Máster Interuniversitario de 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 en la IES

Autor: Andrea Maricela Plaza Cordero

Director: Antonio José Segovia Henares

Memoria

Febrero 2015 – Julio 2015

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

© Andrea Maricela Plaza Cordero

Reservados todos los derechos. Está prohibida la reproducción parcial o total de esta obra por cualquier medio o procedimiento, comprendidos: la impresión, reprografía, el microfilme, el tratamiento informático o cualquier otro sistema, así como la distribución de ejemplares mediante alquiler o préstamo, sin la autorización escrita del autor o de los límites que autorice la Ley de Propiedad Intelectual

Agradecimientos

Un nuevo sueño se ha cumplido, gracias a las personas inigualables que día a día supieron apoyarme, recordándome que caerse es muestra de aprendizaje y levantarse es símbolo de valentía. Le agradezco a Dios, por mostrarme el camino y siempre ser un guía en los peores momentos.

A mi padre Luis Antonio Plaza Merchán, que ahora en el cielo cuida mi camino y sigue mis pasos, siempre voy a recordarle como el hombre trabajador que luchó siempre por su familia inculcándonos el trabajo duro, la bondad y disciplina.

A mis dos madres María Inés Cordero y Marcia Eulalia Plaza, que en cada sueño y locura me apoyan incondicionalmente, a mi abuelita que ha sabido guiarme por el camino recto y a mi mamá que con una palabra de consuelo siempre supo ver lo mejor de la peor situación, sin ustedes nada de esto sería posible. Sólo puedo agradecerles y prometerles que siempre estaré ahí cuando me necesiten.

Al Lcdo. Fernando Pesántez, a quien considero un ejemplo a seguir y con su apoyo fue posible este sueño, de igual manera a una gran amiga Adrianita García, que me incentivó para seguir mis sueños y siempre estuvo pendiente con sus consejos y apoyo.

A mis amigas Andrea Flores, Verónica Clavijo y Pilar Morquecho quienes me han apoyado y brindando su amistad.

A mi tutor Antonio José Segovia Henares que es un excelente profesor, supo guiarme en cada una de las etapas, a pesar de la distancia siempre sentí su apoyo y ayuda, de igual manera un agradecimiento a todos los consultores de las diferentes asignaturas.

Dedicatoria

Este logro va dedicado a mis padre que aunque no se encuentra presente, siempre será mi fuerza y empuje ante momentos de problema. Siempre lo recordaré. Este solo es el comienzo Papahuish, junto a usted y toda mi familia, sé que voy a seguir adelante. Siempre llevaré sus palabras en el corazón y en la mente. Usted es mi papi y siempre será así. Gracias por ser mi padre.

A mis dos madres, que me enseñaron que una mujer debe luchar por lo que quiere, pero teniendo presente que la inteligencia siempre está de la mano con la humildad. Gracias.

De igual manera va dedicado a toda mi familia, que me dan fuerzas para seguir adelante y siempre tienen una oración.

"Al final del camino de la vida, no te preguntarán "que tienes", sino "quien eres" ¿Cuál será tu respuesta?"
René Juan Trossero

Resumen

En la actualidad la información es considerada como uno de los mayores activos en una Empresa, dedicándole una gran cantidad de recursos y esfuerzos para su protección.

La seguridad de la información involucra implementar estrategias para gestionar la información, estableciendo políticas, controles de seguridad, tecnologías y los procedimientos para salvaguardar y proteger la información y los sistemas que la administran. Cabe mencionar que estas estrategias deben ser revisadas y mejoradas continuamente, para asegurar que cumplan con las necesidades actuales de la Empresa. Bajo tal premisa, el Sistema de Gestión de Seguridad de la Información (SGSI) es usado por la Alta Dirección para llevar a cabo las políticas y los objetivos de seguridad.

El presente Trabajo Fin de Máster consiste en la Elaboración de un Plan de Implementación bajo la norma ISO/IEC 27001:2013 para la IES, ya que la misma es genérica y por ende aplicable en cualquier tipo de Empresa.

La norma ISO/IEC 27001:2013 define los requisitos necesarios para establecer, efectuar, proteger y renovar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), además se incluyen los requisitos para el análisis y tratamiento de los riesgos en materia de seguridad de la información, alineados al contexto propio de la Empresa.

Abstract

At present, information is considered to be one of the most important assets of a company, and thus a lot of resources and efforts are devoted to its protection.

Information security is about implementing strategies to manage information, by establishing policies, security controls, technologies and procedures to safeguard and protect information and the systems that manage it. It is worth mentioning that these strategies should be revised and improved continuously in order to make sure they meet the current needs of a company. In this regard, the Information Security Management System (SGSI, in Spanish) is used by senior management to carry out security policies and objectives.

This final master's degree project is about creating an implementation plan following the ISO/IEC 27001:2013 norm for IES, since it is generic and thus applicable to any type of company.

The ISO/IEC 27001:2013 norm determines the requirements needed to establish, accomplish, protect and continuously renew the Information Security Management System. The requirements needed to analyze and treat risks in information security of a company have also been included.

1 Fase 1: Situación Actual: Contextualización, Objetivos y Análisis Diferencial

1.1 Introducción del Proyecto

Como punto inicial debemos tener presente que la información es un activo muy importante en toda Organización, no sólo porque estamos inmersos en la sociedad de la información, sino además, por los cambios que se han presentado en un mundo globalizado e interconectado.

La ISO/IEC 9000:2005 define a la información como los “datos que poseen significado”.

Las Organizaciones pequeñas o grandes, públicas o privadas, de cualquier sector se encuentran inmersas bajo amenazas de ataques hacia sus vulnerabilidades como: bajo nivel y software malicioso (buffers overflow, malware de propagación automática, malware oculto, malware lucrativo, etc), de red (sniffers de Ethernet, modificación de direcciones MAC, ARP poisoning, amenazas en ICP, amenazas en OSPF y BGP, entre otros), de aplicaciones web (inyección de scripts, inyección de código, inyección de ficheros, entre otros) y de ingeniería social.

Bajo la anterior premisa la seguridad de la información debe abarcar la protección de la información en todas sus formas, es decir: impresa, oral, electrónica, óptica, etc.; y en cualquier punto de su ciclo de vida como en la creación, mantenimiento, distribución, almacenamiento, archivo y destrucción. La seguridad debe proteger a la información de acceso, uso, divulgación, interrupción y destrucción que no esté autorizada.

Una buena implementación de la gestión de la Seguridad de la Información puede llevar al éxito a una Organización, de allí que la alta dirección debe conocer la importancia de su implementación y brindar su apoyo al iniciar con el SGSI. Por lo tanto, la seguridad de la información no le compete sólo al Departamento Informático o a un grupo específico, sino a toda la Organización, ya que todos trabajan con información que requiere de una gestión coordinada y transversal.

Las Organizaciones no se encuentran solas ante la gestión de la seguridad de la información, ya que existe la ISO/IEC 27000 siendo una norma internacionalmente aceptada que provee de un conjunto de estándares de seguridad. En base a la ISO 27001 la seguridad debe proveerle a la información de los pilares de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y no repudio, y trazabilidad).

A pesar de no encontrarse reglamentada la implementación de la ISO/IEC 27000, las Organizaciones lo están incorporando, ya que brinda una imagen positiva con sus clientes y trabajadores generando una ventaja competitiva, asegurando la continuidad de los procesos ante riesgos y amenazas, reduciendo el número de incidentes e interrupciones, racionalizando los recursos, por mencionar algunas ventajas.

En la actualidad el no proteger la información, ya no es ni una idea remota en una Organización, todo gira en base a ella y su criticidad, por lo tanto si una Organización no protege uno de sus activos más importantes sólo estará caminando hacia el fracaso y su destrucción.

El presente documento plasma la seguridad de la información en base a la norma ISO/IEC 27000: Conjunto de normas y estándares que proporcionan un marco de gestión de la seguridad de la información aplicable a cualquier organización para una Institución de Educación Superior (IES).

1.1.1 Objetivos del Proyecto

El objetivo que tiene el presente proyecto es elaborar un Plan de Implementación de la ISO/IEC 27001:2013 en la Institución de Educación Superior, mediante el ciclo de DEMING (PDCA).

- **Plan:** Definir el estado de la IES, cuál es su negocio, los recursos, la estructura, es decir se debe realizar un análisis de la situación actual.

- **Do:** Seleccionar los indicadores que van a evaluar la eficiencia y eficacia de los controles que se implementaron.

- **Check:** Es crucial monitorizar la implementación del SGSI para determinar su eficacia y cumplimiento, para lo cual deberá existir un procedimiento. Esta fase se deberá hacer mínimo una vez al año interviniendo el Comité de Dirección en la parte estratégica.

- **Act:** Luego de revisar el SGSI, todos los registros serán usados para determinar e implementar planes de mejora, acciones correctivas y preventivas.

1.2 Conociendo la ISO/IEC 27001 e ISO/IEC 27002

La serie 27K es un conjunto de normas desarrolladas por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) para todo tipo y tamaño de Organización.

A continuación se presenta una breve historia de la ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

- **1901:** Normas “British Standars”:
  La Institución Británica de Estándares (BSI) fue la primera entidad nacional de normalización a nivel mundial fundada en 1901, siendo la responsable de publicar las normas, en España lo es AENOR. BSI publicó las normas: BS 5750 en 1979, BS 7750 en 1992, BS 8800 en 1996 que luego darían origen a la ISO 9001, la ISO 14001 y OSHAS 18001 respectivamente.

- **1905:** BS 7799-1
  La norma BS 7799-1 proporciona una guía de buenas prácticas para la gestión de la seguridad de la información.

- **1998:** BS 7799-2
  La norma BS 7799-2 nace de la revisión de la norma anterior, definiendo en esta los requisitos del sistema de gestión de seguridad de la información para que sea certificable, a diferencia de la anterior que no brindaba dicha característica.

- **1999:** BS 7799-1, BS 7799-2
  Revisión de ambas partes.

- **2000:** ISO/IEC 17799:2000
  ISO convierte la primera parte de BS 7799 a la norma ISO 17799 sin realizar cambios significativos.

- **2002:** BS 7799-2
  Se revisa la segunda parte de la norma BS 7799 adecuándola a la filosofía ISO para la gestión de sistemas.

- **2005:** ISO/IEC 27001, ISO/IEC 17799
  En este año se realizan dos grandes cambios, el primero fue el 15 de Octubre del 2005 la adaptación de BS 7799-2 en la ISO/IEC 27001 y además se realizó la revisión y actualización de la ISO 17799.

- **2007:** ISO/IEC 27002:2005, UNE-ISO/IEC 27001:2007
  La ISO 17799:2005 es renombrada a la ISO/IEC 27002:2005 el 1 de Julio del 2007 manteniendo su año de edición (2005), y el 28 de Noviembre de 2007 la ISO/IEC 27001 es publicada con una nueva versión, en España la UNE-ISO/IEC 27001:2007

- **2009:** UNE-ISO/IEC 27001:2007/1M:2009, UNE-ISO/IEC 27002:2009

Se publica en España un documento adicional que contempla modificaciones conocido como UNE-ISO/IEC 27001:2007/1M:2009, y en el mismo año el 9 de diciembre de 2008 se publica UNE-ISO/IEC 27002:2009.

- **2013:** ISO/IEC 27001
  La última versión de la ISO/IEC 27001 e ISO/IEC 27002 se tiene a la fecha del 25 de Septiembre de 2013.

1.2.1 ISO/IEC 27001

La ISO/IEC 27001 es una norma certificable que provee las especificaciones para la implementación del sistema de gestión de seguridad de la información en cualquier tipo de Empresa (grande o pequeña, pública o privada). La certificación consiste en que una entidad de certificación confirma que la Empresa o en mi caso la IES cumple con los requerimientos para brindar una correcta administración de la seguridad de la información.

La norma fue publicada la primera vez en 2005 y su última versión fue el 25 de Septiembre de 2013, la misma que a diferencia de la anterior presentó cambios a nivel de estructura de la parte principal, eliminación de algunos requerimientos como la documentación de ciertos procesos, las medidas preventivas y en el Anexo A se disminuyó la cantidad de controles de 133 a 114, e incrementó el número de dominios pasando de tener 11 a 14.

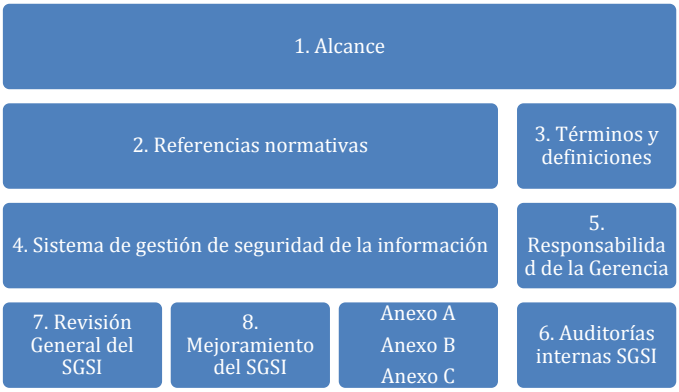


Ilustración 1 ISO/IEC 27001:2005

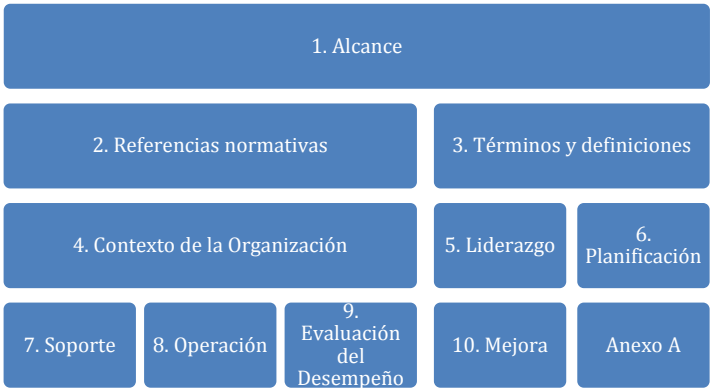


Ilustración 2 ISO/IEC 27001:2013

La norma consta de los siguientes apartados:

- Apartado 0: Introducción
- Apartado 1: Alcance
- Apartado 2: Referencias Normativas
- Apartado 3: Términos y Definiciones

- Apartados 4 al 10: Se encuentran definidos los requerimientos, que se presentan a continuación:

4. **Contexto de la Organización:** Este apartado trata sobre la Empresa, aquí se debe comprender la organización y su contexto, las necesidades y expectativas de las partes interesadas, determinar el alcance del sistema de gestión de seguridad de la información y definir si se encuentra implementado el SGSI.

5. **Liderazgo:** En este apartado la alta dirección debe demostrar su liderazgo y compromiso con la implementación del plan de gestión de seguridad de la información, verificar que las responsabilidades y roles referentes a la seguridad de la información sean asignados y comunicados correctamente, y establecer la política de seguridad de la información.

6. **Planificación:** Este apartado tiene como objetivo que la Empresa planifique el sistema de gestión de seguridad de la información determinando los riesgos y amenazas a los que se encuentra expuesta la Empresa y su posterior definición y aplicación de un proceso de riesgos, en base a los objetivos de la seguridad de la información.

7. **Soporte:** Definición de los recursos necesarios para el establecimiento, implementación y actualización del SGSI, teniendo como insumo la definición del perfil de los responsables, además deberá realizar la concienciación entre los dueños de la información. Además se debe determinar la necesidad de las comunicaciones internas y externas, y generar la documentación respectiva.

8. **Operación:** Este apartado trata sobre la planificación, ejecución y control de los procesos necesarios para cumplir con los requerimientos del SGSI, poniendo en ejecución el plan de riesgos para mitigar los problemas ante un posible ataque y llevando un control de las modificaciones mediante la respectiva documentación.

9. **Evaluación del Desempeño:** Se mide el rendimiento y eficacia del SGSI, mediante la planificación de auditorías internas en intervalos de tiempo planificados. La alta dirección deberá revisar la conveniencia, adecuación y eficacia de la implementación del SGSI en la organización.

10. **Mejora:** Son las acciones y/o medidas que la Empresa deberá ejecutar al producirse una no conformidad, además como todo proceso, el SGSI se encuentra bajo actualización permanente mejorando la idoneidad, adecuación y eficacia.

- Anexo: Objetivos de control y controles de referencia.

1.2.2 ISO/IEC 27002

La ISO/IEC 27002 provee de un conjunto de buenas prácticas para la gestión de la seguridad de la información. En esta norma se especifican los requisitos necesarios para definir, implementar, mantener y mejorar constantemente el sistema de gestión de seguridad de la información, y para evaluar y tratar los riesgos relacionados a la seguridad de la información en todo tipo de Empresa.

En la Ilustración 3 se puede observar el ciclo de vida la ISO/IEC 27002, presentado los cambios más relevantes en cada una de las versiones.

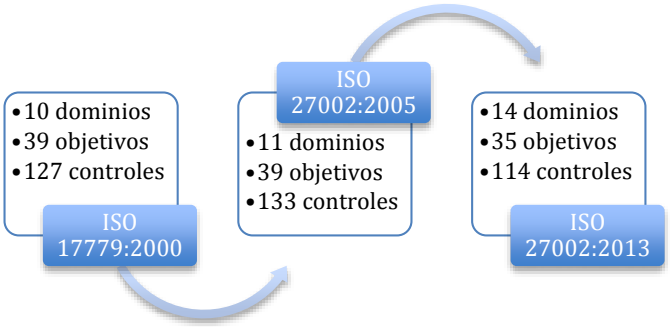


Ilustración 3 Ciclo de vida de la ISO/IEC 27002

La norma consta de los siguientes apartados:

- Apartado 0: Introducción
- Apartado 1: Alcance
- Apartado 2: Referencias Normativas
- Apartado 3: Términos y Definiciones
- Apartado 4: Estructura de esta norma
- Apartados 5 al 18: Cada apartado posee uno o más dominios que recogen uno o más objetivos de control de seguridad y estos a su vez uno o más controles.

  A continuación se presentan los controles definidos en la norma:

  5. Políticas de Seguridad de la Información.
  6. Organización de la seguridad de la información.

7. Seguridad de los Recursos Humanos.
8. Gestión de activos.
9. Controles de acceso.
10. Criptografía.
11. Seguridad física y ambiental.
12. Seguridad en la operativa.
13. Seguridad en las telecomunicaciones.
14. Adquisición, desarrollo y mantenimiento de los sistemas de información.
15. Relaciones con los proveedores.
16. Gestión de incidentes en la seguridad de la información.
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
18. Cumplimiento.

1.3 Contextualización

La empresa seleccionada es una Institución de Educación Superior, no se mencionará el nombre por motivos de seguridad y se la tratará en todo el documento como IES.

La IES está ubicada en Ecuador teniendo su matriz en la ciudad de Cuenca y sede en Quito, posee 21 años de vida institucional mediante la Ley de Creación en el Registro Oficial de la República del Ecuador. Al momento alberga aproximadamente 22453 estudiantes entre el nivel de grado y posgrado matriculados en este periodo, y 1780 empleados entre administrativos y docentes.

La razón de la IES es hacia los jóvenes, brindándoles una formación que vincula valores con experiencia profesional.

La IES es una entidad cofinanciada, es decir, que recibe asignaciones y rentas del Estado. Al momento se encuentra regulada por el Consejo de Educación Superior (CES) y el Consejo de Evaluación, Acreditación y Aseguramiento de la calidad de la Educación Superior (CEAACES), quienes tienen las funciones de planificar, regular y coordinar el Sistema de Educación Superior garantizando una educación de calidad, y realizar procesos continuos de evaluación y acreditación asegurando la calidad de las carreras y programas, respectivamente.

En los últimos años el Ecuador está atravesando un cambio radical a nivel Educativo, donde el eje primordial es la educación, que se encuentra fundamentando a nivel de operatividad en los sistemas de información mediante la conectividad con tecnologías de información, es decir, es primordial salvaguardar la información de los estudiantes, proyectos, investigaciones, entre otros, brindando confidencialidad, integridad y disponibilidad.

La IES tiene un proceso implementado de SGSI, pero no cumple el objetivo de gestión continua, es decir no es un proceso que sigue una normativa o política, de allí que es necesario implementar un plan de implementación de la ISO/IEC 27001:2013.

Los objetivos propuestos por la IES para la implementación del SGSI son:

- Proveer a la información de confidencialidad, integridad, disponibilidad, autenticidad y no repudio, y trazabilidad.
- Proveer calidad en términos de seguridad, mediante una metodología clara y metódica, donde los empleados se encuentran comprometidos en brindar protección a la información.
- Reducir el número de incidentes e interrupciones en base al análisis de los riesgos permitiendo verificar la mitigación de riesgos y la aparición de nuevos.
- Asegurar la continuidad de los procesos ante riesgos y amenazas, ya que no se va a improvisar ante la presencia de un incidente, mas bien se van a tener definidas las acciones dando respuestas más rápidas y concretas.
- Definir claramente los roles y responsabilidades a nivel legal y operativo con relación a la seguridad de la información.

1.3.1 Organigrama

Los servicios en el ámbito de tecnologías de información y comunicación se encuentran centralizadas en el Departamento de Tecnologías de Información y Comunicación. En la Ilustración 4 se observa el organigrama del Departamento Informático, donde existen diferentes roles y responsabilidades inherentes a la seguridad.

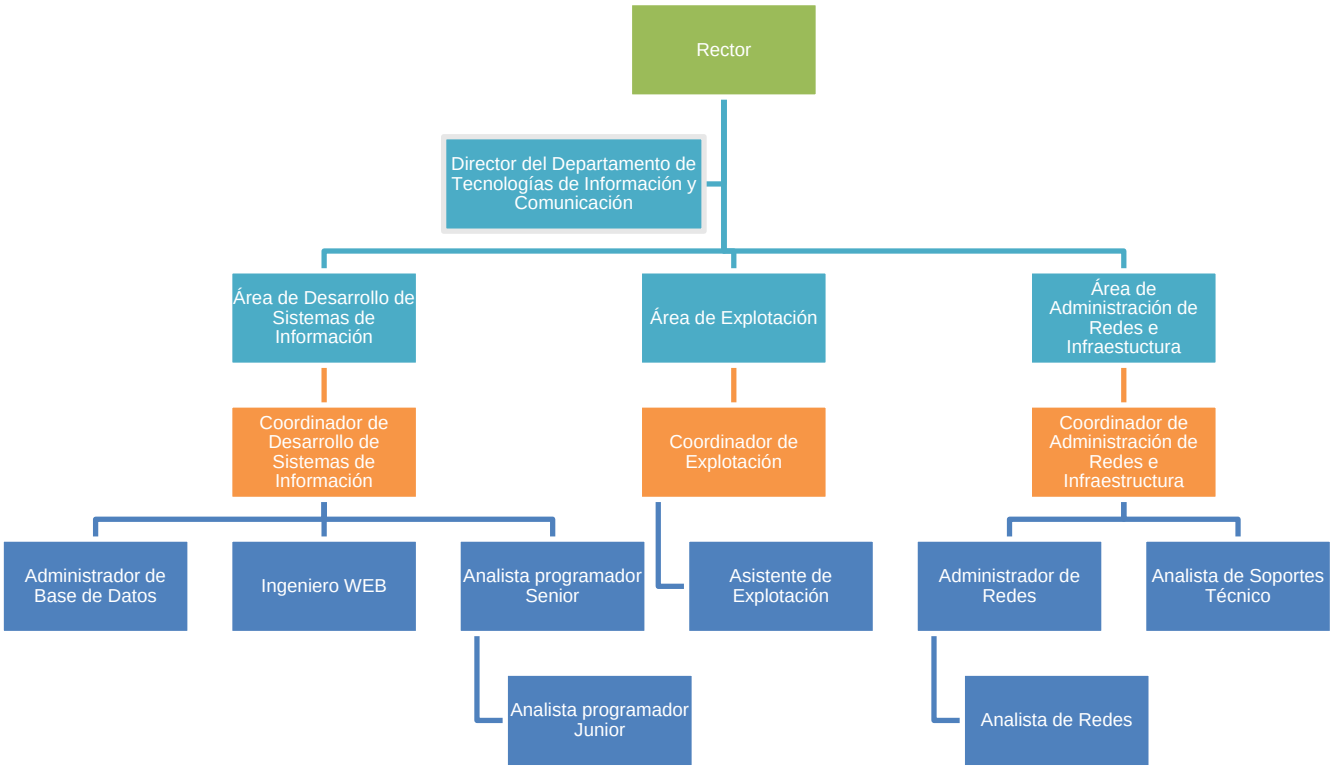


Ilustración 4 Organigrama del Departamento Informático

Director del Departamento Informático: Entre sus funciones tiene la tarea de gestionar las TICS de la IES en el área Académica, Administrativa y Financiera, manteniendo la correcta comunicación en la Red.

Área de Desarrollo de Sistemas de Información: Tiene como objetivo el desarrollo e implementación de los sistemas de información para automatizar los procesos en las diferentes áreas de la IES, además deberá actualizar los procesos que se encuentran en producción.

Funciones Generales:

- Participar en el establecimiento de estrategias para desarrollar el plan de desarrollo de los sistemas de información.
- Analizar, diseñar, desarrollar e implementar los procesos automatizados de las IES.
- Determinar un plan de mantenimiento y actualización de los sistemas de información que se encuentran en producción.
- Generar los documentos técnicos.
- Analizar, diseñar, desarrollar, implementar, documentar y actualizar a nivel de Base de Datos garantizando la integridad de la información.
- Desarrollar estrategias de auditoría de los sistemas de información.
- Realizar copias seguras de la información.
- Administrar los sitios WEB.
- Analizar, diseñar e implementar proyectos de las tecnologías Web.
- Proponer políticas y normas para los sitios Web.

Área de Explotación: Tiene como objetivo brindar asesoría a los usuarios en el manejo de los sistemas de información que se encuentran implementados en la IES.

Funciones Generales:

- Generar los manuales de los sistemas en producción.
- Proveer asistencia a los usuarios sobre el manejo de los sistemas de información.
- Desarrollar los reportes.

Área de Administración de Redes e Infraestructura: Tiene como objetivo gestionar las redes de comunicaciones, brindar soporte y mantenimiento de los equipos informáticos y conectividad garantizando que se ejecuten correctamente las funciones de las TICs en la IES.

Funciones Generales:

- Analizar, diseñar, implementar y administrar las redes de comunicaciones.
- Proveer asistencia técnica a los usuarios.
- Instalar y configurar los equipos informáticos.
- Gestionar las altas y bajas de los usuarios.
- Administrar cuentas de usuarios.
- Presentar propuesta de infraestructura y redes.
- Mantenimiento de los equipos (resolución de averías).
- Realizar copias seguras de la información.
- Evaluar e implementar la topología física y lógica de la red.
- Mantener un inventario de los activos informáticos de la IES.

Cabe mencionar que los roles y responsabilidades a nivel de seguridad no sólo competen al Departamento de Tecnologías de Información y Comunicación, sino a toda la IES desde la alta dirección que sería el Consejo Superior hasta la parte operativa que son administrativos y docentes.

1.3.2 Arquitectura de Red

La IES ha implementado una arquitectura de red tratando de gestionar la seguridad de la información. En la Ilustración 5 podemos observar una vista de alto nivel de la red, en donde se presentan los componentes principales de la arquitectura de Red de la IES.

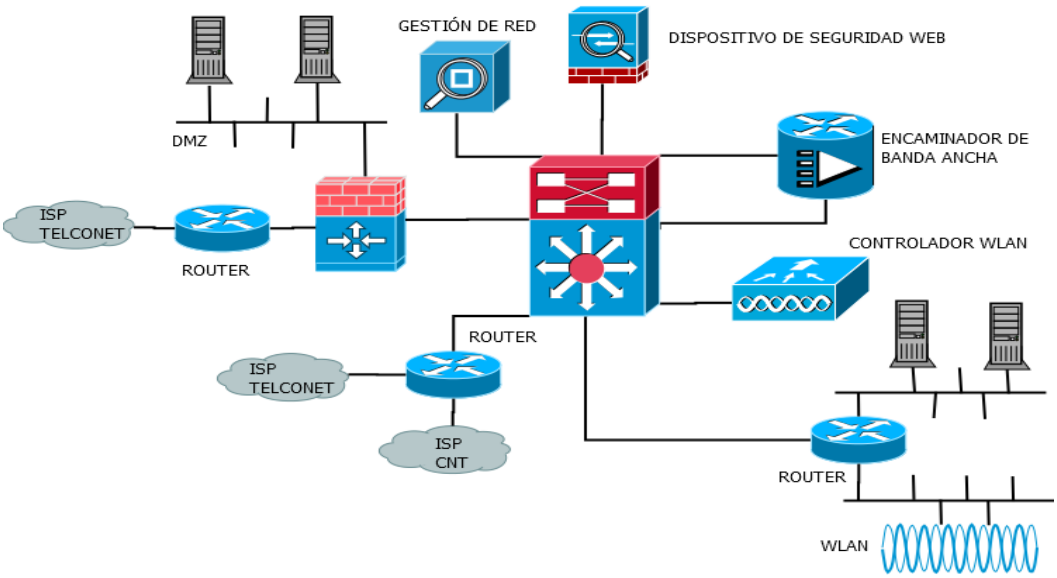


Ilustración 5 Diagrama de Red

1.3.3 Objetivo del SGSI

La seguridad de la información puede presentar diversos puntos de vista, con diferentes objetivos y con distintas aproximaciones, estos dependerán de los objetivos de negocio de la IES para su definición. Cabe mencionar que el objetivo de la implantación del SGSI en la IES debe estar claramente alineado a los objetivos de la institución y presentar conjuntamente el indicador que medirá su resultado.

A continuación presento los objetivos del SGSI con sus indicadores:

1. Proteger los activos de información de la IES en base a las dimensiones de seguridad, esto se podrá medir mediante el siguiente indicador:

   - Documento de Análisis de Riesgos donde se plasme el análisis de las amenazas a las que se encuentran expuestos los activos de la IES.
     - Control y análisis del riesgo residual.
     - Porcentaje de incidencias presentadas y controladas.
     - Porcentaje de reducción de amenazas anual.

$$\left(\frac{amenazas\ controladas}{total\ de\ incidentes}\right) * 100$$

2. Fortalecer los controles que aseguren los niveles de seguridad, esto se podrá medir con el siguiente indicador:

   - Documento de Gestión de Riesgos, donde se comparará el estado actual y el previsto de los controles de la norma ISO/IEC 27002:2013.

$$(Controles\ implementados) - (Controles\ actualizados + Controles\ previsto)$$

3. Formar al personal de la IES en materia de seguridad de la información, esto se podrá medir con el siguiente indicador:

   - Plan de Proyectos, donde se debe establecer un plan para la formación y concienciación del personal, el indicador medirá la eficacia del control de formación.

$$\frac{(suma\ total\ de\ valoraciones) * 10}{total\ personal\ capacitado}$$

4. Garantizar la seguridad continua de la información, esto se podrá medir con el siguiente indicador:

   - Presentación y aprobación de los planes de continuidad de negocio.
     - Definición de las situaciones críticas.
     - Asignación de responsabilidades.
     - Definición de las acciones de respuesta.
     - Mantenimiento.

$$\left(\frac{amenazas\ controladas\ en\ los\ límites}{total\ de\ incidentes}\right) * 100$$

1.3.4 Alcance del SGSI

La seguridad de la información debe estar gestionada en los ámbitos que la IES considere oportuno, recordemos que el proceso de implantación es continuo de maduración y mejora, siendo recomendable empezar abarcando con los procesos críticos para la IES, y posteriormente se irá implementando para los demás procesos.

Bajo la anterior premisa, la implementación de la seguridad de la información se va a realizar en la matriz de la IES, que se encuentra ubicada en la ciudad de Cuenca, bajo el siguiente escenario:

- La gestión de la seguridad de la información de la IES que cubre los sistemas de información Académicos, Financieros y de Recursos Humanos, la red de comunicación LAN, la seguridad en las telecomunicaciones, la parte física y ambiental, los equipos para procesamiento de datos según la declaración de aplicabilidad versión 2.

Se va a excluir el Ambiente Virtual de Aprendizaje, los equipos y dispositivos móviles, la red LAN, los computadores de administrativos y docentes, y de los laboratorios, infraestructura y redes de la sede Quito.

1.4 Objetivo del Plan del Director

El Plan del Director o comúnmente conocido como Plan de Seguridad de la Información tiene como objetivo específico recopilar los proyectos generados a partir de un análisis de la situación actual de la IES con el objetivo de reducir los riesgos a niveles aceptables, dichos proyectos son priorizados en base al alcance del tiempo (corto, mediano y largo plazo). El Plan del Seguridad deberá ser presentado al Consejo Superior para su aprobación y asignación de recursos necesarios antes de que empiece la ejecución de los proyectos. En la Ilustración 6 se visualizan las fases del PDS.

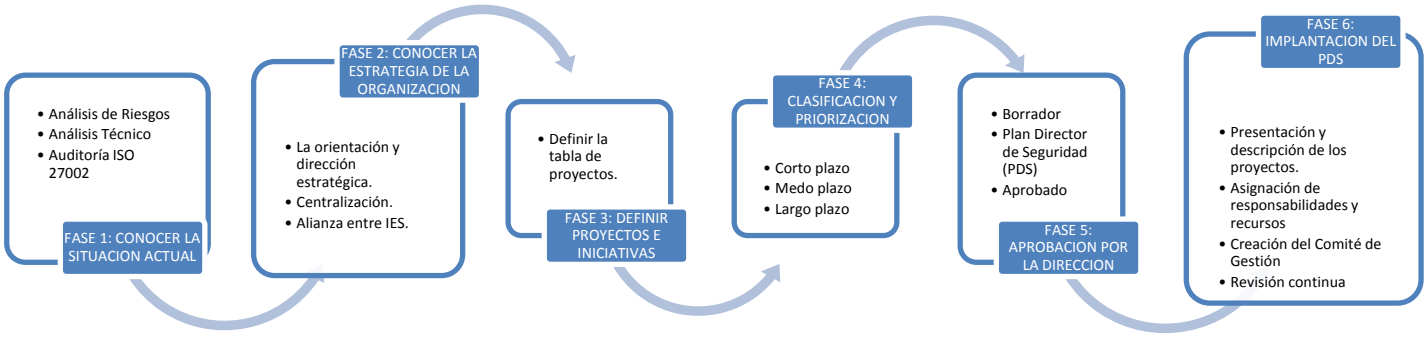


Ilustración 6 Fases del PDS

En base al plan estratégico de la IES y la presencia de los organismos revisores CES y CEAACES los objetivos del Plan de Director son:

1. Conocer el estado actual de la seguridad de la información en la IES.
2. Garantizar la integridad, confidencialidad y disponibilidad de la información académica en todas las etapas de su ciclo de vida.
3. Establecer los roles y responsabilidades en lo referente a la seguridad de la información.
4. Definir los controles para minimizar el impacto ante la presencia de ataques o vulnerabilidades de seguridad que puedan afectar a la continuidad del negocio por causas como: robo de la información, acceso no autorizado y mal uso de la misma, garantizando la continuidad del negocio y de los sistemas de información.
5. Implementar un Sistema de Gestión de Seguridad de la Información en concordancia a la norma ISO/IEC 27001:2013 y al plan estratégico.
6. Mejorar la imagen de la IES ante la comunidad universitaria y estudiantil, en materia de seguridad de la información.

1.5 Análisis Diferencial

En el presente apartado se va a realizar el análisis de los controles implantados en la IES vs controles necesarios según la norma ISO 27001:2013 e ISO/IEC 27002:2013, dando como resultado el análisis de la madurez de los controles hasta el momento implementados.

El análisis diferencial (GAP Analysis) permite conocer el estado general de la IES en relación a la seguridad de la información permitiendo definir el alcance. Se está usando como métrica el modelo de madurez de COBIT 5.0 (Control Objectives for Information and related Technology). En la Tabla 1 se definen los niveles de capacidad a usarse en el análisis diferencial.

Nivel	Descripción
5. Optimizado	El proceso predecible es mejorado de forma continua.
4. Predecible	El proceso predecible se encuentra en ejecución dentro de los límites definidos.
3. Establecido	El proceso gestionado se encuentre implementado mediante un proceso definido.
2. Gestionado	El proceso ejecutado se encuentra implementado mediante una gestión (planificado, supervisado y ajustado) y los resultados se encuentran establecidos, controlados y mantenidos adecuadamente.
1. Ejecutado	El proceso implementado alcanza su propósito.
0. Incompleto	El proceso no se encuentra implementado o no alcanza el propósito definido. Además existe muy poca o ninguna evidencia de haberse presentado un logro sistemático del propósito del proceso.

Tabla 1 Niveles de capacidad de COBIT 5

En el Anexo 01 se encuentra el Análisis Diferencial realizado en base a la ISO/IEC 27001:2013 e ISO/IEC27002:2013. En la Ilustración 7 se puede apreciar el estado de implementación de la norma ISO/IEC 27001:2013, cabe mencionar que en su mayoría el estado se encuentra como "Incompleto", presentando un 31.82% de requerimientos ejecutados.

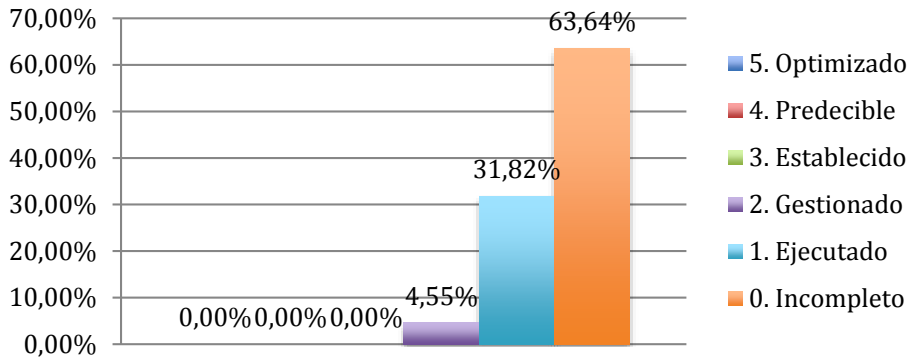


Ilustración 7 Estado de Implementación del SGSI

En la Ilustración 8 se observa mediante un gráfico de radar el estado de implementación de los requisitos de la norma ISO/IEC 27001:2013 de la IES, como dato importante puedo mencionar que la IES posee requerimientos implementados si no es en su totalidad definidos, pero existe un trabajo realizado.

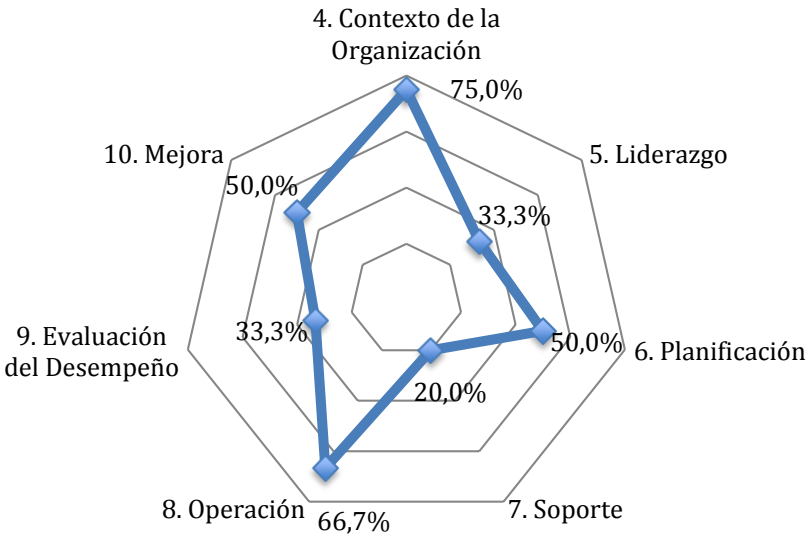


Ilustración 8 Estado de implementación ISO/IEC 27001:2013

Como se aprecia en la Ilustración 9 los controles se encuentran en valores muy similares, sobresaliendo el estado “Incompleto”, esto se debe a que muchos controles se encuentran en ejecución pero no es una política oficial, sino mas bien una práctica tomada por el Departamento.

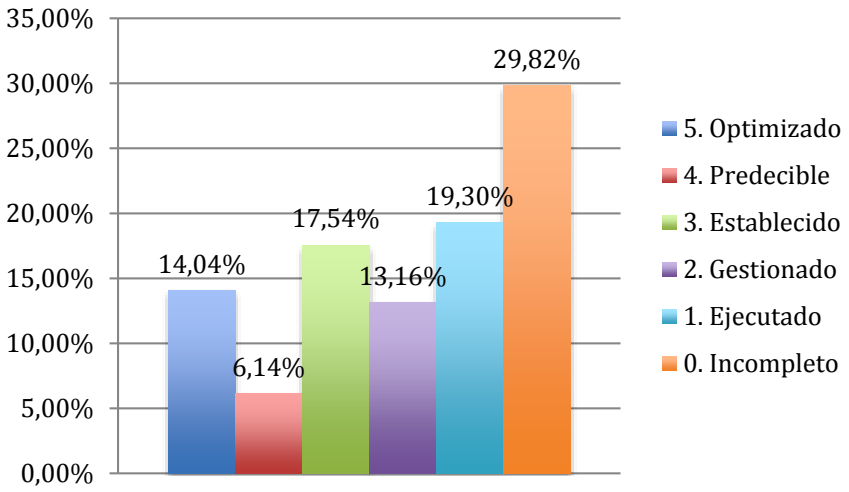


Ilustración 9 Estado de madurez de los controles

En la Ilustración 10 se observa mediante un gráfico de radar el estado de madurez de los controles en base a la norma ISO/IEC 27002:2013, donde se aprecia que la IES posee controles establecidos y que se encuentran en ejecución, pero hay otro, la Política de seguridad de la información que no sido definido.

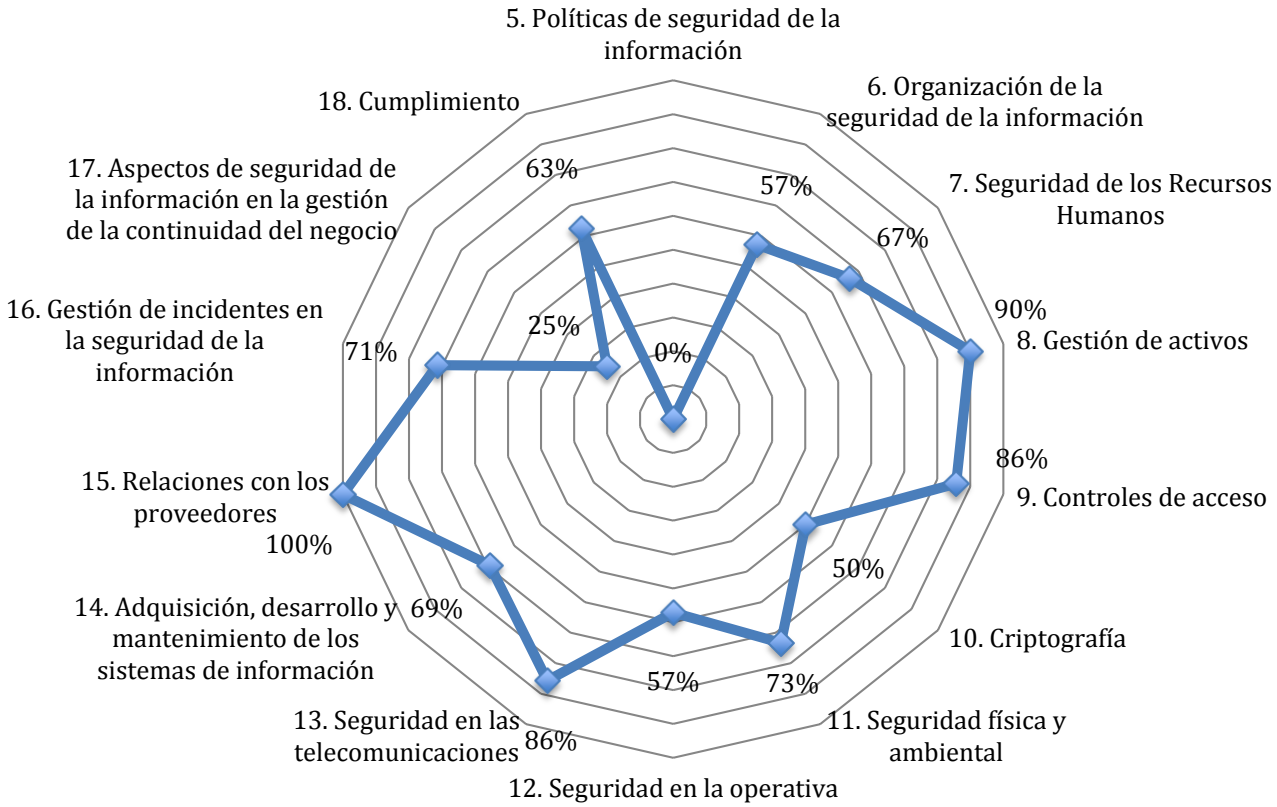


Ilustración 10 Estado de madurez ISO/IEC 27002:2013

2 Fase 2: Sistema de Gestión Documental

2.1 Introducción

En esta fase se va a definir la documentación básica para implementar el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001.

Se debe disponer de una normativa común de seguridad que regule como la IES va a trabajar en materia de seguridad de la información, pero antes de definirlo la IES debe claramente haber identificado los tipos de documentos con los cuales va a trabajar y la forma de identificarlos.

Recordemos que es muy importante cumplir con esta fase, ya que estos documentos van a servir de evidencia para certificar el SGSI.

2.1.1 Jerarquización de Documentación

Un punto primordial a tratar en la gestión documental son los tipos de documentos que se crean, ya que esto facilitará la gestión de los mismos. En caso de no hacerlo, la IES no sabrá que documentos tiene y el personal no conocerá si su carácter es o no normativo, entre otras consideraciones.

Se realizó una analogía con la norma ISO/IEC 9000 que trata sobre la calidad, los documentos se han clasificado según la siguiente pirámide jerárquica de documentos:

Políticas: Este documento va a recoger las directrices estratégicas mediante las cuales se van a regir en temas de seguridad de la información. Cabe mencionar que se pueden definir políticas de seguridad de primer nivel y segundo. Los controles definidos en dicho documento son de estricto cumplimiento, salvo que se encuentre alguna excepción.
Debe ser aprobado por el Consejo Superior y su divulgación es a todo el personal.

Normas y guías: Este documento plasma el proceso que debe seguir todo el personal de la IES, son implementados con la finalidad de mejorar la eficiencia de la seguridad de la información y optimizar recursos. Cabe mencionar que las normas son de cumplimiento obligatorio, mientras que las guías recogen las buenas prácticas y su aplicación puede ser total o parcial.
Debe ser aprobado por el Consejo Superior o por el Comité Informático, según corresponda y su divulgación corresponderá a los docentes y personal administrativo especificados en el documento.

Procedimiento: Este documento posee un conjunto de acciones a realizar, suelen intervenir actores de diferentes departamentos, su aplicación es obligatorio.
Debe ser aprobado por el responsable de su elaboración y su divulgación corresponderá a los docentes y personal administrativo especificados en el documento.

Manuales/Instrucciones: Este documento contiene las instrucciones detalladas para usar ciertas máquinas o realizar algunas acciones, su actualización suele depender de los cambios a nivel tecnológico de las máquinas, y suelen ser de cumplimiento obligatorio. Cabe mencionar que los fabricantes suelen proporcionar los manuales, aunque si pueden ser generados por el responsable de su manipulación.
Debe ser aprobado por el responsable y su divulgación se realiza a los actores involucrados.

Otros documentos: Se refiere a cualquier documento que no se encuentre definido en los antes mencionados, pudiendo ser formularios/plantillas en formato de papel o electrónico, experiencias, entre otros.

La IES posee el Departamento de Gestión Documental que ha definido la estructura de los documentos en base a la jerarquización proporcionando el siguiente esquema:

SGSI_TipoDocumento_NombreDocumento_Version

- **SGSI:** Es la sigla que identifica que el documento corresponde al Sistema de Gestión de Seguridad de la Información.
- **Tipo Documento (PO – NO/GU – PR – MA/IN – OD):** Identifica el tipo de documento, se tomarán las dos primeras letras de los tipos de documentación.
- **Nombre Documento:** Se tomará como máximo las cuatro iniciales del nombre del documento.
- **Versión (Año-XX):** Comprende al año de su creación y el número de su versión.

2.1.2 Nivel de Confidencialidad de Documentación

Dependiendo del tipo de documentación y la información, el documento estará restringido a los niveles de confidencialidad (público, interno y confidencial) que se encuentran definidos en la Política de Clasificación de la Información.

El nivel de confidencialidad debe estar establecida en el encabezado del manual de documentación.

2.1.3 Manual de Documentación

Tiene como objetivo estandarizar la estructura, forma, gestión, presentación, difusión y registro de toda la documentación que genere la IES, con el objetivo de transmitir una imagen sólida, generar documentación homogénea y de calidad que pueda ser identificada claramente siendo de fácil lectura y consulta, y sobre todo asegurar que se está trabajando con la última versión.

Todo documento tendrá la siguiente estructura:

- **Encabezado:** Todas las hojas deberán tener el mismo encabezado que tendrá una tabla donde se encuentra el logo de la IES, el tipo de documento, el código, entre otros datos, como se ilustra en la Tabla 2.

SGSI	**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**	Código: <Código>
		Nivel de Confidencialidad: <Nivel>
	Aprobado por: <Nombre Apellido>	Autorizado por: <Nombre Apellido>
	Aprobación: <AAAA/MM/DD>	Autorización: <AAAA/MM/DD>

Tabla 2 Encabezado del Manual de Documentación

- **Pie de página:** Todas las hojas deberán tener el mismo pie de página donde se indicará el número de página y el título del documento, como se aprecia en la Ilustración 11.

3 | <TÍTULO DEL DOCUMENTO>

Ilustración 11 Pie de página del Manual de Documentación

- **Portada:** En la primera hoja se deberá indicar el título del documento y el nombre de la Institución de Educación Superior.

- En la segunda hoja se incluyen dos tablas que registrarán: Registro de Cambios y Registro de Firmas, como se observa en la Tabla 3 y Tabla 4, respectivamente.

Nro. Cambio	Motivo del cambio	Fecha del cambio	Elaborado por
<Nro. 1>	<Motivo 1>	<AAAA/MM/DD>	<Nombre Apellido>

Tabla 3 Registro de Cambios del Manual de Documentación

Elaborado	Aprobado	Autorizado
<Nombre Apellido> <Cargo>	<Nombre Apellido> <Cargo>	<Nombre Apellido> <Cargo>

Tabla 4 Registro de Firmas del Manual de Documentación

- En la tercera hoja se incluirá el Índice de Contenido, Índice de Figuras e Índice de Tablas.
- En la cuarta hoja se va a desarrollar el documento, mediante las siguientes secciones:
  - **Introducción**: Esta sección es obligatoria y debe contener una breve descripción del documento, indicando las consideraciones más importantes, que ayudarán al lector para que tenga una idea del resto del documento.
  - **Alcance:** En esta sección se debe indicar a quien va a afectar el desarrollo del documento o el nivel al que va a abarcar.
  - **Objetivos:** En esta sección se debe indicar los objetivos que se esperan alcanzar con el desarrollo del documento.
  - **Anexos:** Los anexos se usarán para proporcionar información adicional a la documentación obligatoria del documento, no es obligatorio, sólo se incluirán en caso de considerarlo oportuno. Los anexos se identifican con letras ordenadas alfabéticamente.

En el Anexo 02 se encuentra el Manual de Documentación.

2.1.4 Difusión de Documentación

El Departamento de Gestión Documental será el encargado de custodiar los documentos originales, según las directrices establecidas. En el caso de manuales/instrucciones y otros documentos, los originales serán custodiados por los responsables del Departamento asegurando la disponibilidad y accesibilidad.

El Departamento de Comunicación y Publicaciones una vez aprobado el documento deberá comunicar al personal responsable en base al tipo de documento. Todo documento que sea de tipo público se lo colgará en la página web en su respectiva sección.

Si el documento es de tipo privado o confidencial, el Responsable de Seguridad de la Información deberá remitir el documento de manera impresa al encargado del departamento y/o área de la información, y archivar el acuse de recibo donde además, se incluirá una sección donde indique que ha leído el documento y acepta los términos de la misma.

En cada departamento y/o área el propietario de la información deberá poseer impreso el documento de Políticas de Seguridad de la Información y velar por su cumplimiento.

A continuación presento el esquema documental usado por la IES, todos los documentos mencionados se encuentran como anexos.

2.2 Esquema Documental

Para verificar que el Sistema de Gestión de Seguridad de la Información se encuentra implementado en la IES se necesitan los siguientes documentos:

2.2.1 Política de Seguridad

En este documento corresponde al primer nivel de la pirámide jerárquica en seguridad de la información, en la que se va a definir los principios, medidas y líneas de actuación globales en referencia a la Seguridad de la Información de la IES para protegerse contra amenazas que podrían afectar a los objetivos de la seguridad (confidencialidad, integridad y disponibilidad de la información); posterior será puesto en conocimiento de todos los empleados y de las partes interesadas según el alcance definido del SGSI para su implementación y guía de toma de decisiones.

El estándar ISO/IEC 27002:2013 establece en su apartado 5 “Políticas de Seguridad de la Información” una guía para su implementación.

La política de seguridad se va a concretar en políticas, normas, guías y estándares de segundo nivel, que será revisada anualmente y de igual manera será aprobada por el Consejo Superior, donde se deja clara constancia de su compromiso con la seguridad de la información mediante una acta.

Este documento no entra en mucho detalle ni es muy extenso, ya que será presentado a todo el personal de la IES y a terceras personas.

En el Anexo 03 se encuentra a detalle la Política de Seguridad para la IES.

2.2.2 Procedimiento de Auditorías Internas

Uno de los puntos principales en la implementación de un Sistema de Gestión de Seguridad de la Información es la revisión y propuesta de mejora continua de los controles o medidas de seguridad implantadas en la IES.

La Auditoría Interna o de primera parte va a ser realizado por personal de la IES. Tiene como finalidad realizar una autoevaluación de la implementación del SGSI, no es una auditoría de certificación.

El documento de Procedimiento de Auditoría Interna plasma las fases necesarias para desarrollar una auditoría interna, además incluye el perfil del equipo auditor y los requisitos generales, se lo puede encontrar en el Anexo 04.

2.2.3 Gestión de Indicadores

La norma ISO/IEC 27004:2009 orienta sobre el desarrollo y uso de los indicadores y la medición para evaluar la eficacia del control o controles implementados en un Sistema de Gestión de Seguridad de la Información especificados en la ISO/IEC 27001:2013.

Esta norma se centra en el modelo PDCA, que consiste en un ciclo continuo de mejora que se basa en las siguientes etapas:

- **Plan:** Consiste en establecer el SGSI y definir los indicadores en base a los criterios y consideraciones que se presentan en el Anexo 05.

Luego de haber elegido la medida de seguridad, métrica o indicador, es necesario determinar la estrategia de seguridad mediante los objetivos estratégicos, los cuales poseen un conjunto de indicadores que tienen como función medir el grado de cumplimiento del objetivo.

Un punto primordial a considerar por la IES en la definición de la métrica, son los recursos destinados, ya que no es rentable que las métricas consideren un costo mayor que el resultado que van a generar, pudiendo ser un grave error la implementación de una métrica que genere mayor costo que inversión, por lo tanto es recomendable justificar los recursos y el esfuerzo utilizado para obtener dicha información.

- **Do:** Consiste en adaptar los controles y procedimientos para obtener los datos necesarios, y comunicarlos al cuadro de mando. Un elemento crítico es el personal, ya que ellos serán los encargados de obtener, procesar y comunicar los datos tomados al cuadro de mando. Este personal deberá estar cualificado para dichas tareas, ya que en caso de cometer un error, los datos obtenidos no servirán y resultarán en pérdida para la IES en dinero y tiempo, por lo tanto la IES debe formarles a dicho personal e invertir recursos para que la extracción de datos se realice correctamente.

  Luego de que el personal haya obtenido los datos, deberá comunicar al cuadro de mando para tener una visión clara de los resultados y ayudar a la IES para la toma de decisiones.

- **Check:** Consiste en revisar los datos obtenidos de las métricas implementadas, y así conocer claramente lo que está sucediendo en la IES y si las métricas son rentables y útiles. Cabe mencionar que cada etapa guarda relación y muy importante, puesto que si se tomaron los datos erróneamente la decisión que tome la IES también va a ser errónea provocando pérdidas.

  Se recomienda tomar en consideración las opiniones de los empleados que deben gestionar las métricas y obtener los datos, ya que ellos al realizar el trabajo operativo y encontrarse a un nivel más cercano, tendrán una perspectiva más clara.

- **Act:** No sirve de nada haber establecido, implementado y revisado los datos si no se toman medidas de mejora, por lo tanto esta fase consiste en revisar las métricas implementadas con el fin de verificar que sigan cumpliendo con los objetivos planteados en la primera fase y que sigan generando valor a la IES.

  Las revisiones deben seguir los siguientes puntos para considerar al indicador como útil:

  - Evaluar la eficiencia del SGSI.
  - El costo de mantener el indicador y la obtención de los datos no sea superior al costo que aporta dicha información a la IES.
  - Indicar la evolución de los objetivos de seguridad.
  - Los objetivos de los indicadores no sean muy bajos porque siempre saldrían como cumplidos o correctos, dando una imagen errónea de la realidad de la IES.

El objetivo de que la IES tenga un procedimiento de gestión de indicadores es que la IES conozca los valores de seguridad, realice una evaluación de la eficiencia del SGSI, incluya niveles de seguridad que serán una guía para las revisiones del SGSI y realizar una evaluación de la efectividad de haber implementado los controles de seguridad de la información.

Con el transcurso del tiempo y como vaya madurando las métricas y el sistema de gestión de seguridad de la información, muchos de los indicadores establecidos se habrán actualizado, eliminado e incluso se crearán nuevos.

El documento Gestión de Indicadores se encuentra articulado a la norma ISO/IEC 27004:2009 donde se presenta el procedimiento para definir los indicadores acoplándolo a la realidad de la IES, se lo puede encontrar en el Anexo 05.

2.2.4 Procedimiento de Revisión por la Dirección

Uno de los puntos cruciales es la revisión que realiza el Consejo Superior de la implementación del SGSI en la IES, ya que dentro de la norma ISO/IEC 27001:2013 se encuentran controles específicos sobre la Organización y por ende es necesario ratificar el compromiso de la alta dirección en la gestión del SGSI.

La norma ISO/IEC 27001:2013 define los puntos de entrada y las salidas, logrando con ellos verificar y dar un seguimiento de los procedimientos, controles o medidas implementadas para garantizar el correcto funcionamiento del SGSI.

Se recomienda que esta revisión se realice anualmente para poder establecer nuevas estrategias o mejoras continuas en caso que los controles definidos no estén dando como resultado los objetivos esperados.

El documento de Procedimiento de Revisión por la Dirección evidencia el compromiso de la alta dirección, además de ser uno de los requisitos de la norma ISO/IEC 27001:2013 y para una certificación. Está redactado sin tecnicismos, ya que tiene como objetivo el ser una guía para el seguimiento y evaluación del desempeño del SGSI para el Consejo Superior; se lo puede encontrar en el Anexo 06.

2.2.5 Gestión de Roles y Responsabilidades

La norma ISO/IEC 27001:2013 establece la importancia de contar con documentación en donde se identifiquen los roles y responsabilidades mediante un esquema organizativo como es el Comité de Seguridad, que debe estar conformado por una persona de Dirección, ya que como se ha indicado es importante el compromiso y conocimiento de la alta Dirección, en nuestro caso del Consejo Superior. Cabe señalar que este esquema corresponde al nivel de la Seguridad de la Información, el mismo que debe tener el apoyo del Rector de la IES.

Además, se recomienda que no existan roles con más de un responsable, ya que llevaría a la confusión del personal, lo que se puede hacer es nombrar un Coordinador que regule las responsabilidades.

En el Anexo 07 se encuentra el documento de Gestión de Roles y Responsabilidades. Todas las normas y reglas expuestas en este documento van a afectar a todos, salvo que se exprese lo contrario.

2.2.6 Metodología de Análisis de Riesgos

Sin duda alguna una de las fases más importantes es el Análisis de Riesgos, donde se deben identificar las necesidades de seguridad de la IES en base a las vulnerabilidades y amenazas a las que se encuentra expuesto, además deberá cuantificar el impacto de que se produzcan ante los activos de la IES.

El Análisis de Riesgos no es una medida de seguridad sino mas bien permite identificar los peligros a los que se encuentra expuesta la IES, y con esta información podrá responder las siguientes preguntas y tomar las medidas necesarias.

1. ¿Qué hay que proteger?
2. ¿De qué o quién hay que proteger, y por qué?
3. ¿Cómo nos vamos a proteger?

Luego de haber dado respuesta a las preguntas, la IES podrá tomar las respectivas decisiones para mitigar los riesgos que presentan las amenazas y vulnerabilidades.

Existen diferentes metodologías que permiten realizar un análisis de riesgos, cada una con sus características particulares, pero todos se fundamentan en los mismos aspectos: Identificación y valoración de activos, Valoración de amenazas y vulnerabilidades y la Gestión de Riesgos.

La IES ha escogido como método de Análisis de Riesgos a MAGERIT, ya que es una metodología que presenta los siguientes objetivos:

1. Concientizar a los responsables de los sistemas de información de la presencia de riesgos y la necesidad de mitigarlos.
2. Brindar un método sistemático para analizar los riesgos.
3. Proveer las medidas de seguridad de información oportunas para mantener los riesgos en niveles aceptables, es decir, bajo el umbral de riesgo definido por la IES.
4. Preparar a la IES para los procesos de evaluación, auditoría y certificación.

La ventaja de usar MAGERIT es que las decisiones serán más fáciles de tomar, ya que los resultados se expresa con valores económicos, pero al mismo tiempo refleja una desventaja, porque hay que traducir todas las valoraciones en valores económicos, haciéndola costosa. La IES considera que el beneficio de usar MAGERIT es mayor que el costo.

En el Anexo 08 se presenta a detalle la Metodología de Análisis de Riesgos MAGERIT.

2.2.7 Declaración de Aplicabilidad

La norma ISO/IEC 27001:2013 incluye como requisito que exista la Declaración de Aplicabilidad de los controles, según la norma ISO/IEC 27002:2013 Código de buenas prácticas en la gestión de la seguridad de la información.

Por cada control se procedió a indicar si aplica o no, con su respectiva justificación. Este documento es considerado como uno de los más importantes, puesto que corresponde un elemento fundamental para la implementación de los controles de seguridad y como herramienta en la realización de una auditoría.

En el Anexo 09 se presenta la Declaración de Aplicabilidad.

3 Fase 3: Análisis de Riesgos

3.1 Introducción

Esta fase tiene como objetivo el identificar los activos de la IES, las vulnerabilidades y amenazas a las que se encuentra expuesto.

El análisis de riesgos corresponde al proceso de identificación de los riesgos, su magnitud y las áreas que requieren medidas de protección. Se debe tener claro que en esta fase no se genera una medida de seguridad, sino la identificación de las vulnerabilidades y amenazas a las que está expuesta la IES, por lo tanto aquí no se va a evitar que la Universidad sufra ataques.

Muchas instituciones invierten dinero en realizar cambios a nivel de seguridad, pero no tienen claro porque lo hicieron en ciertas áreas ni si van a lograr responder a los incidentes a los que están expuestos, esto se debe a que no han analizado lo que necesita la institución, de allí nace el Análisis de Riesgos siendo una de las fases esenciales para que los cambios e inversiones que se realicen se ajusten a la realidad y necesidad de la Institución.

Existen diversos métodos para realizar Análisis de Riesgos, cada uno con sus características propias, ventajas y desventajas, pero en general todos trabajan y analizan con los mismos elementos que son: activos, amenazas y vulnerabilidades. Como se ha mencionado anteriormente, se va a usar la Metodología de Análisis de Riesgos MAGERIT.

El Análisis de Riesgos es la relación entre la identificación y valoración de activos, y la estimación de amenazas y vulnerabilidades.

3.2 Inventario de Activos

En esta sección se va a realizar el inventario de activos de la IES en base a los procesos propios, es decir, se va a listar todos los recursos según el alcance del SGSI que presentan valor a la IES y por lo tanto deben ser protegidos ante amenazas.

En la Tabla 5 se presenta la clasificación de los activos de la IES en base a la metodología MAGERIT que se detalla en el Anexo 08. Esta tabla se encuentra estructurada mediante el código de identificación del activo, la denominación, una breve descripción que indica sobre el activo y el propietario del mismo.

Código	Denominación	Descripción	Propietario
[D] Datos/Información			
D-001	Información académica	Datos de los estudiantes, proyectos, investigaciones, notas, etc.	Vicerrector Académico
D-002	Información financiera	Datos sobre balances, prepuestos, cuentas, costos, etc.	Secretario Técnico de Finanzas
D-003	Información del personal	Datos sobre contratos, sueldos, datos personales de los empleados (docentes y administrativos), nóminas, etc.	Secretario Técnico de Recursos Humanos
D-004	Información institucional	Datos sobre reglamentos, normativas, resoluciones, convenios, etc.	Secretaría General
D-005	Datos del Sistema Académico, Financiero y de Recursos Humanos	Base de Datos Oracle Standard Edition 11g, que almacena los datos académicos, financieros y del personal.	Administrador de Base de Datos
D-006	Código Fuente	Código fuente de las aplicaciones de la	Coordinador de Desarrollo

		IES.	de Sistemas de Información
D-007	Logs	Registros de los servidores.	Administrador de Base de Datos
D-008	Backups	Copias de respaldo de los datos de las aplicaciones de la IES.	Administrador de Base de Datos
[K] Claves criptográficas			
K-001	Certificado de clave pública	Certificado del estándar internacional ITU (CCITT) X.509 para las claves de cifrado para las VPN entre las sedes, el acceso remoto y firmas digitales.	Responsable de Seguridad de la Información
[S] Servicio			
S-001	Sistema Académico	Sistema que se encarga de controlar todo lo académico para el nivel de Grado y Posgrado como son: las inscripciones, matrículas, proyectos, resoluciones, calificaciones, académicos, paracadémicos, evaluación docente, entre otros.	Vicerrector Académico
S-002	Sistema Financiero	Sistema que se encarga de controlar todo lo referente a la contabilidad de la IES como son: balances, presupuestos, cuentas, costos, activos fijos, adquisiciones, facturación, flujo de caja, entre otros.	Secretario Técnico de Finanzas
S-003	Sistema de Recursos Humanos	Sistema que se encarga de controlar todo lo referente al personal de la IES como son: contratos, sueldos, datos personales de los empleados, nóminas, entre otros.	Secretario Técnico de Recursos Humanos
S-004	World Wide Web	Servicio contratado a TELCONET y CNT, permitiendo a todo el campus de la IES acceder a internet.	Director del Departamento de Tecnologías de Información y Comunicación
S-005	Correo electrónico	Servicio contratado a Microsoft.	Director del Departamento de Tecnologías de Información y Comunicación
S-006	Portal WEB	Muestra a la comunidad universitaria y externos información de la IES como son: noticias, eventos, procesos académicos, entre otros.	Coordinador de Desarrollo de Sistemas de Información
S-007	Proxy	Servidor WSA que permite controlar el tráfico de internet, proteger contra malware y controlar las aplicaciones.	Administrador de Redes
S-008	Almacenamiento de ficheros	Servidor Windows Server 2012 R2 que brinda alojamiento de ficheros.	Administrador de Redes
S-009	Servicio Web para docentes y estudiantes	Muestra a los docentes recursos como: horarios, proyectos, evaluaciones, entre otros; y a los estudiantes su información académica.	Coordinador de Desarrollo de Sistemas de Información
S-010	Servicio de directorio	Servidor Active Directory.	Administrador de Redes
S-011	Telefonía IP	Permite la comunicación interna y externa.	Administrador de Redes
S-012	Videoconferencia	Permite realizar videoconferencias entre las distintas sedes de la IES.	Administrador de Redes
S-013	Servicio de copias de seguridad	Se encarga de realizar las copias de seguridad de toda la información académica de la IES.	Administrador de Base de Datos
[SW] Software			
SW-001	Sistema Operativo de los servidores	Sistema operativo instalado en los servidores: Gnu/Linux centOS 5, Red Hat Enterprise Linux Server Release	Coordinador de Administración de Redes e Infraestructura

		5.8, Windows Server 2003 R2 Enterprise Edition VHD, Windows Server 2008 R2 Enterprise Edition x64.	
SW-002	Sistema Operativo del personal	Sistema operativo instalado en los computadores de docentes, administrativos y laboratorios: Windows XP Professional con SP3, Windows 7 Professional, Windows 8.1 Pro.	Director del Departamento de Tecnologías de Información y Comunicación
SW-003	Software Académico	Se refiere a todas las aplicaciones académicas usadas para los distintos laboratorios de la IES como son: Oracle, Labwie, Mathworks, Autodesk, Scilab, Arcgis, Cisco Packet Tracer, GIMP, Netbeans, Eclipse, Master Suite CS6, ANSYS, Mysql, Oracle VM VirtualBox, entre otros.	Director del Departamento de Tecnologías de Información y Comunicación
SW-004	Software para Desarrollo	Se refiere a las aplicaciones usadas en el Área de Desarrollo de Sistemas de Información: Oracle Forms, java, JSP, CSS, JSF 2.0, PHP, RICHFACES, WebServices, entre otros.	Director del Departamento de Tecnologías de Información y Comunicación
SW-005	Software Institucional	Se refiere a todas las aplicaciones usadas en los diversos departamentos y/o áreas como son: utilitarios de Microsoft Office 2013, Open Office, Open Project, Do PDF, Adobe Reader, Panda Antivirus Pro 2015, entre otros.	Director del Departamento de Tecnologías de Información y Comunicación
SW-006	Antivirus	Ofrece el servicio de antivirus (Panda Antivirus Pro 2015) a todos los equipos de la IES.	Analista de Soportes Técnico
SW-007	Sistema Gestor de Base de Datos	Base de Datos Oracle Standard Edition 11g.	Administrador de Base de Datos
[HW] Hardware			
HW-001	Servidores	Servidor Proxy CISCO WSA S670, Cisco Unified CM Administration, servidor Blade H22, servidor ibm x3500 m3. IBM e xSeries 336 883756U Ubuntu 2x 3.8 Xeon, 4 GB, 2x240 GB SATA, 2xG LAN, servidor Dell Poweredge 2850 2 Xeon 292 Gb 6 Gb 12x S/ Juros,Servidor Rack Dell PowerEdge r710 Biprocesador Xeon Quad Core 2,4 Ghz.	Coordinador de Administración de Redes e Infraestructura
HW-002	Videoconferencia	Sistema Polycom RealPresence Group 300. La IES posee: 2 salas en Rectorado, 1 sala en la matriz Cuenca y 1 sala en el Departamento de TIC	Coordinador de Administración de Redes e Infraestructura
HW-003	Computadores para el personal Administrativo	200 computadores entre portátiles y de escritorios para el personal administrativo.	Coordinador de Administración de Redes e Infraestructura
HW-004	Computadores para docentes	300 computadores entre portátiles y de escritorios para docentes.	Coordinador de Administración de Redes e Infraestructura
HW-005	Computadores para el personal de Desarrollo	25 computadores entre portátiles y de escritorios para el personal del Departamento de TIC.	Coordinador de Desarrollo de Sistemas de Información
HW-006	Impresoras	80 impresoras en la matriz y 15 en el Rectorado.	Coordinador de Administración de Redes e Infraestructura
HW-007	Backbone LAN	Posee un CISCO Catalyst 6500 Series y un Catalyst 3560 E.	Coordinador de Administración de Redes e

			Infraestructura
HW-008	LAN y Firewall	Se refiere a los routers, switches y la estructura necesaria para brindar la respectiva comunicación en la campus de la IES. El firewall posee un CISCO ASA 5505	Coordinador de Administración de Redes e Infraestructura
HW-009	Telefonía IP	La IES posee un contrato con Cisco para los siguientes dispositivos de telefonía IP: Cisco Unified IP Phone 524G, Cisco Unified IP Phone 7975G y Cisco Unified SIP Phone 3911.	Coordinador de Administración de Redes e Infraestructura
[COM] Redes de Comunicaciones			
COM-001	WIFI	Wireless access point para interconectar los equipos.	Administrador de Redes
COM-002	LAN	Se refiere a las configuraciones para permitir conectividad en la matriz Cuenca como son: creación de VLANs, configuraciones, entre otros.	Administrador de Redes
COM-003	VPN	Son las configuraciones para realizar las conexiones de redes virtuales privadas.	Administrador de Redes
[Media] Soportes de Información			
Media-001	Backups	Se realizan copias de seguridad de los datos que se encuentran en los sistemas de la IES.	Administrador de Base de Datos
Media-002	Documentos Académicos	Son los documentos de los estudiantes de la IES como son: Record Académico, calificaciones, trámites, actas de grado, resoluciones, entre otros. Esta información se encuentra impresa.	Secretaría de Campus
Media-003	Documentos Institucionales	Son los documentos de la IES como son: Proyectos Académicos, resoluciones del Consejo Superior, convenios, entre otros. Esta información se encuentra impresa y de forma digital.	Secretaría General
Media-004	Documentos técnicos	Son los documentos técnicos sobre la infraestructura de la IES, manuales de usuario, configuraciones de equipos, entre otros. Esta información se encuentra impresa.	Director del Departamento de Tecnologías de Información y Comunicación
[AUX] Equipamiento auxiliar			
AUX-001	Generador Eléctrico	Existe un generador eléctrico FG Wilson.	Coordinador de Administración de Redes e Infraestructura
AUX-002	Destructores de papel	Existen 5 destructores de papel en Rectorado y 20 en la matriz Cuenca.	Analista de Soportes Técnico
[L] Instalaciones			
L-001	Matriz Cuenca	Está instalación corresponde a las aulas, laboratorios, oficinas administrativas y de investigación.	Vicerrector de Sede
L-002	Rectorado	Este edificio posee las oficinas administrativas.	Vicerrector General
L-003	Departamento TIC	Centro de procesamiento de datos de la matriz Cuenca.	Director del Departamento de Tecnologías de Información y Comunicación
[P] Personal			
P-001	Alta Dirección	Está conformado por: Vicerrector	Rector

		General, Vicerrector de Sede, Vicerrector Académico, Coordinadores Académicos de Sede y las distintas Secretarías.	
P-002	Director del Departamento de TIC	Es el Director del Departamento de Tecnologías de Información y Comunicación	Alta Dirección
P-003	Área de Desarrollo de Sistemas de Información y Área de Administración de Redes e Infraestructura	Se refiere al Administrador de Base de Datos, Ingenieros WEB, Analistas Programadores Senior y Analistas Programadores Junior.	Director del Departamento de Tecnologías de Información y Comunicación
P-004	Área de Explotación	Se refiere a los Asistentes de Explotación.	Coordinador de Explotación
P-005	Personal administrativo	Se refiere a todo el personal que realiza tareas administrativas en la matriz Cuenca como en Rectorado.	Vicerrector de Sede
P-006	Seguridad Privada	Se refiere al servicio de seguridad privada que se encuentra contratada a una Empresa externa.	Vicerrector de Sede
P-007	Docentes	Se refiere al tipo de personal académico universitario (titular agregado, titular principal, titular principal investigador, invitado, ocasional).	Vicerrector de Sede
P-008	Estudiantes	Hace referencia a: graduados, egresados y estudiantes (normales, huéspedes y oyentes) de la IES.	Vicerrector de Sede

Tabla 5 Inventario de activos

3.3 Valoración de los Activos

Trata de dar al activo un valor cualitativo usando el análisis de MAGERIT en su Libro III (punto 2.1) añadiéndole un valor cuantitativo (económico). Esta valoración se encuentra a detalle en el Anexo 8.

3.3.1 Dependencia de Activos

Se debe considerar que los activos se encuentran jerarquizados, es decir, existe una dependencia entre activos; los que se encuentran en la parte superior son los dependientes de los que se encuentran en el nivel inferior, por lo tanto ante la presencia de una amenaza en el activo inferior tendrá como consecuencia un daño sobre el activo superior por la presencia de la dependencia.

Se ha procedido a realizar el análisis de dependencias de los activos considerados de nivel “Muy Alto” de los activos esenciales:

- [D] Datos/Información
  - D-001 Información Académica.
  - D-002 Información Financiera.
  - D-003 Información del Personal
  - D-005 Datos del Sistema Académico, Financiero y de Recursos Humanos.
- [S] Servicios
  - S-001 Sistema Académico

[D] Datos/Información

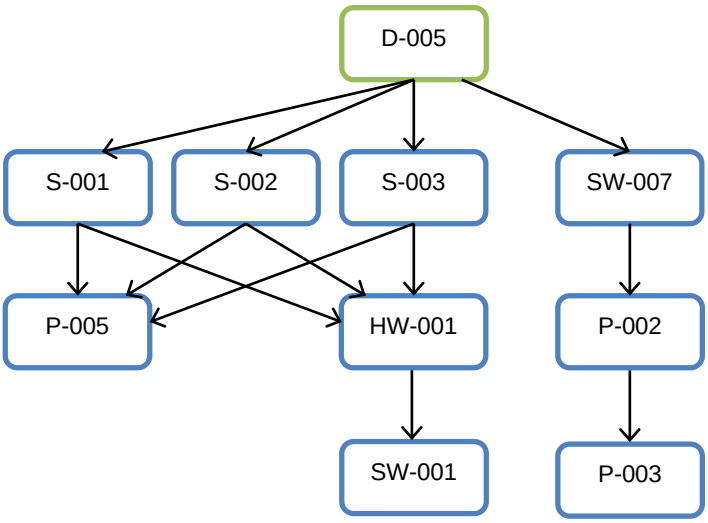


Ilustración 12 Dependencia del activo “Datos del Sistema Académico, Financiero y de Recursos Humanos”

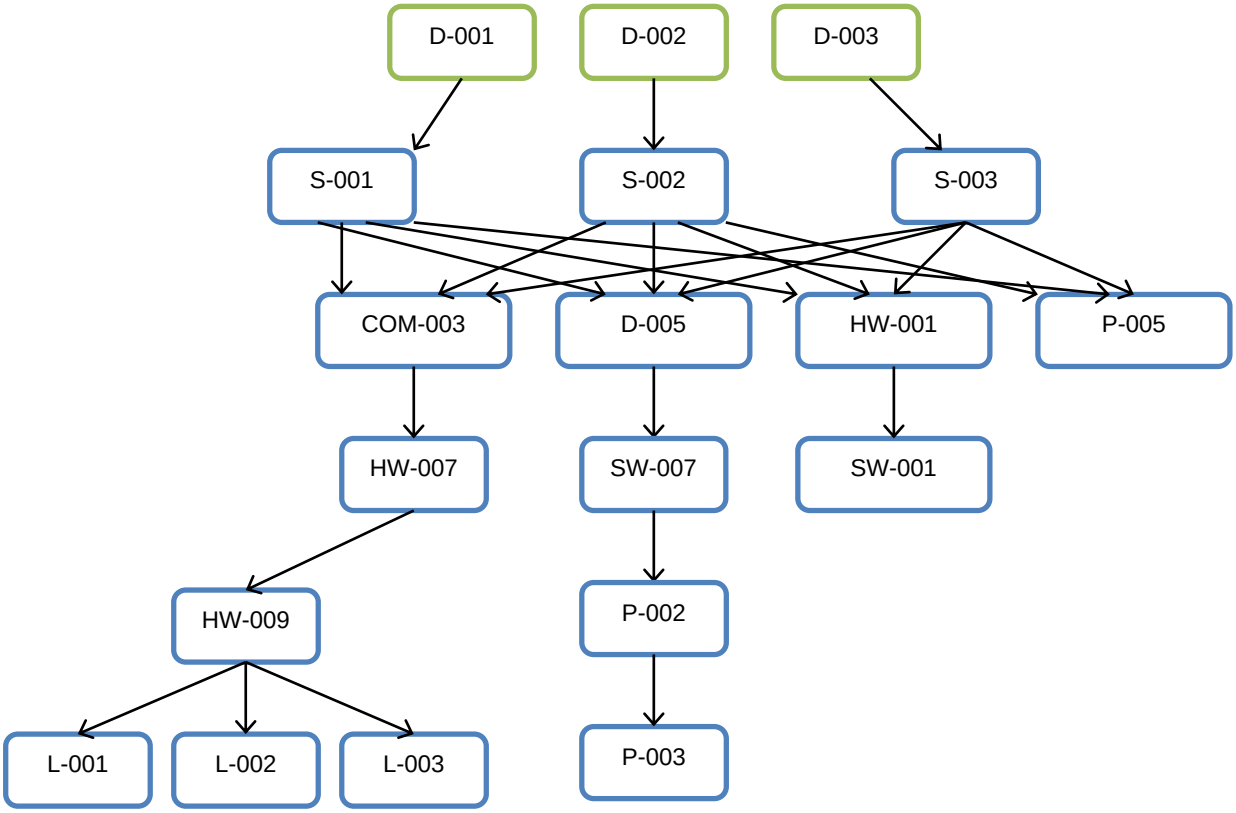


Ilustración 13 Dependencia del activo “Información Académica”, Información Financiera” e “Información del personal”

[S] Servicios

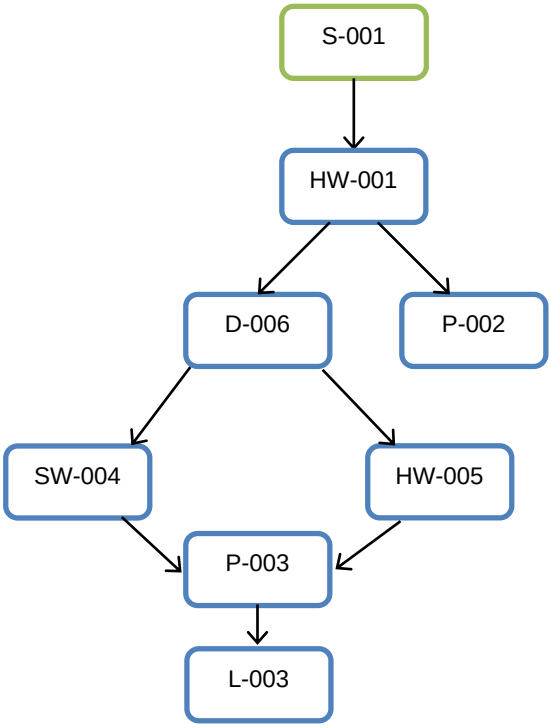


Ilustración 14 Dependencia del activo “Sistema Académico”

3.3.2 Valoración de Activos y Dimensiones de Seguridad

El valor del activo puede ser propio o acumulado, tomando en consideración los siguientes aspectos:

- Valor de reposición: El valor que tiene que reponer la Empresa en caso de que no se tenga el activo.
- Valor de configuración: El valor desde que se compra el activo hasta que se configure y esté listo para su uso.
- Valor de uso del activo: El valor que pierde durante el tiempo que no se puede utilizar el activo para la función que desempeña dentro de los procesos de la Empresa.
- Valor de pérdida de oportunidad: El valor que pierde la Empresa por no disponer del activo.

La criticidad corresponde al nivel de importancia del activo en los procesos de la IES y el nivel de protección que se necesita para mantener las dimensiones de la seguridad.

Junto a la valoración de los activos se debe incluir los aspectos más críticos que ayudarán cuando se deba definir las salvaguardas, por lo tanto, se debe realizar la valoración ACIDA que dará como resultado la medición de la criticidad en las cinco dimensiones. Esta medición permitirá valorar el impacto de una amenaza sobre el activo que no esté cubierto sobre la salvaguarda.

A continuación se presentan las dimensiones de seguridad tomadas del Libro 2 “Catálogo de Elementos” (punto 3) de la metodología MAGERIT.

- **Disponibilidad:** Se refiere a la capacidad para que la IES o el proceso autorizado tenga acceso a la información cuando lo necesiten. La interrogante a responder es: *¿Qué importancia tendría que el activo no estuviera disponible?*
- **Integridad:** El activo de información no ha sido alterado de manera no autorizada. La interrogante a responder es: *¿Qué importancia tendría que los datos fueran modificados fuera de control?*

- **Confidencialidad:** La información no se pone a disposición, ni se revela a personas, entidades o procesos que no estén autorizados. La interrogante a responder es: *¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?*
- **Autenticidad:** Se refiere a la capacidad de garantizar la identidad de los usuarios y procesos que manejan la información. La interrogante a responder es: *¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree o que lo datos no fueran imputables a quien se cree?*
- **Trazabilidad:** Las actuaciones de la IES pueden ser reproducidos mediante una secuencia de acciones determinando quien fue el autor de la acción. La interrogante es: *¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio o del acceso a los datos?*

Una vez que se han definido claramente cada una de las dimensiones, se usará la escala de valoraciones que se presenta en la Tabla 6. Hay que evitar asignar a todos los activos la valoración de 10 – Daño muy grave.

Valor	Criterio
10	Daño muy grave a la IES
7 - 9	Daño grave a la IES
4 - 6	Daño importante a la IES
1 - 3	Daño menor a la IES
0	Irrelevante para la IES

Tabla 6 Valoración Dimensiones de Seguridad

Luego de haber determinado la dependencia de activos, realizado la valoración y determinado las dimensiones de seguridad, se podrá generar la tabla de resumen de valoración de activos donde se incluye además los aspectos críticos del mismo.

Código	Denominación	Valoración Cuantitativa	Valoración Cualitativa	Dimensiones				
				Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
[D] Datos/Información								
D-001	Información académica	$ 200.000,00	Muy Alto	6	9	4	2	4
D-002	Información financiera	$ 200.000,00	Muy Alto	5	9	7	2	4
D-003	Información del personal	$ 200.000,00	Muy Alto	4	8	6	2	4
D-004	Información institucional	$ 200.000,00	Muy Alto	4	8	6	2	3
D-005	Datos del Sistema Académico, Financiero y de Recursos Humanos	$ 200.000,00	Muy Alto	8	9	6	6	3
D-006	Código Fuente	$ 75.000,00	Alto	4	8	8	2	5
D-007	Logs	$ 10.000,00	Bajo	2	5	2	2	8
D-008	Backups	$ 40.000,00	Medio	4	6	8	3	2
[K] Claves criptográficas								
K-001	Certificado de clave pública	$ 40.000,00	Medio	2	8	9	9	2
[S] Servicio								
S-001	Sistema Académico	$ 200.000,00	Muy Alto	9	6	6	9	9
S-002	Sistema Financiero	$ 200.000,00	Muy Alto	5	6	6	9	9
S-003	Sistema de Recursos Humanos	$ 40.000,00	Medio	5	5	5	8	7

S-004	World Wide Web	$ 40.000,00	Medio	7	0	0	0	2
S-005	Correo electrónico	$ 10.000,00	Bajo	7	3	7	6	0
S-006	Portal WEB	$ 40.000,00	Medio	4	5	1	2	0
S-007	Proxy	$ 75.000,00	Alto	5	2	5	0	4
S-008	Almacenamiento de ficheros	$ 40.000,00	Medio	3	6	4	3	2
S-009	Servicio Web para docentes y estudiantes	$ 10.000,00	Bajo	4	2	4	4	2
S-010	Servicio de directorio	$ 10.000,00	Bajo	4	4	8	4	4
S-011	Telefonía IP	$ 5.000,00	Muy Bajo	6	2	8	1	0
S-012	Videoconferencia	$ 5.000,00	Muy Bajo	4	0	4	0	0
S-013	Servicio de copias de seguridad	$ 75.000,00	Alto	7	7	5	5	4
[SW] Software								
SW-001	Sistema Operativo de los servidores	$ 75.000,00	Alto	7	8	2	4	5
SW-002	Sistema Operativo del personal	$ 10.000,00	Bajo	4	3	2	1	1
SW-003	Software Académico	$ 75.000,00	Alto	6	6	2	0	0
SW-004	Software para Desarrollo	$ 40.000,00	Medio	5	2	6	3	0
SW-005	Software Institucional	$ 10.000,00	Bajo	2	1	0	0	0
SW-006	Antivirus	$ 10.000,00	Bajo	5	5	1	0	0
SW-007	Sistema Gestor de Base de Datos	$ 75.000,00	Alto	8	9	8	8	8
[HW] Hardware								
HW-001	Servidores	$ 200.000,00	Muy Alto	9	8	4	8	2
HW-002	Videoconferencia	$ 75.000,00	Alto	4	2	0	0	0
HW-003	Computadores para el personal Administrativo	$ 40.000,00	Medio	5	1	0	3	4
HW-004	Computadores para docentes	$ 40.000,00	Medio	5	3	3	0	0
HW-005	Computadores para el personal de Desarrollo	$ 40.000,00	Medio	7	5	2	7	4
HW-006	Impresoras	$ 10.000,00	Bajo	1	1	0	0	0
HW-007	Backbone LAN	$ 75.000,00	Alto	9	2	2	3	2
HW-008	LAN y Firewall	$ 40.000,00	Medio	7	2	2	4	2
HW-009	Telefonía IP	$ 40.000,00	Medio	4	2	1	0	0
[COM] Redes de Comunicaciones								
COM-001	WIFI	$ 40.000,00	Medio	5	2	0	0	0
COM-002	LAN	$ 75.000,00	Alto	9	3	9	4	4
COM-003	VPN	$ 10.000,00	Bajo	6	2	8	4	4
[Media] Soportes de Información								
Media-001	Backups	$ 40.000,00	Medio	3	6	2	5	4
Media-002	Documentos Académicos	$ 75.000,00	Alto	4	6	5	5	4
Media-003	Documentos Institucionales	$ 40.000,00	Medio	2	3	2	5	4
Media-004	Documentos técnicos	$ 10.000,00	Bajo	3	4	2	4	2
[AUX] Equipamiento auxiliar								
AUX-001	Generador Eléctrico	$ 75.000,00	Alto	5	5	0	5	2
AUX-002	Destructores de papel	$ 5.000,00	Muy Bajo	1	0	5	2	1
[L] Instalaciones								
L-001	Matriz Cuenca	$ 200.000,00	Muy Alto	7	4	4	0	0
L-002	Rectorado	$ 40.000,00	Medio	3	4	4	0	0
L-003	Departamento TIC	$ 75.000,00	Alto	5	4	4	0	0
[P] Personal								
P-001	Alta Dirección	$ 10.000,00	Bajo	6	4	6	0	0

P-002	Director del Departamento de TIC	$ 10.000,00	Bajo	7	6	8	0	0
P-003	Área de Desarrollo de Sistemas de Información y Área de Administración de Redes e Infraestructura	$ 40.000,00	Medio	9	6	7	0	0
P-004	Área de Explotación	$ 10.000,00	Bajo	7	6	5	0	0
P-005	Personal administrativo	$ 40.000,00	Medio	4	2	6	0	0
P-006	Seguridad Privada	$ 10.000,00	Bajo	4	4	8	0	0
P-007	Docentes	$ 40.000,00	Medio	6	4	2	0	0
P-008	Estudiantes	$ 75.000,00	Alto	4	2	1	0	0

Tabla 7 Valoración de los activos y dimensiones de seguridad

3.4 Análisis de Amenazas

Los activos de la IES se encuentran expuestos a amenazas[1] que pueden ser explotadas por las vulnerabilidades, es crucial para una correcta toma de decisiones el contar con un análisis de amenazas, en donde se podrá ver con claridad que activos deben ser protegidos y ante que amenazas.

Para el análisis de las amenazas se va a usar el Libro 2 "Catálogo de Elementos" de la metodología MAGERIT, el mismo que clasifica en los siguientes grupos:

- Desastres naturales.
- De origen industrial.
- Errores y fallos no intencionados.
- Ataques intencionados.

En la Tabla 8 presento el análisis de amenazas del activo "Información Académica" en donde por activo se ha identificado la frecuencia con la que se puede producir la amenaza y el impacto en las distintas dimensiones de seguridad. Cabe mencionar que en el Anexo 10 se detalla el Análisis de las Amenazas de todos los activos presentados en las secciones anteriores.

Análisis de Amenazas		Tipo de Activo	
		[D] Datos / Información	
Código	**Amenazas**	D-001	$ 200.000,00
[N] Desastres naturales			
[N.1]	Fuego		
[N.2]	Daños por agua		
[N.*]	Desastres naturales		
[I] De origen industrial			
[L.1]	Fuego		
[I.2]	Daños por agua		
[I.*]	Desastres naturales		
[I.3]	Contaminación mecánica		
[I.4]	Contaminación electromagnética		
[I.5]	Avería de origen físico o lógico		
[I.6]	Corte del suministro eléctrico		
[I.7]	Condiciones inadecuadas de temperatura o humedad		
[I.8]	Fallo de servicios de comunicaciones		

[1] Acción, persona, incidencia, etc.; que pueda provocar un daño, riesgo o posible peligro para el activo de la Empresa.

[I.9]	Interrupción de otros servicios y suministros esenciales			
[I.10]	Degradación de los soportes de almacenamiento de la información			
[I.11]	Emanaciones electromagnéticas			
[E] Errores y fallos no intencionados				
[E.1]	Errores de los usuarios	[D] 40% [I] 70%	0,005479	70%
		[C] 40% [A] 0% [T] 0%	$ 767,06	
[E.2]	Errores del administrador	[D] 40% [I] 90%	0,00274	90%
		[C] 40% [A] 0% [T] 0%	$ 493,20	
[E.3]	Errores de monitorización (log)			
[E.4]	Errores de configuración			
[E.7]	Deficiencias en la organización			
[E.8]	Difusión de software dañino			
[E.9]	Errores de re-encaminamiento			
[E.10]	Errores de secuencia			
[E.15]	Alteración accidental de información	[D] 0% [I] 60%	0,005479	60%
		[C] 0% [A] 0% [T] 0%	$ 657,48	
[E.18]	Destrucción de información	[D] 50% [I] 0%	0,005479	50%
		[C] 0% [A] 0% [T] 0%	$ 547,90	
[E.19]	Fugas de información	[D] 0% [I] 0%	0,00274	60%
		[C] 60% [A] 0% [T] 0%	$ 328,80	
[E.20]	Vulnerabilidades de los programas (software)			
[E.21]	Errores de mantenimiento/actualización de programas (software)			
[E.23]	Errores de mantenimiento/actualización de equipos (hardware)			
[E.24]	Caída del sistema por agotamiento de recursos			
[E.25]	Pérdida de equipos			
[E.28]	Indisponibilidad del personal			
[A] Ataques intencionados				
[A.3]	Manipulación de registros de actividad (log)			
[A.4]	Manipulación de la configuración			
[A.5]	Suplantación de la identidad del usuario	[D] 0% [I] 70%	0,00274	90%

		[C] 40%	$ 493,20	
		[A] 90%		
		[T] 0%		
[A.6]	Abuso de privilegios de acceso	[D] 30%	0,005479	60%
		[I] 60%		
		[C] 20%	$ 657,48	
		[A] 0%		
		[T] 0%		
[A.7]	Uso no previsto			
[A.8]	Difusión de software dañino			
[A.9]	Re-encaminamiento de mensajes			
[A.10]	Alteración de secuencia			
[A.11]	Acceso no autorizado	[D] 0%	0,00274	80%
		[I] 65%		
		[C] 80%	$ 438,40	
		[A] 0%		
		[T] 0%		
[A.12]	Análisis de tráfico			
[A.13]	Repudio			
[A.14]	Interceptación de información (escucha)			
[A.15]	Modificación deliberada de la información	[D] 0%	0,00274	90%
		[I] 90%		
		[C] 0%	$ 493,20	
		[A] 0%		
		[T] 0%		
[A.18]	Destrucción de información	[D] 60%	0,00274	60%
		[I] 0%		
		[C] 0%	$ 328,80	
		[A] 0%		
		[T] 0%		
[A.19]	Divulgación de información	[D] 0%	0,00274	40%
		[I] 0%		
		[C] 40%	$ 219,20	
		[A] 0%		
		[T] 0%		
[A.22]	Manipulación de programas			
[A.23]	Manipulación de los equipos			
[A.24]	Denegación de servicio			
[A.25]	Robo			
[A.26]	Ataque destructivo			
[A.27]	Ocupación enemiga			
[A.28]	Indisponibilidad del personal			
[A.29]	Extorsión			
[A.30]	Ingeniería social			
			$ 5.424,72	

Tabla 8 Análisis de amenazas

El análisis de riesgo residual, se realiza teniendo en consideración lo(s) controle(s) de seguridad que la IES ha implementado hasta el momento, obteniendo el riesgo real. En el Anexo 10 se puede apreciar el riesgo residual que fue calculado en base al activo y amenaza, mediante el siguiente cálculo:

$$(Impacto * Probabilidad)$$

Hay que considerar que los riesgos casi en su totalidad no son eliminables, es decir, no se puede eliminar al 100% la amenaza hacia el activo de la IES, pero lo que se puede realizar es gestionar correctamente las acciones a seguir para la amenaza.

3.5 Impacto Potencial y Nivel de Riesgo Aceptable

Luego de conocer los activos que forman parte de los procesos propios de la IES y haberles asignado su respectivo valor económico, se debe determinar el impacto potencial que generará la materialización de las amenazas. Este dato es muy importante, ya que con esta información la IES podrá decidir que activos brindarles mayor protección y ante que amenazas, teniendo un medio de verificación de las medidas implementadas.

3.5.1 Nivel de Riesgo Aceptable

Una vez identificadas las amenazas por activo y estimado el impacto que provocaría su materialización, se ha fijado el nivel de riesgo aceptable, a partir del cual se deberá asumir las medidas necesarias para reducir el nivel de riesgo. Cabe mencionar que se tendrá presente que el costo del control no deberá superar el costo del activo a proteger.

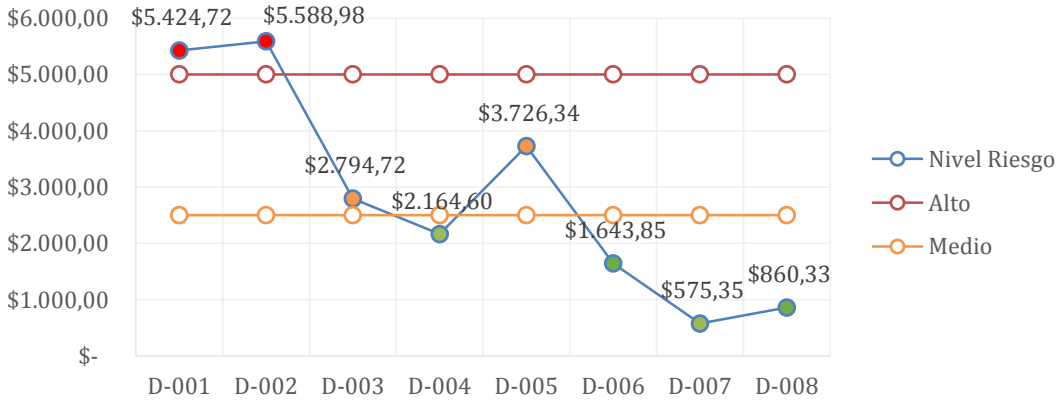


Ilustración 15 [D] Datos/Información

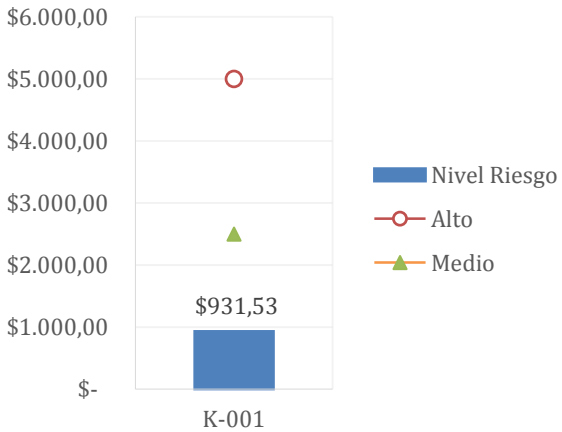


Ilustración 16 [K] Claves Criptográficas

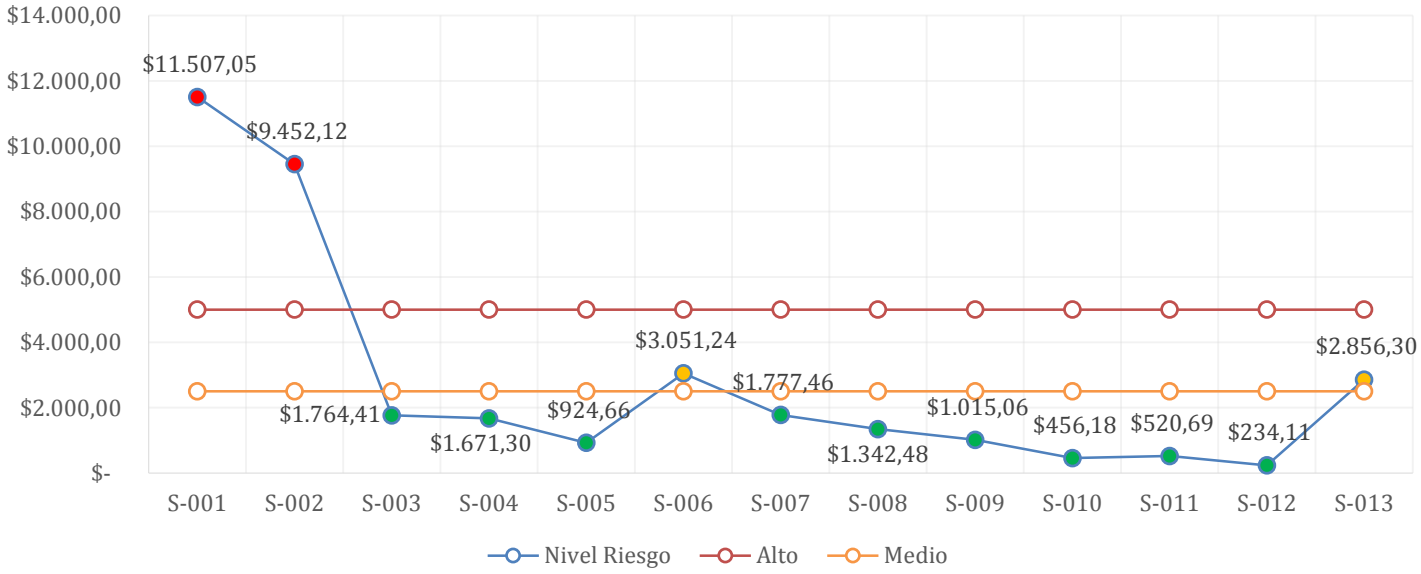


Ilustración 17 [S] Servicio

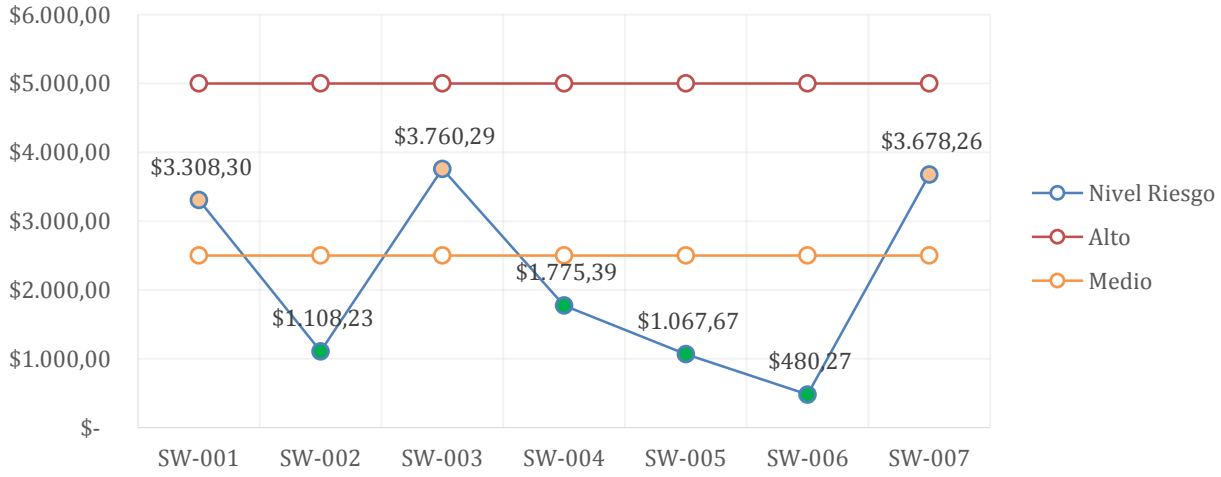


Ilustración 18 [SW] Software

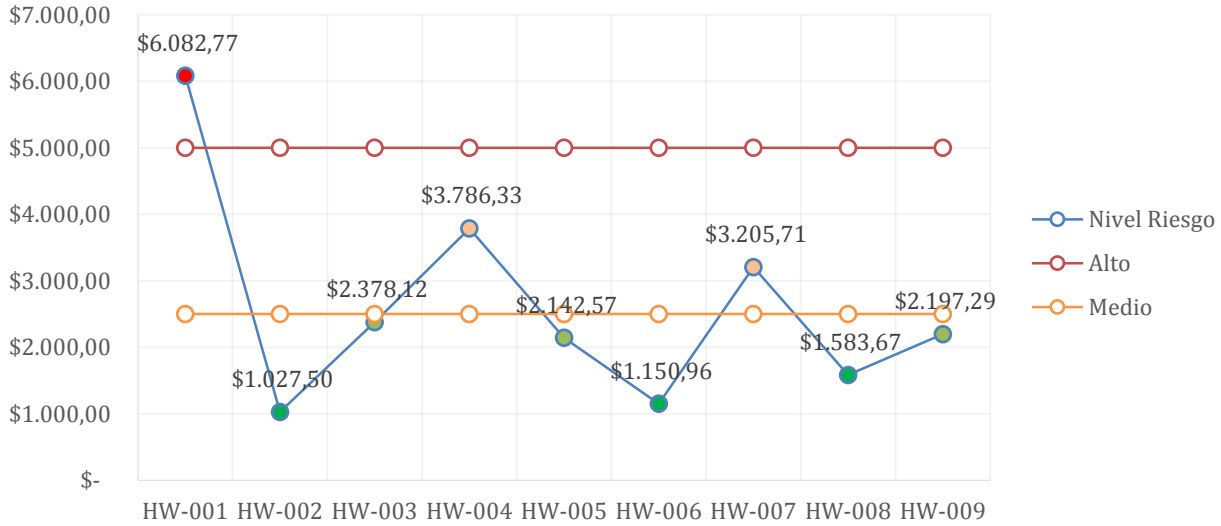


Ilustración 19 [HW] Hardware

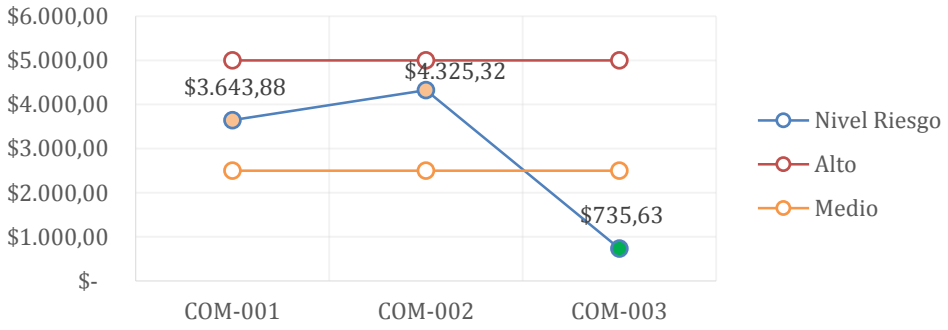


Ilustración 20 [COM] Redes de Comunicaciones

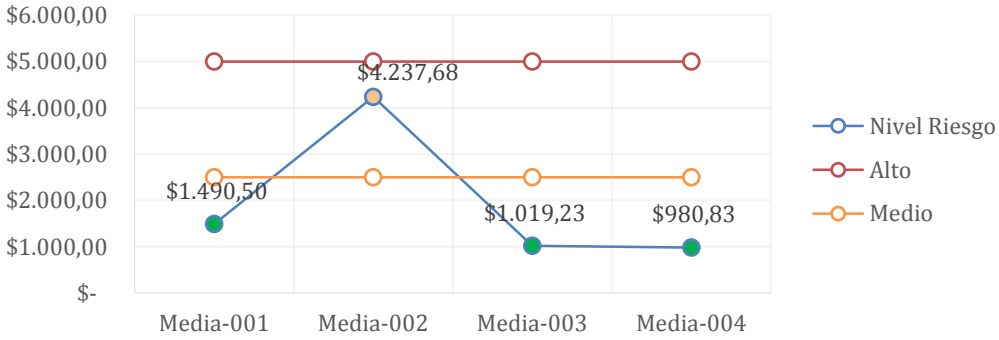


Ilustración 21 [Media] Soportes de Información

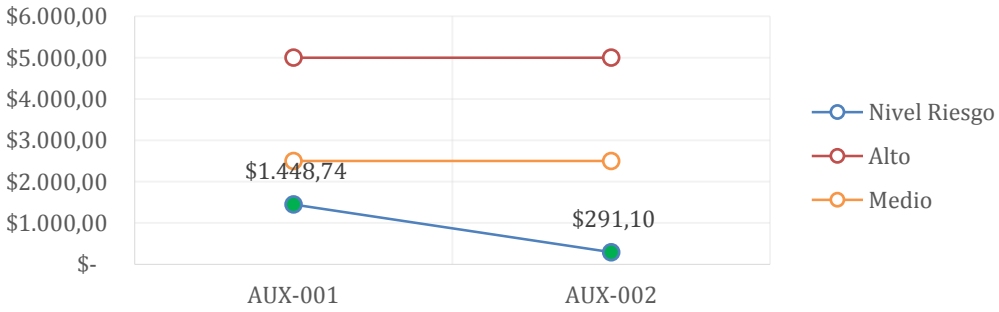


Ilustración 22 [AUX] Equipamiento Auxiliar

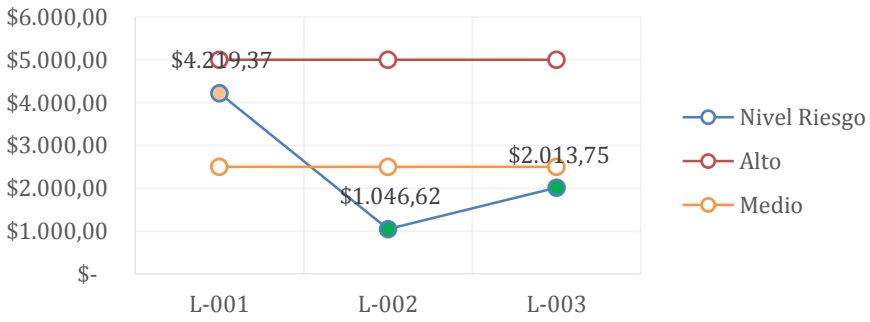


Ilustración 23 [L] Instalaciones

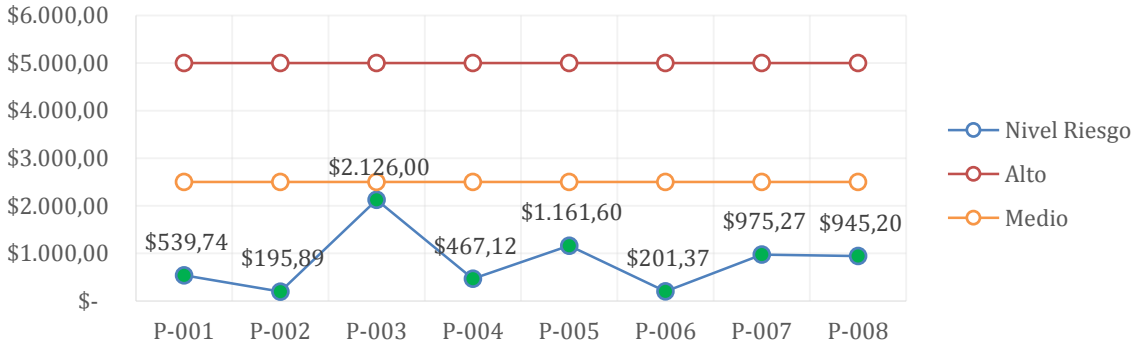


Ilustración 24 [P] Personal

3.5.2 Aprobación por parte de la Dirección.

El nivel de riesgo aceptable tiene que estar aprobado por el Consejo Superior de la IES, y se tienen que definir los criterios para establecer dicho nivel.

CONSEJO SUPERIOR DE LA IES

AÑO XX

RESOLUCIONES – ACTA N°7

24 DE ABRIL DE 2015

El Consejo Superior de la IES, en sesión ordinaria celebrada el 24 de abril de 2015, resolvió:

1. **LECTURA Y APROBACIÓN DE RESOLUCIONES DEL ACTA DE LA SESIÓN ANTERIOR DE FECHA 17 DE ABRIL DE 2015**

   RESOLUCIÓN N° 113-04-2015-04-14: Aprobar las resoluciones del Acta de sesión ordinaria del Consejo Superior celebrada el 17 de abril de 2015.

2. **SEGUIMIENTO DE LAS RESOLUCIOENS DEL ACTA ANTERIOR.**

3. **TEMAS PLANTEADOS POR EL COMITÉ DE SEGURIDAD**

   RESOLUCIÓN N° 114-04-2015-04-14: El Consejo Superior, previo informe del Comité de Seguridad, resuelve: Aprobar el Nivel de Riesgo Residual correspondiente al año 2015 de acuerdo a lo siguiente:

   Luego de realizar el Análisis de Riesgos se ha definido el umbral de riesgo asumible considerando los siguientes aspectos:

   - **Coste de implantación de las salvaguardias frente al coste de asumir el riesgo.**
   - **Priorización de activos.**
   - **Tipos de amenazas.**

   En la Tabla 1 se observa el nivel de riesgo y el número de activos de la IES que son afectados.

Nivel	Rango	N° Activos
Alto	valor > 5000 $	5
Medio	2500 $ < valor > 5000 $	13
Bajo	0 $ < valor > 2500 $	40

Tabla 1 Valoración Riesgo Aceptable

e-mail: rector@ies.edu.ec – www.ies.edue.c – **Cuenca-Ecuador**

4 Fase 4: Propuestas de Proyectos

4.1 Introducción

Luego de la planificar se deberá implementar el Plan de gestión de riesgos o Plan de seguridad, es decir implementar los controles adecuados, con los responsables, el presupuesto aprobado, entre otros, con el fin de evitar los daños intrínsecos al factor de riesgo.

Este plan de tratamiento deberá garantizar un funcionamiento efectivo y eficiente de la IES en materia de seguridad de la información, controles internos efectivo y un adecuado lineamiento con las leyes y reglamentos vigentes tanto a nivel dela IES como del país.

Ante la importancia de la efectividad del Plan de gestión de riesgos, la IES debe adoptar determinadas medidas y controles encaminados en modificar, reducir e incluso eliminar el riesgo. En todos los casos, existe un costo asociado que la IES deberá asumir, sin embargo en caso de no tomar ninguna medida contra el riesgo, la IES deberá estar consciente de la presencia del riesgo y las pérdida que ocasionaría en caso de efectivizarse.

La decisión de tomar o no una medida de control, no es algo que se deba tomar a la ligera, ya que corresponde a un análisis donde se compara el costo de su implementación, con el costo de las posibles pérdidas que derivarían de la no adopción de los controles. Sólo ahí podríamos determinar si debemos o no actual ante el riesgo.

Este plan debe ser presentado a la alta Dirección para su aprobación y el apoyo económico, luego comenzarán a ejecutarse los proyectos.

4.2 Propuestas

Como se ha explicado en el apartado anterior, el primer paso corresponde a determinar los riesgos a los que se expone la IES y en base al nivel de riesgo aceptable que el Consejo Superior decidió asumir se determinarán los riesgos que se van a tratar. En la
Tabla **9** se presentan los riegos con su definición en base al Libro 2 “Catálogo de Elementos” de la metodología MAGERIT.

En base a los riesgos se han determinado como proyectos los siguientes:

1. **Elaboración y divulgación de las políticas de Seguridad de la Información:** Al momento existe un documento donde se encuentran plasmadas siete políticas en materia de seguridad de la información, sin embargo se ve la necesidad de completarlo, ya que muchas áreas y/o departamentos no presentan una política definida a nivel de la IES y en otros casos, a pesar de existir no se ha difundido de la manera adecuada, provocando el desconocimiento por parte del personal y por ende la presentación de riesgos como es el uso no previsto, abuso de privilegios de acceso, suplantación de la identidad del usuario, entre otros.

2. **Plan de concienciación (capacitación y formación del personal):** Se ha evidenciado un alto grado de problemas y riesgos que se han originado por la falta de conocimiento y/o concienciación que posee el personal académico y/o administrativo de la IES. Esto ha desembocado en que la institución se encuentre en un momento de tensión, ante tal premisa se considera como uno de los proyectos ejes y fundamentales.

3. **Plan de virtualización de servidores:** Uno de los riesgos que se ha presentado aunque en menor frecuencia pero con mayor impacto es la caída del sistema por agotamiento de recursos y la denegación de servicios, esto responde a que la IES ha crecido de una manera considerable en estos últimos años; teniendo un crecimiento del 5% a nivel del personal y del 15% a nivel

estudiantil, a quienes hay que dar respuesta en los diferentes sistemas y funcionalidades que provee la IES y de las nuevas que se desea implementar por la nueva legislación. Ante tal premisa he considerado como un proyecto la virtualización de los servidores.

4. **Plan de continuidad:** Uno de los proyectos que nunca pueden faltar en una institución es el Plan de continuidad. Toda institución debe estar consciente que a pesar de haber implementado todos los controles en base a la ISO 27000, siempre pueden presentarse situaciones que no se podrán evitar. Para hacer frente ante estas situaciones, es necesario crear planes de continuidad del negocio, que tienen como objetivo evitar que los procesos propios de la IES queden interrumpidos por un largo intervalo de tiempo. Por poner un caso, en períodos de matrículas el sistema no puede dejar de brindar sus servicios, ya que de ello depende todo un calendario de actividades y procesos que se generan del mismo.

Cabe mencionar, que para los proyectos se ha estimado el tiempo por tarea en días laborables, ya que dependiendo de la fecha de inicio del proyecto, podrían presentarse feriados, días no laborables y otras tareas, además en el presupuesto se ha establecido el número de horas que se dedicará a la tarea por el número de responsables. Estos valores tendrán un margen de error del 5% debido a consideraciones que pueden cambiar, como es el número de integrantes en una Comisión.

A continuación se relaciona cada proyecto con el riesgo que está mitigando o controlando.

Código	Denominación	Descripción	Proyecto 1	Proyecto 2	Proyecto 3
[E] Errores y fallos no intencionados					
[E.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	x	x	
[E.15]	Alteración accidental de la información	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	x	x	
[E.21]	Errores de mantenimiento/actualización de programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	x		
[E.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.			x
[A] Ataques intencionados					
[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	x	x	
[A.6]	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	x	x	

[A.7]	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	x	x	
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.		x	
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.			x
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.		x	
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	x	x	
[A.19]	Divulgación de información	Revelación de información.		x	
[A.23]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	x		
[A.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.			x

Tabla 9 Asignación de los Proyectos a Riesgos

En el Anexo 10 se encuentra el Plan de gestión de riesgos con más detalle.

4.2.1 Elaboración y divulgación de las políticas de Seguridad de la Información

En base al análisis realizado sobre los riesgos y sus activos, y el documento Anexo 01, se ha determinado que uno de los riesgos a los que se enfrenta la IES es el mínimo establecimiento de Políticas de Seguridad de la Información. Todas las políticas, normas, estatutos, entre otros; en materia de seguridad de la información han sido desarrollados por iniciativa del área y/o departamento quien lo implementa, sin embargo, no han sido divulgados por medio de un plan controlado ni un equipo de trabajo designado por la IES.

Para ello, el Comité de Seguridad de la Información ha elaborado un proyecto de elaboración y divulgación de las políticas de seguridad en base al Anexo 03, cubriendo el siguiente aspecto:

- Formación básica en las políticas de seguridad de la información de la IES.

Este proyecto tiene como objetivos:

- Cumplir con el control 5.1.1 Políticas de seguridad de información del dominio 5, ya que en el Análisis Diferencial se le asignó el estado Incompleto, es decir, el proceso no alcanzaba el propósito definido, además que existe muy poca evidencia de haberse presentado un logro sistemático del propósito del proceso.

- Conseguir el nivel de Gestionado en los controles que se encuentren en un nivel inferior al indicado, en el dominio 7 Seguridad de los Recursos Humanos, dominio 8 Gestión de Activos y dominio 11 Seguridad física y ambiental en el objetivo 11.2 Seguridad de los equipos.

Dentro de las actividades de planificación tenemos las siguientes:

1. Análisis y definición de las políticas de seguridad.

   En el Anexo 03 se encuentran definidas siete políticas de seguridad de la información, como se observa en la Tabla 10**,** de allí se determinaron las políticas a desarrollar que brindarán protección de los activos de la información en base a la presentación de los riesgos que se encuentran en la Tabla 9.

   El Responsable de Seguridad de la Información será quien deberá analizar cada una de las políticas definidas y determinar las faltantes en base a los riesgos y sus activos, además de determinar cuales deberán ser actualizadas. Se estima que la tarea tendrá una duración de 10 días laborables.

Políticas definidas	Políticas a desarrollar
Política de Alto Nivel	Política de Manejo de Activos
Política de Control de Acceso	Política de Divulgación de Información
Política de puesto de trabajo despejado y bloque de pantalla	Política de Gestión de Pruebas en el Desarrollo Seguro
Política de Desarrollo Seguro	
Política de Clasificación de la Información	
Política de Uso de Correo Electrónico	
Política de Gestión de Incidentes	

Tabla 10 Políticas definidas y a desarrollar

2. Creación de las políticas de seguridad.

   Las políticas serán desarrolladas por el Responsable de Seguridad de la Información, en coordinación con los Directores de las áreas y/o departamentos, y el procurador de la IES y el Responsable funcional de la información en caso de considerarse necesaria su participación. Se estima que la tarea tendrá una duración de 20 días laborables.

   Estas políticas abarcarán a todo activo de información en cualquier momento de su ciclo de vida (creación o captura, mantenimiento, distribución y uso, almacenamiento, archivo y destrucción) y en todas sus formas (oral, escrita, impresa, electrónica, óptica, electromagnética, entre otros).

   Las políticas aplican a todo el personal de la IES, ya sea administrativo y/o docente, a los estudiantes, y a las partes externas que presten sus servicios a la IES.

3. Reunión de aprobación con el Consejo Superior.

   Luego de que las políticas hayan sido elaboradas, el Comité de Seguridad de la Información deberá elevarlas hacia el Consejo Superior de la IES para su aprobación. Se estima que la tarea tenga una duración de 1 día laborable.

4. Difusión de las políticas de seguridad de la información.

   Si las políticas ya han sido aprobadas, el siguiente paso es difundirlas inmediatamente a todo el personal de la IES en los siguientes grupos:

   - Difusión al personal administrativo.
   - Difusión a la comunidad académica de la IES.
   - Difusión a estudiantes.

Se estima que la tarea tenga una duración de 25 días laborables.

El Responsable de la Seguridad de la Información será el coordinador y responsable de difundir las políticas conjuntamente con el Director del Departamento de Comunicación.

Se estima que el proyecto completo tenga una duración de 56 días laborables. La difusión se realizará a todo el personal de la IES dentro del horario laboral, ya que su asistencia será considerado de caracter obligatorio, caso contrario tendrán la debida amonestación.

El presupuesto destinado se presenta en la siguiente tabla:

FASE	Cantidad	Descripción	Costo por unidad	Costo Total
Análisis y definición de las políticas de seguridad	8 horas x 10 días x 1 persona	Análisis de las políticas existentes	$ 15,00	$ 1200,00
Creación de las políticas de seguridad	4 horas x 20 días x 2 personas	Crear las políticas Incluye al procurador	$ 15,00	$ 2400,00
	2 horas x 7 días x 1 personas	Modificar las políticas	$ 15,00	$ 210,00
Reunión para aprobación	4 horas x 1 día x 6 personas	1ra Reunión del Consejo Superior	$ 15,00	$ 360,00
Difusión de las políticas de seguridad	5 horas x 10 días x 2 personas	Creación del modelo de difusión	$ 15,00	$ 1500,00
	4 horas x 15 días x 3 personas	Difusión a personal académico y administrativo, y estudiantes	$ 8,00	$1440,00
	1	Material de difusión	$ 1500,00	$ 1500,00
Extras	2 remesas	Hojas	$ 10,00	$ 20,00
	1	Extras (impresiones, esferos)	$ 30,00	$ 30,00
				$ 8660,00

Tabla 11 Presupuesto Proyecto 1

El precio total del proyecto 1 es de $ 8660,00. Se debe considerar que el costo de horas, se encuentra dentro del sueldo del empleado, ya que las tareas serán desarrolladas por personal de la IES y no se ha contratado a nadie para ninguna actividad.

4.2.2 Plan de Concienciación (capacitación y formación del personal)

Uno de los riegos que afecta al mayor número de activos y genera a su vez un incremento en el número de riesgos es el poco o nulo nivel de concienciación del personal de la IES en materia de seguridad de la información, siendo un fenómeno que se ha evidenciado en la comunidad universitaria.

El Comité de Seguridad de la Información ha elaborado en colaboración con el Departamento de Salud Ocupacional un proyecto de concienciación en base al Anexo 03 cubriendo los siguientes aspectos:

- Capacitación de las políticas de seguridad de la información de la IES.
- Capacitación en la legislación tanto de la IES como el Reglamento de Régimen Académico del CES y la Ley Orgánica de Educación Superior del Ecuador.

Este proyecto tiene como objetivo:

- Conseguir el nivel de Gestionado en los controles que presenten un nivel inferior a este, en el dominio 7 Seguridad de los Recursos Humanos.

Dentro de las actividades de planificación tenemos las siguientes:

1. Detección de necesidades.

El Responsable de Seguridad de la Información será quien determine los tipos de capacitaciones y a quienes van dirigidos, además de clasificarlas y/o presentar una jerarquización de las necesidades de capacitación en base a un cronograma de actividades.

Cabe señalar que esta fase será el punto eje y principal para el desarrollo de las siguientes, ya que un análisis incompleto provocará que no todos los riesgos sean tratados.

En la Tabla 12 se muestra un listado de las capacitaciones que fueron identificadas en base a los riesgos presentados por la IES en su Anexo 10 y 11.

Capacitaciones	Personal	
	Administrativo	Académico
Capacitación de las políticas de seguridad de la información de la IES	x	x
Capacitación del Departamento Financiero	x	
Capacitación del Departamento RRHH	x	
Capacitación a nivel de legislación Académica	x	x
Capacitación en materia de Ingeniería social	x	x
Capacitación en el manejo de activos	x	X

Tabla 12 Capitaciones

En el proyecto se ha determinado que las capacitaciones se integren en grupos:

- Personal interno de la IES que colaborará impartiendo las capacitaciones de las políticas de seguridad, legislación Académica, manejo de activos, del Departamento Financiero y de RRHH.
- Empresa consultora que se encargará de las capacitaciones de ingeniería social.

El responsable tendrá como tarea en esta fase la de elaborar el cronograma de actividades y seleccionar un grupo de Empresas capacitadoras quienes deberán presentar sus proyectos.

Se estima que la tarea tenga una duración de 5 días laborables.

2. Reunión de aprobación con el Consejo Superior.

   El responsable de las capacitaciones será el Comité de Seguridad de la Información en colaboración con el Departamento de Salud Ocupacional, siendo el primero quien deba elevar el proyecto al Consejo Superior para su aprobación.

   En el Consejo Superior analizará el cronograma para las capacitaciones desarrolladas por parte del personal interno de la IES, y la selección de la Empresa capacitadora.

   Se estima que la tarea tenga una duración de 1 día laborable, ya que el Consejo Superior podrá solicitar información adicional y/o aclaraciones en caso de considerarlo pertinente.

3. Ejecución.

   Luego de la aprobación del proyecto de concienciación, se deberá ejecutar en base al cronograma de actividades presentado por cada uno de los responsables. En el caso del personal interno se ha seleccionado un equipo de trabajo, quien brindará las capacitaciones y quienes fueron instruidos con anterioridad. Se estima que la tarea tenga una duración de 20 días laborables.

   El tiempo de instrucción que menciono no es considerado como una capacitación, ya que el equipo de trabajo posee los conocimientos y experticia suficiente, mas bien la instrucción fue un mecanismo de coordinación necesario.

4. Evaluación.

Posterior a la ejecución de las capacitaciones, el Responsable de Seguridad de la Información deberá realizar una evaluación que permitirá valorar la eficacia de las capacitaciones en el desarrollo de sus actividades diarias.

Esta actividad no será desarrollada por el personal encargado de la capacitación, ya que se trata de garantizar la transparencia. Recordemos, que lo importante de esta evaluación es determinar los conocimientos del personal ante los procesos que generan mayor número de riesgos.

Esta evaluación será usada como herramienta de estudio en futuras capacitaciones. Se estima que la tarea tenga una duración de 10 días laborables.

Se estima que el proyecto completo tenga una duración de 36 días laborables. Las capacitaciones se realizarán dentro del horario laboral y su participación será de carácter obligatorio, caso contrario tendrán su debida amonestación. Sólo en casos considerados como excepcionales, el personal podrá asistir fuera de su horario de trabajo, como es el caso del personal que tienen turnos durante la noche o en su caso sus actividades no le permitan presentarse a las capacitaciones.

El presupuesto destinado se presenta en la siguiente tabla:

FASE	Cantidad	Descripción	Costo por unidad	Costo Total
Detección de necesidades	3 horas x 5 días x 1 persona	Detectar capacitaciones y a quienes va dirigido.	$ 15,00	$ 225,00
Reunión para aprobación	5 horas x 1 días x 6 personas	1ra Reunión del Consejo Superior	$ 15,00	$ 450,00
Ejecución	1	Empresa capacitadora	$ 6000,00	$ 6000,00
	3 horas x 10 días x 4 personas	Capacitaciones por personal interno	$ 15,00	$1800,00
	1	Material de capacitación	$ 1000,00	$ 1500,00
	1	Refrigerios	$ 800,00	$ 800,00
Evaluación	3 horas x 10 días x 3 personas	Evaluación de los resultados	$ 10,00	$ 900,00
				$ 11675,00

Tabla 13 Presupuesto Proyecto 2

El precio total del proyecto 2 es de $ 11675,00. Se debe considerar que en este proyecto se ha contratado una Empresa capacitadora.

4.2.3 Plan de Virtualización de Servidores

La virtualización se refiere a la abstracción de los recursos que posee el equipo, es decir, es la creación de una versión virtual de un recurso del computador, como puede ser el sistema operativo, una plataforma de hardware, entre otros, todo dependerá cual sea nuestro objetivo.

En base al Anexo 10 y 11, hemos podido evidenciar que una de las amenazas a las que se encuentra sujeta la IES es la caída del sistema por agotamiento de recursos y denegación de servicio. Esto se debe a que la institución ha ido creciendo considerablemente tanto a nivel del personal con un 5% y a nivel estudiantil del 15%. Además, el Ecuador está atravesando un período de cambio en el ámbito educativo que obliga a toda institución académica a cambiar sus sistemas informáticos para dar respuesta a las mejoras implementadas.

El Comité de Seguridad de la Información ha elaborado un proyecto de virtualización de servidores en base al Anexo 10 y 11 cubriendo los siguientes aspectos:

- Servidor de Datos.
- Servidor de Página Web.

El proyecto tiene como objetivos:

- Simplificar la gestión de las copias de seguridad y la recuperación ante incidentes.
- Reducir el tiempo de inactividad por actualizaciones y/o mantenimiento.
- Crear un entorno de prueba de forma rápida y fácil que permita validar parches y actualizaciones antes de implementar en el servidor de producción.
- Conseguir el nivel de Gestionado en los controles que presenten un nivel inferior a este, en el dominio 7 Seguridad de los Recursos Humanos.

Dentro de las actividades de planificación tenemos las siguientes:

1. Planificación.

   El Responsable de Seguridad en colaboración con el Coordinador de Administración de Redes e Infraestructura deberá planificar la infraestructura virtual. Como datos de entrada se debe analizar el inventario de la infraestructura física y las aplicaciones, teniendo como puntos claves para su análisis los siguientes:

   - Indicar si se va a adquirir hosts de virtualización o se van a usar equipos existentes.
   - Determinar si es necesario realizar cambios a nivel de red para garantizar la conectividad.
   - Indicar si la virtualización afectará a las copias de seguridad y recuperación ante la presencia de incidentes, y en caso de ser afirmativo especificar cuál será el cambio a realizar.
   - Determinar la reconfiguración en caso de ser necesario.

   Se estima que la tarea tenga una duración de 7 días laborables.

2. Reunión de aprobación con el Consejo Superior.

   El Comité de Seguridad de la Información será el responsable de elevar el proyecto al Consejo Superior para su aprobación, el mismo que analizará la pertinencia del proyecto en relación costo y la capacidad de gestión y migración, de allí se determinará la fecha de implementación y la designación del responsable del proyecto. Se estima que la tarea tenga la duración de 1 día laborable.

3. Implantación.

   Luego de la aprobación del proyecto se deberá implementar en base a lo especificado en el documento presentado ante el Consejo Superior. Los responsables de esta actividad serán el Coordinador de Administración de Redes e Infraestructura y el Responsable de Seguridad. Dentro de esta actividad se encuentran las pruebas que se deberán desarrollar para dar por implementado el plan de virtualización. Se estima que tenga una duración de 40 días laborables, esto se debe a que se debe adquirir el equipo, sistemas y herramientas que se hayan incluido en el costo del proyecto.

Aproximadamente el proyecto completo tendrá una duración de 48 días laborables. No se ha incluido dentro del proyecto la fase de mejora y/o mantenimiento, ya que esto dependerá de la planificación realizada en la primera actividad.

El presupuesto destinado se presenta en la siguiente tabla:

FASE	Cantidad	Descripción	Costo por unidad	Costo Total
Planificación	5 horas x 7 días x 2 personas	Determinar los planes.	$ 15,00	$ 1050,00
Reunión para aprobación	2 horas x 1 día x 6 personas	Reunión del Consejo Superior	$ 15,00	$ 180,00
Implantación	8 horas x 20 días x 2 personas	Implantar el proyecto	$ 15,00	$ 4800,00

	1	Adquisición de equipos, sistemas, entre otros	$ 3500,00	$ 3500,00
				$ 9530,00

Tabla 14 Presupuesto Proyecto 3

El precio total del proyecto 3 es de $ 9530,00. Se debe considerar que en este proyecto únicamente los costos de equipos y/o sistemas corresponden a valores que la IES deberá facilitar, los demás corresponden a horas de trabajo del personal interno de la institución.

4.2.4 Plan de Continuidad del Negocio

El Plan de Continuidad del Negocio es un proyecto que no puede faltar en ninguna IES, ya que tiene como objetivo que la institución esté preparada ante situaciones que no suelen ocurrir. Se ha evidenciado que estas situaciones suelen darse y sus resultados son catastróficos llegando hasta incluso al cierre de las empresas, por lo tanto, este plan pretende evitar la interrupción de los procesos considerados principales por la IES. Los planes de continuidad de negocio son definidos para cuando falle el sistema y no por si falla.

El Comité de Seguridad de la Información ha elaborado un proyecto de continuidad del negocio en base al Anexo 01, 03 y 10 presentando las siguientes características:

- El plan se encontrará en un proceso de mejora continua.
- Su orientación será hacia la recuperación de los procesos considerados como críticos por la IES.
- Su diseñado deberá responder hacia la integración con el resto de elementos de la seguridad.
- Automatizar un conjunto de tareas evitándola planificación en el momento de crisis.

Este proyecto tiene como objetivos:

- Brindar una respuesta de forma rápida y ágil a las situaciones que los controles implementados no han podido controlar.
- Conseguir el nivel de Gestionado en los controles que se encuentren en un nivel inferior al mencionado, en el dominio 17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

Dentro de las actividades de planificación tenemos las siguientes:

1. Planificación del PCN.

   En esta actividad el Comité de Seguridad de la Información determinará por cada área y/o departamento de Tecnologías de la Información la estructura del plan de continuidad de negocio, y el responsable por cada uno de los planes como se presenta en la Tabla 15, se ha obviado el Área de Explotación para una segunda fase. Se estima que tenga una duración de 2 días laborables.

Descripción	Responsable
Plan de continuidad de Desarrollo de Sistemas de Información	Coordinador de Desarrollo de Sistemas de Información
Plan de continuidad de Redes e Infraestructura	Coordinador de Administración de Redes e Infraestructura

Tabla 15 Planes de Continuidad

   Cabe señalar que cada plan de continuidad de negocio será diferente, es decir, deberá ser totalmente personalizado por cada área y/o departamento teniendo siempre como objetivo conseguir que la interrupción de los procesos de la IES sean en el menor tiempo y con un costo mínimo.

2. Desarrollo del PCN.

Cada responsable por área y/o departamento deberá definir las acciones necesarias para proceder a la recuperación ante un desastre, indicando a detalle las acciones para recuperar la normalidad de los procesos. Esta tarea se estima que tenga una duración de 7 días laborables.

3. Reunión de aprobación con el Consejo Superior.

   El Comité de Seguridad de la Información deberá elevar el proyecto al Consejo Superior para su aprobación, en donde se analizarán los planes y determinará su aprobación y responsables en caso de considerarlo conveniente. Se estima que la tarea tenga una duración de 1 día laborable.

4. Implantación del PCN.

   Posterior se deberá dar inicio a la implantación en las fechas indicadas en el cronograma del proyecto. Entre las actividades a desarrollar se presenta la compra de equipos, designar ubicaciones, personal y el resto de herramientas necesarias para ejecutar los planes.

   Esta tarea tiene como encargado al Responsable de Seguridad de la Información, quien deberá coordinador con cada uno de los representantes de los planes sobre el desarrollo de los mismos. Se estima que la tarea tenga una duración de 30 días laborables como máximo. Cabe mencionar que cada plan tendrá su propio cronograma de actividades.

5. Evaluación y mantenimiento del PCN.

   Esta actividad trata sobre la actualización de los planes en base a las evidencias y registros que fueron generadas por las pruebas.

   El Responsable de Seguridad de la Información será el encargado de analizar las pruebas y determinar la propuesta de cambio, que será presentado ante el Comité de Seguridad de la Información. Se estima que la tarea tenga una duración de 7 días laborables.

Se estima que el proyecto completo tenga una duración de 51 días laborables. Las entrevistas se desarrollarán dentro del horario laboral de los empleados, tratando de evitar al máximo interrumpir sus actividades.

El presupuesto destinado se presenta en la siguiente tabla:

FASE	Cantidad	Descripción	Costo por unidad	Costo Total
Planificación	6 horas x 2 días x 4 persona	Determinar los planes.	$ 15,00	$ 720,00
Desarrollo	6 horas x 7 días x 2 personas	Recopilar información, determinar procesos críticos y estrategias	$ 15,00	$ 1260,00
Reunión para aprobación	2 horas x 1 día x 6 personas	Reunión del Consejo Superior	$ 15,00	$180,00
Implantación	8 horas x 30 días x 2 personas	Implantar los planes	$ 15,00	$7200,00
	1	Adquisición de equipos, sistemas, entre otros	$ 3000,00	$ 3000,00
Evaluación y mantenimiento	4 horas * 17 días x 1 personas	Evaluación de los resultados	$ 15,00	$ 1020,00
				$ 13380,00

Tabla 16 Presupuesto Proyecto 4

El precio total del proyecto 4 es de $ 13380,00. El costo de horas, se encuentra dentro del sueldo del empleado, ya que las tareas serán desarrolladas por personal de la IES y no se ha contratado personal externo.

4.3 Resumen de la Planificación de Proyectos

En la Ilustración 25 e Ilustración 26 se aprecian cada uno de los proyectos identificados en el apartado anterior, con sus respectivas actividades, responsables y tiempo aproximado.

ESCA

mié 16/09/15 — mar 29/09/15

25 may '15 | 15 jun '15 | 06 jul '15 | 27 jul '15 | 17 ago '15 | 07 sep '15 | 28 sep '15 | 19 oct '15

DIAGRAMA DE GANTT

	Nombre de tarea	Duración	Comienzo	Fin
1	**Propuestas de Proyectos**	**187 días**	**lun 18/05/15**	**mar 02/02/16**
2	**Elaboración y divulgación de las políticas de Seguridad de la Información**	**56 días**	**lun 18/05/15**	**lun 03/08/15**
3	Análisis y definición de las políticas de seguridad	10 días	lun 18/05/15	vie 29/05/15
4	Creación de las políticas de seguridad	20 días	lun 01/06/15	vie 26/06/15
5	Reunión de aprobación con el Consejo Superior	1 día	lun 29/06/15	lun 29/06/15
6	Difusión de las políticas de seguridad de la información	25 días	mar 30/06/15	lun 03/08/15
7	Fin del primer proyecto	0 días	lun 03/08/15	lun 03/08/15
8	**Plan de concienciación**	**36 días**	**mar 04/08/15**	**mar 22/09/15**
9	Detección de necesidades	5 días	mar 04/08/15	lun 10/08/15
10	Reunión de aprobación con el Consejo Superior	1 día	mar 11/08/15	mar 11/08/15
11	Ejecución	20 días	mié 12/08/15	mar 08/09/15
12	Evaluación	10 días	mié 09/09/15	mar 22/09/15
13	Fin del segundo proyecto	0 días	mar 22/09/15	mar 22/09/15
14	**Plan de virtualización de servidores**	**48 días**	**mié 23/09/15**	**vie 27/11/15**
15	Planificación	7 días	mié 23/09/15	jue 01/10/15
16	Reunión de aprobación con el Consejo Superior	1 día	vie 02/10/15	vie 02/10/15
17	Implantación	40 días	lun 05/10/15	vie 27/11/15
18	Fin del tercer proyecto	0 días	vie 27/11/15	vie 27/11/15
19	**Plan de continuidad**	**47 días**	**lun 30/11/15**	**mar 02/02/16**
20	Planificación del PCN	2 días	lun 30/11/15	mar 01/12/15
21	Desarrollo del PCN	7 días	mié 02/12/15	jue 10/12/15
22	Reunión de aprobación con el Consejo Superior	1 día	vie 11/12/15	vie 11/12/15
23	Implantación del PCN	30 días	lun 14/12/15	vie 22/01/16
24	Evaluación y mantenimiento del PCN	7 días	lun 25/01/16	mar 02/02/16
25	Fin del cuarto proyecto	0 días	mar 02/02/16	mar 02/02/16

Ilustración 25 Actividades_Fases de la Propuesta de Proyectos

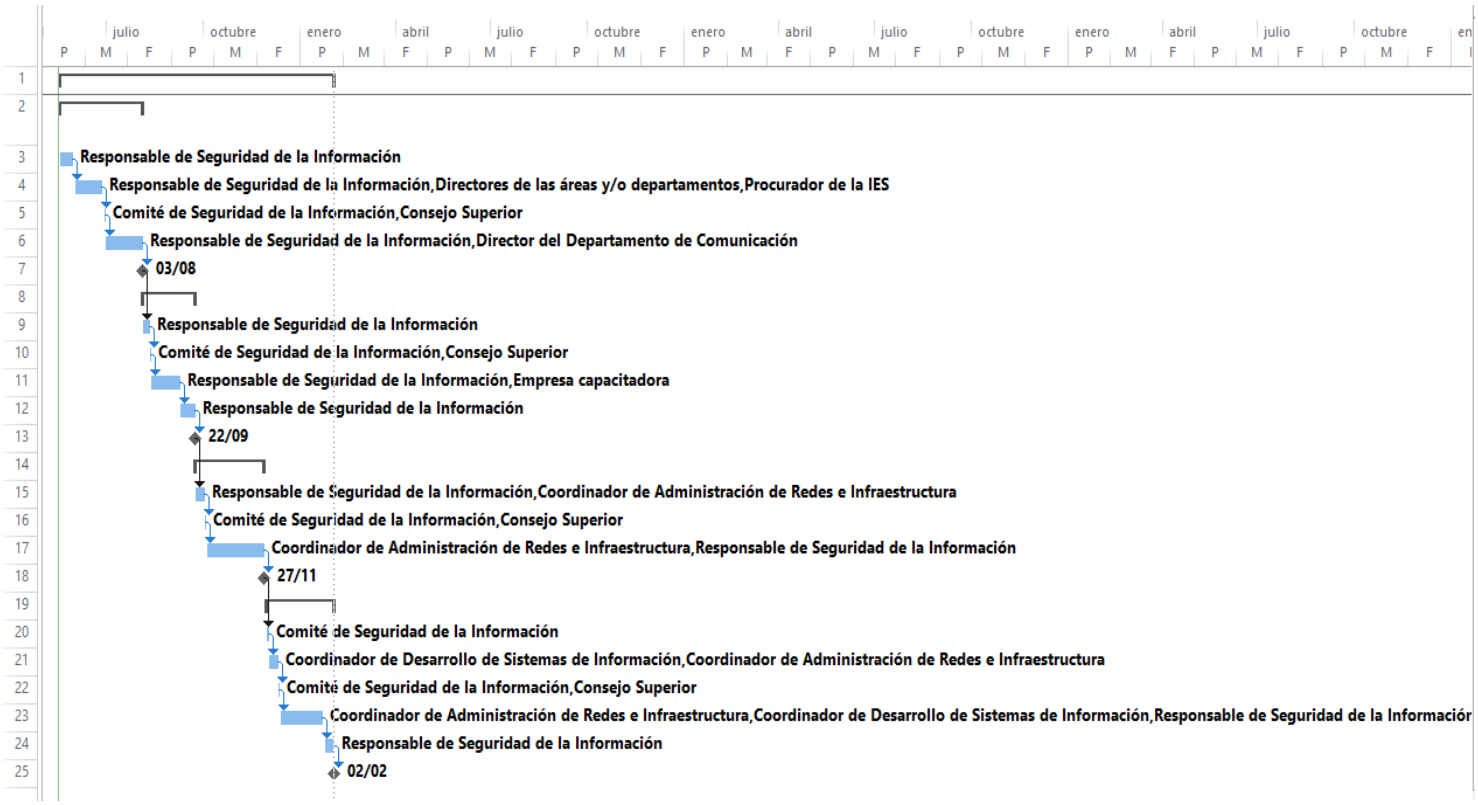


Ilustración 26 Responsables_Fases de la Propuesta de Proyectos

4.4 Evolución de los Resultados

Los proyectos que se han definido en el apartado anterior generan una reducción del riesgo en los activos y por ende en el cumplimiento de los dominios de control en base a la ISO/IEC 27002:2013.

En la Tabla 17 se puede apreciar la comparación del estado de madurez de los controles en este momento y cuando se hayan implementado los proyectos.

Objetivo	Control	Estado actual	Estado previsto
5. Políticas de seguridad de la información			
5.1 Dirección de gestión de seguridad de la información	5.1.1 Políticas de seguridad de la información	0. Incompleto	2. Gestionado
	5.1.2 Revisión de las políticas de seguridad de la información	0. Incompleto	2. Gestionado
6. Organización de la seguridad de la información			
6.1 Organización interna	6.1.1 Roles y responsabilidades de seguridad de información	0. Incompleto	1. Ejecutado
	6.1.2 Segregación de funciones	1. Ejecutado	2. Gestionado
	6.1.3 Contacto con las autoridades	4. Predecible	4. Predecible
	6.1.4 Contacto con los grupos de interés especial	3. Establecido	3. Establecido
	6.1.5. Seguridad de la información en la gestión de proyectos	0. Incompleto	0. Incompleto
6.2 Los dispositivos móviles y el teleworking	6.2.1 Política de dispositivo móvil	0. Incompleto	0. Incompleto
	6.2.2 Teleworking	1. Ejecutado	1. Ejecutado
7. Seguridad de los Recursos Humanos			
7.1 Previo al empleo	7.1.1 Proyección	5. Optimizado	5. Optimizado
	7.1.2 Términos y condiciones de empleo	4. Predecible	4. Predecible
7.2 Durante el empleo	7.2.1 Responsabilidades de la gestión	3. Establecido	3. Establecido
	7.2.2 Concienciación sobre la seguridad de la información, la educación y la formación	0. Incompleto	2. Gestionado
	7.2.3 Proceso disciplinario	0. Incompleto	2. Gestionado
7.3 Terminación y cambio de empleo	7.3.1 La terminación o el cambio de las responsabilidades laborales	3. Establecido	2. Gestionado
8. Gestión de activos			
8.1 Responsabilidad de los activos	8.1.1 Inventario de los activos	5. Optimizado	5. Optimizado
	8.1.2 Propiedad de los activos	3. Establecido	3. Establecido
	8.1.3 Uso aceptable de los activos	2. Gestionado	2. Gestionado
	8.1.4 Restitución de activos	4. Predecible	4. Predecible
8.2 Clasificación de la información	8.2.1 Clasificación de la información	5. Optimizado	5. Optimizado
	8.2.2 Etiquetado de la información	5. Optimizado	5. Optimizado
	8.2.3 Manipulación de los activos	5. Optimizado	5. Optimizado
8.3 Manejo de soportes	8.3.1 Gestión de soportes extraíbles	1. Ejecutado	2. Gestionado
	8.3.2 Eliminación de los soportes	0. Incompleto	2. Gestionado
	8.3.3 Transferencia de medios físicos	1. Ejecutado	2. Gestionado
9. Control de acceso			
9.1 Requisitos de	9.1.1 Políticas de control de acceso	5. Optimizado	5. Optimizado

negocio para el control de accesos	9.1.2 Acceso a las redes y servicios de red	5. Optimizado	5. Optimizado
9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios	1. Ejecutado	2. Gestionado
	9.2.2 Gestión de los derechos de acceso de los usuarios	1. Ejecutado	2. Gestionado
	9.2.3 Gestión de los derechos de acceso con privilegios	2. Gestionado	2. Gestionado
	9.2.4 Gestión de información confidencial de autenticación de usuarios	0. Incompleto	2. Gestionado
	9.2.5 Revisión de los derechos de acceso de los usuarios	3. Establecido	3. Establecido
	9.2.6 Remoción o ajuste de los derechos de acceso	5. Optimizado	5. Optimizado
9.3 Responsabilidades de los usuarios	9.3.1 Uso de información confidencial para la autenticación	0. Incompleto	2. Gestionado
9.4 Control de acceso a sistemas y aplicaciones	9.4.1 Restricción del acceso a la información	5. Optimizado	5. Optimizado
	9.4.2 Procedimientos seguros de inicio de sesión	3. Establecido	3. Establecido
	9.4.3 Gestión de contraseñas de usuario	1. Ejecutado	1. Ejecutado
	9.4.4 Uso de programas de servicios públicos privilegiados	1. Ejecutado	1. Ejecutado
	9.4.5 Control de acceso al código fuente de los programas	1. Ejecutado	1. Ejecutado
10. Criptografía			
10.1 Controles criptográficos	10.1.1 Política sobre el uso de controles criptográficos	0. Incompleto	0. Incompleto
	10.1.2 Gestión de claves	3. Establecido	3. Establecido
11. Seguridad física y ambiental			
11.1 Áreas seguras	11.1.1 Perímetro de seguridad física	5. Optimizado	5. Optimizado
	11.1.2 Controles físicos de entrada	5. Optimizado	5. Optimizado
	11.1.3 Seguridad en oficinas, salas e instalaciones	4. Predecible	4. Predecible
	11.1.4 Protección contra amenazas externas y ambientales	4. Predecible	4. Predecible
	11.1.5 Trabajo en áreas seguras	0. Incompleto	0. Incompleto
	11.1.6 Áreas de acceso público, carga y descarga	0. Incompleto	0. Incompleto
11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección del equipo	3. Establecido	3. Establecido
	11.2.2 Instalaciones de suministro	4. Predecible	4. Predecible
	11.2.3 Seguridad del cableado	3. Establecido	3. Establecido
	11.2.4 Mantenimiento del equipo	3. Establecido	3. Establecido
	11.2.5 Salida de activos fuera de las dependencias de la empresa	2. Gestionado	2. Gestionado
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	0. Incompleto	2. Gestionado
	11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	3. Establecido	3. Establecido
	11.2.8 Equipo informático de usuario desatendido	1. Ejecutado	1. Ejecutado
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	0. Incompleto	2. Gestionado

12. Seguridad en la Operativa			
12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación	0. Incompleto	0. Incompleto
	12.1.2 Gestión de cambios	0. Incompleto	1. Ejecutado
	12.1.3 Gestión de capacidades	0. Incompleto	0. Incompleto
	12.1.4 Separación de entornos de desarrollo, prueba y producción	2. Gestionado	2. Gestionado
12.2 Protección contra código malicioso	12.2.1 Controles contra el código malicioso	1. Ejecutado	1. Ejecutado
12.3 Copias de seguridad	12.3.1 Copias de seguridad de la información	2. Gestionado	2. Gestionado
12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad	0. Incompleto	1. Ejecutado
	12.4.2 Protección de los registros de información	1. Ejecutado	1. Ejecutado
	12.4.3 Registros de actividad del administrador y operador del sistema	1. Ejecutado	1. Ejecutado
	12.4.4 Sincronización de relojes	5. Optimizado	5. Optimizado
12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción	1. Ejecutado	1. Ejecutado
12.6 Gestión de la vulnerabilidad técnica	12.6.1 Gestión de las vulnerabilidades técnicas	0. Incompleto	0. Incompleto
	12.6.2 Restricciones en la instalación de software	3. Establecido	3. Establecido
12.7 Consideraciones de las auditorías de los sistemas de información	12.7.1 Controles de auditoría de los sistemas de información	0. Incompleto	1. Ejecutado
13. Seguridad en las Telecomunicaciones			
13.1 Gestión de la seguridad en las redes	13.1.1 Controles de red	2. Gestionado	2. Gestionado
	13.1.2 Seguridad asociados a servicios en red	5. Optimizado	5. Optimizado
	13.1.3 Segregación de redes	2. Gestionado	2. Gestionado
13.2 Intercambio de información con partes externas	13.2.1 Políticas y procedimientos de intercambio de información	0. Incompleto	0. Incompleto
	13.2.2 Acuerdos de intercambio	5. Optimizado	5. Optimizado
	13.2.3 Mensajería electrónica	2. Gestionado	2. Gestionado
	13.2.4 Acuerdos de confidencialidad y secreto	1. Ejecutado	1. Ejecutado
14. Adquisición, desarrollo y mantenimiento de los sistemas de información			
14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de los sistemas de información	2. Gestionado	2. Gestionado
	14.1.2 Seguridad de los servicios accesibles por redes públicas	1. Ejecutado	1. Ejecutado
	14.1.3 Protección de las transacciones de servicios de aplicación	3. Establecido	3. Establecido
14.2 Seguridad en los procesos de desarrollo y soporte	14.2.1 Política de desarrollo seguro	5. Optimizado	5. Optimizado
	14.2.2 Procedimientos de control de cambios en los sistemas	2. Gestionado	2. Gestionado
	14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	3. Establecido	3. Establecido
	14.2.4 Restricciones a los cambios en los paquetes de software	0. Incompleto	1. Ejecutado

	14.2.5 Uso de principios de ingeniería en protección de sistemas	2. Gestionado	2. Gestionado
	14.2.6 Seguridad en entornos de desarrollo	1. Ejecutado	1. Ejecutado
	14.2.7 Externalización del desarrollo de software	0. Incompleto	0. Incompleto
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	5. Optimizado	5. Optimizado
	14.2.9 Pruebas de aceptación	0. Incompleto	2. Gestionado
14.3 Datos de prueba	14.3.1 Protección de los datos utilizados en pruebas	0. Incompleto	2. Gestionado
15. Relaciones con los proveedores			
15.1 Seguridad de la información en la relación con el proveedor	15.1.1 Política de seguridad de la información para proveedores	3. Establecido	3. Establecido
	15.1.2 Tratamiento del riesgo dentro de los acuerdos con el proveedor	3. Establecido	3. Establecido
	15.1.3 Cadena de proveedor en tecnologías de la información y comunicación	3. Establecido	3. Establecido
15.2 Gestión de la prestación de servicio del proveedor	15.2.1 Supervisión y revisión de los servicios prestados de los proveedores	2. Gestionado	2. Gestionado
	15.2.2 Gestión de cambios en los servicios prestados por los proveedores	3. Establecido	3. Establecido
16. Gestión de incidentes en la seguridad de la información			
16.1 Gestión de incidentes de seguridad de la información y mejoras	16.1.1 Responsabilidades y procedimientos	0. Incompleto	1. Ejecutado
	16.1.2 Notificación de los incidentes de seguridad de la información	1. Ejecutado	1. Ejecutado
	16.1.3 Notificación de los puntos débiles de seguridad de la información	1. Ejecutado	2. Gestionado
	16.1.4 Valoración de los eventos de seguridad de la información y toma de decisiones	2. Gestionado	2. Gestionado
	16.1.5 Respuesta a incidentes de seguridad de la información	1. Ejecutado	1. Ejecutado
	16.1.6 Aprendizaje de los incidentes de seguridad de la información	2. Gestionado	2. Gestionado
	16.1.7 Recopilación de evidencias	0. Incompleto	1. Ejecutado
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio			
17.1 Continuidad de la seguridad de la información	17.1.1 Planificación de la continuidad de la seguridad de la información	0. Incompleto	2. Gestionado
	17.1.2 Implementación de la continuidad de la seguridad de la información	0. Incompleto	2. Gestionado
	17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	0. Incompleto	2. Gestionado
17.2 Redundancias	17.2.1 Disponibilidad de instalaciones de procesamiento de información	3. Establecido	3. Establecido
18. Cumplimiento			
18.1 Cumplimiento de los requisitos legales	18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	0. Incompleto	1. Ejecutado

y contractuales	18.1.2 Derechos de propiedad intelectual (DPI)	3. Establecido	3. Establecido
	18.1.3 Protección de los registros de la organización	2. Gestionado	2. Gestionado
	18.1.4 Protección de datos y privacidad de la información personal	1. Ejecutado	1. Ejecutado
	18.1.5 Regulación de los controles criptográficos	0. Incompleto	0. Incompleto
18.2 Revisiones de la seguridad de la información	18.2.1 Revisión independiente de la seguridad de la información	0. Incompleto	0. Incompleto
	18.2.2 Cumplimiento de las políticas y normas de seguridad	4. Predecible	4. Predecible
	18.2.3 Comprobación del cumplimiento	1. Ejecutado	1. Ejecutado

Tabla 17 Estado actual y previsto de la norma ISO/IEC 27002:2013

Como medio de comprobación de los resultados en la Ilustración 27 se observa el estado actual del cumplimiento de los dominios previo a la implementación de los proyectos descritos en el apartado anterior. De esta manera se tendrá un mecanismo de verificación cuando se desarrolle la auditoría, que será una fase previa a la implementación de los proyectos en la IES.

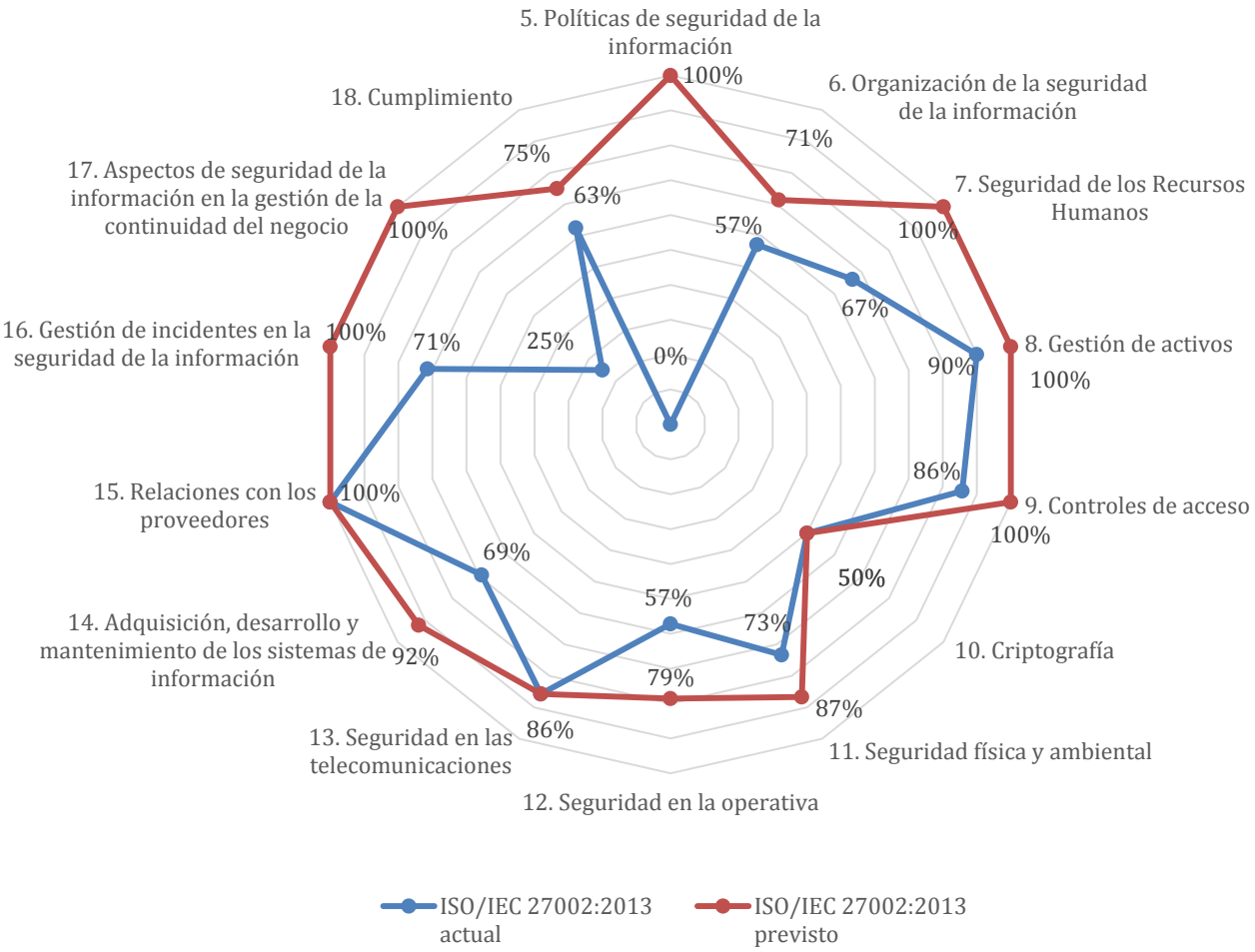


Ilustración 27 Estado de madurez actual y previsto de la ISO/IEC 27002:201

En la Ilustración 28 se aprecia como con la implementación de los proyectos y las políticas de seguridad de la información los controles poseen un nivel de gestión aceptable.

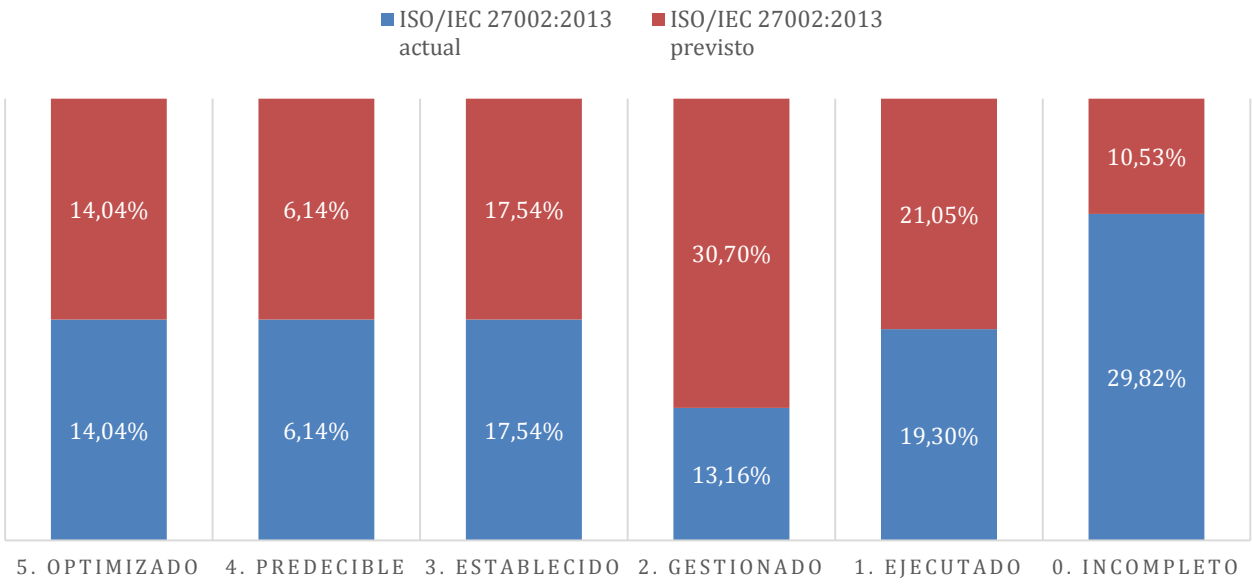


Ilustración 28 Estado de madurez actual y previsto de los controles

5 Fase 5: Auditoría de Cumplimiento

5.1 Introducción

Auditoría es un proceso ejecutado por un auditor que busca obtener registros, declaraciones de hechos u otra información conocida como evidencias de auditoría que servirán para determinar si el hecho que está siendo auditado cumple con los criterios de auditoría. Estos criterios de auditoría son las políticas, procedimientos, procesos o requisitos que son usados como elementos de referencia para compararlos con la realidad de la IES.

Toda evidencia de auditoría debe ser verificable, pertinente y evaluable de manera objetiva, es decir, las pruebas que se realicen determinarán el cumplimiento del proceso o sistema auditado.

Existen diversos tipos de auditoría y hechos a ser auditados, mas lo importante en toda auditoría es seguir los principios que garanticen su objetividad y un análisis sistémico, y sea algo más que la opinión de un experto.

A continuación menciono algunos de los principios a ser considerados:

- **Conducta ética:** El auditor deberá actuar con integridad, confidencialidad y discreción, provocando una relación de confianza entre el auditado y auditor. Recordemos que, la información a manejar en muchos casos es confidencial, por lo tanto deberá siempre existir este código de conducta ética en el auditor, lo cual puede estar explícito en su contrato.
- **Presentación justa:** El auditor tiene la obligación de informar verazmente y con exactitud los hallazgos realizados y las conclusiones extraídas en base a la evidencia. El auditado no puede deslingarse del proceso que se está realizando, por lo tanto siempre debe estar en continua comunicación con el auditor conociendo los obstáculos significativos encontrados, los aspectos no tratados y las razones que lo provocaron.
- **Cuidado profesional:** El auditor además de poseer la confianza del auditado, debe poseer la competencia profesional y técnica necesaria, lo cual se suele acreditar mediante títulos académicos, certificaciones profesionales, años de experiencia, hoja de vida, entre otros.
- **Independencia:** El auditor debe ser imparcial y objetivo en sus conclusiones, por lo tanto será independiente de la actividad auditada, esto no significa que el auditor sólo deba ser externo a la institución, sino mas bien, indica que no debe haber formado parte ya sea directa o indirectamente de la actividad o control a ser auditada, porque no podría emitir un juicio de auditoría, por estar influenciado.

  El auditor tiene que mantener un estado mental objetivo durante todo el proceso de auditoría, para evitar conflictos de intereses que inhabilitarían la auditoría.
- **Evidencia:** El elemento fundamental en toda auditoría es la evidencia, que conducirá a las conclusiones de auditoría confiable y reproducible. El proceso de una auditoría comienza con la obtención de la evidencia mediante diversos mecanismos, posterior su análisis y confrontación con los criterios de auditoría que generan la presencia o no de un hallazgo de auditoría. De allí que la evidencia debe basarse en muestras de información disponibles y de hechos verificables.

El Plan de Auditoría está bajo las directrices que se establecieron en el documento SGSI_PR_AI_2015-01, donde se describe todo el procedimiento para Auditorías Internas en materia de seguridad de información.

5.2 Plan de Auditoría

La presente Auditoría de Cumplimiento se realiza en la ciudad de Cuenca provincia del Azuay en cumplimiento del Plan Anual de Auditoría de Cumplimiento 2015 aprobada mediante Resolución de Consejo Superior N° 100-01-2014-01-13, responsable de normar, supervisar y evaluar los procedimientos y correcto funcionamiento de las diferentes áreas, habiéndose aplicado procedimientos de auditoría que se consideran necesarios de acuerdo a lo analizado.

5.2.1 Información General

Objetivo General del Plan

El objetivo general de la auditoría a realizar es revisar y analizar los controles, sistemas, procedimientos y políticas en materia de seguridad informática, a fin de verificar el estado de implementación del Sistema de Gestión de Seguridad de la Información.

El objeto del presente documento es recopilar los diferentes aspectos a revisar dentro de la aplicación que está siendo auditada. Se realizará una justificación sobre los controles revisados.

Este documento será la guía a usar para la Coordinación entre el equipo auditor y la IES al momento de realizar la planificación, programar las pruebas a realizar y gestionar las debidas autorizaciones que permitan proceder con la auditoría. Bajo la anterior premisa, se establece que el documento servirá para definir la estrategia de prueba que se seguirá, en caso de ser considerado necesario.

Objetivos Específicos

- Evaluar el control que se tiene sobre los procedimientos implementados.
- Verificar el cumplimiento de las disposiciones y reglamentos que coadyuven al mantenimiento del orden en materia de seguridad de la información.
- Evaluar los procedimientos de control, analizar su estandarización y su cumplimiento.

Alcance

La presente auditoría se rige a la verificación del estado de cumplimiento de los controles de seguridad de la norma ISO/IEC 27002:2013 en base a la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información y las políticas propuestas.

Inventario de las políticas

Se ha revisado los documentos que posee la IES como son procedimientos, políticas, procesos, planes, entre otros, en base a lo cual se ha realizado una clasificación dependiendo del tipo de documento, es decir, si corresponde a un documento interno de la IES o si es externo.

- **Documentos internos:**
  - Política de Seguridad de la Información.
  - Política de Alto Nivel.
  - Política de Control de Acceso.
  - Política de puesto de trabajo despejado y bloqueo de pantalla.
  - Política de Desarrollo Seguro.
  - Política de Clasificación de la Información
  - Política de uso de Correo Electrónico.
  - Política de Gestión de Incidentes.
  - Política de Manejo de Activos.
  - Política de Divulgación de Información.
  - Política de Gestión de Pruebas en el desarrollo seguro.
  - Procedimiento de Auditorías Internas.
  - Procedimiento de Revisión por la Dirección.
  - Gestión de Indicadores.
  - Gestión de Roles y Responsabilidades.
  - Metodología de Análisis de Riesgos.
  - Declaración de Aplicabilidad.

- Plan de concienciación.
- Plan de virtualización de servidores.
- Plan de elaboración y divulgación de las políticas de SI.

- **Documentos externos:**
  - Ley Orgánica de Educación Superior.
  - Reglamento de Régimen Académico del CES.
  - Reglamento Interno de Régimen Académico de la IES.
  - Norma ISO/IEC 27001:2013.
  - Norma ISO/IEC 27002:2013.

Plazos temporales:

Este plan de auditoría se ejecutará previsiblemente entre las fechas 18 de mayo de 2015 y 28 de mayo de 2015.

5.2.2 Procedimientos de control de las pruebas

Entorno de prueba requerido. No existe la necesidad de generar un entorno de prueba, por lo tanto se está trabajando sobre los sistemas y procedimientos en pruebas, los cuales se encuentran implementados.

Estado de las pruebas. Se procederá a realizar pruebas de cumplimiento, que tienen como propósito como su nombre lo indica, comprobar el cumplimiento de los controles con la normativa y procedimientos que describe el control, obteniendo así evidencia sobre si los controles se encuentran funcionando o no.

Gestión de las incidencias. Si en el transcurso de la auditoría se detecta una vulnerabilidad grave que pueda comprometer la seguridad de la información se procederá de la siguiente manera:

- Se comunica al Responsable de Seguridad de la Información la incidencia y circunstancias que la provocaron, para que el mismo tome las medidas que considere convenientes.
- El detalle de la incidencia se documentará en el informe de auditoría.

Se considera una vulnerabilidad grave las siguientes situaciones:

- Una filtración o modificación no autorizada de información considerada como confidencial.
- Un malfuncionamiento que pueda provocar una denegación de servicio.
- Un proceso mal ejecutado que pueda provocar problemas legales.
- Cualquier incidente que pueda ocasionar un estado inoperable.

5.2.3 Definición de las pruebas

Estrategia de prueba. El presente Plan de Auditoría se centra en la comprobación de la implementación del Sistemas de Gestión de Seguridad de la Información, por lo cual se revisará cada dominio y control de la norma ISO/IEC 27002:2013 para garantizar la confidencialidad, integridad y disponibilidad de la información.

Objetivo	Control	Justificación

#. Dominio [<Promedio objetivo> - <CMM>]							
#.# Objetivo	<Promedio control>	<CMM>	#.#.# Control 1	<Efectividad>	<CMM>	<Justificación>	
			#.#.3 Control n	<Efectividad>	<CMM>	<Justificación>	<Tipo de hallazgo de auditoría>

Tabla 18 Formato para las pruebas de cumplimiento

Cada CMM por control poseerá un estado, en base al detalle que presento a continuación:

- Naranja: Control ha superado el estado actual.
- Verde: Control pose un estado inferior con respecto al estado previsto.
- Rojo: Control posee un estado inferior a lo indicado en el estado actual.
- Rosado: Control ha superado el estado previsto.
- Sin color: Control no ha cambiado su estado

Recogida de información. El objetivo de esa fase es la comprobación de la información relativa a la aplicación auditada que puede ser obtenida de forma legítima en base a los documentos, registros e historial que posee la IES.

Las evidencias que cumplan con sus características mínimas se confrontarán contra los criterios de auditoría para determinar si se ha realizado un hallazgo o no, y de qué tipo.

Los hallazgos se clasifican de la siguiente manera:

- **No conformidad mayor:** Se incumple completamente con la norma.
- **No conformidad menor:** Se incumple un punto de un apartado de la política o norma.
- **Observación:** Es una recomendación, que podría convertirse en No Conformidad, en caso de no ser tratado.
- **Oportunidad de mejora:** Es sólo una recomendación.

5.3 Metodología Empleada

Como metodología se está trabajando con el estándar ISO/IEC 27002:2013, en donde dada uno de los controles será evaluado mediante el modelo de madurez CMM como se ilustra en la Tabla 19.

Nivel	Efectividad	Descripción
L5. Optimizado	100%	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.
L4. Gestionado y medible	95%	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
L3. Proceso definido	90%	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
L2. Reproducible, pero intuitivo	50%	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
L1. Inicial / Ad-hoc	10%	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
L0. Inexistente	0%	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
N/A	N/A	No aplica

Tabla 19 Modelo de madurez CMM

5.4 Evaluación de la Madurez

Para la evaluación de la madurez se está usando el modelo de madurez de capacidades o CMM, este es un modelo de evaluación de procesos de la IES.

Objetivo			Control			Justificación	
5. Políticas de seguridad de la información [97.5% - L5]							
5.1 Dirección de gestión de seguridad de la información	97.5%	L5	5.1.1 Políticas de seguridad de la información	100%	L5.	Las políticas se encuentran definidas e implementadas, además están en un proceso de mejora constante.	
			5.1.2 Revisión de las políticas de seguridad de la información	95%	L4.	Existe un plan que permitirá la revisión de las políticas.	**Observación:** Existe un plan de revisión de las políticas de seguridad de la información con su respectiva planificación, pero no se ha ejecutado.
6. Organización de la seguridad de la información [64.2% - L3]							
6.1 Organización interna	77%	L3	6.1.1 Roles y responsabilidades de seguridad de información	100%	L5.	La IES ha implementado el documento SGSI_PR_RR_2015-001 en donde el Comité de Seguridad ha asignado roles y funciones en materia de seguridad de la información	
			6.1.2 Segregación de funciones	90%	L3.	Existe una segregación de las funciones que han tenido conflictos.	
			6.1.3 Contacto con las autoridades	95%	L4.	Se presenta una sistemática comunicación con las autoridades de la IES (Consejo Superior).	
			6.1.4 Contacto con los grupos de interés especial	90%	L3.	Existe un proceso que mantiene el contacto con otras áreas.	
			6.1.5. Seguridad de la información en la gestión de proyectos	10%	L1.	El Departamento de TIC ha implementado seguridad de la información en la gestión de proyectos, pero no	

						se encuentra definido a nivel corporativo.	
6.2 Los dispositivos móviles y el teleworking	0%	L0	6.2.1 Política de dispositivo móvil	0%	L0.	Se ha identificado la necesidad de una Política de dispositivo móvil, pero no existe nada definido estrictamente.	**No conformidad mayor:** No existe una Política de dispositivo móvil.
			6.2.2 Teleworking	N/A	N/A.	En base al documento Declaración de Aplicabilidad SGSI_OT_DA_2015-01, no aplica.	
7. Seguridad de los Recursos Humanos [71.6% - L3]							
7.1 Previo al empleo	97.5%	L5	7.1.1 Proyección	100%	L5.	Se ha evidenciado que existe un conjunto de procedimientos antes de contratar a un nuevo personal, en donde se verifican los antecedentes de los empleados, la legalidad de los documentos. Esta tarea se lo realiza en el Departamento de Recursos Humanos	
			7.1.2 Términos y condiciones de empleo	95%	L4.	Se han revisado los contratos donde se encuentra plasmado las responsabilidades a nivel de seguridad de la información.	
7.2 Durante el empleo	48.3%	L2	7.2.1 Responsabilidades de la gestión	90%	L3.	Los empleados conocen sobre las medidas de seguridad de la información que han sido establecidas.	
			7.2.2 Concienciación sobre la seguridad de la información, la educación y la formación	45%	L2.	Se ha evidenciado que dentro de las propuestas de proyectos se incluye un plan de concienciación con la propuesta de seis capacitaciones.	**No conformidad menor:** Existe el proyecto de cada una de las capacitaciones, pero no se ha contratado a la Empresa Capacitadora.

			7.2.3 Proceso disciplinario	10%	L1.	En la Reglamento de Procesos Disciplinarios y de Aplicación del Art. 207 de la Ley Orgánica de Educación Superior, de la IES se establecen las sanciones a empleados y estudiantes por infracciones.	**No conformidad menor:** Existe el Reglamento respectivo pero se incumple con el artículo de sanciones graves.
7.3 Terminación y cambio de empleo	90%	L3	7.3.1 La terminación o el cambio de las responsabilidades laborales	90%	L3.	El Departamento de Recursos Humanos posee un proceso para la terminación o cambio de responsabilidades, que se encuentra gestionado por el Departamento de TIC.	**Oportunidad de mejora:** Se recomienda que el proceso sea traducido como una política de la IES.
8. Gestión de activos [73.7% - L3]							
8.1 Responsabilidad de los activos	83.8%	L3	8.1.1 Inventario de los activos	100%	L5.	Existe la Política de Clasificación de la Información SGSI_PO_SI_2015-01, lo cual además se encuentra plasmado en el documento SGSI_PR_AR_2015-01.	
			8.1.2 Propiedad de los activos	90%	L3.	Existe la Política de Clasificación de la Información SGSI_PO_SI_2015-0 y en el documento SGSI_OT_AR_2015-01, en la cual se establece los propietarios por cada activo.	
			8.1.3 Uso aceptable de los activos	50%	L2.	Existe una gestión para el uso y procesamiento de la información y los activos.	**Observación:** Se recomienda actualizar el proceso de gestión para el uso y procesamiento de la información y los activos.
			8.1.4 Restitución de activos	95%	L4.	Dentro de la propuesta de proyectos se ha definido la Política de manejo de activos.	

8.2 Clasificación de la información	98.7%	L5	8.2.1 Clasificación de la información	100%	L5.	Existe la Política de Clasificación de la Información SGSI_PO_SI_2015-01, que se encuentra aprobada por el Consejo Superior he implementada.	
			8.2.2 Etiquetado de la información	100%	L5.	El Departamento de Gestión Documental provee una política de etiquetado de la información dentro de la IES.	
			8.2.3 Manipulación de los activos	96%	L5.	El Departamento de Gestión Documental provee del procedimiento de la manipulación de los activos.	**Oportunidad de mejora:** Se recomienda revisión del procedimiento ya que se encuentra alineado al documento SGSI_PO_Si_2015-01 Política de Clasificación de la Información.
8.3 Manejo de soportes	35.3%	L2	8.3.1 Gestión de soportes extraíbles	10%	L1.	Existe el respectivo procedimiento para la gestión de soportes extraíbles en base a su clasificación.	**No conformidad menor:** Se incumple con un punto del procedimiento donde se indica el uso de las plantillas.
			8.3.2 Eliminación de los soportes	46%	L2.	Dentro de la propuesta de proyectos se ha definido la Política de manejo de activos, pero no existe una capacitación formal.	**Oportunidad de mejora:** Se recomienda dentro de la propuesta de proyectos incluir la Capacitación sobre la eliminación de los soportes.
			8.3.3 Transferencia de medios físicos	50%	L2.	Existe un proceso para gestionar la transferencia de soportes físicos.	
9. Control de acceso [66.6% - L3]							
9.1 Requisitos de negocio para el control de accesos	100%	L5	9.1.1 Políticas de control de acceso	100%	L5.	Existe la Política de Control de Acceso SGSI_PO_SI_2015-01, que se encuentra aprobada por el Consejo Superior he implementada.	
			9.1.2 Acceso a las redes y servicios	100%	L5.	Existen mecanismos que	

			de red			regulan que empleados administrativos, docentes y estudiantes tengan acceso a las redes y sus servicios.	
9.2 Gestión de acceso de usuario	70.5%	L3	9.2.1 Gestión de altas/bajas en el registro de usuarios	85%	L3.	Existe un proceso definido que regula la gestión de altas/bajas del personal de la IES.	
			9.2.2 Gestión de los derechos de acceso de los usuarios	50%	L2.	El proceso para gestionar los derechos de acceso de los usuarios, se realiza en base al usuario, servicio y/o sistema.	
			9.2.3 Gestión de los derechos de acceso con privilegios	50%	L2.	El Área de Explotación gestiona los derechos de accesos privilegiados.	
			9.2.4 Gestión de información confidencial de autenticación de usuarios	50%	L2.	Se ha evidenciado que existe un proceso de gestión de información confidencial de autenticación de usuarios.	
			9.2.5 Revisión de los derechos de acceso de los usuarios	88%	L3.	Anualmente los propietarios de los activos entregan un listado de derecho de accesos de los usuarios que tienen a su cargo.	**Observación:** Los listados de acceso a nivel de red no son considerados.
			9.2.6 Remoción o ajuste de los derechos de acceso	100%	L5.	Existe un proceso monitorizado que permite la remoción o ajuste de los derechos, que es tratado por el Departamento de Recursos Humanos y por el Departamento de TIC.	
9.3 Responsabilidades de los usuarios	50%	L2	9.3.1 Uso de información confidencial para la autenticación	50%	L2.	Se ha evidenciado dentro de los contratos un punto donde se especifica sobre el uso de la información confidencial para autenticación.	

						Además, existe la Política de puesto de trabajo despejado y bloqueo de pantalla SGSI_PO_SI_2015-01.	
9.4 Control de acceso a sistemas y aplicaciones	52%	L3	9.4.1 Restricción del acceso a la información	100%	L5.	Existe la Política de Control de Acceso SGSI_PO_SI_2015-01 donde tienen establecidos los permisos a la información compartida.	
			9.4.2 Procedimientos seguros de inicio de sesión	90%	L3.	En base a la Política de Control de Acceso están definidos e implementados los controles.	
			9.4.3 Gestión de contraseñas de usuario	10%	L1.	Dentro de la Política de Control de Acceso SGSI_PO_SI_2015-01 se explica la responsabilidad de la gestión de las contraseñas. Internamente cada intervalo de tiempo al empleado dependiendo de su rol, se le solicita la modificación de su contraseña.	**No conformidad mayor:** No existe una política particular o dentro del documento Política de Control de Acceso SGSI_PO_SI_2015-01 una sección específica sobre la gestión de las contraseñas.
			9.4.4 Uso de programas de servicios públicos privilegiados	10%	L1.	Los sistemas considerados de nivel crítico se encuentran altamente protegidos por los controles específicos.	**Oportunidad de mejora:** Se recomienda que dicho control sea revisado y actualizado.
			9.4.5 Control de acceso al código fuente de los programas	50%	L2.	Dentro de la Política de Control de Acceso SGSI_PO_SI_2015-01 se evidencia el control de acceso lógico a los sistemas informáticos institucionales.	
10. Criptografía [25% - L2]							
10.1 Controles criptográficos	25%	L2	10.1.1 Política sobre el uso de controles	0%	L0.	No existe una política sobre el uso de controles	**No conformidad mayor:** No existe una

			criptográficos			criptográficos para la protección de la información	política particular para el uso de controles criptográficos.
			10.1.2 Gestión de claves	50%	L2.	Existe un proceso que brinda la funcionalidad de gestión de claves, donde establece cada que intervalo de tiempo la generación de nuevas claves.	
11. Seguridad física y ambiental [72.5% - L3]							
11.1 Áreas seguras	80%	L3	11.1.1 Perímetro de seguridad física	100%	L5.	Se han establecido los controles que permiten la protección del perímetro.	
			11.1.2 Controles físicos de entrada	100%	L5.	Se ha evidenciado que dependiendo del área y/o información están implementados controles físicos de entrada como son: tarjetas, controles de vigilancia, geometría de la mano, entre otros.	**No conformidad menor:** Se ha evidenciado que existe problemas con el control de geometría de la mano.
			11.1.3 Seguridad en oficinas, salas e instalaciones	95%	L4.	Se ha evidenciado que existen los controles de protección para oficinas como son: Rectorado, Centros de Investigación, aulas de cómputo, entre otros	
			11.1.4 Protección contra amenazas externas y ambientales	95%	L4.	En la IES existen los controles y medidas respectivas tomadas en caso de amenazas externas y ambientales.	
			11.1.5 Trabajo en áreas seguras	10%	L1.	Ciertas áreas han establecido e implementado un conjunto de normas de gestión para el trabajo en zonas comunes.	
			11.1.6 Áreas de acceso público, carga y descarga	N/A	N/A.	En base al documento Declaración de	

						Aplicabilidad SGSI_OT_DA_2015-01, no aplica.	
11.2 Seguridad de los equipos	68.3%	L3	11.2.1 Emplazamiento y protección del equipo	90%	L3.	Los equipos de la IES destinados para la gestión de la información se encuentran ubicados adecuadamente garantizando la protección del equipo y la seguridad del personal.	
			11.2.2 Instalaciones de suministro	95%	L4.	Dentro de la propuesta de proyectos se ha definido el Plan de virtualización de servidores.	
			11.2.3 Seguridad del cableado	90%	L3.	Existen normas establecidas para cableado estructurado, como la norma ANSI/TIA/EIA-568-A, pero no en todos los bloques.	**Oportunidad de mejora:** A pesar de que existen las normas establecidas. No todas las instalaciones cuentan con cableado estructurado.
			11.2.4 Mantenimiento del equipo	90%	L3.	Dentro de la propuesta de proyectos se ha definido la Política de manejo de activos, donde se establece el proceso del mantenimiento de los equipos.	
			11.2.5 Salida de activos fuera de las dependencias de la empresa	50%	L2.	Existe un conjunto de normas donde se ha definido el procedimiento para la salida de equipos fuera de las dependencias, pero se ha evidenciado que no es una política formal por parte de la IES.	**No conformidad mayor:** Dentro de la Política de manejo de activos no existe una norma o artículo donde se legisle dicho proceso.
			11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	10%	L1.	No existe ninguna política donde se establezca la seguridad cuando los equipos salen de la IES, es un proceso intuitivo.	**No conformidad mayor:** Dentro de la Política de manejo de activos no existe una norma o artículo donde se legisle dicho proceso.

			11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	90%	L3.	Existe un proceso formal implementado en el Área de Infraestructura que indica el procedimiento cuando se da de baja un equipo o se pretende reutilizar.	
			11.2.8 Equipo informático de usuario desatendido	10%	L1.	Todos los equipos del personal administrativo y docentes restringen el acceso al transcurrir un tiempo que el equipo ha sido desatendido, de igual manera sucede con los sistemas informáticos.	
			11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla	90%	L3.	Existe la Política de puesto de trabajo despejado y bloqueo de pantalla SGSI_PO_SI_2015-01, que se encuentra aprobada por el Consejo Superior he implementado.	
12. Seguridad en la Operativa [29.3% - L2]							
12.1 Responsabilidades y procedimientos de operación	17.5%	L2	12.1.1 Documentación de procedimientos de operación	10%	L1.	La mayoría de los procedimientos se encuentran documentados, pero no es un proceso definido ni tampoco realizado por todos los Departamentos.	
			12.1.2 Gestión de cambios	10%	L1.	Existen procesos a nivel de área y/o departamento que trata los cambios según su realidad, pero no existe una plantilla o proceso definido a nivel de la IES.	
			12.1.3 Gestión de capacidades	0%	L0.	El uso de los recursos no se encuentra monitoreado	

			12.1.4 Separación de entornos de desarrollo, prueba y producción	50%	L2.	Las áreas de desarrollo, pruebas y producción se encuentran separadas para evitar modificaciones no autorizadas, pero no es un proceso autorizado por el Consejo Superior.	
12.2 Protección contra código malicioso	50%	L2	12.2.1 Controles contra el código malicioso	50%	L2.	La IES posee una política formal que prohíbe el uso de software no autorizado. Se encuentran implementados controles de seguridad que prohíben el acceso a sitios no permitidos, además los equipos y servidores tienen instalados antivirus y los respectivos firewalls.	
12.3 Copias de seguridad	50%	L2	12.3.1 Copias de seguridad de la información	50%	L2.	Semanalmente se realiza una copia de seguridad de la información considerada como crítica, además el procedimiento para realizarlo se encuentra documentado y se lleva a cabo mediante procedimientos ya establecidos.	
12.4 Registro de actividad y supervisión	32.5%	L2	12.4.1 Registro y gestión de eventos de actividad	10%	L1.	Existe un registro de eventos de actividad de los usuarios.	
			12.4.2 Protección de los registros de información	10%	L1.	Los registros de seguridad de la información se encuentran protegidos de accesos no autorizados.	
			12.4.3 Registros de actividad del administrador y operador del sistema	10%	L1.	Se evidencia la presencia de registros de actividad del administrador y	

						operador de los sistemas informáticos.	
			12.4.4 Sincronización de relojes	100%	L5.	Los relojes de todos los servidores se encuentran sincronizados, mediante un procedimiento que revisa periódicamente la sincronización. Se usa el protocolo NTP.	
12.5 Control del software en explotación	10%	L1	12.5.1 Instalación del software en sistemas en producción	10%	L1.	Sólo el Analista de Soportes Técnico puede instalar y/o actualizar el software operativo, aplicaciones y bibliotecas.	
12.6 Gestión de la vulnerabilidad técnica	45%	L2	12.6.1 Gestión de las vulnerabilidades técnicas	0	L0.	No se ha definido responsable para la gestión de las vulnerabilidades técnicas.	**Oportunidad de mejora:** Se recomienda incluir dentro del documento SGSI_PR_RR_2015-01 al responsable de dicha tarea.
			12.6.2 Restricciones en la instalación de software	90%	L3.	Sólo con la debida autorización se instala software adicional en los equipos. Se ha establecido un listado con los tipos de software a instalar y los usuarios que tienen permiso.	
12.7 Consideraciones de las auditorías de los sistemas de información	10%	L1	12.7.1 Controles de auditoría de los sistemas de información	10%	L1.	Todos los sistemas de información tienen activo el registro de eventos de seguridad, pero no se ha definido una política o documentación sobre el proceso.	
13. Seguridad en las Telecomunicaciones [66.7% - L3]							
13.1 Gestión de la seguridad en las redes	66.7%	L3	13.1.1 Controles de red	50%	L2.	Se ha evidenciado un proceso de control de la red mediante firewalls, tablas de enrutamiento, entre otros.	

			13.1.2 Seguridad asociados a servicios en red	100%	L5.	La IES ha implementado los respectivos controles que se encuentran gestionados.	
			13.1.3 Segregación de redes	50%	L2.	La red de la IES presenta segregación en base a la criticidad, usuario e información que protege.	
13.2 Intercambio de información con partes externas	66.7%	L3	13.2.1 Políticas y procedimientos de intercambio de información	N/A	N/A.	En base al documento Declaración de Aplicabilidad SGSI_OT_DA_2015-01, no aplica.	
			13.2.2 Acuerdos de intercambio	100%	L5.	Se cuenta con acuerdos de intercambio de información como en el proceso de pago de servicios, teniendo los procedimientos que garanticen la trazabilidad y la protección de la información. Estos procesos son revisados en base a lo que estipulan los acuerdos.	
			13.2.3 Mensajería electrónica	90%	L3.	Dentro de la Política de Uso de correo electrónico SGSI_PO_SI_2015-01 se gestiona la protección de la información.	
			13.2.4 Acuerdos de confidencialidad y secreto	10%	L1.	En los contratos se plasma los acuerdos de confidencialidad en base a su cargo y la información que va a tratar.	
14. Adquisición, desarrollo y mantenimiento de los sistemas de información [68.3% - L3]							
14.1 Requisitos de seguridad de los sistemas de información	63.3%	L3	14.1.1 Análisis y especificación de los requisitos de los sistemas de información	90%	L3.	En los requisitos de actualización o para nuevos sistemas de información se incluye el nivel de seguridad.	
			14.1.2 Seguridad de los servicios	10%	L1.	Existen medidas de protección para	

			accesibles por redes públicas			la información que es transmitida por las redes públicas.	
			14.1.3 Protección de las transacciones de servicios de aplicación	90%	L3.	Existe un proceso definido para la protección de las transacciones de los servicios de aplicación evitando la transmisión incompleta, enrutamiento erróneo, entre otros.	
14.2 Seguridad en los procesos de desarrollo y soporte	67.5%	L3	14.2.1 Política de desarrollo seguro	100%	L5.	Existe la Política de Desarrollo Seguro SGSI_PO_SI_2015-01, que se encuentra aprobado por el Consejo Superior he implementado.	
			14.2.2 Procedimientos de control de cambios en los sistemas	50%	L2.	El procedimiento para el control de cambios se basa en una nomenclatura que define el tipo de cambio, versión, sistema, entre otros datos. No está definido formalmente por la IES.	**Observación:** El Responsable de Seguridad de Información conjuntamente con el Director del Departamento de TIC deberán elevar la propuesta al Consejo Superior para su aprobación.
			14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma	90%	L3.	Cuando se realizan cambios en las plataformas, antes de poner en producción se realiza una revisión y un conjunto de pruebas verificando que el procedimiento es el correcto y que no se van a presentar problemas al momento que se encuentre en producción con los usuarios.	
			14.2.4 Restricciones a los cambios en los paquetes de software	10%	L1.	Sólo en el área Administrativa se ha implementado el proceso en caso de cambios en los paquetes de	

						software.	
			14.2.5 Uso de principios de ingeniería en protección de sistemas	90%	L3.	Todos los sistemas de información se encuentran desarrollados mediante un conjunto de principios de ingeniería para sistemas seguros, que se encuentra gestionado bajo un proceso.	
			14.2.6 Seguridad en entornos de desarrollo	10%	L1.	La IES ha implementado diversos mecanismos para proteger el entorno de desarrollo de accesos no autorizados, modificaciones o robo de la información. Pero no es un proceso que se encuentre documentado.	
			14.2.7 Externalización del desarrollo de software	N/A	N/A.	En base al documento Declaración de Aplicabilidad SGSI_OT_DA_2015-01, no aplica.	
			14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	100%	L5.	Dentro de la propuesta de proyectos se ha definido la Política de gestión de pruebas en el desarrollo seguro, donde se incluyen las pruebas de funcionalidad con sus respectivas plantillas.	
			14.2.9 Pruebas de aceptación	90%	L3.	Dentro de la propuesta de proyectos se ha definido la Política de gestión de pruebas en el desarrollo seguro.	
14.3 Datos de prueba	90%	L3	14.3.1 Protección de los datos utilizados en pruebas	90%	L3.	Dentro de la propuesta de proyectos se ha definido la Política de gestión de pruebas en el desarrollo seguro.	

15. Relaciones con los proveedores [82% - L3]							
15.1 Seguridad de la información en la relación con el proveedor	90%	L3	15.1.1 Política de seguridad de la información para proveedores	90%	L3.	Dentro de la Política de relaciones con proveedores se evidencia los requisitos necesarios para mitigar los riesgos cuando proveedores acceden a activos de la IES.	
			15.1.2 Tratamiento del riesgo dentro de los acuerdos con el proveedor	90%	L3.	Con cada proveedor se establece un proceso para mitigar los riesgos en base al contrato, que es revisado y actualizado por los respectivos involucrados, por ejemplo: Procuraduría.	
			15.1.3 Cadena de proveedor en tecnologías de la información y comunicación	90%	L3.	En el contrato además se incluye los requisitos para mitigar los riesgos a nivel de Tecnologías de la Información y Comunicación.	
15.2 Gestión de la prestación de servicio del proveedor	70%	L3	15.2.1 Supervisión y revisión de los servicios prestados de los proveedores	50%	L2.	Dentro de las funciones del Director de Departamento de TIC está el controlar regularmente de los servicios prestados por los proveedores mediante la respectiva auditoría.	
			15.2.2 Gestión de cambios en los servicios prestados por los proveedores	90%	L3.	Dentro de las funciones del Director de Departamento de TIC está el controlar los cambios de los servicios prestados por los proveedores considerando la información, los procesos, la criticidad y los	

						riesgos.	
16. Gestión de incidentes en la seguridad de la información [55.7% - L3]							
16.1 Gestión de incidentes de seguridad de la información y mejoras	55.7%	L3	16.1.1 Responsabilidades y procedimientos	90%	L3.	Existe un procedimiento de Roles y Responsabilidades SGSI_PR_RR_2015-01.	
			16.1.2 Notificación de los incidentes de seguridad de la información	90%	L3.	Existe la Política de Gestión de Incidentes SGSI_PO_SI_2015-01, que se encuentra aprobado por el Consejo Superior he implementado.	
			16.1.3 Notificación de los puntos débiles de seguridad de la información	50%	L2.	Existe un proceso establecido donde el usuario al encontrar un punto débil en la seguridad del sistema informático deberá remitirlo a su superior. El proceso no se encuentra oficializado.	
			16.1.4 Valoración de los eventos de seguridad de la información y toma de decisiones	50%	L2.	Los incidentes de seguridad de información se encuentran clasificados en base a diferentes indicadores como tipo de riesgo, criticidad, prioridad, entre otros.	
			16.1.5 Respuesta a incidentes de seguridad de la información	50%	L2.	Los incidentes de seguridad se responden en base a los procedimientos establecidos por la IES.	**Oportunidad de mejora:** A pesar de que existe el proceso establecido no todos los empleados responden en base al procedimiento.
			16.1.6 Aprendizaje de los incidentes de seguridad de la información	50%	L2.	El aprendizaje de los incidentes de seguridad de la información se encuentra gestionado mediante un procedimiento que empieza desde el análisis y la resolución del	

						incidente.	
			16.1.7 Recopilación de evidencias	10%	L1.	El Departamento de TIC ha implementado un proceso para identificar, recolectar, adquirir y almacenar las evidencias.	
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio [90% - L3]							
17.1 Continuidad de la seguridad de la información	90%	L3	17.1.1 Planificación de la continuidad de la seguridad de la información	90%	L3.	Dentro de la propuesta de proyectos se ha definido el Plan de Continuidad.	
			17.1.2 Implementación de la continuidad de la seguridad de la información	90%	L3.	Dentro de la propuesta de proyectos se ha definido el Plan de Continuidad.	
			17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	90%	L3.	Dentro de la propuesta de proyectos se ha definido el Plan de Continuidad.	
17.2 Redundancias	90%	L3	17.2.1 Disponibilidad de instalaciones de procesamiento de información	90%	L3.	La IES posee instalaciones con sus equipos para proveer de procesamiento de información en caso de algún inconveniente, se han realizado las pruebas y se ha verificado la disponibilidad de los sistemas ante un desastre.	
18. Cumplimiento [33.1% - L2]							
18.1 Cumplimiento de los requisitos legales y contractuales	32%	L2	18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	10%	L1.	Se han definido los requisitos reglamentarios y contractuales.	
			18.1.2 Derechos de propiedad intelectual (DPI)	90%	L3.	Se encuentran establecidos los procedimientos que garantizan el derecho de propiedad intelectual y el uso de software privado.	**Oportunidad de mejora:** Se recomienda incluir en el Plan de Concienciación una capacitación sobre propiedad intelectual.
			18.1.3 Protección de los registros de	50%	L2.	Los registros se encuentran	

			la organización			protegidos contra la pérdida, destrucción y falsificación	
			18.1.4 Protección de datos y privacidad de la información personal	10%	L1.	Existe una Política para la protección de los datos personales.	**No conformidad menor:** Los empleados no conocen sobre la Política para la Protección de los datos personales.
			18.1.5 Regulación de los controles criptográficos	0%	L0.	No existe una regulación de los controles criptográficos	
18.2 Revisiones de la seguridad de la información	35%	L2	18.2.1 Revisión independiente de la seguridad de la información	0%	L0.	No existe una política que defina cuando se realizan las revisiones.	
			18.2.2 Cumplimiento de las políticas y normas de seguridad	95%	L4.	Los responsables de cada departamento y/o área revisan el cumplimiento de las normas, políticas y procedimientos de seguridad que se encuentran establecidos.	
			18.2.3 Comprobación del cumplimiento	10%	L1.	Los sistemas de información son revisados para determinar el cumplimiento de las políticas de seguridad.	

Tabla 20 Estado de madurez de la norma ISO/IEC 27002:2013

5.5 Presentación de los Resultados

A continuación presento una Ilustración de pastel donde podemos verificar que la mayoría de controles se encuentran bajo un proceso definido, lo cual es un gran avance, ya que podemos determinar que los empleados están cumpliendo con la implementación de los proyectos definidos.

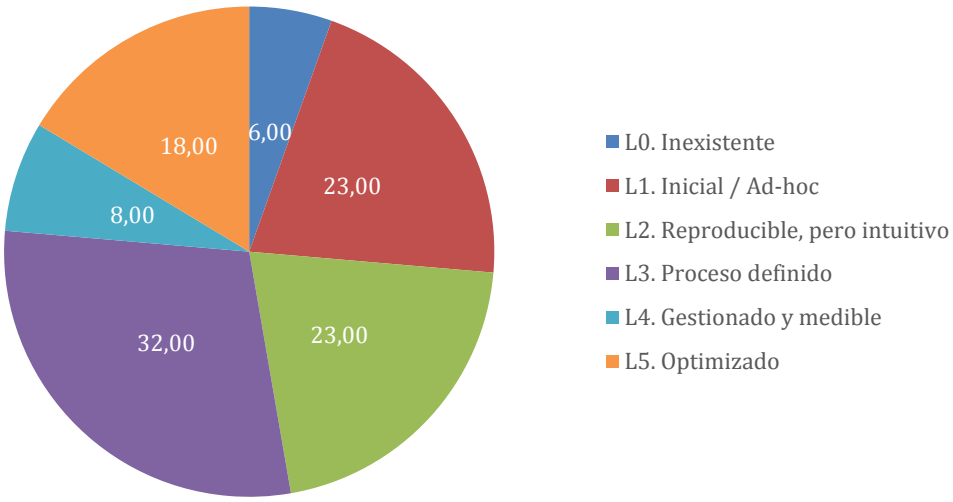


Ilustración 29 Modelo de madurez CMM de los controles

En la Ilustración 30 se presenta una visión más detallada usando el diagrama de radar que muestra el cumplimiento por control de la norma ISO/IEC 27002:2013.

Como se puede observar y al comparar con la Ilustración 27 las políticas implementadas han generado el resultado esperado e inclusive en doce controles se ha superado su estado. No se ha presentado en ningún momento un estado inferior al actual, pero si existen hallazgos considerables que deben ser elevados a Consejo Superior para ser tratados.

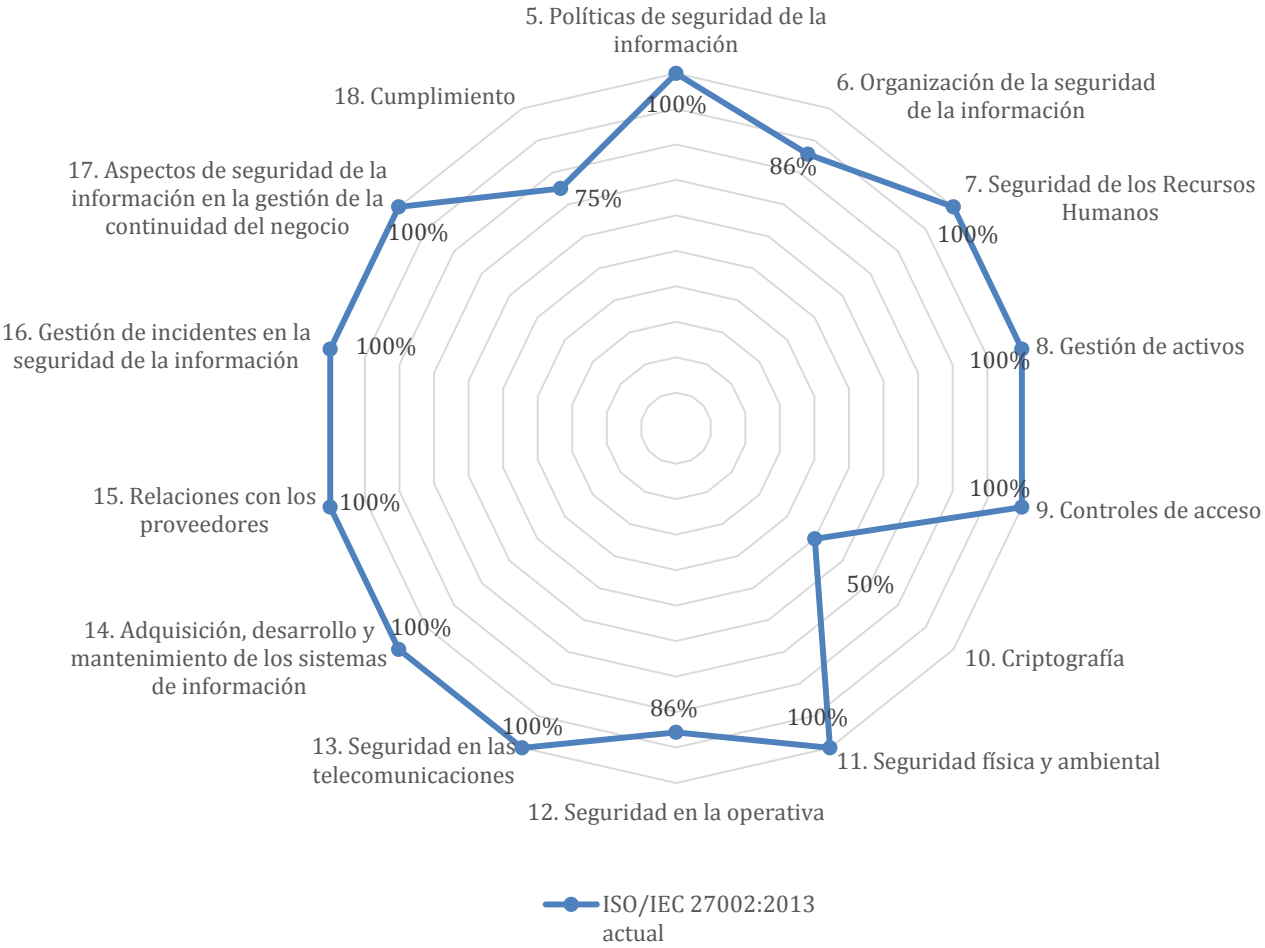


Ilustración 30 Estado de madurez CMM ISO/IEC 27002:2013

5.6 Reporte de Auditoría

Al finalizar la ejecución de la auditoría, el equipo auditor deberá transmitir sus conclusiones al Consejo Superior, mediante un informe lo más simple y directo posible, dando énfasis a la información considerada como relevante, así como los distintos hallazgos.

A continuación presento el reporte de la auditoría, en base a la Metodología de Análisis de Riesgos SGSI_PR_AR_2015-01, la Declaración de Aplicabilidad SGSI_OT_DA_2015-01 y la Gestión de Riesgos SGSI_OT_GR_2015-01.

AUDITORÍA DE CUMPLIMIENTO – REPORTING DE LA AUDITORÍA
Auditor Interno
Cuenca, Ecuador / Mayo 2015

Introducción

En el mes de marzo de 2015 el Consejo Superior decidió implementar el Sistema de Gestión de Seguridad de la Información donde se generaron cuatro propuestas de proyectos que menciono a continuación:

1. **Elaboración y divulgación de las políticas de Seguridad de la Información:** Ante los riesgos identificados se vio la necesidad de implementar tres políticas, adicional a las ya establecidas por la IES. Además se incluyó la divulgación de las políticas de Seguridad de la Información.

2. **Plan de concienciación (capacitación y formación del personal):** Se han generar seis capacitaciones por la falta de conocimiento y/o concienciación que posee el personal académico y/o administrativo de la IES, en materia de políticas de seguridad de la información.

3. **Plan de virtualización de servidores:** Se estableció un plan de virtualización de servidores como respuesta a la caída del sistema por agotamiento de recursos y la denegación de servicios.

4. **Plan de continuidad:** A pesar de haber implementado todos los controles en base a la norma ISO/IEC 27000, es recomendable poseer un plan de continuidad ante situaciones que no se puedan evitar. La IES ha implementado el Plan de continuidad de Desarrollo de Sistemas de Información y el Plan de continuidad de Redes e Infraestructura.

Objetivo

El objetivo principal fue revisar y analizar los controles, sistemas, procedimientos y políticas en materia de seguridad de la información, a fin de verificar el estado de implementación del Sistema de Gestión de Seguridad de la Información en base a la norma ISO/IEC 27001:2013 realizado entre el 05 de marzo de 2015 y el 28 de mayo de 2015.

Alcance

La presente auditoría se rigió a la verificación del estado de cumplimiento de los controles de seguridad de la norma ISO/IEC 27002:2013 en base a la declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información y las políticas propuestas.

Visión general de la metodología

Cada control fue evaluado usando la metodología de madurez CMM, donde se comparó el estado previsto con el estado actual. Los insumos usados fueron normativa interna y externa, procedimientos, estándares, normas, los registros respectivos, informes, actas y cualquier otro documento que respalde la actividad.

A continuación se presentan las desviaciones identificadas en la IES:

No conformidad mayor:

- 6.2.1 Política de dispositivo móvil: No existe una Política de dispositivo móvil.
- 9.4.3 Gestión de contraseñas de usuario: No existe una política particular o dentro del documento Política de Control de Acceso SGSI_PO_SI_2015-01 una sección específica sobre la gestión de las contraseñas.
- 10.1.1 Política sobre el uso de controles criptográficos: No existe una política particular para el uso de controles criptográficos.
- 11.2.5 Salida de activos fuera de las dependencias de la empresa, 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones: Dentro de la Política de manejo de activos no existe una norma o artículo donde se legisle dicho proceso.

No conformidad menor:

- 7.2.2 Concienciación sobre la seguridad de la información, la educación y la formación: Existe el proyecto de cada una de las capacitaciones, pero no se ha contratado a la Empresa Capacitadora.
- 7.2.3 Proceso disciplinario: Existe el Reglamento respectivo pero se incumple con el artículo de sanciones graves.
- 8.3.1 Gestión de soportes extraíbles: Se incumple con un punto del procedimiento donde se indica el uso de las plantillas.
- 11.1.2 Controles físicos de entrada: Se ha evidenciado que existe problemas con el control de geometría de la mano.
- 18.1.4 Protección de datos y privacidad de la información personal: Los empleados no conocen sobre la Política para la Protección de los datos personales.

Observación:

- 5.1.2 Revisión de las políticas de seguridad de la información: Existe un plan de revisión de las políticas de seguridad de la información con su respectiva planificación, pero no se ha ejecutado.
- 8.1.3 Uso aceptable de los activos: Se recomienda actualizar el proceso de gestión para el uso y procesamiento de la información y los activos.
- 9.2.5 Revisión de los derechos de acceso de los usuarios: Los listados de acceso a nivel de red no son considerados.
- 14.2.2 Procedimientos de control de cambios en los sistemas: El Responsable de Seguridad de Información conjuntamente con el Director del Departamento de TIC deberían elevar la propuesta al Consejo Superior para su aprobación.

Oportunidad de mejora:

- 7.3.1 La terminación o el cambio de las responsabilidades laborales: Se recomienda que el proceso sea traducido como una política de la IES.
- 8.2.3 Manipulación de los activos: Se recomienda revisión del procedimiento ya que se encuentra alineado al documento SGSI_PO_Si_2015-01 Política de Clasificación de la Información.
- 8.3.2 Eliminación de los soportes: Se recomienda dentro de la propuesta de proyectos incluir la Capacitación sobre la eliminación de los soportes.
- 9.4.4 Uso de programas de servicios públicos privilegiados: Se recomienda que dicho control sea revisado y actualizado.

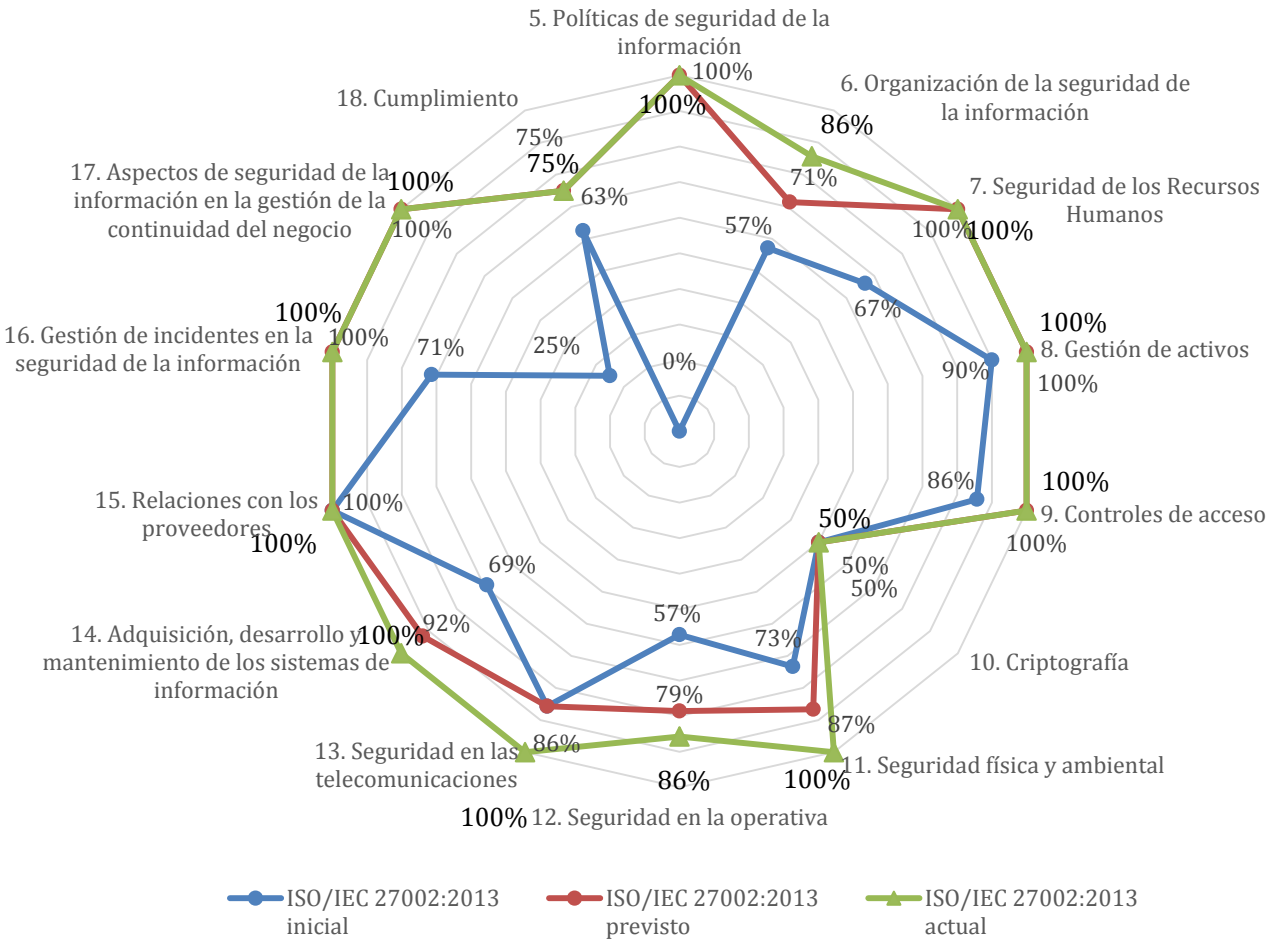
- 11.2.3 Seguridad del cableado: A pesar de que existen las normas establecidas. No todas las instalaciones cuentan con cableado estructurado.
- 12.6.1 Gestión de las vulnerabilidades técnicas: Se recomienda incluir dentro del documento SGSI_PR_RR_2015-01 al responsable de dicha tarea.
- 16.1.5 Respuesta a incidentes de seguridad de la información: A pesar de que existe el proceso establecido no todos los empleados responden en base al procedimiento.
- 18.1.2 Derechos de propiedad intelectual (DPI): Se recomienda incluir en el Plan de Concienciación una capacitación sobre propiedad intelectual.

Conclusiones

En base a la información presentada en el apartado anterior y el documento SGSI_OT_GR_2015-01, puedo concluir que el 28% de controles se encuentran con un proceso definido y ejecutado en donde la IES participa en el proceso, por lo tanto las capacitaciones planteadas han dado buenos resultados, mientras que el 20% se encuentra en un estado inicial /ad-hoc y reproducible pero intuitivo, esto se debe a que el mismo personal está generando políticas, lo cual es positivo, ya que tratan de generar sus procedimientos, que obviamente posterior deberán ser elevados al Consejo Superior para su aprobación.

El 16% de procesos se encuentran en un estado optimizado, es decir, se encuentran bajo constante mejora. Otro punto positivo a considerar, es que únicamente el 5% no posee una política establecida, estas son las conformidades mayores presentadas en el apartado anterior.

Cabe señalar, que se observó que ningún proceso tuvo una caída, es decir, el control presentaba el mismo estado o superior a lo que tenía en el estado actual al momento de inicializar el plan de implementación de la norma ISO/IEC 27001: 2013.



Recomendaciones

Se recomienda considerar la inclusión en la propuesta de proyectos la creación de las siguientes políticas, ya que no tiene ninguna información

- Política de dispositivo móvil.
- Gestión de contraseñas de usuario.
- Política sobre el uso de controles criptográficos.
- Salida y seguridad de activos fuera de las dependencias de la IES.

Sin otro particular, le agradezco su atención.

Atentamente,

Auditor
XXXXXXXXXXX

6 Fase 6: Presentación de Resultados y Entrega de Informes

6.1 Introducción

Un entregable es cualquier producto tangible o intangible elaborado como parte de un proyecto, los cuales son representados por esquemas, prototipos, análisis, sistemas, entre otros. Cabe señalar que un entregable no sólo es el producto final, sino además son los procesos, los cambios organizativos y toda información considerada primordial para que el desarrollo del plan.

Los entregables tienen que estar enmarcados entre los requisitos del plan de implementación y los objetivos definidos.

A continuación menciono los entregables a presentar:

- **Informe ejecutivo:** Se debe presentar un breve análisis de los aspectos más importantes del Plan de Implementación de la ISO/IEC 27001:2013, va antes de la presentación y es lo primero que la alta dirección revisará, por lo que debe ser concisa incluyendo la motivación, el enfoque del plan y las principales conclusiones.

- **Memoria descriptiva:** Corresponde el documento final que contiene las fases desarrolladas, con los respectivos anexos que servirán de evidencia de los resultados obtenidos.

6.2 Entregables

6.2.1 Informe Ejecutivo

INFORME EJECUTIVO
Ing. Andrea Maricela Plaza Cordero
Cuenca, Ecuador / Junio 2015

El TFM ha consistido en la elaboración de un Plan de Implementación de la ISO/IEC 27001:2013 en una Institución de Educación Superior, no se menciona el nombre por motivos de seguridad y se la trató en todo el documento como IES.

La IES está ubicada en Ecuador teniendo su matriz en la ciudad de Cuenca y sede en Quito, posee 21 años de vida institucional mediante la Ley de Creación en el Registro Oficial de la República del Ecuador. Al momento alberga aproximadamente 22453 estudiantes entre el nivel de grado y posgrado matriculados en este periodo, y 1780 empleados entre administrativos y docentes.

Al momento el Ecuador se encuentra en un estado de cambio, donde las leyes y normativas que rigen la educación han sido modificadas, teniendo la IES que acoplarse a los nuevos retos que ello implica, además la información que manejan y en su mayoría es de carácter confidencial donde la seguridad juega un papel importante, por no decir crucial. Por lo tanto, la IES está consciente que es un momento decisivo donde hay que tomar acciones encaminadas a reforzar la seguridad de la información alineadas al plan estratégico de la IES y el marco normativo vigente.

Posterior a la decisión del Consejo Superior en implementar dicho plan y brindar todo el apoyo ante el mismo, se debió identificar si se iba a trabajar con personal interno o se iba a contratar asesoría. Considerando la vida institucional de la IES y que la implementación es un proceso necesario de forma inmediata, el Consejo Superior decidió crear un Comité de Seguridad de la Información quien será el encargado del plan.

Se realizaron las reuniones de inicio del proyecto para concienciar al personal de la IES de la importancia de su implementación y de su apoyo para que su ejecución se realice correctamente, en este sentido, la decisión de que el personal interno se encargue del desarrollo del plan ha facilitado el análisis.

A continuación se presentan las fases realizadas del Plan de Implementación de la norma ISO/IEC 27001:2013:

- Se realizó el análisis diferencial (GAP Analysis) comparando los controles implantados en la IES vs los controles necesarios en base a la norma ISO/IEC 27001 e ISO/IEC 27002:2013, con el objetivo de conocer el estado actual de la IES y definir el alcance y objetivos de la implantación del Sistema de Gestión de Seguridad de la Información.

  Alcance: La implementación de la seguridad de la información se va a realizar en la matriz de la IES, que se encuentra ubicada en la ciudad de Cuenca, bajo el siguiente escenario: *La gestión de la seguridad de la información de la IES que cubre los sistemas de información Académicos, Financieros y de Recursos Humanos, la red de comunicación LAN, la seguridad en las telecomunicaciones, la parte física y ambiental, los equipos para procesamiento de datos según la declaración de aplicabilidad versión 2.*

- Posterior se definió la documentación necesaria y básica para implementar el SGSI, ya que es fundamentar disponer de una normativa común de seguridad que regule la documentación, además de identificar los documentos mínimos.

- Luego se realizó la Valoración de Activos y Dimensiones de Seguridad, donde por cada activo se estableció el valor que tendría que la amenaza sea explotada por alguna vulnerabilidad. Con esta información se procedió a identificar el nivel de riesgo aceptable, el mismo que fue Aprobado por parte del Consejo Superior según resolución.

- Implementación del Plan de gestión de riesgos, en donde se presenta una propuesta de proyectos que servirán para reducir la presencia del riesgo. La IES debe estar consciente que con dichas medidas no va a eliminar la presencia del riesgo, sino se va a controlar en caso de presencia.

Las fases fueron desarrolladas siguiendo las directrices de la norma ISO/IEC 2700:2013 y las metodologías seleccionadas. Cabe señalar, que en el desarrollo se visualizó claramente la importancia de la definición del alcance del SGSI, ya que de ello se identificaron los activos, los cuales fueron pieza fundamental para todo el proceso. Además la elección de la metodología MAGERIT a mi parecer es la correcta, ya que fue más fácil a la hora de la toma de decisiones por parte del Consejo Superior.

Cuando se han realizado todas las fases de implementación de los proyecto se determinó el estado de cumplimiento de los mismos mediante una Auditoría, que realizó personal interno de la IES. Cabe señalar que el equipo auditor no formó parte directa e indirecta del proceso de Implementación del Sistema de Gestión de Seguridad de la Información.

Los datos obtenidos de la auditoría fueron presentados al Consejo Superior, quienes serán responsables de tomar las decisiones que consideren pertinente.

A continuación presento las desviaciones identificadas en base a un conjunto de pruebas realizadas entre ellas entrevistas, encuestas, análisis de documentación interna y externa, pruebas en el sistema, entre otros.

No conformidad mayor (incumple completamente con la norma)

- No existe una Política de dispositivo móvil.

- No existe una política particular o dentro del documento Política de Control de Acceso SGSI_PO_SI_2015-01 una sección específica sobre la gestión de las contraseñas.
- No existe una política particular para el uso de controles criptográficos.
- Dentro de la Política de manejo de activos no existe una norma o artículo donde se legisle dicho proceso.

No conformidad menor (incumple un punto de un apartado de la política o norma)

- Existe el proyecto de cada una de las capacitaciones, pero no se ha contratado a la Empresa Capacitadora.
- Existe el Reglamento respectivo pero se incumple con el artículo de sanciones graves.
- Se incumple con un punto del procedimiento donde se indica el uso de las plantillas.
- Se ha evidenciado que existe problemas con el control de geometría de la mano.
- Los empleados no conocen sobre la Política para la Protección de los datos personales.

Todos los documentos fueron desarrollados bajo el manual de documentación, e información que poseía la IES en materia de seguridad fue adaptada.

Para concluir deseo señalar que todo el proceso fue tratado con cuidado y siempre alineado a la misión y visión de la IES, a su plan estratégico y la normativa vigente tanto interna como externa. La propuesta de implementación del SGSI dio a la Alta Dirección una visión sobre la importancia de la seguridad en la información, y como su apoyo y compromiso son piezas fundamentales. Se encontraban implementadas iniciativas a nivel de área y/o departamento, mas al no estar alineados a una política de seguridad, no tenían los resultados esperados y en muchas ocasiones generaban el resultado opuesto al deseado. Debo rescatar el compromiso del personal administrativo en la implementación, y como en muchas áreas y/o departamentos identifican la importancia de la seguridad de la información.

6.2.2 Memoria descriptiva

En la memoria descriptiva se incluye a detalle todo el proceso para la Implementación del Sistema de Gestión de Seguridad de la Información.

A continuación se encuentran las fases de las que está conformado:

- **Fase 1: Situación Actual: Contextualización, Objetivos y Análisis Diferencial:** Descripción la situación actual de la IES según la normativa ISO/IEC 27001:2013 e ISO/IEC 27002:2012.

- **Fase 2: Sistema de Gestión Documental:** Establecimiento de la documentación básica inicial para implementar el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001.

- **Fase 3: Análisis de Riesgos:** Identificación de los activos de la IES, las vulnerabilidades y amenazas a las que se encuentra expuesto.

- **Fase 4: Propuestas de Proyectos:** Definición e implementación de los controles adecuados, con los responsables y el presupuesto, con el objetivo de evitar los daños intrínsecos al factor de riesgo.

- **Fase 5: Auditoría de Cumplimiento:** Verificación de los controles, realizado por un auditor con el fin de comprobar si se han cumplido el objetivo establecido.

6.2.3 Presentaciones

- **Presentación inicial a la IES:** Presentación antes de abordar el Plan de Implementación del SGSI donde se establecen las claves del mismo y se expone la importancia de su implementación.

- **Presentación del estado de cumplimiento de los controles de seguridad:** Presentación donde se establece el estado de cumplimiento de los controles de seguridad en la IES, que posterior serán los objetivos a cumplir

  El objetivo de la presentación es servir de base para la aprobación de los proyectos propuestos.

- **Presentación final a la IES:** Presentación donde se expone el plan a realizar, los aspectos organizativos, el plan de acción, los principales resultados del estudio y el resumen del cumplimiento e impacto de la ejecución de los proyectos.

Definición de términos

Activo: Son los elementos que posee la Organización y que deben protegerse.

Alcance de la auditoría: Es el acuerdo mutuo entre auditor y auditado sobre qué se va a realizar en la auditoría.

Amenaza: Son todo tipo de situaciones que podrían suceder en la Organización y que afectarían a los activos, provocando que éstos no funcionen correctamente.

Análisis de riesgo intrínseco: Estudio que se realiza sin tener en consideración las medidas de seguridad implantadas en la Organización.

Análisis de riesgo residual: Estudio que se realiza teniendo en consideración las medidas de seguridad implantadas en la Organización.

Análisis de Riesgos: Proceso de identificación de los riesgos, determinando la magnitud y las áreas que requieren las medidas de protección

Análisis Diferencial: Es un análisis de los controles implantados vs controles necesarios según la norma ISO 27001:2005, dando como resultado el análisis de la madurez.

Auditado: Es la Empresa a la que se va a auditar.

Auditor/Equipo auditor: Es el grupo de personas que van a ejecutar la auditoría.

Auditoría interna: Son ejecutadas por el equipo auditor que puede estar formado por personal de la Empresa o un equipo externo. El destinatario final de los resultados es la Empresa.

Business Impact Analysis (BIA): Proceso que consiste en identificar los procesos relacionados con la misión de la IES y analizar el impacto en la gestión comercial de la Empresa que provocaría la interrupción de los mismos por un incidente.

Carta de Asignación de Auditoría: Documento donde se describe la asignación de las tareas que el equipo auditor tiene que realizar.

COBIT (Objetivo de control para la información y tecnologías relacionadas): Es un modelo desarrollado por ISACA para auditar la gestión y control de los sistemas de información y tecnología.

Consejo Superior: Es el máximo órgano colegiado académico y administrativo de cogobierno, responsable de asegurar el cumplimiento de la misión y visión institucionales.

Control o salvaguarda: Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

Cuadro de mando: Es una herramienta de gestión que facilita la toma de decisiones, ya que recoge el conjunto de indicadores que sirven a la alta dirección dar una visión del estado de la seguridad de la información.

Evidencia de auditoría: Conjunto de registros, declaraciones de un hecho u otra información que se obtenga durante el proceso de auditoría que deberá cumplir con las características de ser verificable, pertinente y objetivo.

Hallazgos de la auditoría: Es el resultado de la evaluación de la evidencia de la auditoría frente a los criterios de la auditoría.

Impacto: Son las consecuencias que se producen cuando una amenaza aprovecha la vulnerabilidad de la Organización para dañar el activo.

Incidente: Es una violación o amenaza a la Política de Seguridad de la información, mediante una serie de eventos indeseados inesperados que amenazan la seguridad de la información.

ISO/IEC 27000: Revisión de los estándares de la serie 27000.

ISO/IEC 27001: Especificaciones para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

ISO/IEC 27002: Es el código de buenas prácticas en la gestión de la seguridad de la información.

ISO/IEC 27004: Especificación de las técnicas y métricas de medida aplicables para determinar la eficacia del SGSI y de los controles relacionados.

MAGERIT: Es una metodología de Análisis y Gestión de Riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica.

PDCA (plan-do-check-act): El ciclo Deming o más conocido como el círculo de vicios, es un método de mejora continua de la calidad.

Plan de Auditoría: Documento donde se encuentran las decisiones más importantes sobre la estrategia para el desarrollo de la auditoría de gestión.

Plan de continuidad del negocio: Documento donde se plasman los mecanismos que la institución va a seguir en caso de que falle el sistema.

Política de seguridad de la información: Establece los principios y líneas de actuación globales en materia de seguridad de la información, alineados a los objetivos del negocio.

Pruebas de cumplimiento: Tienen como objetivo comprobar si se implementan los controles tal y como se indican en la normativa de referencia.

Recovery Point Objective (RPO): Se refiere a la cantidad de información que la Empresa considera tolerable de pérdida ante un incidente, lo cual dependerá del volumen de transacciones por tiempo y los mecanismos de backup.

Recovery Time Objective (RTO): se refiere al tiempo que una Empresa puede permitir la falta de funcionamiento de sus procesos sin afectar la continuidad del negocio, lo cual dependerá de la criticidad de cada proceso o aplicación.

Riesgo: Es la medida de la posibilidad para que se materialice la amenaza.

Salvaguarda: Es un mecanismo de protección frente a las amenazas, existen diferentes tipos dependiendo si se desea prevenir o corregir un incidente.

Seguridad de la Información: Se ocupa de la seguridad de la información en todas sus formas y en cualquier momento de su ciclo de vida.

Seguridad Informática: Se ocupa de la seguridad de los sistemas de información.

Sistema de Gestión de Seguridad de la Información (SGSI): Es un **c**onjunto de políticas y acciones relacionadas entre sí que permiten alcanzar el objetivo en materia de seguridad de la información.

Vulnerabilidad: Son las diferentes debilidades que presentan los activos de la Organización y que los hacen susceptible a amenazas.

Bibliografía citada

CES. (2013). Reglamento de Régimen Académico. Ecuador.
Electrónica, C. S. (s.f.). MAGERIT v3.0.
IES. (2013). Plan Estratégico. Ecuador.
IES. (2014). Reglamento Interno de Régimen Académico. Ecuador.
ISACA. (s.f.). Control Objectives for Information and related Technology.
Ley Orgánica de Educación Superior. (2012). Ecuador.
Norma ISO/IEC 27000:2014. (15 de Enero de 2014). Tercera, 38.
Norma ISO/IEC 27001:2013. (1 de Octubre de 2013). Segunda, 30.
Norma ISO/IEC 27002:2013. (1 de Octubre de 2013). Segunda, 90.
Norma ISO/IEC 9000:2005. (2005).

Anexos

Anexo 01 AnalisisDiferencial_27K (SGSI_OT_AD_2015-01)
Anexo 02 Manual de Documentación (SGSI_MA_DO_2015-01)
Anexo 03 Política de Seguridad (SGSI_PO_SI_2015-01)
Anexo 04 Procedimiento de Auditorías Internas (SGSI_PR_AI_2015-01)
Anexo 05 Gestión de Indicadores (SGSI_PR_I_2015-01)
Anexo 06 Procedimiento de Revisión por la Dirección (SGSI_PR_RD_2015-01)
Anexo 07 Gestión de Roles y Responsabilidades (SGSI_PR_RR_2015-01)
Anexo 08 Metodología de Análisis de Riesgos (SGSI_PR_AR_2015-01)
Anexo 09 Declaración de Aplicabilidad (SGSI_OT_DA_2015-01)
Anexo 10 Análisis de Riesgos (SGSI_OT_AR_2015-01)
Anexo 11 Plan de Gestión de Riesgos (SGSI_OT_GR_2015-01)
Anexo 12 Auditoría de Cumplimiento (SGSI_OT_AC_2015-01)
Anexo 13 Presentación Inicial a la IES (EstadoInicial-TFM-AndreaPlazaCordero)
Anexo 14 Presentación del Estrado de Cumplimiento de los Controles de Seguridad de la Información (EstadoCumplimiento-TFM-AndreaPlazaCordero)
Anexo 15 Presentación Final a la IES (EstadoFinal-TFM-AndreaPlazaCordero)