizar la transparencia, el Responsable de Seguridad de la Información ejecutará la evaluación de las diferentes capacitaciones y se asegurará que dicha evaluación sea de carácter práctica, con diferentes casos y situaciones que se podrían presentar o se presentan comúnmente en la universidad, para valorar el quehacer de los diferentes actores.

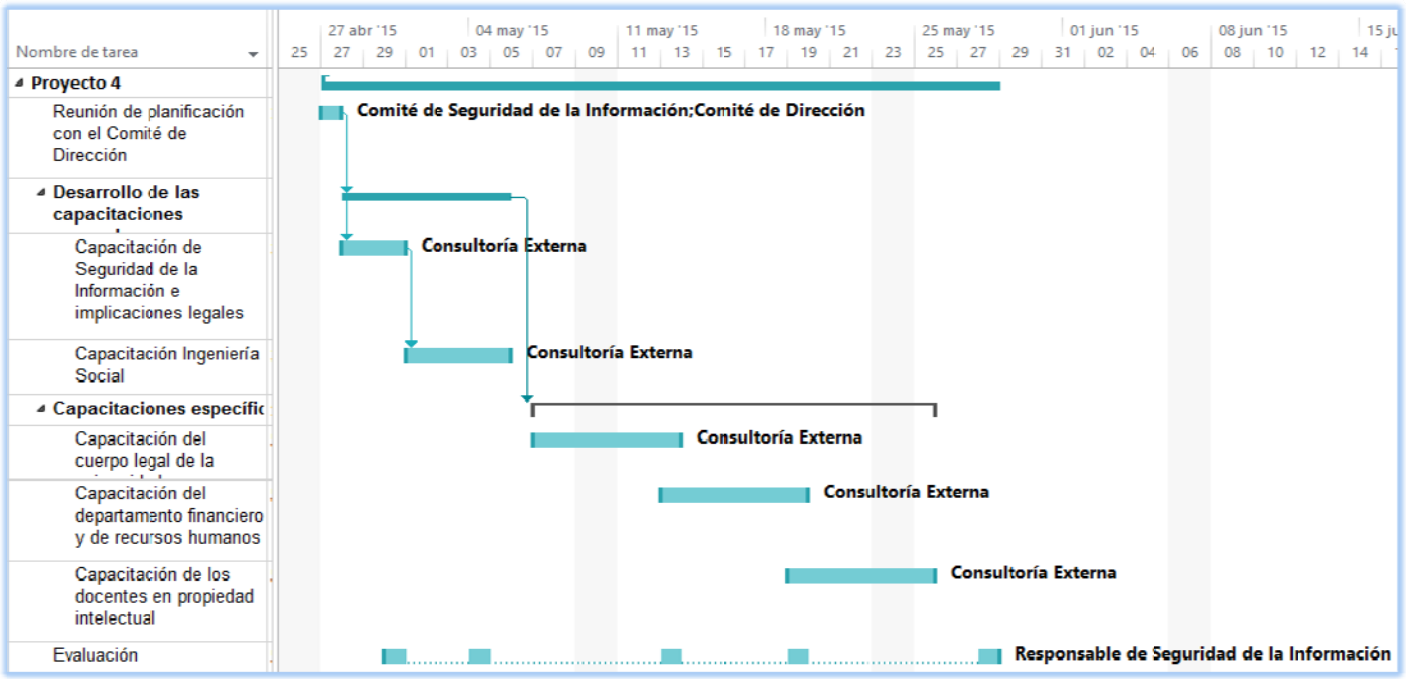


Figura 3.4 Diagrama de Gantt de la planificación del proyecto 4

3.2.4.4 Presupuesto

Rubro	Cantidad	Valor unidad	Subtotal
Consultoría para capacitación en seguridad de la información e implicaciones legales (15 horas)	1	800,00 USD	800,00 USD
Consultoría para capacitación en Ingeniería Social (15 horas)	1	800,00 USD	800,00 USD
Consultoría para capacitación de legislación (20 horas)	1	1.200,00 USD	1.200,00 USD
Consultoría para capacitación de Recursos Humanos (20 horas)	1	1.200,00 USD	1.200,00 USD
Consultoría para capacitación en propiedad intelectual (20 horas)	1	1.200,00 USD	1.200,00 USD
Material para capacitación	1	600,00 USD	600,00 USD
Refrigerios para participantes	1	500,00 USD	500,00 USD
		Total	6.300,00 USD

Tabla 3.11 Presupuesto del proyecto 4

3.2.5 PROYECTO 5: PLAN DE CONTINUIDAD DEL NEGOCIO

Es primordial establecer un plan de continuidad del negocio.

3.2.5.1 Objetivo

Asegurar que la UPS pueda seguir prestando sus servicios académicos y tener la información básica necesaria para el correcto funcionamiento de las actividades administrativas.

Alcanzar el nivel de madurez por lo menos de “Gestionado” en el dominio de la ISO/IEC 27002:2013 “Aspectos de seguridad de la información en la gestión dela continuidad del negocio”

3.2.5.2 Duración

Para este proyecto se estima una duración de un mes.

3.2.5.3 Planificación

1) Reunión de planificación: En esta reunión el Comité de Seguridad de la Información establecerá las diferentes contingencias que el plan debe implementar además asignará los diferentes responsables.
La duración de la reunión es de un día.
Responsable: Comité de Seguridad de la Información

2) Elaboración de los planes de contingencia: Cada área del departamento de Tecnologías de la Información implementará su plan de contingencia garantizando la disponibilidad de los equipos-servicios según las directrices del Comité de Seguridad de la Información.

   a. Plan de contingencia de Infraestructura, el responsable será el Coordinador de Infraestructura.
   b. Plan de contingencia de redes y comunicaciones, el responsable será el Coordinador de Redes y Comunicaciones
   c. Plan de contingencia de explotación, el responsable será el Coordinador de Explotación.

   Para la elaboración de los diferentes planes de contingencia cada área dispondrá de dos semanas.

3) Comprobar el plan y evaluarlo: El plan debe ser puesto a prueba, para ello el Responsable de Seguridad de la Información planificará una evaluación del plan. La duración de esta actividad es de un día.

4) Formación al personal: El personal técnico y administrativo debe contar con la debida preparación para implementar el plan de continuidad. Para esta actividad se prevé una capacitación de 12 horas dosificada en 3 días.
El responsable de la capacitación será el Responsable de Seguridad de la Información.

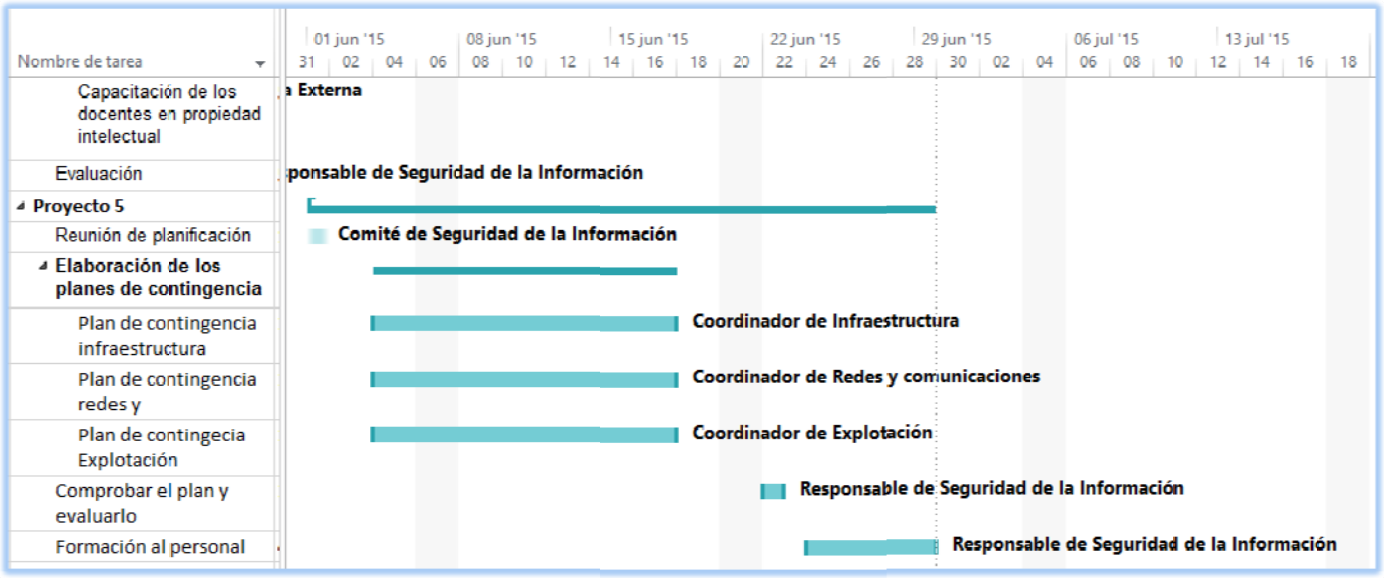


Figura 3.5 Diagrama de Gantt de la planificación del proyecto 5

3.2.5.4 Presupuesto

Rubro	Cantidad	Valor unidad	Subtotal
Horas de personal técnico de TI	160	8,00 USD	1.280,00 USD
Horas de coordinadores del departamento de TI	40	15,00 USD	600,00 USD
Capacitación de responsables del Plan de Continuidad	1	300,00 USD	300,00 USD
		Total	2.180,00 USD

Tabla 3.12 Presupuesto del proyecto 5

Finalmente se presenta la evolución de los proyectos a lo largo del tiempo:

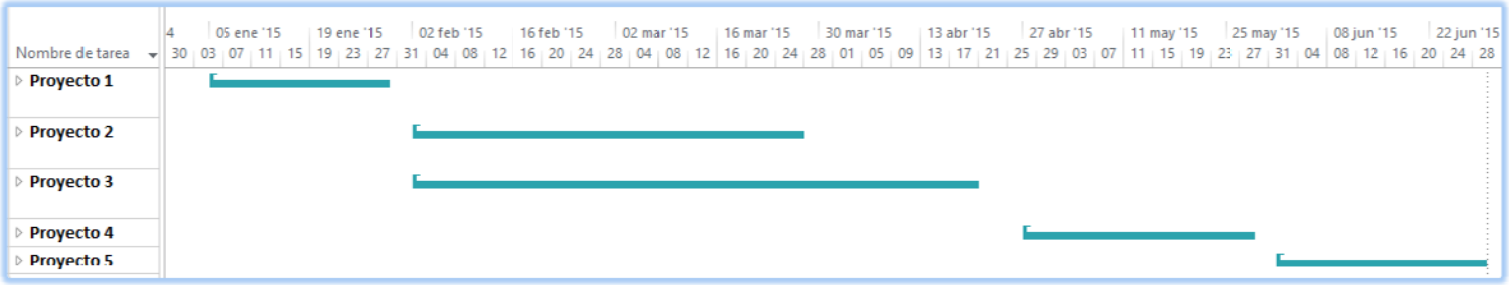


Figura 3.6 Duración total de los proyectos

El tiempo necesario para la implementación de los diferentes proyectos es de 6 meses, la fecha referencial de inicio es el 05 de Enero de 2015, la fecha de culminación el 29 de Junio de 2015, son un presupuesto total de 51.380,00 dólares de los Estados Unidos de América.

3.3 EVOLUCIÓN DE LOS DOMINIOS DE LA ISO/IEC 27002:2013

En la tabla 3.12 se puede ver el estado de madurez de los controles actuales frente al valor esperado:

	DOMINIOS, objetivos, controles	Valor actual	Valor esperado
A5	**5. POLÍTICAS DE SEGURIDAD**		
A5.1	**5.1 Directrices de la Dirección en seguridad de la información**		
A5.1.1	5.1.1 Conjunto de políticas para la seguridad de la información	No existente	Gestionado
A5.1.2	5.1.2 Revisión de las políticas para la seguridad de la información	No existente	Gestionado
A6	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A6.1	**6.1 Organización interna**		
A6.1.1	6.1.1 Asignación de responsabilidades para la seguridad de la información.	Definido	Gestionado
A6.1.2	6.1.2 Segregación de tareas.	Inicial	Gestionado
A6.1.3	6.1.3 Contacto con las autoridades.	Definido	Gestionado
A6.1.4	6.1.4 Contacto con grupos de interés especial.	Inicial	Definido
A6.1.5	6.1.5 Seguridad de la información en la gestión de proyectos.	No existente	Definido
A6.2	**6.2 Dispositivos para movilidad y teletrabajo.**		

A6.2.1	6.2.1 Política de uso de dispositivos para movilidad.	No existente	Definido
A6.2.2	6.2.2 Teletrabajo.	No existente	Limitado
A7	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		
A7.1	**7.1 Antes de la contratación**		
A7.1.1	7.1.1 Investigación de antecedentes.	Limitado	Definido
A7.1.2	7.1.2 Términos y condiciones de contratación.	Definido	Gestionado
A7.2	**7.2 Durante la contratación**		
A7.2.1	7.2.1 Responsabilidades de gestión.	Inicial	Definido
A7.2.2	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Limitado	Definido
A7.2.3	7.2.3 Proceso disciplinario.	No existente	Definido
A7.3	**7.3 Cese o cambio de puesto de trabajo.**		
A7.3.1	7.3.1 Cese o cambio de puesto de trabajo.	Limitado	Definido
A8	**8. GESTIÓN DE ACTIVOS.**		
A8.1	**8.1 Responsabilidad sobre los activos.**		
A8.1.1	8.1.1 Inventario de activos.	Limitado	Gestionado
A8.1.2	8.1.2 Propiedad de los activos.	Inicial	Gestionado
A8.1.3	8.1.3 Uso aceptable de los activos.	Inicial	Definido
A8.1.4	8.1.4 Devolución de activos.	No existente	Definido
A8.2	**8.2 Clasificación de la información.**		
A8.2.1	8.2.1 Directrices de clasificación.	No existente	Definido
A8.2.2	8.2.2 Etiquetado y manipulado de la información.	No existente	Limitado
A8.2.3	8.2.3 Manipulación de activos.	No existente	Limitado
A8.3	**8.3 Manejo de los soportes de almacenamiento.**		
A8.3.1	8.3.1 Gestión de soportes extraíbles.	No existente	Limitado
A8.3.2	8.3.2 Eliminación de soportes.	No existente	Limitado
A8.3.3	8.3.3 Soportes físicos en tránsito.	No existente	Limitado
A9	**9. CONTROL DE ACCESOS.**		
A9.1	**9.1 Requisitos de negocio para el control de accesos.**		
A9.1.1	9.1.1 Política de control de accesos.	No existente	Gestionado
A9.1.2	9.1.2 Control de acceso a las redes y servicios asociados.	Definido	Gestionado
A9.2	**9.2 Gestión de acceso de usuario.**		
A9.2.1	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Definido	Gestionado
A9.2.2	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	No existente	Definido
A9.2.3	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Limitado	Definido
A9.2.4	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Limitado	Definido
A9.2.5	9.2.5 Revisión de los derechos de acceso de los usuarios.	No existente	Limitado

A9.2.6	9.2.6 Retirada o adaptación de los derechos de acceso	Limitado	Definido
A9.3	**9.3 Responsabilidades del usuario.**		
A9.3.1	9.3.1 Uso de información confidencial para la autenticación.	Definido	Gestionado
A9.4	**9.4 Control de acceso a sistemas y aplicaciones.**		
A9.4.1	9.4.1 Restricción del acceso a la información.	Inicial	Limitado
A9.4.2	9.4.2 Procedimientos seguros de inicio de sesión.	Definido	Gestionado
A9.4.3	9.4.3 Gestión de contraseñas de usuario.	Definido	Gestionado
A9.4.4	9.4.4 Uso de herramientas de administración de sistemas.	No existente	Limitado
A9.4.5	9.4.5 Control de acceso al código fuente de los programas	Limitado	Limitado
A10	**10. CIFRADO.**		
A10.1	**10.1 Controles criptográficos.**		
A10.1.1	10.1.1 Política de uso de los controles criptográficos.	No existente	Definido
A10.1.2	10.1.2 Gestión de claves.	Inicial	Definido
A11	**11. SEGURIDAD FÍSICA Y AMBIENTAL.**		
A11.1	**11.1 Áreas seguras.**		
A11.1.1	11.1.1 Perímetro de seguridad física.	Definido	Gestionado
A11.1.2	11.1.2 Controles físicos de entrada.	Limitado	Gestionado
A11.1.3	11.1.3 Seguridad de oficinas, despachos y recursos.	Inicial	Definido
A11.1.4	11.1.4 Protección contra las amenazas externas y ambientales.	Definido	Definido
A11.1.5	11.1.5 El trabajo en áreas seguras.	No existente	Definido
A11.1.6	11.1.6 Áreas de acceso público, carga y descarga.	No existente	Definido
A11.2	**11.2 Seguridad de los equipos.**		
A11.2.1	11.2.1 Emplazamiento y protección de equipos.	Limitado	Definido
A11.2.2	11.2.2 Instalaciones de suministro.	Gestionado	Gestionado
A11.2.3	11.2.3 Seguridad del cableado.	Gestionado	Gestionado
A11.2.4	11.2.4 Mantenimiento de los equipos.	Gestionado	Gestionado
A11.2.5	11.2.5 Salida de activos fuera de las dependencias de la empresa.	No existente	Inicial
A11.2.6	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	No existente	Inicial
A11.2.7	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Inicial	Definido
A11.2.8	11.2.8 Equipo informático de usuario desatendido.	Definido	Gestionado
A11.2.9	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	No existente	Definido
A12	**12. SEGURIDAD EN LA OPERATIVA.**		
A12.1	**12.1 Responsabilidades y procedimientos de operación.**		
A12.1.1	12.1.1 Documentación de procedimientos de operación.	No existente	Definido
A12.1.2	12.1.2 Gestión de cambios.	Inicial	Definido
A12.1.3	12.1.3 Gestión de capacidades.	No existente	Definido
A12.1.4	12.1.4 Separación de entornos de desarrollo, prueba y producción.	No existente	Gestionado
A12.2	**12.2 Protección contra código malicioso.**		

A12.2.1	12.2.1 Controles contra el código malicioso.	Gestionado	Gestionado
A12.3	**12.3 Copias de seguridad.**		
A12.3.1	12.3.1 Copias de seguridad de la información.	Definido	Gestionado
A12.3	**12.4 Registro de actividad y supervisión.**		
A12.4.1	12.4.1 Registro y gestión de eventos de actividad.	Limitado	Definido
A12.4.2	12.4.2 Protección de los registros de información.	No existente	Definido
A12.4.3	12.4.3 Registros de actividad del administrador y operador del sistema.	No existente	Definido
A12.4.4	12.4.4 Sincronización de relojes.	Gestionado	Gestionado
A12.5	**12.5 Control del software en explotación.**		
A12.5.1	12.5.1 Instalación del software en sistemas en producción.	No existente	Definido
A12.6	**12.6 Gestión de la vulnerabilidad técnica.**		
A12.6.1	12.6.1 Gestión de las vulnerabilidades técnicas.	Inicial	Definido
A12.6.2	12.6.2 Restricciones en la instalación de software.	No existente	Definido
A12.7	**12.7 Consideraciones de las auditorías de los sistemas de información.**		
A12.7.1	12.7.1 Controles de auditoría de los sistemas de información.	No existente	Inicial
A13	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**		
A13.1	**13.1 Gestión de la seguridad en las redes.**		
A13.1.1	13.1.1 Controles de red.	Gestionado	Gestionado
A13.1.2	13.1.2 Mecanismos de seguridad asociados a servicios en red.	Definido	Gestionado
A13.1.3	13.1.3 Segregación de redes.	Gestionado	Gestionado
A13.2	**13.2 Intercambio de información con partes externas.**		
A13.2.1	13.2.1 Políticas y procedimientos de intercambio de información.	No existente	Definido
A13.2.2	13.2.2 Acuerdos de intercambio.	No existente	Definido
A13.2.3	13.2.3 Mensajería electrónica.	Gestionado	Gestionado
A13.2.4	13.2.4 Acuerdos de confidencialidad y secreto	Gestionado	Gestionado
A14	**14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**		
A14.1	**14.1 Requisitos de seguridad de los sistemas de información.**		
A14.1.1	14.1.1 Análisis y especificación de los requisitos de seguridad.	Inicial	Limitado
A14.1.2	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Inicial	Limitado
A14.1.3	14.1.3 Protección de las transacciones por redes telemáticas.	No existente	Definido
A14.2	**14.2 Seguridad en los procesos de desarrollo y soporte.**		
A14.2.1	14.2.1 Política de desarrollo seguro de software.	No existente	Definido
A14.2.2	14.2.2 Procedimientos de control de cambios en los sistemas.	Inicial	Definido
A14.2.3	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	No existente	Definido
A14.2.4	14.2.4 Restricciones a los cambios en los paquetes de software.	No existente	Definido
A14.2.5	14.2.5 Uso de principios de ingeniería en protección de	No	Definido

	sistemas.	existente	
A14.2.6	14.2.6 Seguridad en entornos de desarrollo.	No existente	Gestionado
A14.2.7	14.2.7 Externalización del desarrollo de software.	Definido	Definido
A14.2.8	14.2.8 Pruebas de seguridad de los sistemas.	No existente	Gestionado
A14.2.9	14.2.9 Pruebas de aceptación.	No existente	Gestionado
A14.3	**14.3 Datos de prueba.**		
A14.3.1	14.3.1 Protección de los datos utilizados en pruebas.	No existente	Definido
A15	**15. RELACIONES CON SUMINISTRADORES.**		
A15.1	**15.1 Seguridad de la información en las relaciones con suministradores.**		
A15.1.1	15.1.1 Política de seguridad de la información para suministradores.	No existente	Definido
A15.1.2	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	No existente	Definido
A15.1.3	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	No existente	Definido
A15.2	**15.2 Gestión de la prestación del servicio por suministradores.**		
A15.2.1	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Limitado	Gestionado
A15.2.2	15.2.2 Gestión de cambios en los servicios prestados por terceros.	No existente	Gestionado
A16	**16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**		
A16.1	**16.1 Gestión de incidentes de seguridad de la información y mejoras.**		
A16.1.1	16.1.1 Responsabilidades y procedimientos.	No existente	Definido
A16.1.2	16.1.2 Notificación de los eventos de seguridad de la información.	No existente	Definido
A16.1.3	16.1.3 Notificación de puntos débiles de la seguridad.	No existente	Definido
A16.1.4	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	No existente	Definido
A16.1.5	16.1.5 Respuesta a los incidentes de seguridad.	No existente	Definido
A16.1.6	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	No existente	Limitado
A16.1.7	16.1.7 Recopilación de evidencias.	No existente	Definido
A17	**17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DELA CONTINUIDAD DEL NEGOCIO.**		
A17.1	**17.1 Continuidad de la seguridad de la información.**		
A17.1.1	17.1.1 Planificación de la continuidad de la seguridad de la información.	No existente	Definido
A17.1.2	17.1.2 Implantación de la continuidad de la seguridad de la información.	No existente	Definido
A17.1.3	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	No existente	Definido
A17.2	**17.2 Redundancias.**		

A17.2.1	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	Gestionado	Optimizado
A18	**18. CUMPLIMIENTO.**		
A18.1	**18.1 Cumplimiento de los requisitos legales y contractuales.**		
A18.1.1	18.1.1 Identificación de la legislación aplicable.	No existente	Gestionado
A18.1.2	18.1.2 Derechos de propiedad intelectual (DPI).	Inicial	Definido
A18.1.3	18.1.3 Protección de los registros de la organización.	Definido	Gestionado
A18.1.4	18.1.4 Protección de datos y privacidad de la información personal.	No existente	Definido
A18.1.5	18.1.5 Regulación de los controles criptográficos.	No existente	Definido
A18.2	**18.2 Revisiones de la seguridad de la información.**		
A18.2.1	18.2.1 Revisión independiente de la seguridad de la información.	No existente	Definido
A18.2.2	18.2.2 Cumplimiento de las políticas y normas de seguridad.	No existente	Definido
A18.2.3	18.2.3 Comprobación del cumplimiento.	No existente	Definido

Tabla 3.13 Nivel de madurez de los controles ISO/IEC 27002:2013

La figura 3.6 permite apreciar en un diagrama de radio la evolución del SGSI, entre el valor actual y el esperado.

Con el desarrollo, aprobación e implementación de las diferentes políticas de seguridad se espera poder elevar el nivel de madurez de los dominios:

5. Políticas de Seguridad
6. Aspectos Organizativos de la Seguridad de la Información

Los dominios 5 y 6 son elementos fundamentales que permitirán que el SGSI pueda despuntar en otros dominios, de ahí la importancia del proyecto 3 que articulará los diferentes controles Ad-hoc con la política.

En la figura 3.7 podemos apreciar la evolución esperada del SGSI, nótese que el dominio 5 “Políticas de Seguridad” tiene una madurez cero.

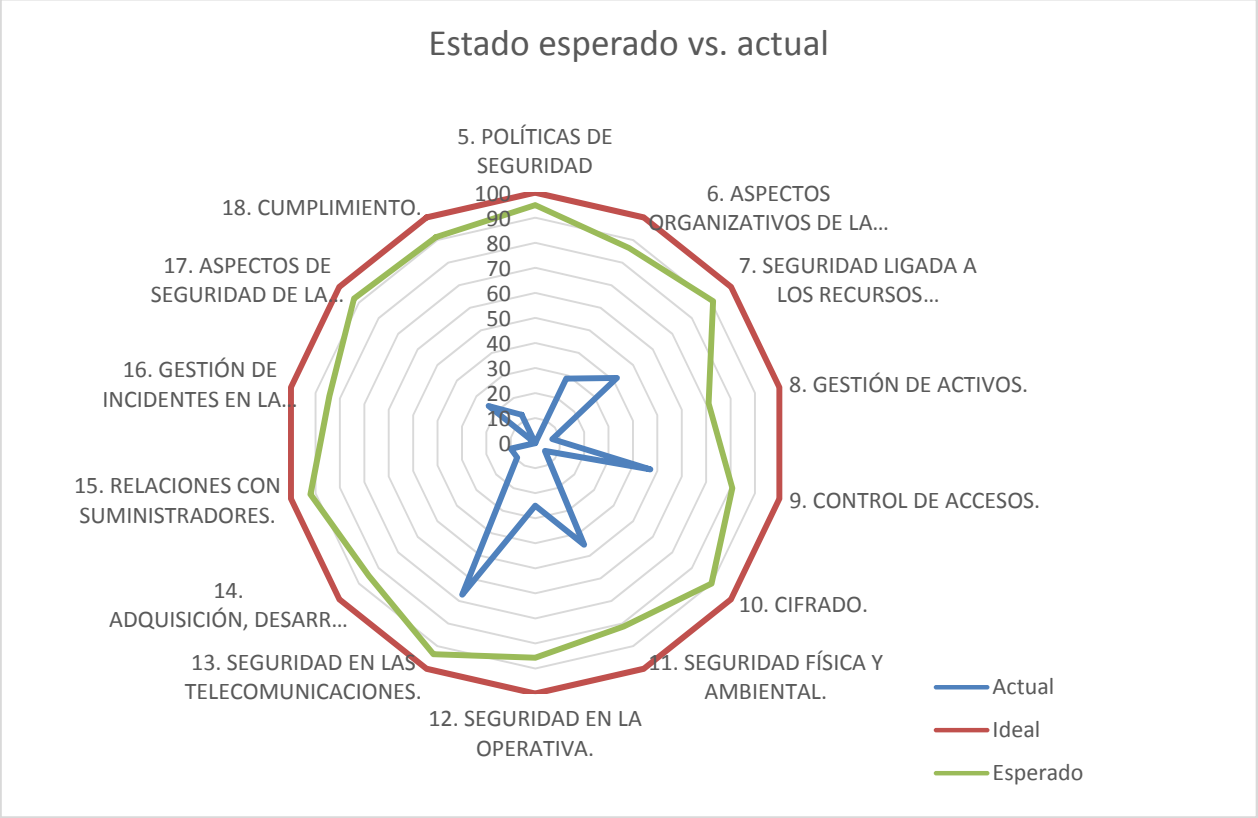


Figura 3.7 Diagrama de radio de los dominios de la norma ISO/IEC 27002:2013

4 CAPÍTULO 5: AUDITORÍA DE CUMPLIMIENTO

De acuerdo al anexo 03 *Procedimiento de Auditorías Internas* se procede a realizar la auditoría, para ello se utiliza las plantillas de planificación y de informe de Auditoría detallas en el citado procedimiento.

4.1 PLAN DE AUDITORÍA

4.1.1 OBJETIVOS

Verificar el estado de implementación y cumplimiento de la norma ISO/IEC 27001:2013 y de los controles establecidos en la declaración de aplicabilidad de la UPS.

4.1.2 INVENTARIO DE POLÍTICAS

4.1.2.1 Políticas Internas

Documento	Tipo	Descripción
Política de Seguridad de la Información	Política	Contiene los lineamientos estratégicos de la seguridad de la información
Política de Alto Nivel	Política	Expresa el compromiso de la Dirección
Política de Clasificación de la Información	Política	
Política de Control de Acceso	Política/Control	Define el control de acceso físico y lógico
Política de Uso de Correo Electrónico	Política/Control	Define el uso correcto del correo electrónico
Política de Desarrollo Seguro	Política/Control	Da las directrices para desarrollo seguro de software
Política de Gestión de incidentes	Política	Da las directrices para gestionar los diferentes incidentes del SGSI
Política de Criptografía	Política/Control	Guía sobre el uso de criptografía y conexiones seguras
Política de Dispositivos Móviles	Política/Control	Directrices sobre el uso y manejo de dispositivos móviles con información de la UPS
Política de manejo de activos	Política/Control	Guía para el correcto uso de activos
Organización de la seguridad de la información	Documento	Documento con los diferentes roles y actores de la seguridad de la información
Procedimiento de Auditorías Internas	Procedimiento	Procedimiento para ejecutar auditorías internas
Gestión de Indicadores	Documento	Procedimiento para el establecimiento y gestión de indicadores
Procedimiento de Revisión por la Dirección	Procedimiento	Procedimiento para guiar a la dirección acerca de la revisión del SGSI
Metodología de Análisis de Riesgos	Documento	Detalle de todo el proceso metodológico para el análisis de riesgos
Declaración de aplicabilidad	Documento	Detalle de todos los controles que deben ser implementados en la UPS

4.1.2.2 Políticas externas

Documento	Tipo	Descripción
Ley Orgánica de Educación Superior (LOES)	Ley nacional de primer orden	Establece los lineamientos sobre la información que necesitan las universidades
Reglamento de Régimen Académico	Reglamento Nacional	Define los aspectos de la democratización del conocimiento
Guías de Evaluación de Carreras de Grado y Programas de Posgrado	Guías de evaluación universitarias a nivel nacional	Define toda la información que las universidades necesitan tener almacenada como evidencias de los procesos de evaluación
Norma ISO/IEC 27001:2013	Norma	
Norma ISO/IEC 27002:2013	Norma	

4.1.1 ALCANCE DE AUDITORÍA

Verificar el nivel de cumplimiento de la norma ISO/IEC 27001:2013 y de los 18 dominios de la norma ISO/IEC 27002:2013 según la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información.

4.1.2 METODOLOGÍA

La declaración de aplicabilidad es la guía fundamental en la ejecución de la auditoría, según los controles declarados, se solicitará el respectivo respaldo documental del control que incluye políticas, normas, estándares y procedimientos, también se exigirá los registros respectivos que servirán como evidencia del proceso, entre ellos están informes, actas, evolución de indicadores.

Cada uno de los controles será evaluado mediante el modelo de madurez CMM que se muestra en la tabla:

Estado	Significado	Valoración cuantitativa
¿ Desconocido	Todavía no ha sido chequeado	0%
No existente	Falta completa de política reconocible, proceso, control, etc.	0%
Inicial	Desarrollo apenas iniciado y requerirá un significante trabajo para completar los requerimientos.	10%
Limitado	Progresando de manera correcta pero todavía no completado	50%
Definido	Desarrollo más o menos completo aunque el detalle es deficiente y/o todavía no se ha implementado y respaldado activamente por la Dirección	90%
Gestionado	Desarrollo está completo, el proceso/control ha sido implementado y recientemente comenzó a operar	95%
Optimizado	El requerimiento es completamente satisfactorio, está operando plenamente como era de esperar, está iniciando el monitoreo y mejora activamente, y existe evidencia substancial para probar todo a los auditores	100%
No aplicable	Este requerimiento no es aplicable a la organización. Nota: Todos los requerimientos en el cuerpo de ISO/IEC 27001 son mandatorios, si el SGSI	

Tabla 3.13 Modelo de madurez CMM utilizado en la Auditoría de Cumplimiento

4.1.3 ENTORNO DE PRUEBAS REQUERIDO

No se requiere ningún entorno específico

4.1.4 PROCEDIMIENTOS DE CONTROL DE LAS PRUEBAS

Se verificará los 27 requerimientos de la ISO/IEC 27001:2013 y a cada requerimiento se le asignará su nivel de madurez.

Por cada domino de la ISO/IEC 27002:2013 se procederá a evaluar el objetivo respectivo mediante el promedio de la valoración de los diferentes controles

4.1.5 DEFINICIÓN DE LAS PRUEBAS

Primeramente se realizará la evaluación de la Declaración de Aplicabilidad, por cada dominio se presentará la siguiente información:

Código	Descripción	Madurez	Valor cuantitativo	Justificación	No Conformidad: Mayor | Menor | Observación | Oportunidad
X	**Dominio**		(Promedio Dominio)		
X.X	**Objetivo**	**(Promedio Objetivo)**			
X.X.1	Control 1	No existente	(Valor Control)		
X.X.2	Control n	No existente	(Valor control)		

Tabla 3.14 Definición del formato para las pruebas de cumplimiento

4.1.6 EJECUCIÓN DE LA AUDITORÍA

Cod.	DOMINIO / Objetivo / Control	Madurez		Justificación	No Conformidad: Mayor | Menor | Observación | Oportunidad
A5	**5. POLÍTICAS DE SEGURIDAD**		**95**		
A5.1	**5.1 Directrices de la Dirección en seguridad de la información**	**95**			
A5.1.1	5.1.1 Conjunto de políticas para la seguridad de la información	Gestionado	95	Todas las políticas están definidas, aprobadas por el Comité de Dirección e implementadas.	
A5.1.2	5.1.2 Revisión de las políticas para la seguridad de la información	Gestionado	95	Existe un plan de revisión de todas las políticas según la sistemática de comunicación.	
A6	**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN**		**75**		
A6.1	**6.1 Organización interna**	**95**			
A6.1.1	6.1.1 Asignación de responsabilidades para la seguridad de la información.	Optimizado	100	Existe el documento de Organización de Seguridad de la información, los cargos se han contratado y se ha redefinido el descriptor de cargos.	
A6.1.2	6.1.2 Segregación de tareas.	Gestionado	95	El descriptor de cargos ha sido actualizado.	

A6.1.3	6.1.3 Contacto con las autoridades.	Gestionado	95	Existe una sistemática de comunicación.	
A6.1.4	6.1.4 Contacto con grupos de interés especial.	Definido	90	En Ecuador casi no existen grupos de interés, la mayoría son grupos de los proveedores, pero no existe nada formalizado.	
A6.1.5	6.1.5 Seguridad de la información en la gestión de proyectos.	Gestionado	95	Todo el personal docente y administrativo ha firmado las clausulas de confidencialidad y ha sido capacitado sobre sus implicaciones en seguridad de la información.	
A6.2	**6.2 Dispositivos para movilidad y teletrabajo.**	**25**			**No conformidad mayor**
A6.2.1	6.2.1 Política de uso de dispositivos para movilidad.	Limitado	50	La política fue definida, pero se está trabajando en los controles.	No Conformidad Menor: Los usuarios llevan en sus dispositivos móviles información confidencial sin ningún tipo de control.
A6.2.2	6.2.2 Teletrabajo.	No existente	0	No existe política aprobada, se mantienen el control Ad-hoc implementado.	No Conformidad Menor: Existen usuarios con responsabilidad de autoridad que realizan conexiones VPN, no se ha definido políticas porque la dirección considera engorroso el proceso.
A7	**7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		**80**		
A7.1	**7.1 Antes de la contratación**	**95**			
A7.1.1	7.1.1 Investigación de antecedentes.	Gestionado	95	El departamento de Recursos Humanos ha incorporado esta práctica en la contratación. Se busca optimizarla mediante la investigación periódica donde se incluye el personal ya contratado.	
A7.1.2	7.1.2 Términos y condiciones de contratación.	Gestionado	95	Todo trabajador debe firmar acuerdo de confidencialidad y aceptar las políticas de seguridad, además reconoce su ámbito de gestión.	
A7.2	**7.2. Durante la contratación**	**65**			
A7.2.1	7.2.1 Responsabilidades de gestión.	Gestionado	95	Todos los trabajadores reconocer su actoría en la seguridad de la información.	
A7.2.2	7.2.2 Concienciación, educación y capacitación en seguridad de la información	Definido	90	El plan de capacitación ha sido ejecutado.	Oportunidad de mejora: Apenas el 80 % de los usuarios ha sido capacitado. El dato es alarmante a nivel de autoridades, ya que el 50% todavía no está capacitado.
A7.2.3	7.2.3 Proceso disciplinario.	Inicial	10	El control se ha quedado estancado en la procuraduría.	No Conformidad Menor: Las políticas hacen referencias que ante el incumplimiento se tomarán los procesos disciplinarios correspondientes, sin embargo estos no están definidos.

A7.3	**7.3 Cese o cambio de puesto de trabajo.**	**95**			
A7.3.1	7.3.1 Cese o cambio de puesto de trabajo.	Gestionado	95	Recursos humanos en coordinación con del Departamento de TIC ha implementado el control y lo mantienen operando.	
A8	**8. GESTIÓN DE ACTIVOS.**		**67**		
A8.1	**8.1 Responsabilidad sobre los activos.**	**83,75**			
A8.1.1	8.1.1 Inventario de activos.	Gestionado	95	Existe la política de clasificación de activos de la información, actualmente los mismos están clasificados por sus respectivos propietarios.	
A8.1.2	8.1.2 Propiedad de los activos.	Gestionado	95	Existe la política de clasificación de activos de la información, actualmente los mismos están clasificados por sus respectivos propietarios.	
A8.1.3	8.1.3 Uso aceptable de los activos.	Limitado	50	Existe la política, está aprobada por dirección, pero no se ha implementado.	No Conformidad Menor: La gestión de indicadores muestra que todavía existen usuarios que no utilizan adecuadamente los activos. La necesidad de implementar los controles es urgente pues los principales activos afectados son los computadores portátiles de los docentes.
A8.1.4	8.1.4 Devolución de activos.	Gestionado	95	Existen controles que se aplican, todos los usuarios firman actas de entrega recepción sobre los activos puestos a su cargo.	
A8.2	**8.2 Clasificación de la información.**	**91,666667**			
A8.2.1	8.2.1 Directrices de clasificación.	Gestionado	95	Existe la política aprobada.	
A8.2.2	8.2.2 Etiquetado y manipulado de la información.	Definido	90	Existe la política y se está en proceso de rediseño los sistemas de información.	
A8.2.3	8.2.3 Manipulación de activos.	Definido	90	Existe la política aprobada, lamentablemente se requiere de 8.2.2 para elevar la madurez a gestionado.	
A8.3	**8.3 Manejo de los soportes de almacenamiento.**	**20**			
A8.3.1	8.3.1 Gestión de soportes extraíbles.	Limitado	50	La diversificación de dispositivos de almacenamiento y la gran cantidad de activos han estancado la tarea.	No Conformidad Menor: La totalidad de equipos cuentan con unidades de CD-DVD funcionales, puertos USB habilitados, no existe ningún control de los dispositivos de almacenamiento de los diferentes usuarios.
A8.3.2	8.3.2 Eliminación de soportes.	Inicial	10	Solo existe control para la información impresa.	
A8.3.3	8.3.3 Soportes físicos en tránsito.	No existente	0	Lamentablemente se requiere que 8.3.1 este implementado para arrancar con estos controles.	

A9	**9. CONTROL DE ACCESOS.**		**94,28**		
A9.1	**9.1 Requisitos de negocio para el control de accesos.**	**97,5**			
A9.1.1	9.1.1 Política de control de accesos.	Gestionado	95	Existe la política, está aprobada por la dirección y se ha implementado.	
A9.1.2	9.1.2 Control de acceso a las redes y servicios asociados.	Optimizado	100	Los controles están operativos, existe monitoreo y capacidad de mejora.	
A9.2	**9.2 Gestión de acceso de usuario.**	**95**			
A9.2.1	9.2.1 Gestión de altas/bajas en el registro de usuarios.	Optimizado	100	Existen controles definidos y procesos a seguir entre Recursos Humanos y el Departamento de TICS.	
A9.2.2	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Gestionado	95	Entre Recursos Humanos y el Departamento de TICS se gestiona estos controles.	
A9.2.3	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Gestionado	95	Entre Recursos Humanos y el Departamento de TICS mediante autorización de las diferentes autoridades.	
A9.2.4	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Gestionado	95	Existen controles definidos y procesos a seguir entre Recursos Humanos y el Departamento de TICS.	
A9.2.5	9.2.5 Revisión de los derechos de acceso de los usuarios.	Definido	90	Existen controles definidos y procesos a seguir entre Recursos Humanos y el Departamento de TICS.	
A9.2.6	9.2.6 Retirada o adaptación de los derechos de acceso	Gestionado	95	Existen controles definidos y procesos a seguir entre Recursos Humanos y el Departamento de TICS.	
A9.3	**9.3 Responsabilidades del usuario.**	**95**			
A9.3.1	9.3.1 Uso de información confidencial para la autenticación.	Gestionado	95	Controles definidos e implementados.	
A9.4	**9.4 Control de acceso a sistemas y aplicaciones.**	**92**			
A9.4.1	9.4.1 Restricción del acceso a la información.	Definido	90	Los sistemas de información se han adaptado a las políticas.	
A9.4.2	9.4.2 Procedimientos seguros de inicio de sesión.	Gestionado	95	Controles definidos e implementados.	
A9.4.3	9.4.3 Gestión de contraseñas de usuario.	Gestionado	95	Controles definidos e implementados.	
A9.4.4	9.4.4 Uso de herramientas de administración de sistemas.	Definido	90	Se gestiona los recursos de HW y SW de los diferentes equipos.	
A9.4.5	9.4.5 Control de acceso al código fuente de los programas	Definido	90	El control todavía presenta deficiencias.	
A10	**10. CIFRADO.**		**90**		
A10.1	**10.1 Controles criptográficos.**	**90**			
A10.1.1	10.1.1 Política de uso de los controles criptográficos.	Definido	90	Se ha definido la política, pero existen sectores donde todavía no se la aplica.	

A10.1.2	10.1.2 Gestión de claves.	Definido	90	Se ha definido la política, pero existen sectores donde todavía no se la aplica.	
A11	**11. SEGURIDAD FÍSICA Y AMBIENTAL.**		**77**		
A11.1	**11.1 Áreas seguras.**	**86,666667**			
A11.1.1	11.1.1 Perímetro de seguridad física.	Gestionado	95	Los diferentes controles se han articulado en un único sistema de control de acceso y monitoreo.	
A11.1.2	11.1.2 Controles físicos de entrada.	Gestionado	95	Dependiendo de las áreas se definen distintos niveles y requisitos de acceso.	
A11.1.3	11.1.3 Seguridad de oficinas, despachos y recursos.	Gestionado	95	Los diferentes controles se han articulado en un único sistema de control de acceso y monitoreo.	
A11.1.4	11.1.4 Protección contra las amenazas externas y ambientales.	Gestionado	95	Los diferentes controles se han articulado en un único sistema de control de acceso y monitoreo.	
A11.1.5	11.1.5 El trabajo en áreas seguras.	Limitado	50	Se ha implementado sistemas biométricos para ingreso a áreas seguras.	
A11.1.6	11.1.6 Áreas de acceso público, carga y descarga.	Definido	90	Se ha adaptado un área para carga y descarga, los proveedores están siendo notificados.	
A11.2	**11.2 Seguridad de los equipos.**	**70,555556**			
A11.2.1	11.2.1 Emplazamiento y protección de equipos.	Definido	90	Controles definidos e implementados.	No Conformidad Menor: No existe ningún control para los dispositivos móviles como laptops y teléfonos.
A11.2.2	11.2.2 Instalaciones de suministro.	Gestionado	95	Existen redundancias de hardware en equipos esenciales.	
A11.2.3	11.2.3 Seguridad del cableado.	Gestionado	95	Todas las instalaciones cuentan con cableado estructurado.	
A11.2.4	11.2.4 Mantenimiento de los equipos.	Gestionado	95	Los equipos tienen mantenimiento periódico definido en las políticas de uso de activos.	Oportunidad de mejora: A pesar de que la política indica que cada seis meses los usuarios deben llevar a mantenimiento sus equipos el 80% no lo ha realizado, ni siquiera existen registros de la última vez que se dio mantenimiento.
A11.2.5	11.2.5 Salida de activos fuera de las dependencias de la empresa.	Inicial	10	Existe la política.	No Conformidad Menor: No existe ningún control para los activos que salen de la UPS.
A11.2.6	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Inicial	10	Existe la política.	No Conformidad Menor: No existe ninguna seguridad para los activos que salen de la UPS.
A11.2.7	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	Limitado	50	No se borra a bajo nivel datos de discos duros.	
A11.2.8	11.2.8 Equipo informático de usuario desatendido.	Gestionado	95	Todos los sistemas de información y sistemas operativos han implementado timeout como uno de los controles.	

A11.2.9	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Gestionado	95	Las políticas y acuerdos de confidencialidad ha concienciado a los usuarios.	
A12	**12. SEGURIDAD EN LA OPERATIVA.**		**94,28**		
A12.1	**12.1 Responsabilidades y procedimientos de operación.**	**92,5**			
A12.1.1	12.1.1 Documentación de procedimientos de operación.	Definido	90	Toda la documentación está en proceso de creación.	
A12.1.2	12.1.2 Gestión de cambios.	Gestionado	95	Existen un control de cambios y procedimientos a seguir.	
A12.1.3	12.1.3 Gestión de capacidades.	Gestionado	95	Las diferentes herramientas de monitoreo se han articulado.	
A12.1.4	12.1.4 Separación de entornos de desarrollo, prueba y producción.	Definido	90	Se han separado los entornos, pero todavía se trabaja con datos de la base real.	
A12.2	**12.2 Protección contra código malicioso.**	**95**			
A12.2.1	12.2.1 Controles contra el código malicioso.	Gestionado	95	Antivirus actualizado y se registra un nivel de actualización de 100%.	
A12.3	**12.3 Copias de seguridad.**	**95**			
A12.3.1	12.3.1 Copias de seguridad de la información.	Gestionado	95	Las copiar siguen un procedimiento bien definido.	
A12.3	**12.4 Registro de actividad y supervisión.**	**95**			
A12.4.1	12.4.1 Registro y gestión de eventos de actividad.	Gestionado	95	La articulación de controles ha permitido gestionar mejor el monitoreo.	
A12.4.2	12.4.2 Protección de los registros de información.	Gestionado	95	La política de backups considera los diferentes logs de los sistemas.	
A12.4.3	12.4.3 Registros de actividad del administrador y operador del sistema.	Gestionado	95	Se registra todas las actividades de los usuarios administradores y se generan backups.	
A12.4.4	12.4.4 Sincronización de relojes.	Gestionado	95	Se utiliza el protocolo NTP.	
A12.5	**12.5 Control del software en explotación.**	**95**			
A12.5.1	12.5.1 Instalación del software en sistemas en producción.	Gestionado	95	Existe un proceso de instalación de software para los usuarios.	
A12.6	**12.6 Gestión de la vulnerabilidad técnica.**	**95**			
A12.6.1	12.6.1 Gestión de las vulnerabilidades técnicas.	Gestionado	95	Son funciones del Responsable de Seguridad de la Información.	
A12.6.2	12.6.2 Restricciones en la instalación de software.	Gestionado	95	Solo mediante autorización se puede instalar software en equipos, el active directory permite el control y monitoreo.	
A12.7	**12.7 Consideraciones de las auditorías de los sistemas de información.**	**95**			
A12.7.1	12.7.1 Controles de auditoría de los sistemas de información.	Gestionado	95	Estos procesos están desarrollados y gestionados por el Auditor Interno.	
A13	**13. SEGURIDAD EN LAS TELECOMUNICACIONES.**		**93,57**		
A13.1	**13.1 Gestión de la seguridad en las redes.**	**95**			

A13.1.1	13.1.1 Controles de red.	Gestionado	95	Controles gestionados y administrados.	
A13.1.2	13.1.2 Mecanismos de seguridad asociados a servicios en red.	Gestionado	95	Controles gestionados y administrados.	Oportunidad de mejora: Los usuarios consideran los controles restrictivos, no existe una verdadera conectividad. Esto atenta con el principio de la Academia.
A13.1.3	13.1.3 Segregación de redes.	Gestionado	95	Controles gestionados y administrados.	
A13.2	**13.2 Intercambio de información con partes externas.**	**92,5**			
A13.2.1	13.2.1 Políticas y procedimientos de intercambio de información.	Definido	90	Existe la política pero su implementación es parcial.	
A13.2.2	13.2.2 Acuerdos de intercambio.	Definido	90	Se están firmando los diferentes acuerdos, sobre todo con las otras universidades del mundo.	
A13.2.3	13.2.3 Mensajería electrónica.	Gestionado	95	Los controles de Microsoft garantizan esta propiedad.	Oportunidad de mejora: Las políticas de confidencialidad de Microsoft están en contra de las políticas de confidencialidad de la empresa
A13.2.4	13.2.4 Acuerdos de confidencialidad y secreto	Gestionado	95	Firmados por las partes implicadas.	
A14	**14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.**		**60**		
A14.1	**14.1 Requisitos de seguridad de los sistemas de información.**	**90**			
A14.1.1	14.1.1 Análisis y especificación de los requisitos de seguridad.	Definido	90	Actualmente el proceso de toma de requerimientos considera requisitos de seguridad de los usuarios.	
A14.1.2	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Definido	90	Toda la información que se recoge de los usuarios como matrículas, pagos, ficha socio-económica pasa a través de protocolos seguros como https.	
A14.1.3	14.1.3 Protección de las transacciones por redes telemáticas.	Definido	90	Las transacciones electrónicas utilizan firmas digitales provistas por el Banco Central del Ecuador.	
A14.2	**14.2 Seguridad en los procesos de desarrollo y soporte.**	**55,555556**			**No conformidad mayor**
A14.2.1	14.2.1 Política de desarrollo seguro de software.	Gestionado	95	Existe la política, está aprobada y se ha implementado.	
A14.2.2	14.2.2 Procedimientos de control de cambios en los sistemas.	Definido	90	Los controles están definidos pero todavía no se monitorean.	
A14.2.3	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Inicial	10	Existe una gran variedad de plataformas que han provocado. que los controles no sean completos.	No Conformidad Menor: Los controles están incompletos.
A14.2.4	14.2.4 Restricciones a los cambios en los paquetes de software.	Inicial	10	Solo se tiene cubierta el área administrativa.	No Conformidad Menor: Las restricciones a los cambios en los paquetes de software, no se han considerado para el área académica, la universidad cuenta con un número indeterminado de aplicaciones en los laboratorios.

A14.2.5	14.2.5 Uso de principios de ingeniería en protección de sistemas.	Inicial	10	La falta de capacitación o personal capacitado para contratar a estancado la actividad.	
A14.2.6	14.2.6 Seguridad en entornos de desarrollo.	Definido	90	Se está completando los controles.	Observación: Se incumple el literal j de la norma, ya que no existe control sobre el movimiento de datos.
A14.2.7	14.2.7 Externalización del desarrollo de software.	Definido	90	Se ha implementado los controles con algunas de las empresas que brindan desarrollo externo.	
A14.2.8	14.2.8 Pruebas de seguridad de los sistemas.	Inicial	10	Solo existen pruebas de seguridad con los sistemas que realizan transacciones bancarias.	No Conformidad Menor: No existen pruebas de seguridad en los desarrollos de todos los sistemas.
A14.2.9	14.2.9 Pruebas de aceptación.	Gestionado	95	Todos los usuarios deben firmar la aceptación de funcionalidad de las aplicaciones.	
A14.3	**14.3 Datos de prueba.**	**10**			
A14.3.1	14.3.1 Protección de los datos utilizados en pruebas.	Inicial	10	El proceso requiere mucho trabajo.	No Conformidad Menor: Los datos utilizados en pruebas son reflejo de la base de datos real.
A15	**15. RELACIONES CON SUMINISTRADORES.**		**85**		
A15.1	**15.1 Seguridad de la información en las relaciones con suministradores.**	**78,333333**			
A15.1.1	15.1.1 Política de seguridad de la información para suministradores.	Gestionado	95	Se ha definido la política y se ha aprobado.	
A15.1.2	15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.	Definido	90	Los acuerdos están en revisión de las respectivas procuradurías.	
A15.1.3	15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.	Limitado	50	Se está negociando con los principales proveedores.	
A15.2	**15.2 Gestión de la prestación del servicio por suministradores.**	**95**			
A15.2.1	15.2.1 Supervisión y revisión de los servicios prestados por terceros.	Gestionado	95	Se han definido los controles y están operativos.	
A15.2.2	15.2.2 Gestión de cambios en los servicios prestados por terceros.	Gestionado	95	Existen controles para gestionar los cambios.	
A16	**16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**		**80**		
A16.1	**16.1 Gestión de incidentes de seguridad de la información y mejoras.**	**80**			
A16.1.1	16.1.1 Responsabilidades y procedimientos.	Definido	90	Se han definido las responsabilidades y procedimientos.	
A16.1.2	16.1.2 Notificación de los eventos de seguridad de la información.	Definido	90	Los canales de notificación están definidos y operativos.	
A16.1.3	16.1.3 Notificación de puntos débiles de la seguridad.	Gestionado	95	Las políticas de seguridad comprometen a todos los usuarios a reportar incidentes.	

A16.1.4	16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.	Gestionado	95	El responsable de Seguridad de la Información es quien valora los diferentes reportes.	
A16.1.5	16.1.5 Respuesta a los incidentes de seguridad.	Definido	90	El procedimiento está definido y aprobado por la dirección.	
A16.1.6	16.1.6 Aprendizaje de los incidentes de seguridad de la información.	Limitado	50	Existe un procedimiento pero no se ha probado.	
A16.1.7	16.1.7 Recopilación de evidencias.	Limitado	50	Existe un procedimiento pero no se ha probado.	
A17	**17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DELA CONTINUIDAD DEL NEGOCIO.**		**96,25**		
A17.1	**17.1 Continuidad de la seguridad de la información.**	**95**			
A17.1.1	17.1.1 Planificación de la continuidad de la seguridad de la información.	Gestionado	95	Existe el Plan de Continuidad del Negocio donde se han determinado los elementos indispensables.	
A17.1.2	17.1.2 Implantación de la continuidad de la seguridad de la información.	Gestionado	95	Existe el Plan de Continuidad de seguridad de la información.	
A17.1.3	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Gestionado	95	Se ha realizado evaluaciones del plan.	
A17.2	**17.2 Redundancias.**	**100**			
A17.2.1	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	Optimizado	100	Existen redundancias a diferentes niveles, sobre todo en los diferentes CPDs.	
A18	**18. CUMPLIMIENTO.**		**93,125**		
A18.1	**18.1 Cumplimiento de los requisitos legales y contractuales.**	**94**			
A18.1.1	18.1.1 Identificación de la legislación aplicable.	Gestionado	95	Se conoce y actualiza el conocimiento de toda la legislación.	
A18.1.2	18.1.2 Derechos de propiedad intelectual (DPI).	Gestionado	95	En la contratación se firma acuerdos de propiedad intelectual.	
A18.1.3	18.1.3 Protección de los registros de la organización.	Definido	90	La Secretaría Técnica de Gestión Documental está trabajando en la custodia de los registros físicos.	
A18.1.4	18.1.4 Protección de datos y privacidad de la información personal.	Gestionado	95	Se garantiza la confidencialidad de dichos datos.	
A18.1.5	18.1.5 Regulación de los controles criptográficos.	Gestionado	95	Se utiliza certificados digitales y firmas digitales legalmente establecidas.	
A18.2	**18.2 Revisiones de la seguridad de la información.**	**91,666667**			
A18.2.1	18.2.1 Revisión independiente de la seguridad de la información.	Definido	90	El SGSI está implementado recientemente y dentro su planificación existe la revisión independiente.	
A18.2.2	18.2.2 Cumplimiento de las políticas y normas de seguridad.	Gestionado	95	Esta auditoría es parte de dicho control.	
A18.2.3	18.2.3 Revisión técnica del cumplimiento.	Definido	90	No se ha realizado ninguna auditoría técnica de	

				cumplimiento.	

Tabla 3.15 Pruebas de cumplimiento

Una vez realizado el cumplimiento de la Declaración de Aplicabilidad se procede a evaluar el estado de madurez del SGSI con respecto a los requerimientos mandatorios de la norma ISO/IEC 27001:2013.

Sección	Requerimiento ISO/IEC 27001	Estado
4	**Contexto de la organización**	
4,1	**Contexto Organizacional**	
4,1	Determinar los objetivos organizacionales del SGSI y cuestiones que podrían afectar su efectividad	Gestionado
4,2	**Partes Interesadas**	
4.2 (a)	Identificar partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Optimizado
4.2 (b)	Determinar sus requerimientos relevantes de seguridad de la información y obligaciones	Gestionado
4,3	**Alcance del SGSI**	
4,3	Determinar y documentar el alcance del SGSI	Optimizado
4,4	**SGSI**	
4,4	Establecer, implementar, mantener y mejorar continuamente un SGSI acorde al estándar	Gestionado
5	**Liderazgo**	
5,1	**Liderazgo y compromiso**	
5,1	Alta dirección debe demostrar liderazgo y compromiso con el SGSI	Definido
5,2	**Política**	
5,2	Documentar la política de seguridad de la información	Gestionado
5,3	**Roles organizacionales, responsabilidades y autoridades**	
5,3	Asignar y comunicar roles y responsabilidades de la seguridad de la información	Gestionado
6	**Planear**	
6,1	**Acciones para dirigir riesgos y oportunidades**	
6.1.1	Diseñar/planificar el SGSI para satisfacer los requerimientos, direccionar riesgo y oportunidades	Gestionado
6.1.2	Definir y aplicar un proceso de evaluación del riesgo de seguridad de la información	Gestionado
6.1.3	Documentar y aplicar un proceso de tratamiento del riesgo de la seguridad de la información	Gestionado
6,2	**Objetivos de la seguridad de la información y planes**	
6,2	Establecer y documentar los objetivos de seguridad de la información y planes	Definido
7	**Soporte**	
7,1	**Recursos**	
7,1	Determinar y establecer recursos para el SGSI	Definido
7,2	**Competencia**	
7,2	Determinar, documentar y hacer disponibles las competencias necesarias	Gestionado
7,3	**Concienciación**	
7,3	Establecer un programa de concienciación de la seguridad	Optimizado
7,4	**Comunicación**	
7,4	Determinar las necesidades para comunicación interna y externa relevante a el SGSI	Definido
7,5	**Información Documentada**	
7.5.1	Proveer documentación requerida por el estándar más lo que requiere la organización	Definido
7.5.2	Proveer títulos de documentos, autor, etc formato consistente y revisarlos y aprobarlos	Gestionado
7.5.3	Controlar apropiadamente la documentación	Gestionado
8	**Operación**	

8,1	**Plan operacional y control**	
8,1	Planear, implementar, controlar y documentar el proceso del SGSI para gestión de riesgos	Optimizado
8,2	**Evaluar el riesgo de la seguridad de la información**	
8,2	Documentar regularmente los activos y los riegos de seguridad de la información y sus cambios	Definido
8,3	**Tratamiento del riesgo de la seguridad de la información**	
8,3	Implementar un plan de tratamiento del riesgo y documentar los resultados	Gestionado
9	**Evaluación del rendimiento**	
9,1	**Monitorear, medir, analizar y evaluar**	
9,1	Monitorear, medir, analizar y evaluar el SGSI y los controles	Definido
9,2	**Auditoría Interna**	
9,2	Planear y conducir auditorías internas del SGSI	Gestionado
9,3	**Revisión de la Dirección**	
9,3	Emprender revisiones de la dirección regulares del SGSI	Definido
10	**Mejora**	
10,1	**No conformidades y acciones correctivas**	
10,1	Identificar, reparar y tomar acciones para prevenir recurrencia de no conformidades, documentando las acciones	Gestionado
10,2	**Mejora continua**	
10,2	Mejorar continuamente el SGSI	Definido

Tabla 3.16 Estado de los requerimientos mandatorios de la ISO/IEC 27001:2013

4.1.7 Listado Detallado de Hallazgos/Desviaciones

Según la "*Plantilla de Informe de Auditoría*" del anexo 03 *Procedimiento de Auditorías Internas* se detallan todos los hallazgos:

Hallazgo N° 1	
Tipo:	No existe control definido
Nombre:	6.2.1 Política de uso de dispositivos para movilidad.
Detalle:	Los usuarios llevan en sus dispositivos móviles información confidencial sin ningún tipo de control, no existe cifrado para los activos de información de la UPS
Tipo de desviación:	No conformidad menor
Evidencia:	No existe documentación sobre controles ni registros de verificación.
Recomendación:	Definir los controles y aprobarlos por el Comité de Seguridad, crear un inventario de equipos móviles de la UPS y pedir inmediatamente a sus propietarios que los entreguen para configurarlos según el control.

Hallazgo N° 2	
Tipo:	No existe política
Nombre:	6.2.2 Teletrabajo.
Detalle:	Existen usuarios con responsabilidad de autoridad que realizan conexiones VPN, no se ha definido políticas porque la dirección considera engorroso el proceso. La seguridad del teletrabajo se basa en un control Ad-hoc
Tipo de desviación:	No conformidad menor
Evidencia:	La propuesta de política ha sido enviada por el Comité de Seguridad pero en el

	Comité de Dirección no existe resolución para tal documento.
Recomendación:	El Comité de Dirección debe dar tramite inmediato a la propuesta de política

Hallazgo N° 3	
Tipo:	Incumplimiento de objetivo de la norma
Nombre:	6.2 Dispositivos para movilidad y teletrabajo.
Detalle:	La suma de no conformidades del hallazgo 1 y del hallazgo 2 impiden cumplir el objetivo de control 6.2
Tipo de desviación:	No conformidad mayor
Evidencia:	Revisar hallazgo 1 y hallazgo 2
Recomendación:	Resolver los hallazgos 1 y 2

Hallazgo N° 4	
Tipo:	Mejorar los niveles de concienciación.
Nombre:	7.2.2 Concienciación, educación y capacitación en seguridad de la información
Detalle:	Apenas el 80 % de los usuarios ha sido capacitado. El dato es alarmante a nivel de autoridades, ya que el 50% todavía no está capacitado en los temas de seguridad de la información.
Tipo de desviación:	Oportunidad de mejora
Evidencia:	Estadísitica de los registros de evaluación.
Recomendación:	Mantener el plan de capacitación para el siguiente año. Dar seguimiento especial a quienes todavía no han seguido la formación o no han aprobado la evaluación.

Hallazgo N° 5	
Tipo:	No existe control definido
Nombre:	7.2.3 Proceso disciplinario.
Detalle:	Las políticas hacen referencias que ante el incumplimiento se tomarán los procesos disciplinarios correspondientes, sin embargo estos no están definidos. El proceso se ha estancada en procuraduría.
Tipo de desviación:	No conformidad menor
Evidencia:	El Comité de Seguridad cuenta con el acuse de recibo de Procuraduría para el documento “Código disciplinario” No existe la respuesta de Procuraduría.
Recomendación:	El Comité de Seguridad mediante solicitud al Procurador con copia al Comité de Dirección debe solicitar gestionar inmediatamente el visto bueno legal del documento.

Hallazgo N° 6	
Tipo:	No implementación de la política aprobada
Nombre:	8.1.3 Uso aceptable de los activos.
Detalle:	La gestión de indicadores demuestra que todavía existen usuarios que no utilizan adecuadamente los activos. La necesidad de implementar los controles es urgente pues los principales activos afectados son los computadores portátiles de los docentes: 1500 equipos portátiles para docentes.

	400 equipos de escritorio para personal administrativo.
Tipo de desviación:	No conformidad menor
Evidencia:	El indicador “Mantenimiento de equipos” en la medición del último semestre indica que un total de 80 usuarios han recibido mantenimiento (4,2%), el valor umbral del indicador es 80%.
Recomendación:	Incentivar mediante un plan, el control de mantenimiento y actualización de equipos, según la política los usuarios deben llevar su equipo por lo menos cada seis meses.

Hallazgo N° 7	
Tipo:	No implementación de la política aprobada
Nombre:	8.3.1 Gestión de soportes extraíbles.
Detalle:	La totalidad de equipos cuentan con unidades de CD-DVD funcionales, puertos USB habilitados, no existe ningún control de los dispositivos de almacenamiento que se puedan conectar a los diferentes 1500 equipos portátiles para docentes y 400 para personal administrativo. La diversificación de dispositivos de almacenamiento y la gran cantidad de activos han estancado la tarea.
Tipo de desviación:	No conformidad menor
Evidencia:	No se registra datos en el indicador “Equipos intervenidos-USB-CD”.
Recomendación:	Ejecutar los controles y establecer un cronograma de configuración de equipos para implementar el control.

Hallazgo N° 8	
Tipo:	El control no abarca la globalidad de elementos que le correspondería cubrir.
Nombre:	11.2.1 Emplazamiento y protección de equipos.
Detalle:	No existe ningún control para los dispositivos móviles como laptops y teléfonos.
Tipo de desviación:	No conformidad menor
Evidencia:	El control no contempla la protección de laptops y dispositivos móviles. Mediante simple observación se puedo constatar laptops y teléfonos móviles desentendidos en zonas de acceso público sin ningún tipo de protección.
Recomendación:	Extender el alcance del control para dispositivos móviles y portátiles.

Hallazgo N° 9	
Tipo:	Mantenimiento de equipos
Nombre:	11.2.4 Mantenimiento de los equipos.
Detalle:	A pesar de que la política indica que cada seis meses los usuarios deben llevar a mantenimiento sus equipos, el 80% no lo ha realizado, sobre todo usuarios de equipos portátiles.
Tipo de desviación:	Oportunidad de mejora
Evidencia:	Los registros de mantenimiento demuestran que el 60% de los usuarios nunca ha

	llevado a mantenimiento su equipo. El 80% no cumple con el último mantenimiento semestral.
Recomendación:	Mediante un comunicado recordarles a los usuarios que el equipo debe ser llevado a mantenimiento cada seis meses. Cuando el usuario lleve su equipo a mantenimiento ejecutar los controles 8.3.1 y 8.1.3.

Hallazgo N° 10	
Tipo:	No existe control definido
Nombre:	11.2.5 Salida de activos fuera de las dependencias de la empresa.
Detalle:	No existe ningún control para los activos que salen de la UPS a pesar de la existencia de la política
Tipo de desviación:	No conformidad menor
Evidencia:	No existencia de control.
Recomendación:	Definir los controles y aprobarlos por el Comité de Seguridad, el control debe incorporar estrategias de verificación para comprobar que los activos se encuentren en su respectiva ubicación.

Hallazgo N° 11	
Tipo:	Inseguridad en equipos y activos que salen de las instalaciones de la UPS
Nombre:	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
Detalle:	No existe un control, por lo tanto no hay medidas de seguridad para los activos que salen de la UPS.
Tipo de desviación:	No conformidad menor
Evidencia:	No existencia de control.
Recomendación:	Definir los controles y aprobarlos por el Comité de Seguridad, el control debe incorporar mecanismos para que el usuario firme la aceptación completa de su responsabilidad para con el activo o equipo que está sacando de las instalaciones. Se debe especificar claramente el proceso disciplinario para quien saque equipos o activos sin autorización.

Hallazgo N° 12	
Tipo:	Restricciones de navegación
Nombre:	13.1.2 Mecanismos de seguridad asociados a servicios en red.
Detalle:	Los usuarios consideran los controles restrictivos, no existe una verdadera conectividad. Esto atenta con el principio de la Academia.
Tipo de desviación:	Oportunidad de mejora
Evidencia:	El control registra 12.404 incidencias en el último mes de docentes que desean navegar por determinada página y solicitan su desbloqueo.
Recomendación:	Se podría crear una regla de control de acceso basada en el horario, de esta manera se puede discriminar entre las horas administrativas y académicas del personal. Para evitar bloqueos innecesarios.

Hallazgo N° 13	
Tipo:	Gestión adecuada del correo electrónico
Nombre:	13.2.3 Mensajería electrónica.

Detalle:	Las políticas de confidencialidad de Microsoft están en contra de las políticas de confidencialidad de la empresa, se debe tener presente que Microsoft se rige a las políticas de los Estados Unidos de América, por lo tanto no es una opción solicitar la adaptación de la política de Microsoft a las necesidades de la UPS.
Tipo de desviación:	Oportunidad de mejora
Evidencia:	Las políticas de Microsoft Outlook ofrecen todas las garantías de confidencialidad al usuario de la cuenta. Se registran 76 solicitudes a Microsoft para acceder a correos institucionales, el 100% han sido rechazadas.
Recomendación:	Realizar un estudio de la implementación de un servidor de correo gestionado y administrado por la UPS.

Hallazgo N° 14	
Tipo:	Controles incompletos
Nombre:	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
Detalle:	Existe una gran variedad de plataformas que han provocado que los controles no sean completos.
Tipo de desviación:	No conformidad menor
Evidencia:	Los controles no se ajustan a los requerimientos de plataformas de 64 bits. Solo existen controles para Windows XP, 7. Existen 300 equipos con Windows 8 cuyo software base no ha sido probado
Recomendación:	Actualizar los controles según el inventario de activos, en el mantenimiento semestral de equipos se debe actualizar cada sistema operativo para evitar la diversificación de plataformas y versiones entre plataformas.

Hallazgo N° 15	
Tipo:	Controles incompletos
Nombre:	14.2.4 Restricciones a los cambios en los paquetes de software.
Detalle:	Las restricciones a los cambios en los paquetes de software, no se han considerado para el área académica, la universidad cuenta con un número no determinado de aplicaciones en los laboratorios. Para el área administrativa el control se ha cumplido para el 100% de equipos
Tipo de desviación:	No conformidad menor
Evidencia:	Existen 215 incidencias de programas que dejaron de funcionar en los laboratorios de la UPS debido a actualizaciones de plataformas, de las cuales 150 no fueron solucionadas.
Recomendación:	Desarrollar los controles respectivos para las áreas de laboratorio de cómputo de la UPS. Se recomienda flexibilizar los aspectos referentes a actualización, instalación y gestión de usuarios administradores con la finalidad de no entorpecer el trabajo académico. Para garantizar el uso de software de legado se recomienda la instalación de máquinas virtuales.

Hallazgo N° 16	
Tipo:	Actualización de control
Nombre:	14.2.6 Seguridad en entornos de desarrollo.
Detalle:	Se incumple el literal j de la norma, ya que no existe control sobre el movimiento de datos

Tipo de desviación:	Observación
Evidencia:	El control no contempla el movimiento de datos.
Recomendación:	Gestionar la creación de la base de datos de pruebas, por cuestiones de confidencialidad no se puede seguir utilizando réplicas de la base de datos real para el desarrollo

Hallazgo N° 17	
Tipo:	Ejecución incompleta del control
Nombre:	14.2.8 Pruebas de seguridad de los sistemas.
Detalle:	No existen pruebas de seguridad en los desarrollos de todos los sistemas. Solo se ha comprobado la existencia de pruebas de seguridad para los sistemas que realizan transacciones bancarias
Tipo de desviación:	No conformidad menor
Evidencia:	No existen registros, ni documentación que demuestre la aplicación de pruebas de seguridad en las aplicaciones no relacionadas con transacciones bancarias.
Recomendación:	Implementar las pruebas de seguridad inmediatamente para todos los desarrollos actuales y futuros de la UPS.

Hallazgo N° 18	
Tipo:	Incumplimiento de objetivo de la norma
Nombre:	14.2 Seguridad en los procesos de desarrollo y soporte.
Detalle:	La suma de no conformidades 14, 15, 16 y 17 impiden cumplir el objetivo de control 14.2
Tipo de desviación:	No conformidad mayor
Evidencia:	Revisar los hallazgos 14, 15, 16 y 17
Recomendación:	Resolver los hallazgos 14, 15, 16 y 17

Hallazgo N° 19	
Tipo:	No existe control
Nombre:	14.3.1 Protección de los datos utilizados en pruebas.
Detalle:	Los datos utilizados en pruebas son reflejo de la base de datos real
Tipo de desviación:	No conformidad menor
Evidencia:	Se comparó 10 reportes generados en el Sistema Nacional Académico, con los mismos 10 reportes generados en la base de datos de prueba. El 100% de reportes de prueba contenían información real.
Recomendación:	Definir inmediatamente un control para que Desarrollo trabaje con datos de prueba ficticios. Se debe crear inmediatamente una base de datos de prueba, para ello se establecerá un equipo de trabajo con un representante del área académica, financiera y de recursos humanos; quienes cargarán los datos de prueba de los diferentes sistemas.

4.1.8 Conclusiones General del Grado de Cumplimiento

Se presenta una visión sintética del nivel de cumplimiento de la norma ISO/IEC 27001:2013

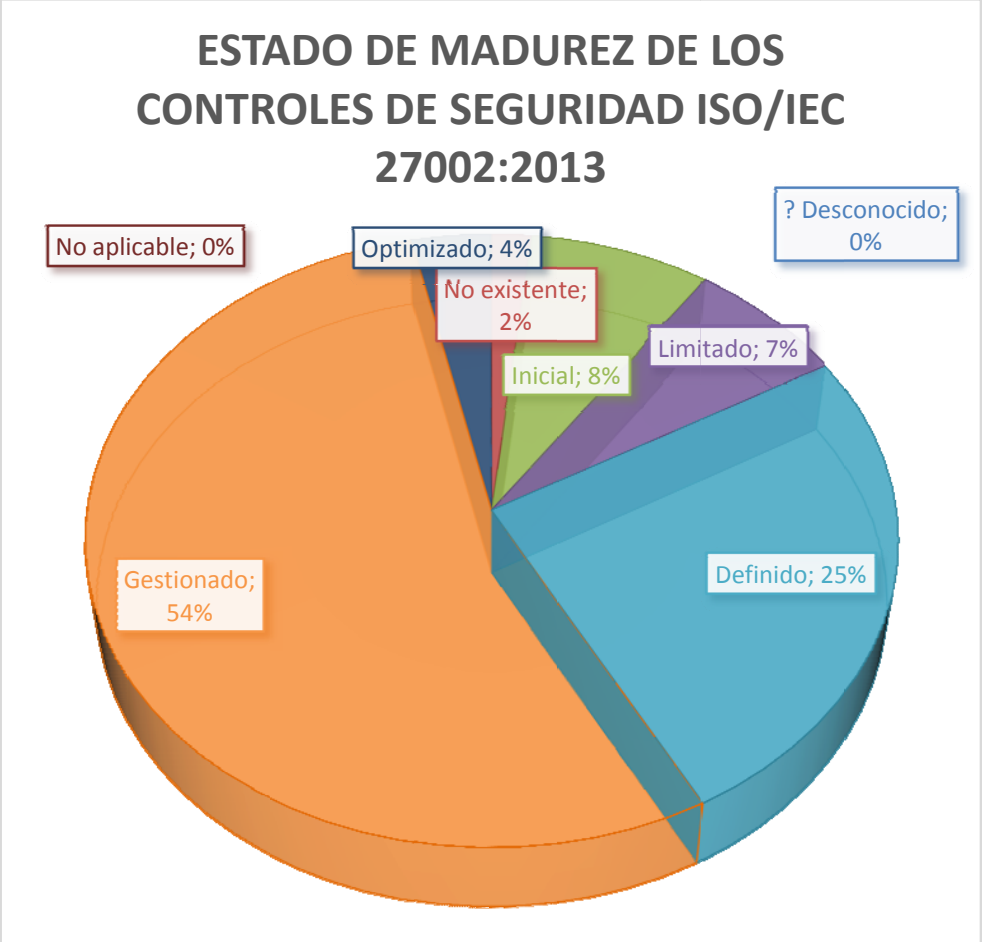


Figura 4.1 Estado de madurez de los apartados de la norma ISO/IEC 27001:2013

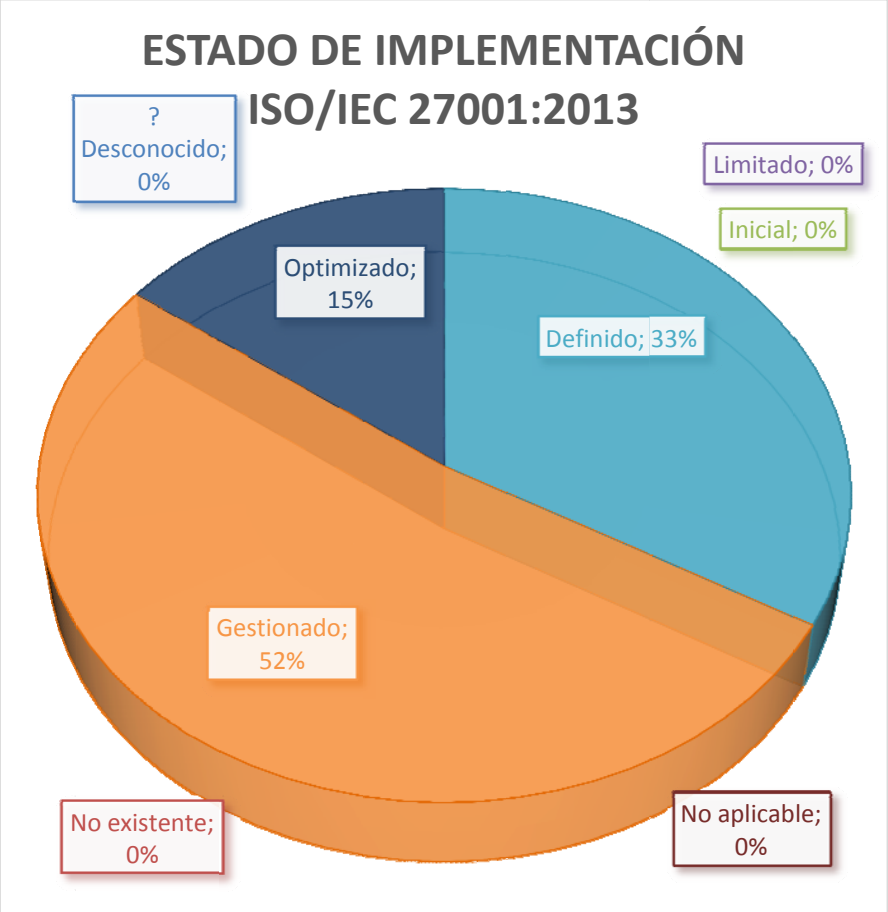


Figura 4.2 Estado de madurez de los controles mandatorios de la Norma ISO/IEC 27001:2013

El diagrama de radar nos permite visualizar la evolución de los diferentes controles en comparación con la evolución esperada, luego de ejecutar los distintos proyectos.

En dominios como el 9(Control de accesos), 12(Seguridad en la Operativa), 17(Aspectos de seguridad de la Información en la gestión de continuidad del negocio) y 18(Cumplimiento) los resultados nos presentan una evolución mejor de lo esperado, debido a que las políticas ayudaron a articular correctamente los diferentes controles Ad-hoc de la UPS.

En cambio dominios como el 6(Aspectos organizativos de la seguridad de la información), 7(Seguridad ligada a los recursos humanos), 8(Gestión de activos), 11(Seguridad física y ambiental), 15(Relaciones con suministradores) y 16(Gestión de incidentes en la seguridad de la información) estuvieron muy cerca de alcanzar los valores de madurez esperados, se debe tener en cuenta que estos dominios prácticamente fueron desarrollados desde cero, ya que todos ellos tienen que ver con elementos referentes a políticas y organización.

En cuanto al resto de dominios el estado de madurez alcanzado ha sido el esperado.

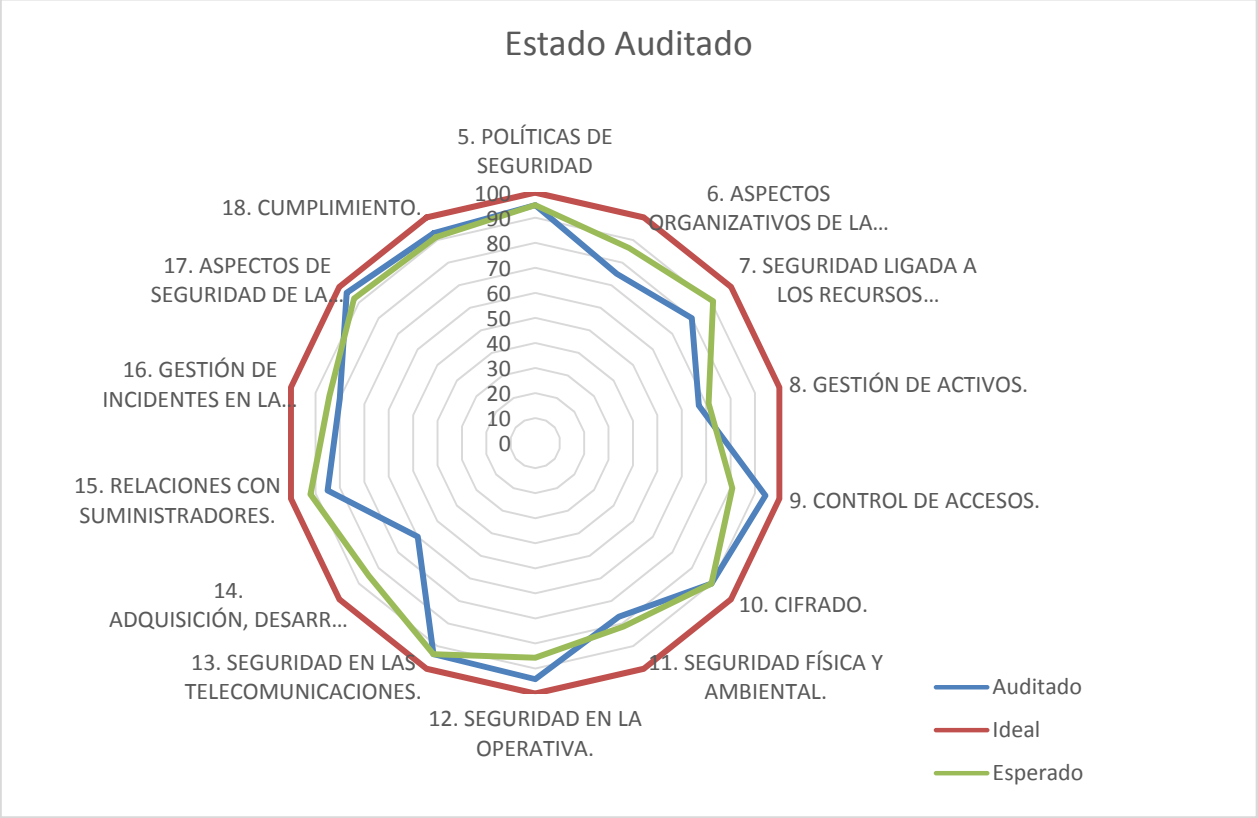


Figura 4.3 Evolución de los dominios de la norma ISO/IEC 27002:2013

4.1.9 *Resumen Ejecutivo*

En el anexo 08 *Resumen Ejecutivo* se puede apreciar el resumen ejecutivo de la auditoría interna de cumplimiento.

5 CAPÍTULO 6: CONCLUSIONES

El caso de la UPS demuestra que las iniciativas Ad-hoc en seguridad de la información al no estar alineadas a una política aprobada por la dirección son ineficientes. Los diferentes controles de seguridad de la información implementados en la UPS requerían complejos y sofisticados sistemas, que dificultaron la usabilidad de los diferentes servicios como sistemas de información, internet, redes, correo electrónico. La seguridad de la información se convirtió en un fin, en lugar de un medio para la gestión eficaz y eficiente de la universidad.

La concienciación de la necesidad de un Sistema de Gestión de Seguridad de la Información, surgió tras cuantiosas inversiones en tecnología y capacitaciones específicas que no produjeron resultados acordes a la inversión realizada.

La implementación del SGSI propuso a las autoridades una nueva visión del problema, entender a la seguridad de la información como un medio para la gestión eficaz y eficiente del negocio, que era necesario el compromiso decidido de la dirección para gestionar una estructura de organización de la seguridad que permita la emisión de políticas, documentos y procedimientos alineados a la misión, visión y plan estratégico institucionales con controles pertinentes a la realidad de la UPS, susceptibles de ser medidos, supervisados y monitoreados con la finalidad de evaluarlos y gestionar mejoras en los mismos, en definitiva la implementación de un verdadero sistema que articule la seguridad de la información.

Se inició la implementación con un estudio diferencial del estado inicial de la UPS, se planteó la sistemática documental que permita la ejecución de un análisis de riesgos que derivó en proyectos, que después de ser ejecutados han permitido a la UPS evolucionar a un nivel de madurez adecuado para solicitar la certificación del sistema según la norma ISO/IEC 27001:2013, finalmente, se completó el ciclo PDCA con la Auditoría Interna de Cumplimiento.

DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2013
- Norma ISO/IEC 27002:2013
- Ley Orgánica de Educación Superior, Ecuador, 2012
- Reglamento de Régimen Académico, Ecuador, 2013
- Reglamento de Evaluación y Acreditación de Programas y Carreras, Ecuador, 2012
- Carta de Navegación 2014-2018, UPS
- **Hodson, Ed** ; ISMS Implementation Tracker, Consultado: 20/septiembre/2014; http://www.iso27001security.com/ISO27k_ISMS_implementation_project_estimator_v1.xlsx

DOCUMENTOS ANEXOS

Anexo 01 AnalisisDiferencial_ISO27002.xlsx	Documento de análisis diferencial
Anexo 02 SGSI-PO-OSI.pdf	Política de Organización de la Seguridad de la información
Anexo 03 SGSI-PR-AI.pdf	Procedimiento de Auditorías Internas
Anexo 04 SGSI-PR-GI.pdf	Gestión de Indicadores
Anexo 05 SGSI-PR-RD.pdf	Procedimiento de Revisión por la Dirección
Anexo 06 SGSI-PR-MAR.pdf	Metodología de Análisis de Riesgos
Anexo 07 SGSI-IT-AR.xlsc	Documento técnico del Análisis de Riesgos
Anexo 08 Resumen_Ejecutivo.pdf	Informe Ejecutivo de la Auditoría Interna