ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

“IMPLEMENTACIÓN DE LA NORMA ISO 27001 PARA GESTIÓN EN SEGURIDAD DE INFORMACIÓN. CASO PRÁCTICO DESITEL”

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA EN SISTEMAS INFORMÁTICOS

PRESENTADO POR:

LUCIA VERÓNICA GUEVARA ESPINOSA

RIOBAMBA – ECUADOR

2012

AGRADECIMIENTO

Quiero agradecer primeramente a Dios por que con su bendición me dio la oportunidad de estar culminando mi carrera profesional.

El agradecimiento infinito a mis maestros, amigos por su cariño, comprensión y ayuda incondicional a lo largo de mis días.

DEDICATORIA

A mi Padre y Madre que sin su ayuda, su apoyo incondicional y su gran amor no podría alcanzar mis sueños.

A mis hermanos Luis, Pablo, Eliana, que han sido mis mejores consejeros y amigos a los ángeles que me acompañan Daniela, Elián, Micaela y tu que estas por llegar.

Y sobre todo a la razón de vida y la luz de mi camino Luis Alejandro.

FIRMAS DE RESPONSABILIDAD

	FIRMA	FECHA
Ing. Iván Menes **DECANO DE LA FACULTAD INFORMÁTICA Y ELECTRÓNICA**	.....	.....
Ing. Raúl Rosero **DIRECTOR DE LA ESCUELA INGENIERÍA EN SISTEMAS**	.....	.....
Ing. Gloria Arcos **DIRECTORA DE TESIS**	.....	.....
Ing. Eduardo Villa **MIEMBRO DEL TRIBUNAL**	.....	.....
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	.....	.....

"Yo, LUCÍA VERÓNICA GUEVARA ESPINOSA soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

Lucia Verónica Guevara Espinosa

ÍNDICE DE ABREVIATURAS

DESITEL	Departamento de Sistemas y Telemática
DOC	Documento
DPI	Derechos de propiedad intelectual
ESPOCH	Escuela Superior Politécnica de Chimborazo
IEC	Comisión Electrotécnica Internacional
ISO	Organización Internacional de Normalización
COBIT	Information System and Audit Control Association
SECURIA	Herramienta integral que cubre el proceso automático
TI	Tecnologías de la información
BSI	British Standard Institute
MAGESID	Metodología Aplicada a la Gestión de la Seguridad de la Información en el DESITEL.
PDCA	Plan(Planificar), Do(Hacer), Check (Verificar), Act (Actuar)
SGSI	Sistema de Gestión de Seguridad de la Información

ÍNDICE DE TÉRMINOS

ACTIVO	Cualquier cosa que tenga valor para la empresa.
PROCEDIMIENTOS	Se definen como la manera especifica de desempeñar una actividad o un proceso
REGISTROS	Son evidencias objetivas, que pueden mostrar a terceros que un requerimiento indicado ha sido implementado.
POLÍTICAS	Son directrices que rigen la actuación de una persona o entidad
DISPONIBILIDAD	Propiedad de estar accesible y utilizar baja demanda de una entidad autorizada.
CONFIDENCIABILIDAD	Propiedad que la información no esta disponible o divulgada a individuos.
SEGURIDAD DE INFORMACIÓN	Preservación de la confidenciabilidad, integridad y disponibilidad de la información.
SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN	Parte del sistema de gestión global, basada en un enfoque del riesgo del negocio para establecer, implementar, operar, realizar seguimientos, revisar, mantener y mejorar la seguridad de la información.
INTEGRIDAD	Propiedad de salvaguardar la exactitud y la totalidad de los activos
ANÁLISIS DE RIESGO	Utilización sistemática de la información para identificar las fuentes y estimar el riesgo.
GESTIÓN DE RIESGO	Actividad coordenada para dirigir y controlar una organización con respecto al riesgo.

INTRODUCCIÓN

Hoy en día, dada la competencia que la globalización y las nuevas reglas del comercio internacional han generado en las empresas en su desarrollo para ser creativas e innovadoras para poder mantenerse en los mercados y poder aumentar su competitividad.

El problema es muy serio. En el siglo XXI cuando la gestión del conocimiento es una característica vital en las empresas se debiera tener formas de poder minimizar ese riesgo de que la información se filtre, se altere o simplemente no esté disponible. cuando se requiera.

La seguridad de la información es una manera preventiva y confiable para se puede utilizar para lograr salvaguardar la información, es decir en nuestro caso la implementación de la Norma ISO 27001 para la Gestión en Seguridad de la Información, caso practico DESITEL.

El Departamento de Sistemas y Telemática por estar en constante crecimiento tecnológico y sabiendo la entrada de información es muy importante para la ESPOCH se ve necesario proteger la información de la misma por que se deberán identificar los activos a hacer un análisis para obtener las posibles opciones de tratamiento para lograr que estas amenazas no puedan causar daño y no penetren en la organización.

La presente cuenta con cuatro capítulos. El primero constará de: la problemática, los antecedentes, justificación, objetivos, y la hipótesis planteada.

El segundo capítulo consta de: un análisis de la guía metodológica, definición de un SGSI, ventajas y desventajas del uso de SGSI, Estándares de la gestión de Seguridad, definición de las Norma ISO 27001, las ventajas de la misma norma y los beneficios de la certificación bajo la norma ISO 27001.

El tercer capítulo consta de la propuesta de una metodología que permita el uso de la norma ISO 27001 en el sistema de gestión de seguridad en los procesos del DESITEL

El cuarto capítulo consta de la implementación de la Norma ISO 27001 en los procesos mas críticos del DESITEL, el análisis y demostración de la hipótesis.

La estructura de este trabajo nos mostrará que una vez utilizado la metodología con el uso de la Norma ISO 27001 se logrará mejoras en la gestión en seguridad de la información que maneja el Departamento de Sistemas y Telemática.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLA

CAPÍTULO I

MARCO REFERENCIAL

En dicho capítulo se explicará la problemática de la investigación

1.1 PROBLEMATIZACIÓN

Departamento de Sistemas y Telemática posee en la actualizad un Data Center ubicado en el cual existen controles de la seguridad de la información de manera específica que permiten realizar un sistema de seguridad en diferentes áreas sean estas: Servidores, Base de Datos, equipo de cómputo, etc. Pero cuanto mayor es el valor de la información gestionada, más importante es asegurarla.

Por lo tanto, es necesario trata estos valores de información por medio de un sistema de gestión de seguridad de la información y en este caso bajo la Norma ISO 27001, la cual nos indica cómo se debe manejar estos activos, como documéntalos de tal manera que nos ayude a seguir procedimientos para proteger y manejar de manera técnica y responsable la información.

1.2 ANTECEDENTES

La información es una de las partes más importantes que posee una organización o empresa y por lo tanto esta debe ser manejada de una manera adecuada sea en su integridad como en su seguridad.

La información manejada y procesada en el Departamento de Sistemas y Telemática de la ESPOCH por medio de software, documentación u otras entradas que requieren ser procesadas adecuadamente en el departamento se gestionan actualmente sin una visión para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), visión que puede ser alcanzada a través de la implementación de la certificación ISO 27001 en el departamento.

En la Escuela Superior Politécnica de Chimborazo, el Departamento de Sistemas y Telemática, cuenta con un Data Center con las siguientes características generales:

EQUIPAMIENTO DEL DATA CENTER DE LA ESPOCH

El equipamiento del Data Center de la ESPOCH consiste en[1]:

- ✓ *Sistema de piso falso.*- El sistema consiste de paneles completamente metálicos recubiertos con vinyl antiestático, y con un sistema de bases y soportes metálicos antisísmico.
- ✓ *Sistemas de detección y extinción de incendios*.- es del tipo por inundación total, con agente limpio para áreas ocupadas (seguro cuando existen personas al interior en caso de descargas).
- ✓ *Racks de equipos y accesorios.*- existen 5 racks de marca APC.
- ✓ *Tablero de distribución eléctrica*.- gabinete metálico con puerta, doble fondo corredizo, base metálica, es alimentado por su respectiva acometida, existen breakers de

[1] Tesis de Grado MAGESID, pág. 16

alimentación para el UPS de 30 KVA, breaker de bypass y de salida de UPS, además tiene dos distribuidores de energía.

- ✓ *Sistema de control de accesos*.- sistema computarizado para tener control total de la entrada y salida del personal a un área específica.

La información puede existir en muchas formas. Puede estar impresa en papel, almacenada electrónicamente, transmitida por correo utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación, etc.

Cualquiera sea la forma que adquiere la información a los medios por los cuales se distribuye o almacena siempre debe ser protegida en forma adecuada.

1.3 JUSTIFICACIÓN

Siendo parte y testigos del gran auge tecnológico de las dos últimas décadas y sobre todo en el área del procesamiento de datos existe la motivación a buscar soluciones, eficientes, y de gran impacto.

Unas de las maneras para tratar a la información es certificarla pero para lograr esto necesitamos de investigar formatos, procesamientos y manuales que nos permitan realizar un tratamiento correcto y lograr la certificación bajo la Norma ISO 27001.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados

voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

El estudio esta basado en los dominios de organización de la seguridad de la información, seguridad física y del entorno, control de acceso y gestión de incidentes de

seguridad[2] documentada y conocida por todos, que se revisa y mejora constantemente como indica la figura I.1.

Figura I.1 Ciclo de análisis del SGSI

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Desarrollar la Norma ISO 27001 para la gestión de seguridad en información para el DESITEL.

1.4.2 OBJETIVO ESPECÍFICO

- Analizar la guía metodológica de implementación de normas en la gestión de la información del Departamento de Sistemas y Telemática.
- Levantamiento y selección de procesos críticos más recurrentes en el DESITEL.
- Definir, desarrollar políticas y manuales para procesos que garanticen el cumplimiento de la seguridad de la información en el DESITEL.

[2] Tesis, MAGESID, pág. 53

- Implementar las políticas y manuales necesarios en los procesos más recurrentes del DESITEL.

1.5 HIPÓTESIS

El cumplimiento de políticas y manuales basados en la Norma ISO 27001, permitirán incrementar la gestión de seguridad en la información (SGSI) en el DESITEL.

CAPÍTULO II

MARCO TEÓRICO

A continuación se presenta el marco teórico de la investigación con el objetivo de dar el sustento al trabajo de investigación a realizar.

2.1 ANÁLISIS DE LA GUÍA METODOLÓGICA EXISTENTE.

La Guía metodológica existente en el DESITEL es un documento de tipo TESIS en que está estipulado es cada uno de los capítulos la siguiente información:

En su primer capítulo cuenta con la problemática del tema es decir antecedentes, justificación del trabajo, objetivos, etc.

En su segundo capítulo nos muestra la sustentación teórica que posee el trabajo y los conceptos, términos y definiciones referentes al trabajo.

En el capítulo tercero cuenta con la estructura básica para realizar la metodología para un SGSI.

En el capítulo cuarto nos da el desarrollo de la metodología con sus fases para lograr estipular los controles que pertenecen a una empresa en este Caso para el DESITEL

La elaboración de una metodología para un SGSI (Sistema de Gestión de Seguridad de la Información) no prueba que una organización sea 100% segura. La seguridad completa no existe, no obstante la adopción de un SGSI proporciona innegablemente ventajas.

Por lo tanto, es necesario elaborar una Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información que permita garantizar la información de una manera amplia de tal forma que involucre toda la información del Departamento, a través de la especificación de las políticas a desarrollar de forma documentada.

Se muestra una metodología estructurada, orientada a la seguridad de la información que reconoce un proceso para implantar, mantener y administrar la seguridad de la información.

Tabla I.I
Dominios de la metodología para SGSI

DOMINIOS	
1	Política de Seguridad
2	Organización de la seguridad de la información
3	Gestión de activos
4	Seguridad de los Recursos Humanos
5	Seguridad física y del entorno
6	Gestión de comunicaciones y operaciones
7	Control de acceso
8	Adquisición, Desarrollo y mantenimiento de sistemas.
9	Gestión de incidentes de seguridad
10	Gestión de continuidad del negocio
11	Cumplimiento

A

continuación los principales objetivos de cada uno de los dominios:

1. **Política de seguridad**: Este grupo está constituido por dos controles:
   - ✓ **Política de seguridad:** (Nivel político o estratégico de la organización): Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.
   - ✓ **Plan de Seguridad:** (Nivel de planeamiento o táctico): Define el "Cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones puntuales que se deberán cumplir.
2. **Organización de la seguridad de la información**: Este segundo grupo de controles abarca once de ellos y se subdivide en:
   - ✓ **Organización Interna:** Compromiso de la Dirección, coordinaciones, responsabilidades, autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.
   - ✓ **Partes externas:** Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios del negocio.
3. **Gestión de activos**: Este grupo cubre cinco controles y se encuentra subdividido en:
   - ✓ **Responsabilidad en los recursos:** Inventario y propietario de los recursos, empleo aceptable de los mismos.
   - ✓ **Clasificación de la información:** Guías de clasificación y denominación, identificación y tratamiento de la información.
4. **Seguridad de los recursos humanos**: Este grupo cubre nueve controles y se encuentra subdividido en:

- ✓ **Antes del empleo:** Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.
- ✓ **Durante el empleo:** Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias. .
- ✓ **Finalización o cambio de empleo:** Finalización de responsabilidades, devolución de recursos, revocación de derechos.

5. **Seguridad física y del entorno**: Este grupo cubre trece controles y se encuentra subdividido en:

- ✓ **Áreas de seguridad:** Seguridad física y perimetral, control físico de entradas, seguridad de locales edificios y recursos, protección contra amenazas externas y del entorno, el trabajo en áreas de seguridad, accesos públicos, áreas de entrega y carga.
- ✓ **Seguridad de elementos:** Ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

6. Gestión de comunicaciones y operaciones:

Este grupo comprende treinta y dos controles, es el más extenso de todos y se divide en:

- ✓ **Procedimientos operacionales y responsabilidades**: Tiene como objetivo asegurar la correcta y segura operación de la información, comprende cuatro controles. Hace especial hincapié en documentar todos los procedimientos,

manteniendo a los mismos y disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar uso inadecuado de los mismos.

- ✓ **Administración de prestación de servicios de terceras partes**: Abarca tres controles, se refiere fundamentalmente, a los casos en los cuales se encuentran asignadas determinadas tareas o servicios del sistema informático.
    - Planificación y aceptación de sistemas
    - Protección contra código móvil y maligno
    - Administración de la seguridad de redes
- ✓ **Manejo de medios:** El objetivo de este grupo es, a través de sus cuatro controles, prevenir la difusión, modificación, borrado o destrucción de cualquiera de ellos o lo que en ellos se guarda.
- ✓ **Intercambios de información**: Este grupo contempla el conjunto de medidas a considerar para cualquier tipo de intercambio de información, tanto en línea como fuera de ella, y para movimientos internos o externos de la organización.
- ✓ **Servicios de comercio electrónico**: Este grupo, supone que la empresa sea la prestadora de servicios de comercio electrónico, es decir no aplica a que los empleados realicen una transacción, por parte de la empresa o por cuenta propia, con un servidor ajeno a la misma.
- ✓ **Monitorización**: Este apartado tiene como objetivo, la detección de actividades no autorizadas en la red y reúne seis controles.

7. **Control de accesos**: Tiene por misión identificar que verdaderamente "sea quien dice ser" El control de acceso es posterior a la autenticación y debe regular que

el usuario autenticado acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas:

- Encauzar al usuario debidamente.
- Verificar el desvío de cualquier acceso, fuera de lo correcto.

El control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema. Para cumplir con este propósito, este apartado lo hace a través de veinte y cinco controles, que los agrupa de la siguiente forma:

- ✓ **Requerimientos de negocio para el control de accesos:** Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.
- ✓ **Administración de accesos de usuarios:** Tiene como objetivo asegurar el correcto acceso y prevenir el no autorizado y, a través de cuatro controles, exige llevar un procedimiento de registro y revocación de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizando periódicas revisiones a intervalos regulares, empleando para todo ello procedimientos formalizados dentro de la organización.
- ✓ **Responsabilidades de usuarios**: Todo usuario dentro de la organización debe tener documentadas sus obligaciones dentro de la seguridad de la información de la empresa. Independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información.
- ✓ **Control de acceso a redes**: Todos los servicios de red deben ser susceptibles de medidas de control de acceso; para ello a través de siete controles, en este grupo, se busca prevenir cualquier acceso no autorizado a los mismos.

- ✓ **Control de acceso a sistemas operativos:** El acceso no autorizado a nivel sistema operativo presupone uno de los mejores puntos de escalada para una intrusión; de hecho son los primeros pasos de esta actividad, pues una vez identificados los sistemas operativos, versiones y parches, se comienza por el más débil y con solo conseguir un acceso de usuario, se puede ir escalando en privilegios hasta llegar a encontrar el de "root"
- ✓ **Control de acceso a información y aplicaciones**: En este grupo, los dos controles que posee están dirigidos a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura.
- ✓ **Movilidad y teletrabajo**: Esta nueva estructura laboral, se está haciendo cotidiana en las organizaciones y presenta una serie de problemas desde el punto de vista de la seguridad: Accesos desde un ordenador de la empresa, personal o público.

8. Adquisición de sistemas de información, desarrollo y mantenimiento

Este grupo reúne 16 controles.

- ✓ **Requerimientos de seguridad de los sistemas de información**: plantea la necesidad de realizar un análisis de los requerimientos que deben exigirse a los sistemas de información.
- ✓ **Procesamiento correcto en aplicaciones**: En este grupo se presentan cuatro controles cuya misión es el correcto tratamiento de la información en las aplicaciones de la empresa.

- ✓ **Controles criptográficos**: objetivo de la criptografía de proteger la integridad, confidencialidad y autenticidad de la información. En este caso, a través de dos controles, lo que propone es desarrollar una adecuada política de empleo de estos controles criptográficos y administrar las calves que se emplean de forma consciente.
- ✓ **Seguridad en los sistemas de archivos**: es que una actividad que denota seriedad profesional, es la identificación de ¿Cuáles son los directorios o archivos que no deben cambiar y cuáles sí?.
- ✓ **Seguridad en el desarrollo y soporte a procesos**: Este apartado cubre cinco controles cuya finalidad está orientada hacia los cambios que sufre todo sistema.
- ✓ **Administración técnica de vulnerabilidades**: pues cuanto antes se tenga conocimiento de una debilidad y las medidas adecuadas para solucionarlas, mejor será para la organización.

9. Gestión de los incidentes de seguridad

Todo lo relativo a incidentes de seguridad queda resumido a dos formas de proceder:

- ✓ **Seguir y perseguir**.

La norma a través de los cinco controles que agrupa, y subdivide en:

- ✓ **Reportes de eventos de seguridad de la información y debilidades**:

Define el desarrollo de una metodología eficiente para la generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas.

- ✓ **Administración de incidentes de seguridad de la información mejoras:**

  Si se poseen los dos mecanismos mencionados en el punto anterior, la siguiente tarea es disponer de una metodología de administración de incidentes, lo cual no es nada más que un procedimiento que describa claramente: pasos, acciones, responsabilidades, funciones y medidas concretas.

10. Gestión de la continuidad de negocio

Este grupo cubre cinco controles y los presenta a través de un solo grupo:

- ✓ **Aspectos de seguridad de la información en la continuidad del negocio**:

  Este grupo tiene como objetivo contemplar todas las medidas tendientes a que los sistemas no hagan sufrir interrupciones sobre la actividad que realiza la empresa.

  Lo primero que considera este grupo es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio.

11. Cumplimiento

Este grupo cubre diez controles y se subdivide en:

- ✓ **Cumplimiento de requerimientos legales**: En este apartado se detallan 6 controles dentro de estos lo primero a considerar es la identificación de la legislación aplicable a la empresa, definiendo explícitamente y documentando todo lo que guarde relación con estos aspectos.
- ✓ **Cumplimiento de políticas de seguridad:** Estándares, técnicas de buenas prácticas: En este grupo a través de **2** controles, se hace hincapié en el control del cumplimiento de estas medidas.

- ✓ **Consideraciones sobre auditorias de sistemas de información**: Las auditorias de los sistemas de información son imprescindibles, a través de sus **2** controles las dos grandes consideraciones son, realizarlas de forma externa o interna[3]

2.2 QUE ES UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados como se muestra en la figura II.1, en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

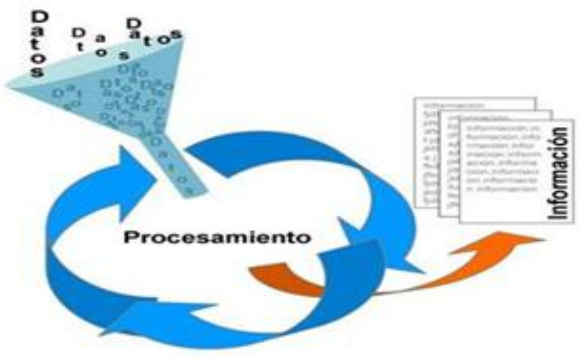


Figura II.1 Procesamiento de un SGSI

[3] Tesis, MAGESID, pág. 58

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- ✓ Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- ✓ Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- ✓ Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.2.1 NATURALEZA DE UN SGSI

Es importante comprender que el ISO 27001 se ha desarrollado como modelo para el establecimiento, la implementación, la operación, el monitoreo, la revisión y la mejora de un SGSI para cualquier clase de organización.

El diseño y la implementación de un SGSI se encuentran influenciados por las necesidades, los objetos, los requisitos de seguridad, los procesos, los empleados, el tamaño, los sistemas de soporte y la estructura de la empresa.

Cada SGSI se confecciona de la manera más adecuada para cada empresa. Eso si se debe cumplir con cada uno de los requisitos de la norma.

- ✓ El sistema de gestión de la seguridad de la información (SGSI) es la parte del sistema de gestión de la empresa, basado en un enfoque de riesgos del negocio, para:
  - Establecer,
  - Implementar,
  - Operar,
  - Monitorear,
  - Mantener y mejorar la seguridad de la información.
- ✓ Incluye.
  - Estructura, políticas, actividades, responsabilidades, prácticas, procedimientos, procesos y recueros.
- ✓ Modelo utilizado para establecer, implementar, monitorear y mejorar el SGSI.
- ✓ El SGSI adopta el siguiente modelo figura II.2:

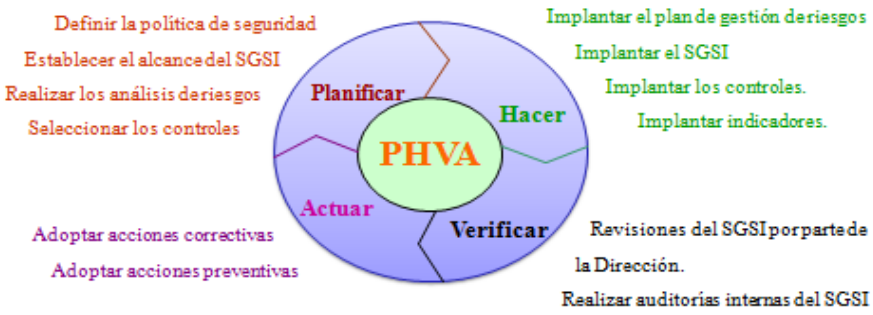


Figura II.2. Descripción del Modelo (PADCK)

2.2.2. PLAN

- ✓ Establecer la política de seguridad, objetivos, metas, procesos y procedimientos relevantes para manejar riesgos y mejorar la seguridad de la información para generar resultados de acuerdo con una política y objetivos marco de la organización.

- ✓ Definir el alcance del SGSI a la luz de la organización.

  - Definir la Política de Seguridad.

  - Aplicar un enfoque sistémico para evaluar el riesgo.

  - No se establece una metodología a seguir.

- ✓ Identificar y evaluar opciones para tratar el riesgo

  - Mitigar, eliminar, transferir, aceptar

  - Seleccionar objetivos de Control y controles a implementar (Mitigar).

  - A partir de los controles definidos por la ISO/IEC 17799

  - Establecer enunciado de aplicabilidad

2.2.3. DO (HACER)

- ✓ Implementar medidas para evaluar la eficacia de los controles

  - Gestionar operaciones y recursos.

  - Implementar programas de Capacitación y concientización.

- Implementar procedimientos y controles de detección y respuesta a incidentes

2.2.4. CHECK

- ✓ Evaluar y medir la performance de los procesos contra la política de seguridad, los objetivos y experiencia práctica y reportar los resultados a la dirección para su revisión.

- ✓ Revisar el nivel de riesgo residual aceptable, considerando:

  - Cambios en la organización.
  - Cambios en las tecnologías.
  - Cambios en los objetivos del negocio.
  - Cambios en las amenazas.
  - Cambios en las condiciones externas (ej. Regulaciones, leyes).
  - Realizar auditorías internas.
  - Realizar revisiones por parte de la dirección del SGSI.

- ✓ Se debe establecer y ejecutar procedimientos de monitoreo para:

  - Detectar errores.
  - Identificar ataques a la seguridad fallidos y exitosos.

- Brindar a la gerencia indicadores para determinar la adecuación de los controles y el logro de los objetivos de seguridad.
- Determinar las acciones realizadas para resolver brechas a la seguridad.
- Mantener registros de las acciones y eventos que pueden impactar al SGSI.
- Realizar revisiones regulares a la eficiencia del SGSI

2.2.5. ACT

- ✓ Tomar acciones correctivas y preventivas, basadas en los resultados de la revisión de la dirección, para lograr la mejora continua del SGSI.
- ✓ Medir el desempeño del SGSI.
- ✓ Identificar mejoras en el SGSI a fin de implementarlas.
- ✓ Tomar las apropiadas acciones a implementar en el ciclo en cuestión (preventiva y correctiva).
- ✓ Comunicar los resultados y las acciones a emprender, y consultar con todas las partes involucradas.
- ✓ Revisar el SGSI donde sea necesario implementando las acciones seleccionadas como la figura II.3.

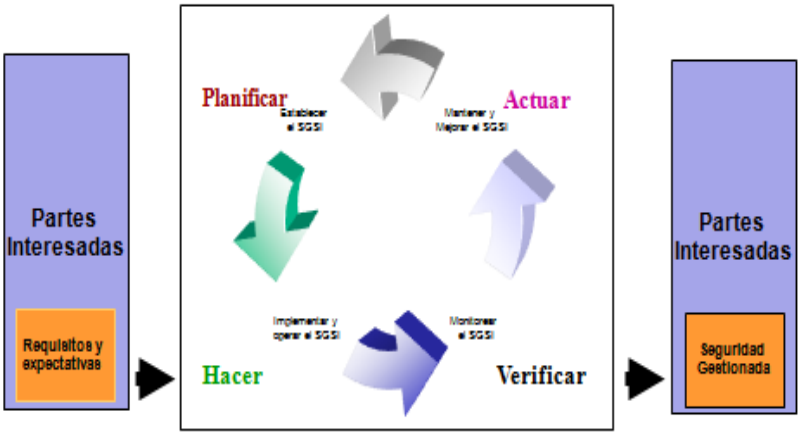


Figura II.3 Ciclo PADCK

2.2.6. VENTAJAS Y DESVENTAJAS DE USO DEL SGSI

VENTAJAS

Se debe tener en cuenta que la seguridad al 100% no existe. La norma establece una metodología y una serie de medidas que al menos busca una mejora continua y que, sin lugar a dudas, aumentará el porcentaje actual de cualquier empresa. Esta mejora en la seguridad se ve reflejada en una serie de ventajas que se describen a continuación.

COMPETITIVIDAD

Es el primer factor que le interesa a cualquier empresa. Esta norma, como se mencionó varias veces, será en el mediano plazo europeo, tan importante como hoy lo es ISO 9000. Es decir, poco a poco las grandes empresas, los clientes y partners comenzarán a exigir esta certificación para abrir y compartir sus sistemas con cualquier PyME. Es natural y lógico que así sea, pues es el único modo que

puede garantizar un equilibrio en las medidas de seguridad entre esas partes. Y para decirlo crudamente, quien no la tenga, se quedará fuera. Ahorro económico.

Las medidas contra incendios: ¿Son un coste o una inversión? ¿Cuánto vale la pérdida de información? Es muy difícil cuantificar este concepto, pero cualquier empresario que sea consciente del coste que poseen sus sistemas informáticos, sabe fehacientemente, que cualquier daño, caída, pérdida, robo, falsificación, suplantación, fallo, error, inconsistencia, virus, demora, saturación, escucha, intrusión, acceso erróneo, respuesta errónea, atentado, catástrofe… puede ser grave. Lo sabe, es más, le teme no sólo al daño concreto, sino a la pérdida potencial que esto implica: imagen, difusión, desconfianza, pérdida de negocios e inversiones, etc. La certificación reduce enormemente estas situaciones. La implementación de la norma, implica una visión de detalle de los sistemas, lo cual hará que las inversiones en tecnología se ajusten a las prioridades que se han impuesto a través del AR, por lo tanto no habrá gastos innecesarios, inesperados, ni sobredimensionados. Se evitan muchos errores o se detectan a tiempo gracias a los controles adecuados; y si se producen, se cuenta con los planes de incidencias para dar respuesta efectiva y en el tiempo mínimo. Se evita fuga de información o dependencia con personas internas y externas.

CALIDAD A LA SEGURIDAD

La implementación de un verdadero SGSI transforma la seguridad en una actividad de gestión. Este concepto por trivial que parezca es trascendente, pues deja de lado un conjunto de actividades técnicas más o menos organizadas, para transformarse en un ciclo de vida metódico y controlado. Es lo que se mencionó al

principio, pone "calidad a la seguridad", que en definitiva, "calidad" es lo que se busca y exige hoy en toda empresa seria.

REDUCE RIESGOS

Partiendo del AR que impone la norma, hasta la implementación de los controles, el conjunto de acciones adoptadas reducirá al mínimo todo riesgo por robo, fraude, error humano (intencionado o no), mal uso de instalaciones y equipo a los cuales está expuesto el manejo de información.

CONCIENCIACIÓN Y COMPROMISO

El estándar crea conciencia y compromiso de seguridad en todos los niveles de la empresa, no sólo al implantarla, sino que será permanente pues se trata de un ciclo. 136 Jamás debe olvidarse: La alta dirección, no tiene por qué tener la menor idea de los aspectos técnicos de la Seguridad Informática, lo que tiene clarísimo es la relación: Coste/Beneficio/Negocio con una visión global de la empresa. Y ahí sí sabrá elegir cuál es el mejor curso de acción, que deberá adoptar para su negocio global.

NORMAS Y ESTÁNDARES

Cumplimiento de la legislación vigente todos los aspectos de conformidades legales de la norma deben responder a la legislación del país, y se verifica su adecuación y cumplimiento. Por lo tanto la certificación garantiza este hecho y a su vez seguramente crea un marco legal que protegerá a la empresa en muchos flancos que antes no tenía cubiertos.

VISIÓN EXTERNA Y METÓDICA DEL SISTEMA

Todo el trabajo realizado para la implementación de la norma, implica una serie de medidas de auditoría interna que ofrecen ya de por sí un importante valor agregado; cada una de ellas responde a una secuencia metódica de controles. Un aspecto a considerar de este trabajo es la tensión y responsabilidad que impone al personal de la empresa, el hecho de estar pendientes de una futura certificación, como objetivo común.

A su vez, llegado el momento de la certificación, los auditores, siguiendo los mismos pasos, darán una visión externa, independiente y totalmente ajena a la rutina de la empresa, que siempre aporta muchos elementos de juicio y acciones de mejora.

SUPERVIVENCIA DE MERCADO

Según un artículo publicado en ComputerWeekly, uno de los principales motores que están llevando al incremento de certificaciones ISO 27001 está siendo la aparición en contratos de sugerencias al proveedor respecto a estar certificado en esta norma. Cada vez más contratos, al principio sólo gubernamentales pero también cada vez más en el sector privado, ya estipulan que el proveedor apropiado debería tener la certificación en ISO 27001 de Seguridad de la Información.

De hecho, algunas empresas que ya tienen la certificación ISO 27001 harán de lobby a favor de incluirlo como requisito en las ofertas de los clientes, obstaculizando a cualquier rival que no la tenga. Por tanto y como nueva

motivación, la certificación de la seguridad puede ser una oportunidad de negocio más que un coste.

DESVENTAJAS

Al iniciar este conjunto de tareas, no cabe duda que se está sobrecargando el ritmo habitual de trabajo de toda la organización, por lo tanto se debe ser consciente de que exigirá un esfuerzo adicional. Los que sufren estos incrementos son las personas, por lo tanto somos nosotros mismos los primeros en encontrarle y descubrirle las desventajas a ISO-27001, sobre todo antes de tomar la decisión de su lanzamiento, pues una vez encaminado.

NO TIENE RETORNO

Una vez que se ha empezado el camino de implementación de la norma ISO-27001, tenemos la opción de certificar o no. Sea cual fuere la elección, el cúmulo de actividades realizadas exige un mantenimiento y mejora continua, sino deja de ser un SGSI, y ello salta a la vista en el muy corto plazo. Es decir no se puede dejar de lado, pues al abandonar un cierto tiempo el SGSI, requerirá un esfuerzo similar a lanzarlo de nuevo. Si a su vez se obtiene la certificación, para que la misma se mantenga en vigencia, anualmente debe ser auditada por la empresa certificadora.

REQUIERE ESFUERZO CONTINUO

Independientemente de las tareas periódicas que implica una vez lanzado el SGSI para los administradores del mismo, el mantenimiento del nivel alcanzado,

requerirá inexorablemente un esfuerzo continuado de toda la organización al completo.

2.3. ESTÁNDARES DE LA GESTIÓN DE SEGURIDAD

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

- 1979. Publicación BS 5750 - ahora ISO 9001
- 1992. Publicación BS 7750 - ahora ISO 14001
- 1996. Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI apareció por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que estableció los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS 7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO 17799. Esta última norma se renombró como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

Figura II.4. Historia de la serie 27001

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

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

En la sección de Artículos y Podcasts encontrará un archivo gráfico y sonoro con la historia de ISO 27001 e ISO 17799 como se muestra la historia en la figura II.4.

2.4. QUE ES LA NORMA ISO 27001

La ISO 27001 es un Estándar Internacional de Sistemas de Gestión de Seguridad de la Información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información.

El objetivo fundamental es proteger la información de su organización para que no caiga en manos incorrectas o se pierda para siempre.

La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es “Organizar la seguridad de la información”, por ello propone toda una secuencia de acciones tendientes al “establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System)” (como podrán apreciar que se recalcará repetidas veces a lo largo del mismo). El ISMS, es el punto fuerte de este estándar.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

- ISMS.
- Valoración de riegos (Risk Assesment)

- Controles

VENTAJAS DEL USO DE ESTA NORMA

El hecho de certificar un SGSI según la norma ISO/IEC 27001 puede aportar las siguientes ventajas a la organización:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

Nota: las organizaciones que simplemente cumplen la norma ISO/IEC 27001 o las recomendaciones de la norma del código profesional, ISO/IEC 17799 no logran estas ventajas.

2.5. BENEFICIO DE UNA CERTIFICACIÓN BAJO LA NORMA ISO 27001

- ✓ Mejora del conocimiento de los sistemas de información, los problemas y los medios de protección.
- ✓ Mejora de la disponibilidad de los materiales y datos.
- ✓ Protección de la información.
- ✓ Diferenciación sobre la competencia y mercado.
- ✓ Algunas licitaciones internacionales empiezan a solicitar una gestión ISO 27001.
- ✓ Reducción de los costos vinculados a incidentes.
- ✓ Posibilidad de disminución de las primas de seguro.

CAPÍTULO III

PROPUESTA PARA DOCUMENTAR PROCESOS COMO SEGURIDAD DE INFORMACIÓN EN EL DESITEL.

3.1. PIRÁMIDE DOCUMENTAL DEL ISO 27001

En una organización, la documentación del modelo esta estructurada por la denominada "pirámide documental de un SGSI" como se ilustra en la figura III.1.

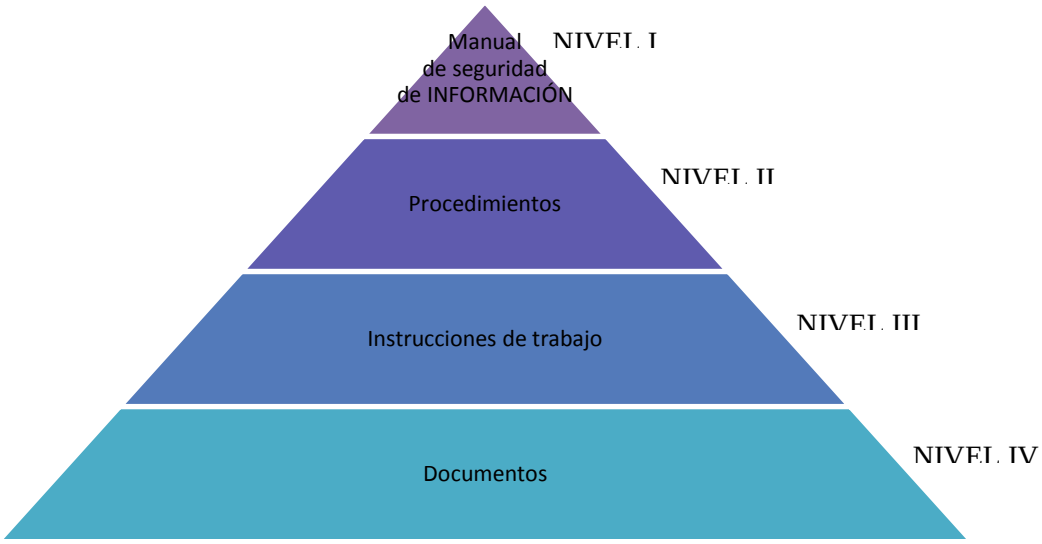


Figura III.1. Pirámide documental de un SGSI

Breve descripción de los cuatro niveles:

NIVEL I.- MANUAL DE SEGURIDAD

Es importante recalcar que el manual de seguridad de información no es un requisito del modelo. No existe clausula que lo exige, pero es una muy buena práctica tenerlo porque organiza la documentación, facilita la auditoria y agrupa la documentación considerada por el modelo ISO 2700, los aspectos básicos que un manual de seguridad debería tener son:

- Enunciados de la política del SGSI.
- Alcance del SGSI
- Procedimientos y controles de soporte.
- Descripción de la metodología de evaluación del riesgo.
- Reporte de evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Declaración de aplicabilidad.

NIVEL II.- PROCEDIMIENTOS

Aquí se realiza una breve descripción de los proceso a documentar es decir ¿Quién hace que y cuando?

NIVEL III.- INTRUCCIONES DE TRABAJO

Una vez analizados los procesos se analizará si requiere una instrucción de trabajo especificando como se realiza las tareas y actividades específicas.

NIVEL IV.- DOCUMENTOS

Aquí obtenida toda la información anteriormente recolectada el SGSI señala validar esta información y posteriormente documentarla como constancia de que se esta tratando procesos que causen algún tipo de riesgo a la Seguridad de Información.

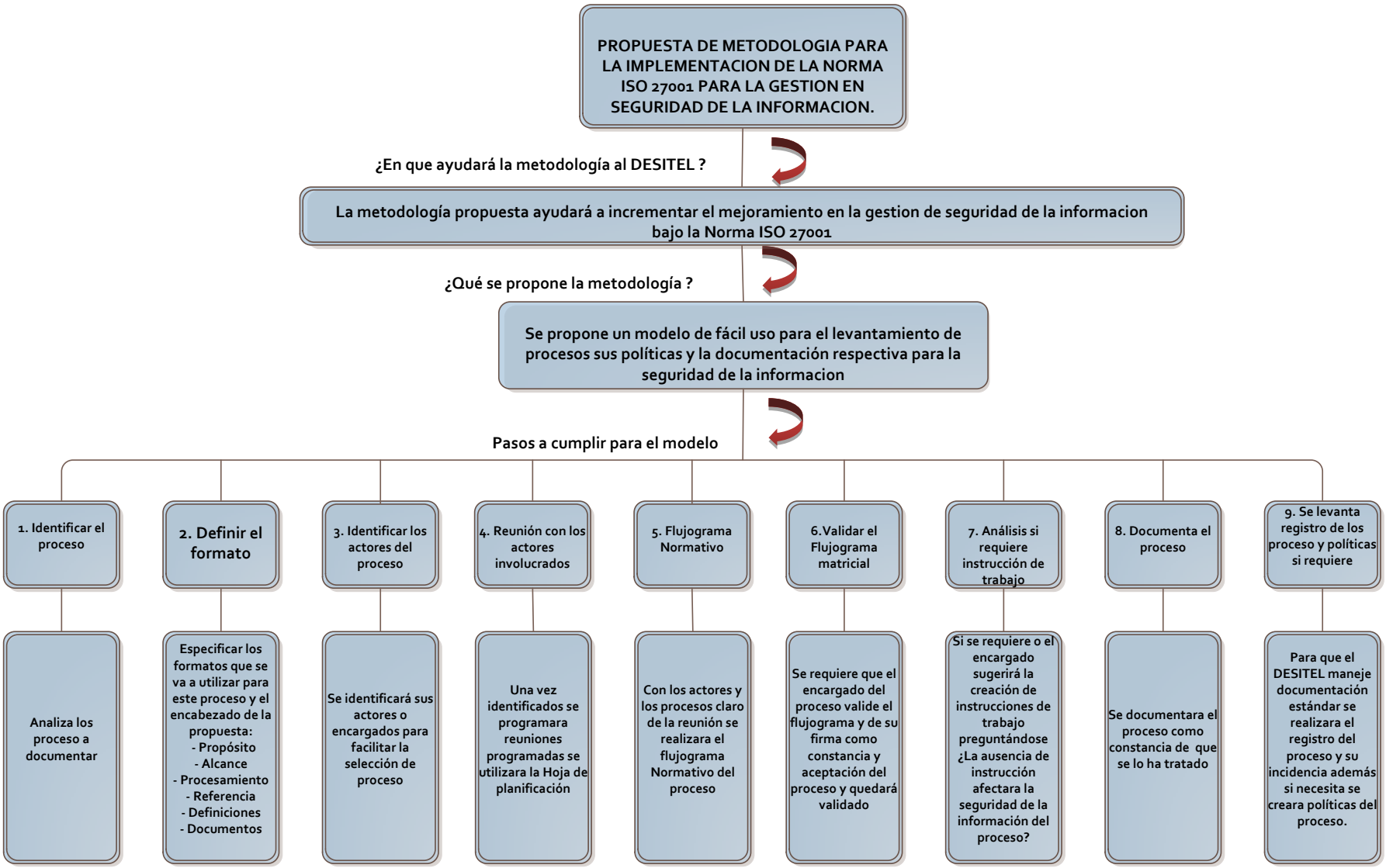


Figura III.2 Propuesta de modelo para los procesos

3.2. MODELO DE LA METODOLOGÍA PARA DOCUMENTAR LOS PROCESOS.

Para lograr una metodología exitosa en el DESITEL se necesitará implantar un modelo que permita un Sistema de Gestión de Seguridad de Información que facilite asegurar la confidencialidad, la integridad y la disponibilidad de la información y que permita su continuidad de funcionamiento en el tiempo, como se muestra la propuesta en la figura 3.3.

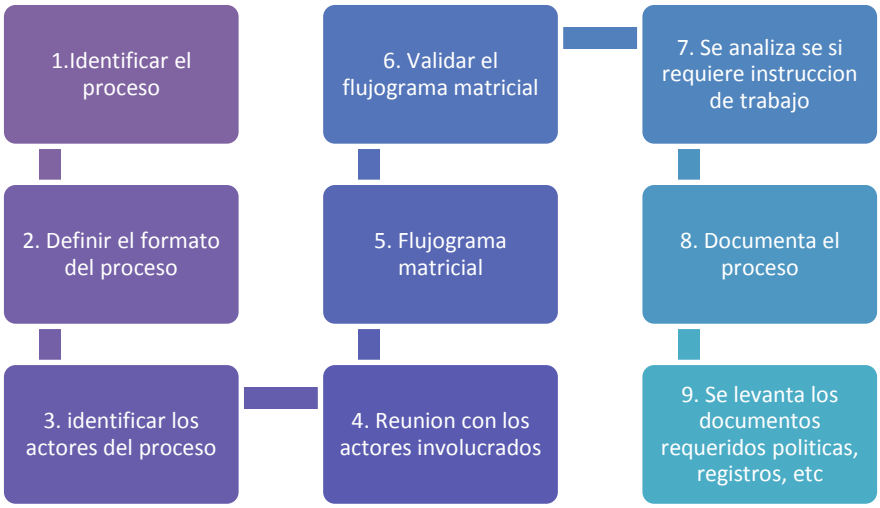


Figura III.3 Propuesta del modelo para documentar procesos.

A continuación se hará una breve explicación de cada uno de los pasos a seguir:

1. **IDENTIFICAR PROCESO DOCUMENTAR**

   Analizar los procedimientos a documentar y ponerlos en un diagrama Gantt para planificar su realización.

2. **DEFINIR EL FORMATO DEL PROCESO**

   Primeramente se deberá especificar con mucha claridad el desempeño de una actividad en particular.

Para organizar la información del proceso tendrá seis aspectos o pautas designadas por la práctica de empresas certificadoras[4].

a. PROPOSITO

El propósito es la razón del proceso. Se debe definir para que se crea el proceso.

b. ALCANCE

Se deberá definir la amplitud que tiene el proceso.

c. PROCESAMIENTO

Se debe pormenorizar cada uno de los actores que intervienen en el proceso así como las actividades que realizan

d. REFERENCIAS

Especificar aquellos documentos que se consideran fuentes de consulta o medios de clarificación de algún punto del proceso.

e. DEFINICIONES

Se explicará algún término que resulte ajeno usuarios.

f. DOCUMENTOS

Los documentos controlados que incida en el proceso que se está elaborando.

3. IDENTIFICAR ACTORES DEL PROCESO

Se identificará a los actores dado sus posiciones o encargos en particular para facilitar la selección utilizaremos la técnica del flujograma de alto nivel.

[4] ISO 27000 Quality System – Model for Quality Assurance in Design, Development Production, 5ª edition, Ginebra, Suiza

Sera adecuado tener pocos actores para facilitar la rapidez en la actividad como en la figura 3.4.

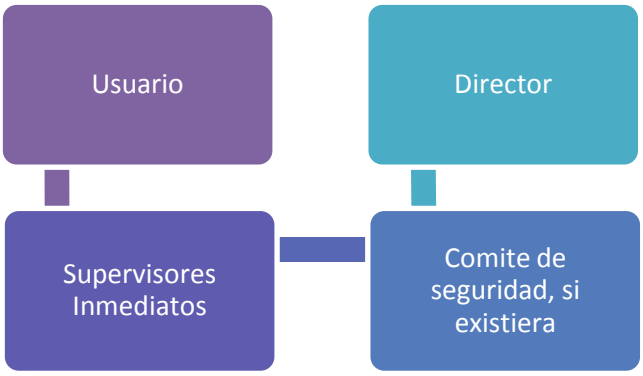


Figura III.4. Ejemplo de flujograma de alto nivel.

4. REUNIÓN DE ACTORES INVOLUCRADOS

Una vez identificados se procederá a reuniones programadas para manejar de manera más adecuada dichas reuniones se utilizará la *Hoja para Planificar la Documentación de Proceso* utilizando como muestra la figura III.5.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**

Figura III.5. Propuesta hoja para planificar el levantamiento del proceso

5. FLUJOGRAMA MATRICIAL NORMATIVO Una vez con los pasos anteriores organizados podemos utilizar una herramienta que nos facilite identificar actores que intervienen y también pormenorizar lo que cada uno de ellos hace, y especificar cuándo interviene.[5]

Los expertos le denominan a esta etapa "Arquitectura del procesamiento" de un proceso usando la nomenclatura de la figura III.6.

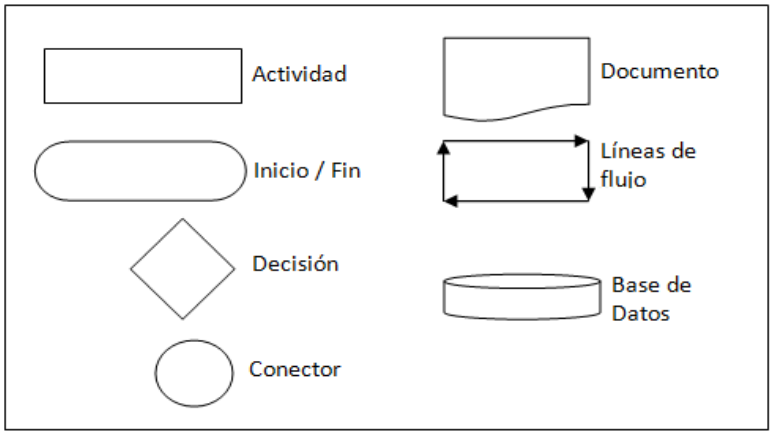


Figura III.6. Nomenclatura de flujograma Matricial

6. VALIDAR EL FLUJOGRAMA

Una vez realizado el flujograma lo rescribiremos con el objetivo de obtener una versión final, el flujograma se deberá llevar a cada persona que participó en su diseño para que lo revise y lo firma como señal de que lo validó. De esta manera quedará constancia de la validez del documento.

7. ANALIZAR SI SE REQUIERE INSTRUCCIÓN DE TRABAJO, REDACTAR Y VALIDAR Teniendo en cuenta los actores involucrados podremos determinar si se requiere instrucciones de trabajo preguntándonos si *¿La*

[5] Para la utilización del flujograma matricial normativo se propone en el punto 5, además nos guiamos en el software MICROSOF Visio 2010.

ausencia de instrucciones de trabajo afectará adversamente la seguridad de la información?

Si fuese necesario se redactará las instrucciones de trabajo.

8. DOCUMENTAR EL PROCESO

Procede a documentar el proceso con el formato establecido de esta manera quedará constancia de que se esta tratando un proceso recurrente.

9. DOCUMENTOS DE SEGURIDAD DE INFORMACIÓN

Para realizar nuestro documento nos deberemos basar en el diseño de flujograma ya que ahí de manera natural aparecerán aquellos documentos que se consideren para el Sistema de Seguridad de Información.

3.3 PROPUESTA DE FORMATOS PARA DOCUMENTAR LOS PROCESOS (3.2, B).

Con el propósito de establecer un manejo adecuado de la documentación en el DESITEL y garantizando la seguridad de la información, se propondrá los siguientes formatos para documentar proceso logrando que el DESITEL cumpla con su misión y se encuentre este Departamento apto para la certificación.

a. PROPUESTA FORMATO DEL PROCESO A DOCUMENTAR.

Como muestra la figura III.7 se realizará el procedimiento del proceso.

(Sello) NOMBRE DEL PROCESO:		**DOCUMENTO:**P02000
EMISIÓN: 23/05/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR
Propósito **Alcance** **Procedimiento**		

Usuario
Supervisor inmediato
Comité de seguridad
Dirección:
Referencias
Definiciones
Documentos

Figura III.7. Formato propuesto desarrollo del proceso

b. PROPUESTA GENERAL DE FORMATO DEL ENCABEZADO Y SU RESPECTIVA DESCRIPCIÓN :

Una vez realizado el procedimiento quedará el registro de todos los procesos como se muestra en la figura III.8.

<<SELLO>>		**TITULO:**	
SERIAL:	FECHA DE EMISIÓN	FECHA DE MODFIFICACION:	APROBACIÓN:
ELABORADO POR:	REVISADO Y APROBADO POR:		NÚMERO DE PÁGINA:
INTRODUCCIÓN: DESCRIPCIÓN:			
I	INSTRUCCIÓN DE TRABAJO		
M	MANUAL		
P	PROCEDIMIENTO		
R	REGISTRO O REPORTE		
L	POLITICA O LINEAMIENTO		

Figura III.8. Formato propuesto para registro del proceso

TITULO: Se indicará el título del documento de manera clara y explicita

SERIAL: El serial será el que nos indique de qué tipo de documento estaremos tratando

Como ejemplo la figura III.9:

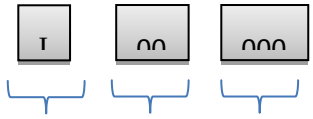


Figura III.9. Caracteres del Serial propuesto

El primer carácter nos indica el tipo de documento seleccionaremos cualquiera de estos caracteres como indica la figura III.10.

I	INSTRUCCIÓN DE TRABAJO
M	MANUAL
P	PROCEDIMIENTO
R	REGISTRO
L	POLITICA O LINEAMIENTO
R	REPORTE

Figura III.10. Letras de identificación para los documentos

El segundo carácter nos indica que área del DESITEL genera la documentación:

Opcionalmente el segundo carácter puede ser remplazado por las siglas de área respectivas como se muestra en la figura III.11.

00	Dirección
01	Secretaria
02	Desarrollo
03	Redes
04	DataCenter

Figura III.11. Numeración para las áreas

Los próximos tres dígitos son tres caracteres numéricos que representan el orden secuencial en el que se va generando los documentos.

FECHA DE EMISIÓN: Nos indicará la fecha en que se ha realizado el documento.

FECHA DE MODIFICACIÓN: Nos indicará si ha existido una modificación y en qué fecha.

APROBACIÓN: Indicará si ha sido aprobada o no el documento.

ELABORADO POR: Indicará los creadores del documento.

REVISADO Y APROBADO POR: Muestra el nombre de quien ha revisado y aprobado en este caso será siempre la Dirección.

NÚMERO DE PÁGINAS: Indicará el número de página para tener una secuencia del documento especificando una de cuantas Ejemplo: 1 de 4

INTRODUCCIÓN: Se describirá la metodología a utilizar para definir si está correctamente usado el serial

DESCRIPCIÓN: Nos indicará una descripción breve del documento.

INSTRUCCIÓN DE TRABAJO: Se define paso a paso el "como" de una actividad.

FORMULARIO: Para anotar los resultados de cualquier actividad el cual podrá convertirse en registro.

MANUAL: Es un documento compuesto por cierta extensión en cuanto a sus páginas, especifica y describe el compromiso, las responsabilidades, las autoridades y metodologías del DESITEL para cumplir los requisitos de la norma ISO 27001.

PROCEDIMIENTOS: Define “quien hace que” y “cuando”, Este documento describe la forma específica para llevar a cabo una actividad o proceso contiene 6 partes: Propósito, Alcance, Procedimiento, Documentos, Definiciones y Referencias

REGISTROS O REPORTE: Sirve para evidenciar o para demostrar a terceros que un requisito está implantado y se ha cumplido, estará detallada la actuación y las personas involucradas y su decisión consta de 4 partes; la detección de incidente, supervisor inmediato, comité de seguridad, Dirección

POLÍTICA O LINEAMIENTO: Sirve para emitir al DESITEL que política se ha optado de manera general o por áreas, posee 6 partes Alcance, Vigencia.

FIRMAS DE RESPONSABILIDAD: Una vez que se ha realizado el informe el responsable deberá firmar, para quede constancia y se de veracidad al documento.

NÚMERO DE RESOLUCIÓN: En el caso de que se emita un documento una vez realizado Consejo Politécnico o directivo se deberá colocar el número de la resolución.

c. PROPUESTA FORMATO DE REGISTRO O REPORTE

Para el registro de incidencias o reporte se utilizará el siguiente formato como se ilustra en la figura III.12.

<table>
<tr><td colspan="4">(SELLO) TITULO:</td></tr>
<tr><td>SERIAL:
R01001</td><td colspan="2">FECHA DE EMISIÓN:23/05/2012</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN:
SI</td></tr>
<tr><td>ELABORADO POR:EQUIPO ISO</td><td colspan="3">REVISADO Y APROBADO POR:
Dr. Carlos Buenaño</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4"></td></tr>
</table>

DETECCIÓN DE INCIDENTES

1. Nombre del Informante 2.Area involucrada
3. Fecha de reporte 4. Lugar del Incidente
5. Tipo de Incidente

-Personas -Actos Internos
-Procesos -Prácticas laborales
-Sistemas -Daño a activos
-Eventos externos -Incumplimiento a normas.
-Aspectos legales

SUPERVISOR INMEDIATO

1. Nombre del Supervisor o encargado 2. Fecha de recepción
3 Se trata de riesgo operativo
-Si
-No
4. Describir la acción tomada si fuese riesgo operativo.
5. Si no es riesgo operativo puede tomar acciones correctivas?
6. Describir acción tomada.

COMITÉ DE SEGURIDAD

1. Revisar instrucción de trabajo y determinar criticidad del riesgo.
Criticidad alta?
-Si
-No
2. Definición de acciones correctivas para mitigar riesgo de criticidad no alta.
3. Recomendación de acciones para mitigar riesgo de criticidad alta.

DIRECCIÓN

1. Descripción de acciones a tomar
FIRMAS DE RESPONSABILIDAD

Figura III.12. Propuesta de formato para un reporte

d. PROPUESTA FORMATO POLÍTICA O LINEAMIENTO

Para el desarrollo de la política del proceso utilizaremos el formato que se muestra en la figura III.13.

(SELLO)	**TITULO:**		
SERIAL: L03001	FECHA DE EMISIÓN:23/05/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR:EQUIPO ISO	REVISADO Y APROBADO POR: Ing. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1
Proceso disciplinario por violación de políticas de seguridad de información Alcance: Vigencia; POLITICA 1.Posibles ocurrencias de incidente de función de nivel de responsabilidad, podrá ser ejemplo: -Llamada verbal de atención -Cuando sea reiterada suspensión laboral -Caso grave se recurrirá al despido NÚMERO DE RESOLUCION			

Figura III.13. Propuesta de formato para una Política

e. PROPUESTA PARA LA ELABORACIÓN DE UNA INSTRUCCIÓN DE TRABAJO

Para la instrucción de trabajo se usará el siguiente formato como se muestra en la figura III.14

(SELLO) INSTRUCCIÓN DE TRABAJO:		**DOCUMENTO:**P02000
EMISIÓN: 23/05/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR:

Probabilidad o frecuencia de ocurrencia	Nivel del impacto o consecuencias		
	Insignificante	Moderado	Crítico
Casi siempre			
A veces			
Raras veces			

Figura III.14. Propuesta de formato para una instrucción de trabajo

CAPÍTULO IV

NORMA ISO 27001 PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN IMPLEMENTACIÓN EN LOS PROCESOS MÁS RECURRENTES EN EL DESITEL.

Una vez establecido en el capítulo anterior la metodología para documentar procesos en base con la utilización de la Norma ISO 27001 se procederá a documentar cada uno de ellos.

ALCANCE DEL MODELO

El presente modelo para el Sistema de Gestión de Seguridad de Información cubrirá los aspectos de seguridad de los activos del Departamento de Sistemas y Telemática, adaptando los procesos más recurrentes en base a la realidad existente en la organización.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN La presente política de seguridad de información se dicta en cumplimiento de las disposiciones institucionales legales vigentes[6], con el objeto de gestionar adecuadamente la seguridad de la información.

[6] En la ESPOCH no existen políticas de Seguridad De Información.

La política de seguridad del SGSI debe ser clara para establecer su cumplimiento a cabalidad, para proveer a la institución dirección y apoyo para la seguridad de la información.[7] Y además debe ser conocida y cumplida por el personal vinculado al departamento, por lo tanto la Política del SGSI para el DESITEL será como se muestra en la figura IV.1.

<table>
<tr><td>  </td><td colspan="3">POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL DESITEL</td></tr>
<tr><td>SERIAL:
P00001</td><td>FECHA DE EMISIÓN:02/09/2012</td><td>FECHA DE MODFIFICACION:-</td><td>APROBACIÓN:
SI</td></tr>
<tr><td>ELABORADO POR: Tesista</td><td colspan="2">REVISADO Y APROBADO POR:
Dr. Carlos Buenaño</td><td>NÚMERO DE PÁGINA:1 de 1</td></tr>
<tr><td colspan="4">Proceso de información sobre nueva política que adopta el DESITEL

ALCANCE: Informar a todos los trabajadores que pertenecen al departamento del DESITEL la política para la gestión de la seguridad de la información bajo la Norma ISO 27001.

VIGENCIA: 3 años a partir de la fecha de emisión

POLITICA

Se protegerá los recursos de información del DESITEL y la tecnología utilizada para su procesamiento, frente amenazas internas o externas, deliberadas o accidentales con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.</td></tr>
</table>

[7] Política de un SGSI de la ISO 17799:2005

Figura IV.1. Propuesta Política para el DESITEL

ACTIVOS Y SUS PROPIETARIOS

Una vez identificados los activos, el siguiente paso a realizar es valorarlos, hay que estimar que valor tienen para la organización, y su importancia para la misma[8]

Para el levantamiento de los procesos más recurrentes en el DESITEL, debemos conocer los activos y sus propietarios[9].

Anexo I: (Activos y propietarios**).**

4.1 LEVANTAMIENTO Y SELECCIÓN DE PROCESOS CRÍTICOS Y MÁS RECURRENTES EN EL DESITEL.

IDENTIFICACIÓN

Para el correcto levantamiento y selección de procesos críticos en el Departamento de Sistemas y Telemática es necesario identificar y analizar cada uno de los procesos que se manejan en este departamento, y especificar que tipo de riesgo presenta cada uno de ellos, de esta manera se garantizará dejar establecido que procesos podrían alterar el funcionamiento correcto del DESITEL.

[8] Valoración de los activos, Tesis MAGESID pág. 44

[9] Los activos se encuentran respaldados en el departamento de activos de la ESPOCH en el documento de CEDULACENSAL

Para esto analizaremos el Interés de la gerencia en aplicar la metodología de la norma e involucrar en el área de desarrollo, de lo contrario, no se comprometería aun mejoramiento en la seguridad de la información.

LEVANTAMIENTO DE PROCESOS CRÍTICOS

Utilizaremos un método cuantitativo para la selección de los procesos más críticos

LEYENDA DE LA CALIFICACIÓN:

1. Proceso de Poco Impacto, o, difícil de hacer algo con él.
2. Bajo el Promedio.
3. Normal o Promedio.
4. Sobre el Promedio.
5. Proceso de Gran Impacto, o, que es muy fácil cambiarlo.

Para esto mostraremos los procesos y realizaremos el análisis en la siguiente tabla:

TABLA IV.I

Selección de Procesos Críticos

Nombre del Proceso	ASPECTOS A TENER EN CUENTA					
	Suscepti-bilidad al Cambio	**Desempeño**	**Impacto en la Empresa**	**Impacto en el Cliente**	**Total**	**Promedio**
Creación de cuenta de correo	2	2	2	2	8	**2**
Cambio de contraseña en la cuenta de correo	3	2	2	2	9	**2,25**
Consulta de Aranceles complementarios de matrículas para estudiantes de pregrado	2	2	2	2	8	**2**
Elaboración de proformas presupuestarias	1	2	2	1	6	**1,5**
Control de sistemas de autentificación Wireless	1	2	3	4	10	**2,5**
Administración y Monitoreo del Sistema de Recaudaciones	2	3	2	2	9	**2,25**
Administración y Monitoreo del Sistema de Retenciones	2	3	2	2	9	**2,25**
Graduación	3	4	4	4	15	**3,75**
Culminación de malla curricular	3	3	2	3	11	**2,75**

Registro de notas acumuladas	4	5	4	5	18	**4,5**
Nombre del Proceso	**ASPECTOS A TENER EN CUENTA**					
	Suscepti-bilidad al Cambio	**Desempeño**	**Impacto en la Empresa**	**Impacto en el Cliente**	**Total**	**Promedio**
Registro de notas principales	4	5	4	5	18	**4,5**
Matriculación de tesis	3	4	3	4	14	**3,5**
Administración y control en la migración de datos de docentes de la ESPOCH	3	4	4	4	15	**3,75**
Administración y control en la migración de datos de estudiantes de la ESPOCH	3	4	4	4	15	**3,75**
Administración de aulas virtuales	2	2	3	2	9	**2,25**
Ingreso de personal técnico al DESITEL	3	2	2	3	10	**2,5**
Salida de personal técnico al DESITEL	3	2	2	3	10	**2,5**

Elaborado Por: Lucia Guevara
Fuente: Reingeniería Informática - Maestría

Para el análisis de los procesos más críticos se propondrá que mayor o igual que 75% o 3, 75 se lo concederá critico como se muestra en la figura IV.2.

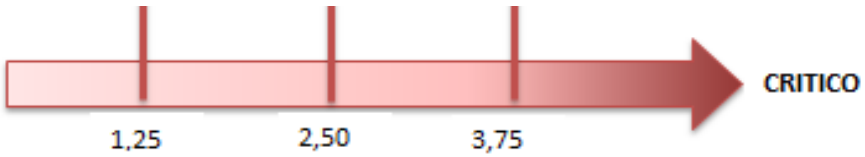


Figura IV.2.Gráfico para describir la criticidad del proceso

En el siguiente punto analizaremos los procesos de acuerdo a la criticidad.

4.2 DESARROLLO DE LOS PROCESOS CRÍTICOS Y MÁS RECURRENTES EN EL DESITEL CON EL USO DE LA METODOLOGÍA PROPUESTA

Para desarrollar la metodología propuesta primeramente identificamos los procesos mas recurrentes en el DESITEL, esta información se obtuvo con la colaboración de las personas que integran el grupo de trabajo en el Departamento de telemática y su Director.

ANEXO II. (Diagrama Gantt de planificación de realización de procesos**)**

a. **PROCESOS:** Registro de notas acumuladas

- **Propósito:** Controlar el registro de notas de los docentes al sistema Académico de la ESPOCH.
- **Alcance:** Para que existe un registro de notas deberá el estudiante estar matriculado en la materia asignada al profesor, el docente debe subir las notas al sistema académico dentro de los periodos señalados además deberá imprimir las actas de notas y entregarlas en la secretaria de la escuela, si el docente no

entregará las notas en la fecha señaladas deberá realizar un oficio al Director de la Escuela, el decide si debe pasar a Consejo Directivo, si fuese el caso se esperará a la resolución y en secretaria se ingresará las notas, caso contrario el Director ingresará las notas y las imprimirá. Si existen casos excepcionales (convalidaciones, examen de suficiencia, etc.) se deberá registrar las resoluciones con las notas del estudiante.

- **Procesamiento:**

  Ing. Alex Tacuri: Encargado del Sistema Académico.

  Director de Escuela: Encargado de dirigir la actividad académica y administrativa de la Escuela.

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los archivos de actas y calificaciones.

- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.
  - Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**:

  Estatutos Politécnicos

- Reglamento de Régimen Académico 2009.

Los actores que intervienen en este proceso son:

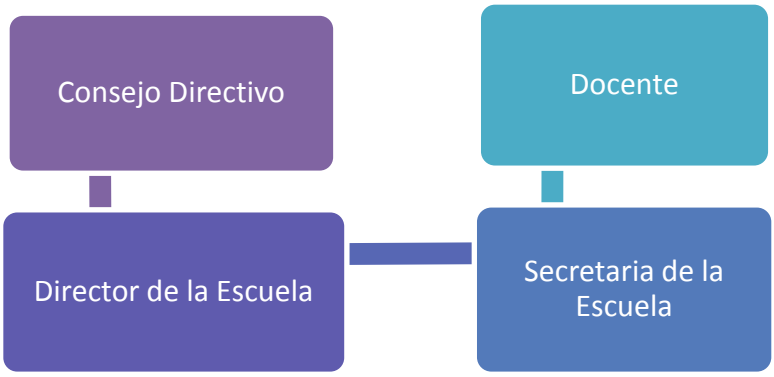


Figura IV.3. Actores del proceso notas acumuladas

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Registro de notas acumuladas	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 2 de agosto del 2012 a partir de las 9 de la mañana	Ninguna

Figura IV.4. Hoja de planificación del proceso notas acumuladas

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

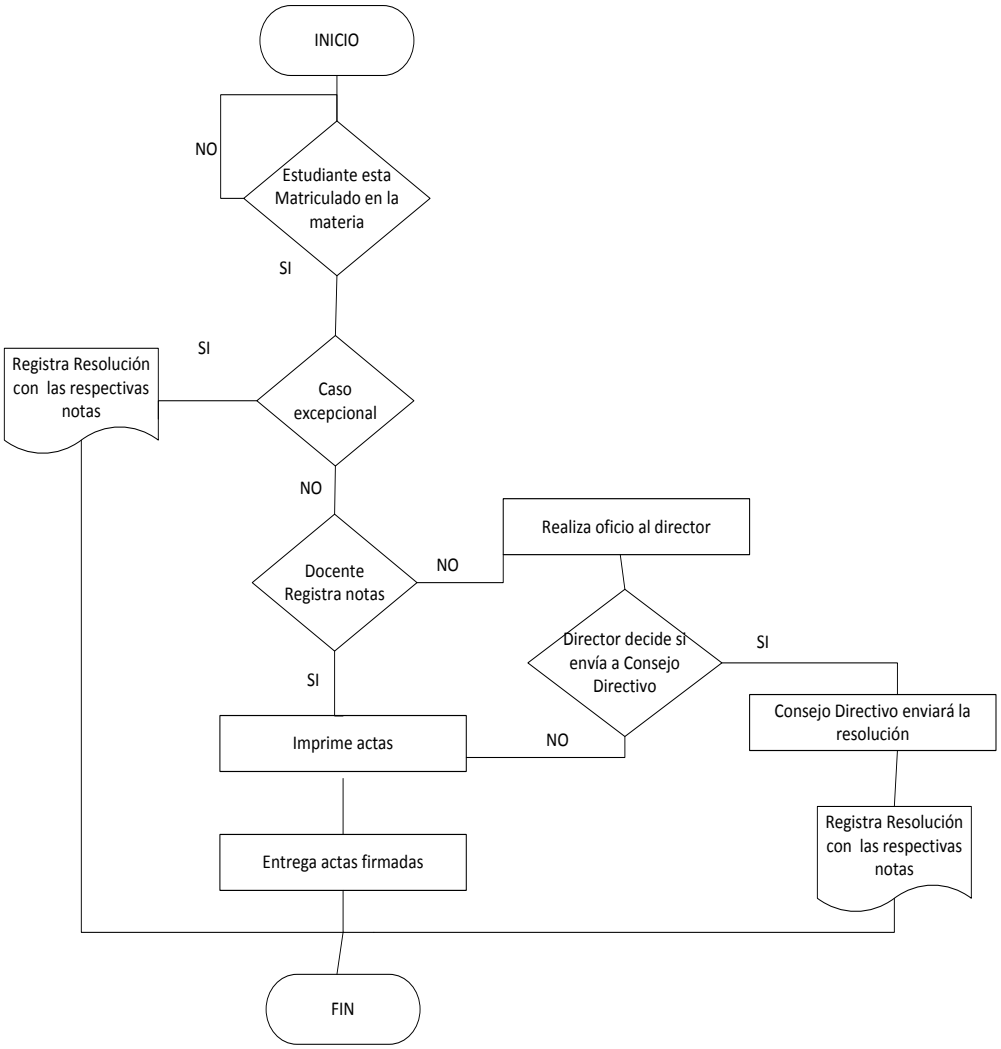


Figura IV.5. Flujograma del proceso notas acumuladas

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

Una vez analizado el proceso de la elaboración de proformas presupuestarias realizaremos de la documentación del proceso en el formato establecido para el mismo:

Para documentar el proceso este quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

REGISTRO DE NOTAS ACUMULADAS

SERIAL: R020010	FECHA DE EMISIÓN:2/09/ 2012	FECHA DE MODFIFICACIO N:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Alex Tacuri

2.Area involucrada
Desarrollo

3. Fecha de reporte
2/09/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : X
-Sistemas: -
-Eventos externos:-
-Aspectos legales: X
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Alex Tacuri

2. Fecha de recepción
2/09/2012

3 Se trata de riesgo operativo

-Si: -
-No: -

4. Describir la acción tomada

El Director de escuela solicitará al Director del DESITEL que realiza los cambios correctivos en el sistema mediante un oficio. El director del DESITEL indicará al encargado del Sistema que haga los cambios.

Figura IV.6. Registro del proceso notas acumuladas

b. PROCESO: Registro notas principales

- **Propósito:** Controlar el registro de notas de los docentes al sistema Académico de la ESPOCH.
- **Alcance:** Para que existe un registro de notas deberá el estudiante tener notas acumuladas y asistencia en la materia, el docente debe subir las notas al sistema académico dentro de los periodos señalados además deberá imprimir las actas de notas y entregarlas en la secretaria de la escuela, si el docente no entregará las notas en la fecha señaladas deberá realizar un oficio al Director de la escuela, el decide si debe pasar a Consejo Directivo, si fuese el caso se esperara a la resolución y en secretaria se ingresará las notas, caso contrario el Director ingresará las notas y las imprimirá.
- **Procesamiento:**

  Ing. Alex Tacuri: Encargado del Sistema Académico.

  Director de Escuela: Encargado de dirigir la actividad académica y administrativa de la Escuela.

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los archivos de actas y calificaciones.

  Secretaria Académica: Encargada de velar por el desarrollo académico Institucional en el ámbito de pregrado y postgrado
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO

27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL".

- Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**:
  - Estatutos Politécnicos
  - Reglamento de Régimen Académico 2009.

Los actores que intervienen en este proceso son:

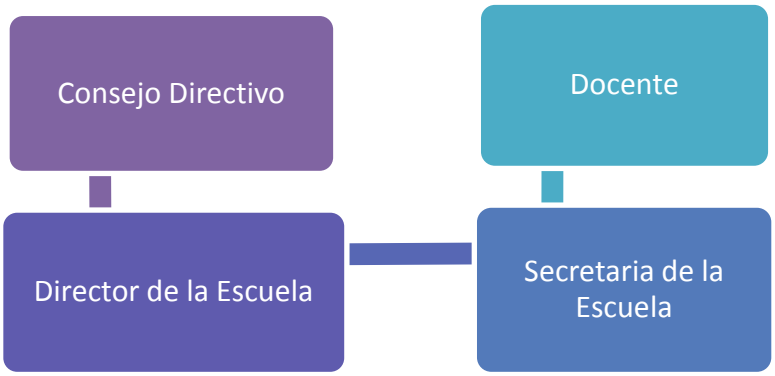


Figura IV.7. Actores del proceso notas principales

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Registro de notas principales	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 6 de agosto del 2012 a partir de las 9 de la mañana	Ninguna

Figura IV.8. Hoja de planificación del proceso notas principales

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

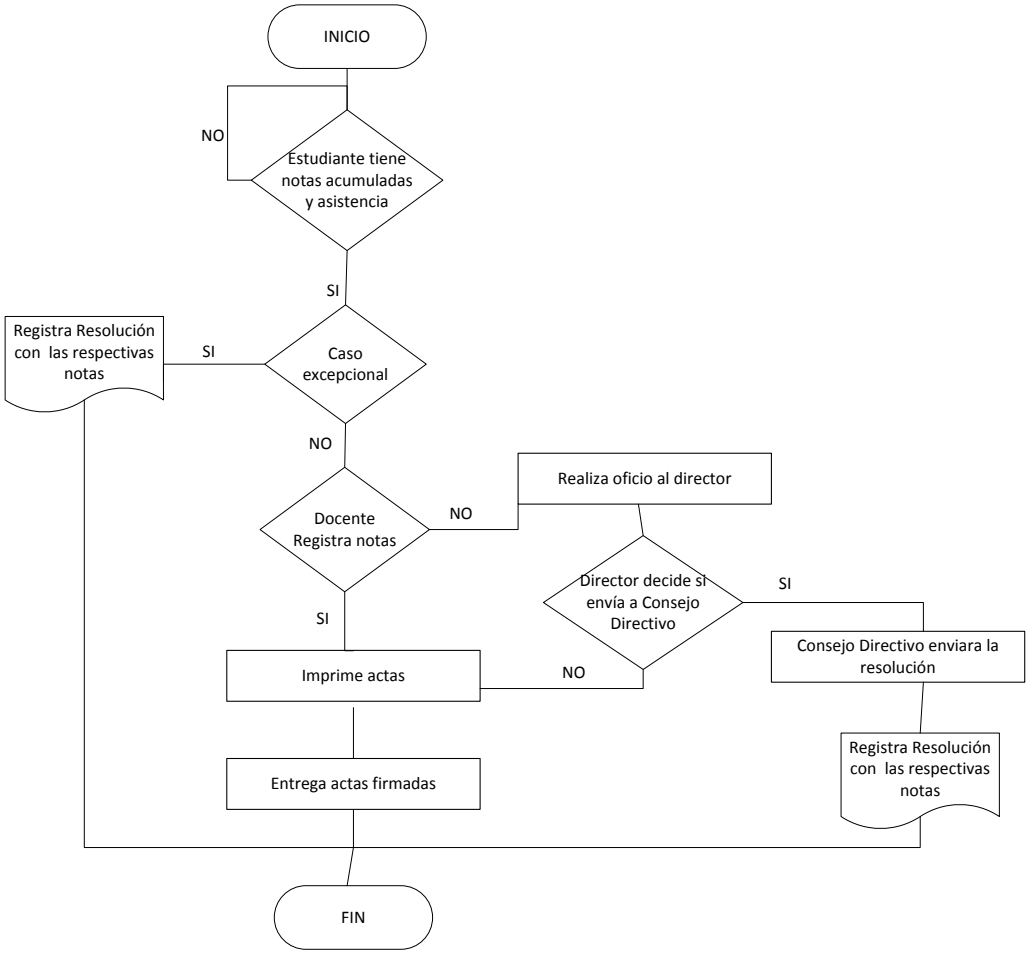


Figura IV.9. Flujograma del proceso notas principales

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Registro de Notas principales	**DOCUMENTO:** P020011
EMISIÓN: 6/08/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Alex Tacuri.

1.0 Propósito

Controlar los registros de notas de los docentes al sistema Académico de la ESPOCH.

2.0 Alcance

Para que exista un registro de notas deberá el estudiante tener notas acumuladas y asistencia en la materia, el docente debe subir las notas al sistema académico dentro de los periodos señalados además deberá imprimir las actas de notas y entregarlas en secretaria de la escuela, si el docente no entregará las notas en la fecha señaladas deberá realizar un oficio al Director de la escuela, el decide si debe pasar a consejo directivo, si fuese el caso se espera a la resolución y en secretaria se ingresará las notas, caso contrario el Director ingresará las notas y las imprimir.

3.0 Procedimiento

Docente

1. Subir las notas al sistema académico
2. Debe imprimir las actas de notas
3. Debe entregar en secretaria las notas impresas
4. Realiza oficio al director si no alcanzo a entregar

Secretaría Escuela

1. Recibe las notas de los profesores

Director de la Escuela

1. Envía oficio a consejo directivo para su análisis
2. Espera resolución de consejo directivo
3. Con la resolución de consejo directivo director registra notas

Consejo Directivo

1. Analiza y aprueba que el director de la escuela registre notas

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis “Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL”

5.0 Definiciones

Acta de notas Principales.- Registro de las notas de un estudiante en exámenes principales

6.0 Documentos

✓ Estatutos Politécnicos ✓ Reglamento de Régimen Académico 2009

Figura IV.10. Procesamiento del proceso notas principales

Una vez analizado el proceso de la elaboración de proformas presupuestarias realizaremos de la documentación del proceso en el formato establecido para el mismo:

REGISTRO DE NOTAS PRINCIPALES

SERIAL: R020011	FECHA DE EMISIÓN:6/08/ 2012	FECHA DE MODFIFICACIO N:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Alex Tacuri

2.Area involucrada
Desarrollo

3. Fecha de reporte
6/09/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: -
-Eventos externos:-
-Aspectos legales: -
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Alex Tacuri

2. Fecha de recepción
2/09/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
El Director de escuela solicitará al Director del DESITEL que realiza los cambios correctivos en el sistema mediante un oficio. El director del DESITEL indicará al encargado del Sistema que haga los cambios.

Figura IV.11. Registro del proceso notas principales

c. **PROCESO:** Administración y control en la migración de datos de docentes de la ESPOCH.

- **Propósito:** Migrar los datos del Sistema Académico al Sistema E-virtual para el uso de la plataforma de los docentes.
- **Alcance:**

  La migración de datos se realizará comprobando si existe primeramente información en el Sistema Académico Institucional si los datos son correctos se supervisará que se migren la información sin interrupción, en el caso de que exista algún inconveniente en la información del Sistema Académico el docente deberá regresar a la Secretaria de la Escuela a la que pertenece y solicitará se registre en el sistema Académico la carga horaria si por algún motivo no se registro correctamente.
- **Procesamiento:**

  Ing. Gustavo Hidalgo: Encargado del Sistema E-virtual.

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los profesores, archivos de actas y calificaciones.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.
  - Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**:
  - No existe ningún documento

Los actores que intervienen en este proceso son:

Figura IV.12. Actores del proceso migración de datos docente

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Administración y control en la migración de datos de docentes de la ESPOCH	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 3 de septiembre del 2012 a partir de las 9 de la mañana	Ninguna

Figura 4.13. Hoja de planificación del proceso migración de datos

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

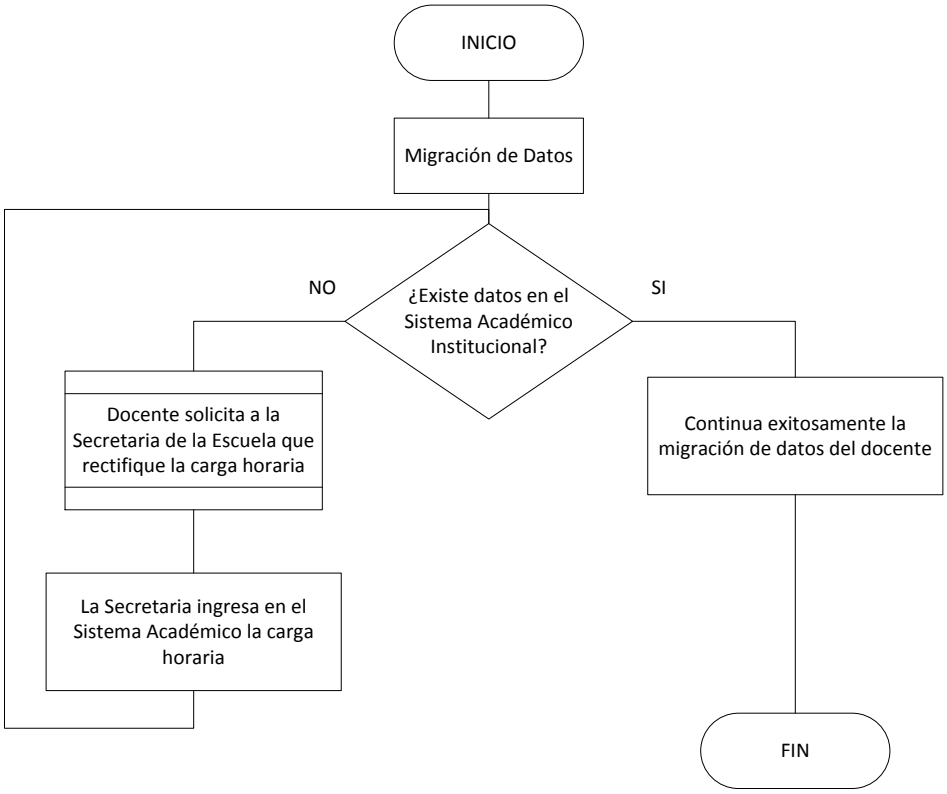


Figura IV.14 Flujograma del proceso migración de datos docente

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Administración y control en la migración de datos de docentes de la ESPOCH	**DOCUMENTO:** P020013
EMISIÓN: 3/09/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Gustavo Hidalgo.

1.0 Propósito

Migrar los datos del Sistema Académico al Sistema E-virtual para el uso de la plataforma de los docentes.

2.0 Alcance

La migración de datos se realizará comprobando si existe primeramente información en el Sistema Académico Institucional si los datos son correctos se supervisará que se migren la información sin interrupción, en el caso de que exista algún inconveniente en la información del Sistema Académico el docente deberá regresar a la Secretaria de la Escuela a la que pertenece y solicitará se registre en el sistema Académico la carga horaria si por algún motivo no se registro correctamente.

3.0 Procedimiento

Docente

1. Comprobar que posee un aula por cada una de sus materias
2. Solicita que se registre correctamente en el sistema académico

Secretaría Escuela

1. Comprueba que estén todas las cargas horarias de un docente
2. Rectificar la carga horaria de un docente.

Encargado del Sistema e-virtual

1. Migrar los datos

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Migrar datos.- Es el traspaso de información de una base de datos a otra.

6.0 Documentos

- ✓ No existe documentos.

Figura IV.15 Procesamiento del proceso migración de datos docente

ADMINISTRACION Y CONTROL EN LA MIGRACIÓN DE DATOS DE DOCENTES DE LA ESPOCH			
SERIAL: R020013	FECHA DE EMISIÓN:3/09/ 2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Gustavo Hidalgo

2.Area involucrada
Desarrollo

3. Fecha de reporte
3/09/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: -
-Eventos externos:-
-Aspectos legales: -
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Gustavo Hidalgo

2. Fecha de recepción
3/09/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
El Técnico Informático solicitará al docente que se acerque a secretaria de la escuela para que la secretaria realice las respectivas rectificaciones en el Sistema Académico.

Figura IV.16 registro del proceso migración de datos docente

d. PROCESO: Administración y control en la migración de datos de estudiantes de la ESPOCH.

- **Propósito:** Migrar los datos del Sistema Académico al Sistema E-virtual para el uso de la plataforma de los estudiantes.
- **Alcance:**

  La migración de datos se realizará comprobando si existe primeramente información en el Sistema Académico Institucional si los datos son correctos se supervisará que se migren la información sin interrupción, en el caso de que exista algún inconveniente en la información del Sistema Académico el docente deberá regresar a la Secretaria de la Escuela a la que pertenece y solicitará se registre en el sistema Académico la matricula en la/s materias que existiera si por algún motivo no se registro correctamente.
- **Procesamiento:**

  Ing. Gustavo Hidalgo: Encargado del Sistema E-virtual.

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los profesores, archivos de actas y calificaciones.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.
  - Microsoft Visio 2010. Formas de diagrama SDL.
- **Documentos**:
  - No existen documentos

Los actores que intervienen en este proceso son:

Figura IV.17 Actores del proceso migración de dataos estudiante

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Administración y control en la migración de datos de estudiantes de la ESPOCH	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 4 de septiembre del 2012 a partir de las 9 de la mañana	Ninguna

Figura IV.18. Hoja de planificación del proceso migración de datos estudiantes

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

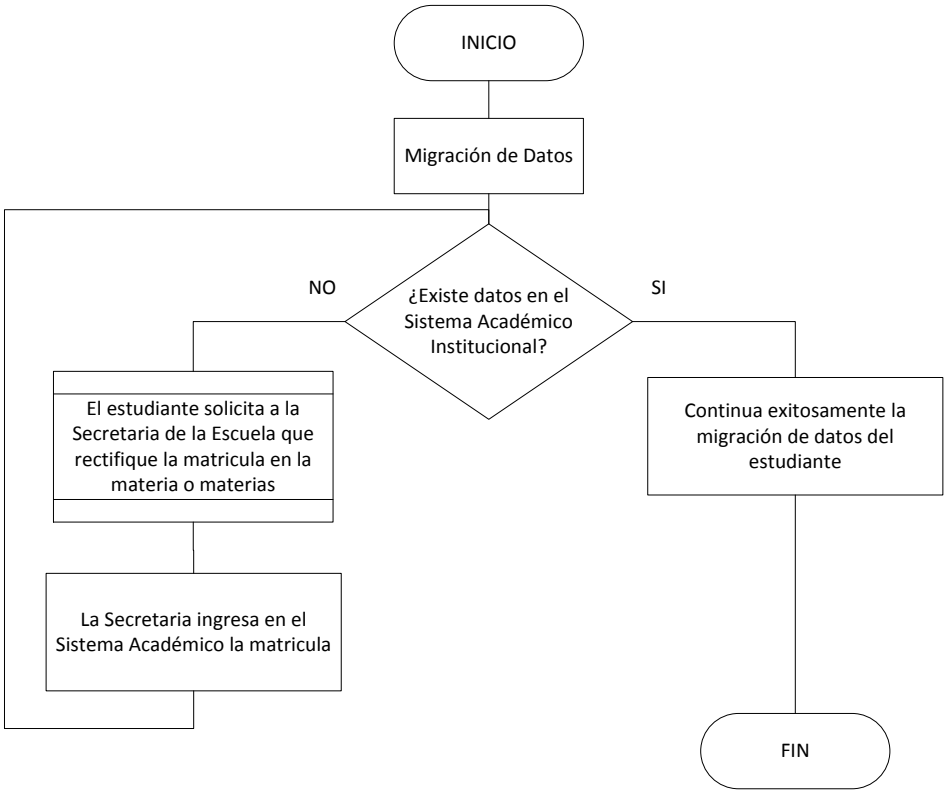


Figura IV.19 Flujograma del proceso migración de datos estudiante

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

Una vez analizado el proceso de administración y control en la migración de datos de estudiantes de la ESPOCH, realizaremos de la documentación del proceso en el formato establecido para el mismo:

	NOMBRE DEL PROCESO: Administración y control en la migración de datos de estudiantes de la ESPOCH	**DOCUMENTO:** P020014
EMISIÓN: 4/09/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Gustavo Hidalgo.

1.0 Propósito

Migrar los datos del Sistema Académico al Sistema E-virtual para el uso de la plataforma de los estudiantes.

2.0 Alcance

La migración de datos se realizará comprobando si existe primeramente información en el Sistema Académico Institucional si los datos son correctos se supervisará que se migren la información sin interrupción, en el caso de que exista algún inconveniente en la información del Sistema Académico el docente deberá regresar a la Secretaria de la Escuela a la que pertenece y solicitará se registre en el sistema Académico la matricula en la/s materias que existiera si por algún motivo no se registro correctamente.

3.0 Procedimiento

Estudiante

1. Comprobar que esta registrado en las aulas virtuales de cada materia matriculada
2. Solicita que se registre correctamente en el sistema académico

Secretaría Escuela

1. Rectifica si algún estudiante no esta matriculado en la materia correspondiente
2. Ingresa matricula.

Encargado del Sistema e-virtual

2. Migrar los datos

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis “Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL”

5.0 Definiciones

Migrar datos.- Es el traspaso de información de una base de datos a otra.

6.0 Documentos

- ✓ No existe documentos.

Figura IV.20 Procesamiento del proceso migración datos estudiante

ADMINISTRACION Y CONTROL EN LA MIGRACIÓN DE DATOS DE ESTUDIANTES DE LA ESPOCH

SERIAL: R020014	FECHA DE EMISIÓN:4/09/ 2012	FECHA DE MODFIFICACIO N:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Gustavo Hidalgo

2.Area involucrada
Desarrollo

3. Fecha de reporte
3/09/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: -
-Eventos externos:-
-Aspectos legales: -
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Gustavo Hidalgo

2. Fecha de recepción
4/09/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
El Técnico Informático solicitará al estudiante que se acerque a secretaria de la escuela para que la secretaria realice las respectivas rectificaciones en el Sistema Académico.

Figura IV.21 Registro del proceso migración datos estudiante

e. PROCESO: Graduación

- **Propósito:** Verificar el proceso de desarrollo del trabajo de graduación en la ESPOCH.
- **Alcance:**

  El estudiante previo al proceso de graduación deberá:

  - Matricular su trabajo de graduación
  - Defensa del trabajo de graduación
  - Incorporación

  La secretaria de la escuela, debe estar presente en el acto de defensa del trabajo de graduación, elaborar el acta con las respectivas calificaciones y firmas de los miembros del Tribunal, transcribir la misma y remitir estos documentos a la Secretaría Académica, para que sean revisados y el estudiante sea declarado apto para su incorporación.
- **Procesamiento:**

  Ing. Alex Tacuri: Encargado del Sistema Académico - OASIs.

  Director de Escuela: Encargado de dirigir la actividad académica y administrativa de la Escuela

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los archivos de actas y calificaciones.

  Secretaria Académica: Encargada de velar por el desarrollo académico institucional en el ámbito de pregrado y postgrado.
- **Referencias:**

- Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.
- Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**:
  - Estatutos Politécnicos
  - Reglamento de Régimen Académico 2009.

Los actores que intervienen en este proceso son:

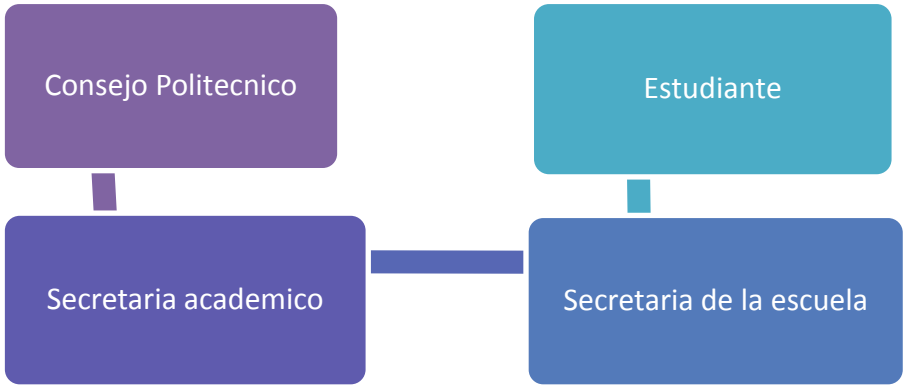


Figura IV.22 Actores que intervienen proceso graduación

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Graduación	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 27 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura IV.23 Hoja de planificación del proceso graduación

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

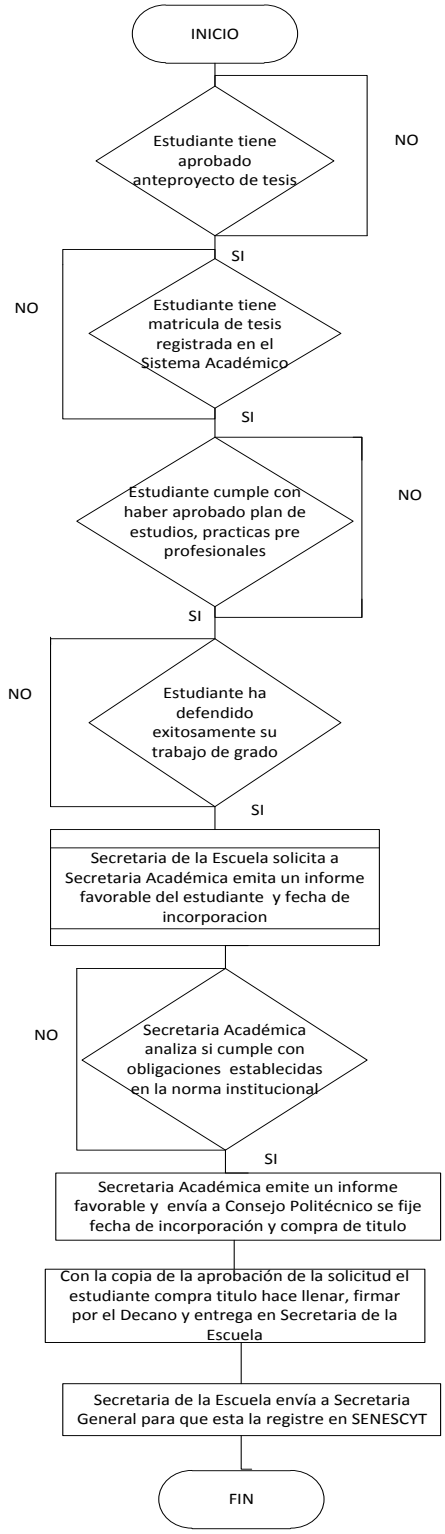


Figura 4.24 Flujograma del proceso graduación

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

Una vez analizado el proceso de la elaboración de proformas presupuestarias realizaremos de la documentación del proceso en el formato establecido para el mismo:

	NOMBRE DEL PROCESO: Graduación	**DOCUMENTO:** P02008
EMISIÓN: 27/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Alex Tacuri.

1.0 Propósito

Verificar el proceso de desarrollo del trabajo de graduación en la ESPOCH.

2.0 Alcance

El estudiante previo al proceso de graduación deberá:

- Matricular su trabajo de graduación.
- Defender el trabajo de graduación.
- Incorporación.

La secretaria de la escuela, debe estar presente en el acto de defensa del trabajo de graduación, elaborar el acta con las respectivas calificaciones y firmas de los miembros del Tribunal, transcribir la misma y remitir estos documentos a la secretaría académica, para que sean revisados y el estudiante sea declarado apto para su incorporación.

3.0 Procedimiento

Secretaria de la escuela

1. Presentar el acta de defensa
2. Elaborar actas respectivas
3. Transcribir las actas de grado

Secretaría Académica

1. Revisar si el estudiante esta apto

Estudiante

1. Cumplir con los requisitos

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Trabajo de graduación.- Documento que realiza el estudiante sobre un tema de investigación demostrando sus habilidades que ha adquirido durante su vida estudiantil.

Acto de defensa.- El día en que el estudiante realizará la defensa del trabajo de graduación

6.0 Documentos

- ✓ Estatutos Politécnicos
- ✓ Reglamento de Régimen Académico 2009

Figura IV.25 Procesamiento del proceso graduación

Para documentar el proceso este quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

	GRADUACIÓN		
SERIAL: R02008	FECHA DE EMISIÓN:27/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Alex Tacuri

2.Area involucrada
Desarrollo

3. Fecha de reporte
27/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : X
-Sistemas: -
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Alex Tacuri

2. Fecha de recepción
27/07/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
En caso de que la información sea mal registrada se solicitará al Director del DESITEL que se realiza las debidas rectificaciones.

Figura IV.26 Registro del proceso graduación

f. PROCESO: Creación de cuenta de correo

- **Propósito**

  Obtener una cuenta de correo institucional en la plataforma live@edu de la ESPOCH.

- **Alcance**

  El solicitante de la cuenta de correo deberá tener alguna relación de dependencia académica o administrativa con la ESPOCH, sea esta permanente o temporal. Se podrá crear una sola cuenta de correo personal.

- **Procedimiento**

  Técnico Informático

  - Genera cuenta de correo
  - Informa al solicitante sobre la cuenta generada

- Politécnicos
  - Solicita cuenta de correo
  - Proporciona contraseña

- **Referencias**

  Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

- **Definiciones**

  Webmaster.- Administrador live@edu institucional.

  Técnico Informático.- Brinda soporte en cada facultad.

- **Documentos**
  - Video manual de creación de cuentas de correo emitido a los técnicos de las facultades vía mail.
  - Política de creación de cuentas de correo institucional.

Los actores que intervienen en este proceso son:

Figura IV.27 Actores del proceso cuentas correo

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Creación de cuenta de correo	Recolección de la información necesaria del proceso	Politécnicos Técnico informático	La reunión se realizó el día 23 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura 4.28. Hoja de planificación del proceso cuentas correo

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

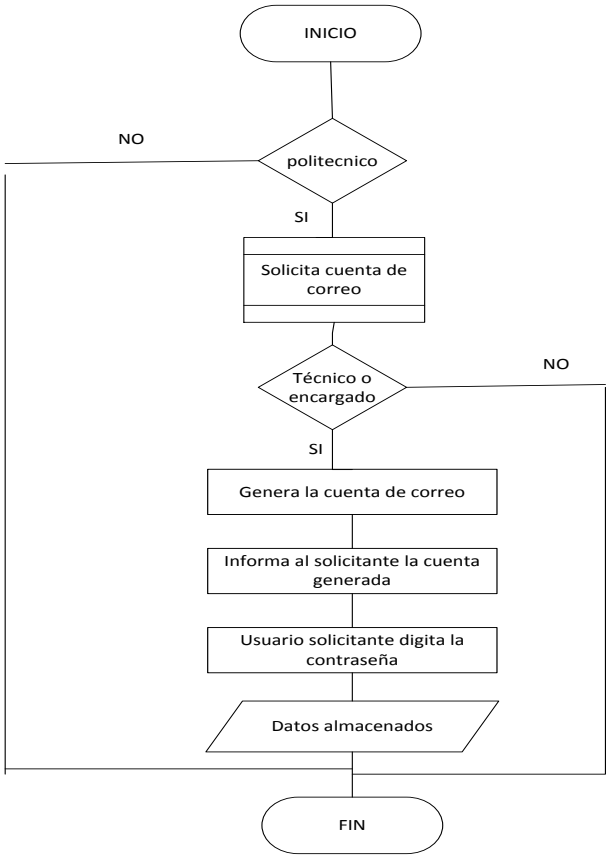


Figura IV.29 Flujograma del proceso cuentas correo

Para documenta el proceso quedar en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

	NOMBRE DEL PROCESO: Creación de cuentas de correo institucionales.	**DOCUMENTO:** P02001
EMISIÓN: 23/05/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Gonzalo Allauca.

1.0 Propósito

Obtener una cuenta de correo institucional en la plataforma live@edu de la ESPOCH.

2.0 Alcance

El solicitante de la cuenta de correo deberá tener alguna relación de dependencia académica o administrativa con la ESPOCH, sea esta permanente o temporal. Se podrá crear una sola cuenta de correo personal.

3.0 Procedimiento

Técnico Informático

1. Genera cuenta de correo
2. Informa al solicitante sobre la cuenta generada

Politécnicos

1. Solicita cuenta de correo
2. Proporciona contraseña

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Webmaster.- Administrador live@edu institucional.

Técnico Informático.- Brinda soporte en cada facultad.

6.0 Documentos

Video manual de creación de cuentas de correo emitido a los técnicos de las facultades vía mail.

Política de creación de cuentas de correo institucional.

Figura IV.30 Procesamiento del proceso cuentas correo

PROCESO DE CREACIÓN DE CUENTAS DE CORREO			
SERIAL: R02001	FECHA DE EMISIÓN:23/07/2012	FECHA DE MODFIFICACION:-	APROBACAION: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Gonzalo Allauca

2.Area involucrada
Desarrollo

3. Fecha de reporte
23/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: X
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: X

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Gonzalo Allauca

2. Fecha de recepción
23/07/2012

3 Se trata de riesgo operativo
-Si: X
-No: -

4. Describir la acción tomada si fuese riesgo operativo.
El Técnico deberá comprobar la información que provee el politécnico para la creación de la cuenta.

5. Describir acción tomada.
El técnico informático pedirá la cedula de ciudadanía o el carnet politécnico para la creación de la cuenta caso contrario no se permitirá la creación de la misma.

Figura IV.31 Registro del proceso cuentas correo

g. PROCESO: Cambio de la contraseña de cuenta de correo

- **Propósito**

  Lograr el cambio de contraseña de la cuenta de correo en la plataforma live@edu de la ESPOCH.

- **Alcance**

  El solicitante de la cuenta pedirá recuperar o cambiar la contraseña.

- **Procedimiento**

  Técnico Informático

  - Envía mail al Webmaster solicitando cambio de contraseña.
  - Informa al solicitante el cambio de clave y entrega clave temporal

  Politécnicos

  - Solicita cambio de contraseña o recuperación de cuenta de correo
  - Proporciona contraseña

  Webmaster

  - Verifica información
  - Entrega clave temporal.

- **Referencias**

  Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis “Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL”

- **Definiciones**

Webmaster.- Administrador live@edu institucional.

Técnico Informático.- Brinda soporte en cada facultad.

- **Documentos**
  - Video manual de creación de cuentas de correo emitido a los técnicos de las facultades vía mail.
  - Política de creación de cuentas de correo institucional.

Los actores que intervienen en este proceso son:

Figura IV.32 Actores del proceso cambio contraseña

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Cambio de la contraseña de cuenta de correo	Recolección de la información necesaria del proceso	Politécnicos Técnico informático Webmaster	La reunión se realizó el día 23 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura IV.33 Hoja de planificación del proceso cambia contraseña

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

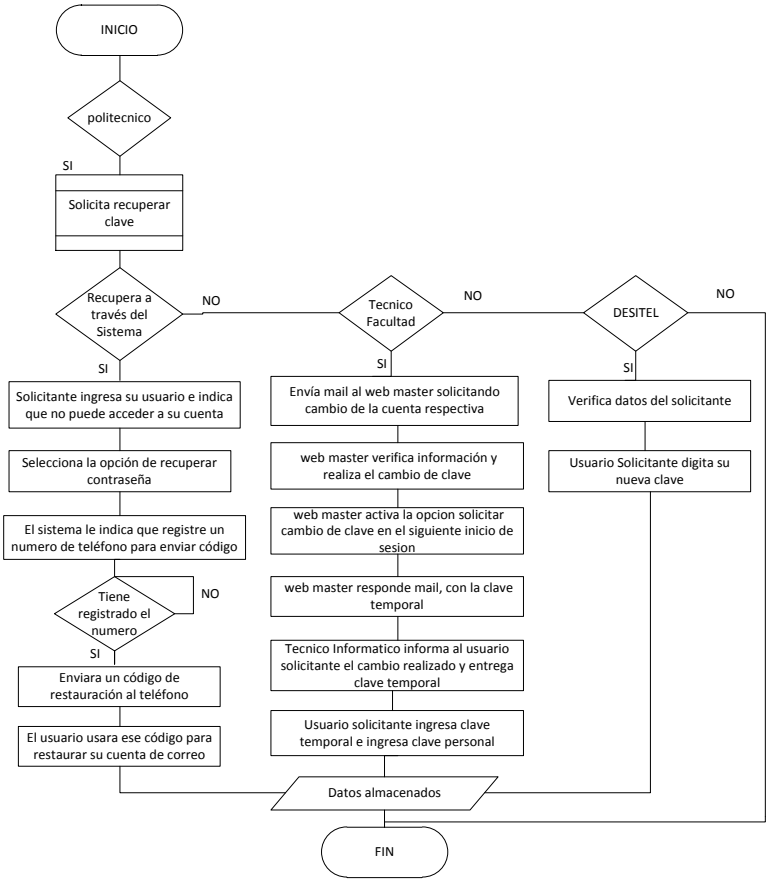


Figura IV.34 Flujograma del proceso cambio contraseña

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

Una vez analizado el proceso de cambio de contraseña de cuenta de correo se determina con el encargado de la plataforma live@edu que no existe ninguna instrucción de trabajo.

Documentación del proceso en el formato establecido para el mismo:

	NOMBRE DEL PROCESO: Cambio de contraseña de cuenta de correo institucional	**DOCUMENTO:** P02002
EMISIÓN: 23/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Gonzalo Allauca.

1.0 Propósito

Lograr el cambio de contraseña de la cuenta de correo en la plataforma live@edu de la ESPOCH.

2.0 Alcance

El solicitante de la cuenta pedirá recuperar o cambiar la contraseña.

3.0 Procedimiento

Técnico Informático

1. Envía mail al Webmaster solicitando cambio de contraseña.
2. Informa al solicitante el cambio de clave y entrega clave temporal

Politécnicos

1. Solicita cambio de contraseña o recuperación de cuenta de correo
2. Proporciona contraseña

Webmaster

1. Verifica información
2. Entrega clave temporal.

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología par documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Webmaster.- Administrador live@edu institucional.

Técnico Informático.- Brinda soporte en cada facultad.

6.0 Documentos

Video manual de creación de cuentas de correo emitido a los técnicos de las facultades vía mail.

Política de creación de cuentas de correo institucional.

Figura IV.35 Procesamiento del proceso cambio contraseña

Para documentar el proceso este quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

PROCESO DE CAMBIO DE CONTRASEÑA DE CUENTA DE CORREO

SERIAL: R02002	FECHA DE EMISIÓN:23/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Gonzalo Allauca

2.Area involucrada
Desarrollo

3. Fecha de reporte
23/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: X
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: X

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Gonzalo Allauca

2. Fecha de recepción
23/07/2012

3 Se trata de riesgo operativo
-Si: X
-No: -

4. Describir la acción tomada si fuese riesgo operativo.
El Técnico deberá comprobar la información que provee el politécnico para el cambio de contraseña.

5. Describir acción tomada.
El técnico informático pedirá al Webmaster ya restauración de contraseña de la

cuenta de correo y con la nueva contraseña temporal solo se la entregará al usuario no a otras personas.

Figura 4.36. Registro del proceso cambio contraseña

h. PROCESO: Consulta de Aranceles complementarios de matricula para estudiantes de pregrado.

- **Propósito:** Obtener por medio de una llamada telefónica el valor a cancelar de la matricula.
- **Alcance:** El solicitante llamará desde cualquier teléfono convencional o celular desde cualquier parte del mundo a un número telefónico institucional definido, el estudiante ingresará su número de cedula sin guion y el IVR indicará automáticamente el valor a pagar. El solicitante deberá tener una matricula en estado Pendiente.
- **Procesamiento:**

  Ing. Gonzalo Allauca: Encargado directo del IVR de AsterisK de la institución.

  Ing. Roberto Larrea: Encargado de VoIp institucional.

  Ing. Juan Carlos Díaz: Encargado del Sistemas de Pagos.

  Usuario.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis "Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL".
  - Microsoft Visio 2010. Formas de diagrama SDL.
- **Documentos**: No existe ningún tipo de documento.

Los actores que intervienen en este proceso son:

Figura IV.37 Actores del proceso aranceles

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Consulta de Aranceles complementarios de matricula para estudiantes de pregrado	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 23 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura 4.38. Hoja de planificación del proceso aranceles

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

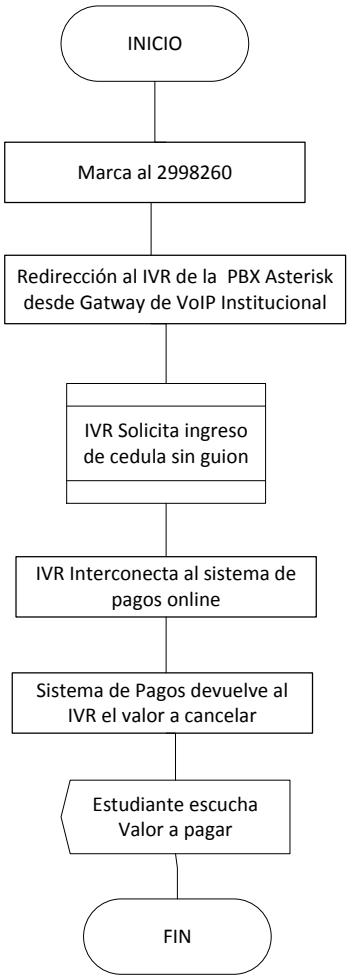


Figura IV.39 Flujograma del proceso aranceles

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Consulta de Aranceles complementarios de matricula para estudiantes de pregrado	**DOCUMENTO:** P02003

EMISIÓN: 23/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Gonzalo Allauca.

1.0 Propósito

Obtener por medio de una llamada telefónica el valor a cancelar de la matricula.

2.0 Alcance

El solicitante llamará desde cualquier teléfono convencional o celular desde cualquier parte del mundo aun NÚMERO telefónico institucional definido, el estudiante ingresará su NÚMERO de cédula sin guion y el IVR indicará automáticamente el valor a pagar. El solicitante deberá tener matricula en estado pendiente.

3.0 Procedimiento

Técnico encargado del IVR de Asterisk

1. Recibe el llamado desde cualquier teléfono fijo o convencional.
2. Solicita ingreso de cedula con guion.
3. Intercomunica al sistema de pagos online.

Técnico encargado del VoIp

1. Re direcciona al IRV desde el Gateway

Técnico encargado del sistema de pagos

1. Devuelve al IVR el valor a cancelar

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

VoIp.- Voz sobre un protocolo de internet

IVR de Asterisk.- Permite la interacción con bases de datos internas del sistema (MySQL o PostgreSQL)

6.0 Documentos

No existe documentos

Figura IV.40 Procesamiento del proceso aranceles

PROCESO DE CONSULTA DE ARANCELES COMPLEMENTARIOS DE MATRICULA PARA ESTUDIANTES DE PREGRADO

SERIAL: R02003	FECHA DE EMISIÓN:23/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Gonzalo Allauca

2.Area involucrada
Desarrollo

3. Fecha de reporte
23/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: X
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Gonzalo Allauca

2. Fecha de recepción
23/07/2012

3 Se trata de riesgo operativo
-Si: X
-No: -

4. Describir la acción tomada si fuese riesgo operativo.
El Técnico deberá comprobar que el usuario politécnico al llamar logre escuchar la cantidad que debe cancelar por su matricula.

5. Describir acción tomada.
Informar a los admirativos de cada equipo y realizar los test necesarios hasta lograr que se escuche el valor a cancelar y las comprobaciones en los sistemas Académicos y Sistema de pagos

Figura IV.41 Registro del proceso aranceles

i. **PROCESO:** Control de Sistemas de autentificación de Wireless de la ESPOCH

- **Propósito:** Control del funcionamiento del servicio Internet inalámbrico en la Institución.
- **Alcance:** El solicitante deberá tener alguna relación de dependencia académica o administrativa con la ESPOCH, sea esta permanente o temporal. Para poder acceder al servicio del Wireless de la Institución, se debe registrar en el sistema su cedula y su contraseña, la duración de este servicio será durante el periodo académico vigente.
- **Procesamiento:**

  Ing. Diego Palacios: Encargado del SAWE.

  Usuario Politécnico.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis "Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL".
  - Microsoft Visio 2010. Formas de diagrama SDL.
- **Documentos**: No existe ningún tipo de documento.

Los actores que intervienen en este proceso son:

Figura IV.42 Actores del proceso autentificación

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Control del Sistema de autenticación Wireless de la ESPOCH	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 26 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura IV.43 Hoja de planificación del proceso autentificación

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

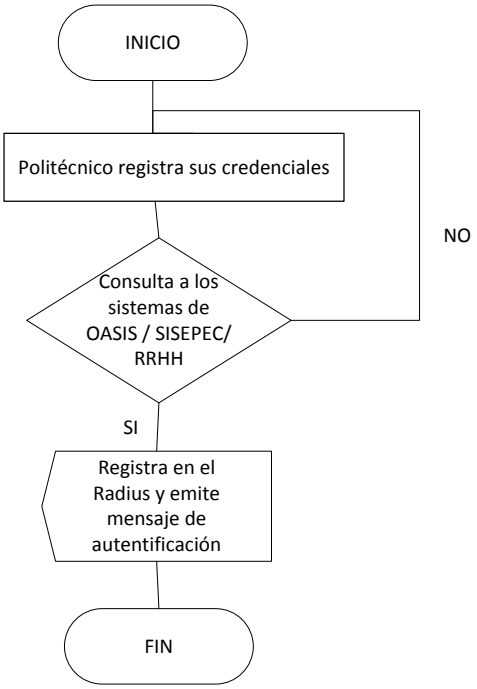


Figura IV.44 Flujograma del proceso autentificación

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

Una vez analizado el proceso control del sistema de autenticación Wireless de la ESPOCH realizaremos de la documentación del proceso en el formato establecido para el mismo:

	NOMBRE DEL PROCESO: Control del Sistema de autenticación Wireless de la ESPOCH	**DOCUMENTO:** P02004
EMISIÓN: 26/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Diego Palacios.

1.0 Propósito

Control del funcionamiento del servicio de internet inalámbrico en la institución.

2.0 Alcance

El solicitante deberá tener algún tipo de relación o dependencia académica o administrativa con la ESPOCH, sea esta permanente o temporal. Para poder acceder al servicio de Wireless de la Institución, se debe registrar en el sistema su cedula y su contraseña, la duración de este servicio será durante el periodo académico vigente.

3.0 Procedimiento

Encargado del SAWE

1. Controla la información de los usuarios registrados.
2. Controla que la información se guarde en el Radius de la Institución.

Usuario Politécnico

1. Registra sus credenciales

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

SAWE.- Sistema de autenticación Wireless ESPOCH.

Figura IV.45 Procesamiento del proceso autentificación

Para documentar el proceso este quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

CONTROL DEL SISTEMA DE AUTENTICACIÓN WIRELESS DE LA ESPOCH

SERIAL: R02004	FECHA DE EMISIÓN:26/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Diego Palacios

2.Area involucrada
Desarrollo

3. Fecha de reporte
26/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: -
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Diego Palacios

2. Fecha de recepción
26/07/2012

3 Se trata de riesgo operativo
-Si: X
-No: -

4. Describir la acción tomada
El técnico podrá a través el sistema controlar el ingreso de usuarios o eliminarlos para que se logré el acceso al uso de internet inalámbrico.

Figura IV.46 Registro del proceso autentificación

j. PROCESO: Administración y monitoreo del sistema de Recaudaciones

- **Propósito:** Administrar y monitorear el sistema de recaudaciones de la ESPOCH.
- **Alcance:** El cliente se acercará a ventanilla, el operador solicita número de cédula si el cliente no existe lo ingresará, caso contrario el cliente solicitará al operador los servicios (matricula, inscripciones, cursos y/o seminarios) o especies valoradas (papel politécnico, certificado de ingles, certificado de educación física), el operador seleccionará el producto o productos y preguntará al cliente la forma de pago (efectivo, cheque o tarjeta de crédito) y genera la factura.
- **Procesamiento:**

  Ing. Diego Palacios: Encargado del Sistema Financiero.

  Cliente.

  Operador: Encargado de registro de cliente y recaudación de rubros por venta de servicio o especie valorada.

  Supervisor: Encargado de la Administración del Sistema y visualización de Reportes.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.

- Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**: No existe ningún tipo de documento.

Los actores que intervienen en este proceso son:

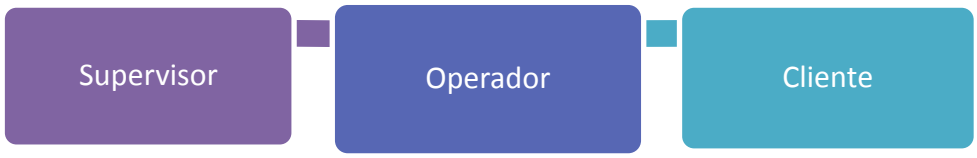


Figura IV.47 Actores del proceso recaudaciones

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Administración y monitoreo del sistema de recaudaciones	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 24 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura 4.48. Hoja de planificación del proceso recaudaciones

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

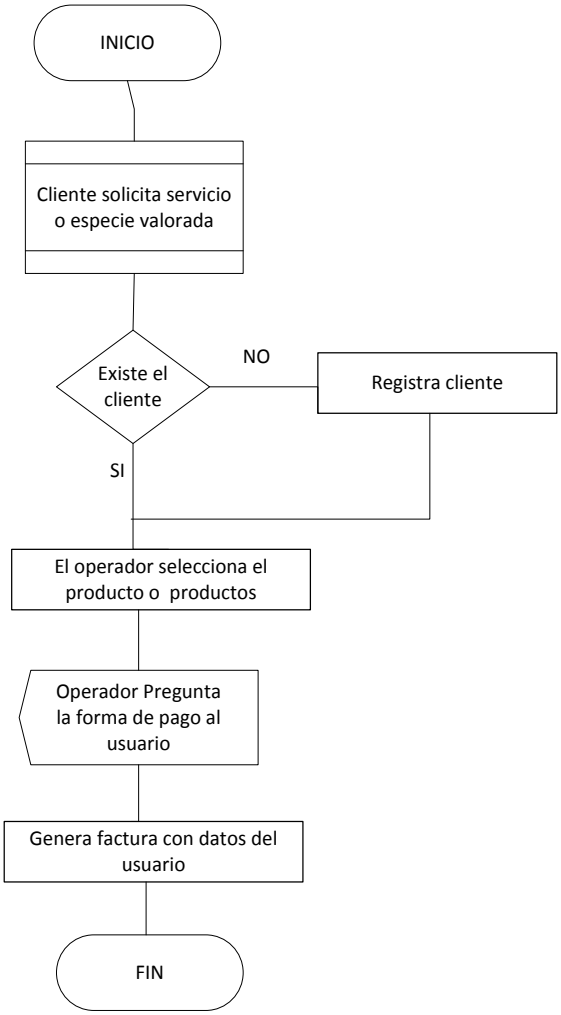


Figura IV.49 flujograma del proceso recaudaciones

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Administración y Monitoreo del Sistema de Recaudaciones	DOCUMENTO: P02005
EMISIÓN: 24/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Diego Palacios.

1.0 Propósito

Administrar y monitorear el sistema de recaudaciones de la ESPOCH.

2.0 Alcance

El cliente se acercará a la ventanilla, el operador solicita NÚMERO de cedula si el cliente no existe lo ingresará, caso contrario el cliente solicitará al operador los servicios o especies valoradas, el operador seleccionará el producto o productos y preguntará al cliente la forma de pago y genera la factura.

3.0 Procedimiento

Operador

1. Ingresa nuevos cliente
2. Selecciona producto o productos
3. Selecciona forma de pago
4. Genera factura.

Usuario

1. Solicita servicio o especie valorada.
2. Cancela por el producto o productos.

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Servicios.- Matrícula, inscripciones, cursos y/o seminarios

Especie valorada.- Papel politécnico, certificado de inglés y/o certificado de educación física, etc.

Forma de Pago.- Se puede cancelar en efectivo, cheque o tarjeta de crédito

6.0 Documentos

No existe documentos

Figura IV.50 Procesamiento del proceso recaudaciones

Una vez analizado el proceso Administración y monitoreo del sistema de recaudaciones realizaremos de la documentación del proceso en el formato establecido para el mismo:

Para documentar el proceso este quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

ADMINISTRACIÓN Y MONITOREO DEL SISTEMA DE RECAUDACIONES

SERIAL: R02005	FECHA DE EMISIÓN:24/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Diego Palacios

2.Area involucrada
Desarrollo

3. Fecha de reporte
24/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: -
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: X
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Diego Palacios

2. Fecha de recepción
24/07/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
Se comunicará al Director del DESITEL el problema y el director comunicará al encargado el problema que se ha suscitado.

Figura IV.51 registro del proceso recaudaciones

k. PROCESO: Administración y monitoreo del sistema de Retenciones

- **Propósito:** Administración y Monitoreo del sistema de retenciones de la ESPOCH.
- **Alcance:** El operador recibirá todos los documentos del tramite de pago al beneficiario, un beneficiario será quien brinda (prestaciones de servicios profesionales o venta de productos), el operador buscará al beneficiario en el sistema si este existe seleccionará el porcentaje de retención y generará la retención, caso contrario si no existe lo registra y continua con el proceso de retención.
- **Procesamiento:**

  Ing. Diego Palacios: Encargado del Sistema Financiero.

  Beneficiario.

  Operador: Encargado del registro de retenciones.

  Supervisor: Encargado de la Administración del Sistema y visualización de Reportes.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.
  - Microsoft Visio 2010. Formas de diagrama SDL.
- **Documentos**: No existe ningún tipo de documento.

Los actores que intervienen en este proceso son:

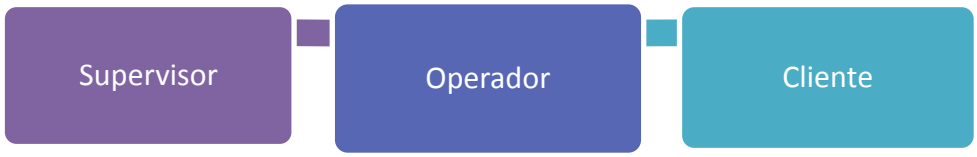


Figura IV.52 Actores del proceso retención

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Administración y monitoreo del sistema de Retenciones	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 25 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura IV.53 Hoja de planificación del proceso retención

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

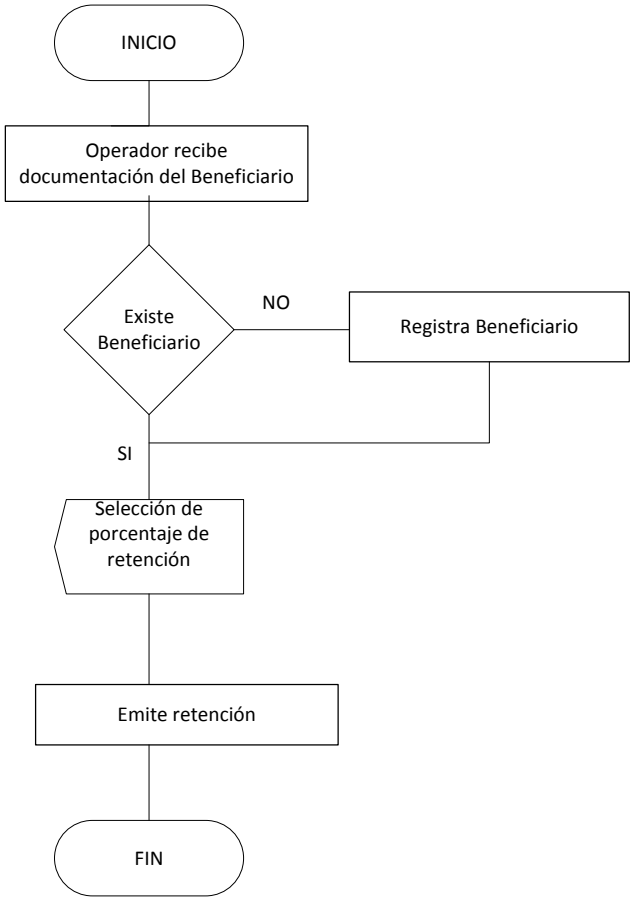


Figura IV.54 Flujograma del proceso retención

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Administración y Monitoreo del Sistema de Retenciones	**DOCUMENTO:** P02006
EMISIÓN: 25/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Diego Palacios.

1.0 Propósito

Administración y monitoreo del sistema de retenciones de la ESPOCH.

2.0 Alcance

El operador recibirá todos los documentos del tramite de pago al beneficiario, un beneficiario será quien brinda (prestaciones de servicios profesionales o venta de productos), el operador buscará al beneficiario en el sistema si existe seleccionará el porcentaje de retención y generará la retención, caso contrario lo registra y continua con el proceso de retención.

3.0 Procedimiento

Operador

1. Recibe los documentos del beneficiario.
2. Registra nuevos beneficiarios si no existen.
3. Selecciona el porcentaje de retención.

Beneficiario

1. Entrega los documentos para el trámite de pago.

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Retención.- Es la cantidad que se retiene de un sueldo, salario u otra percepción para asegurar el pago del impuesto.

6.0 Documentos

No existe documentos

Figura IV.55 Procesamiento del proceso retención

Una vez analizado el proceso Administración y monitoreo del sistema de Retenciones realizaremos de la documentación del proceso en el formato establecido para el mismo:

ADMINISTRACIÓN Y MONITOREO DEL SISTEMA DE RETENCIONES

SERIAL: R02006	FECHA DE EMISIÓN:25/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Diego Palacios

2.Area involucrada
Desarrollo

3. Fecha de reporte
25/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : -
-Sistemas: -
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: X
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Diego Palacios

2. Fecha de recepción
25/07/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
Se comunicará al Director del DESITEL el problema y el director comunicará al encargado el problema que se ha suscitado.

Figura IV.56 Registro del proceso retención

l. PROCESOS: Elaboración de proforma presupuestaria

- **Propósito:** Control de la elaboración de proforma presupuestarias de la ESPOCH.
- **Alcance:** El director de centro de costo que pueden ser (Directores, Decanos, Vice-Decanos coordinadores departamentales) elaboran un presupuesto de su unidad, envían el documento al departamento financiero, realizan un informe y emiten a consejo politécnico, si lo aprueba asigna el presupuesto, si no regresará al Director del centro tiene que repetir todo el proceso ya que ningún Departamento puede trabajar si un presupuesto (salarios, proyectos, etc.)
- **Procesamiento:**

  Ing. Aníbal Herrera: Encargado del proceso en la BD centralizada.

  Directores departamentales: Encargados de realizar la proformas presupuestales.
- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis "Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL".
  - Microsoft Visio 2010. Formas de diagrama SDL.
- **Documentos**: No existe ningún tipo de documento.

Los actores que intervienen en este proceso son:

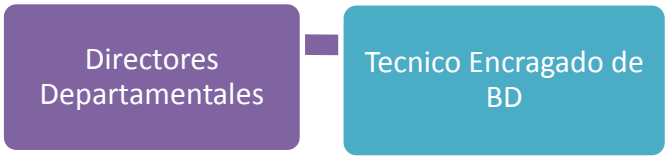


Figura IV.57 Actores del proceso proforma

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Administración y monitoreo del sistema de Recaudaciones	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 27 de julio del 20102 a partir de las 9 de la mañana	Ninguna

Figura IV.58 Hoja de planificación del proceso proforma

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

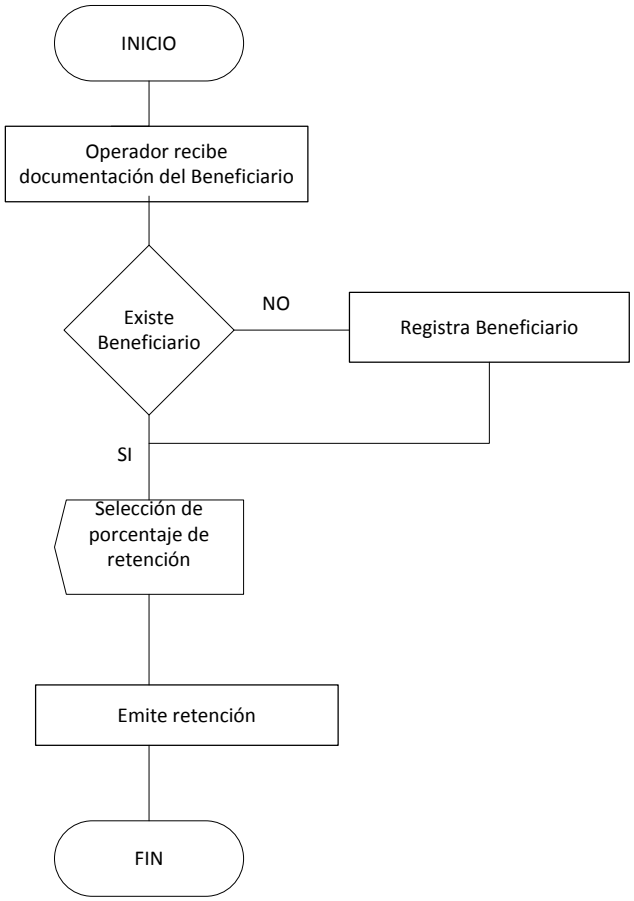


Figura IV.59 Flujograma del proceso proforma

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Elaboración de proforma presupuestarias	**DOCUMENTO:** P02007
EMISIÓN: 27/07/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Aníbal Herrera.

1.0 Propósito

Control de la elaboración de proformas presupuestarias de la ESPOCH.

2.0 Alcance

El director departamental elabora un presupuesto de su unidad, envía el documento al departamento financiero, el departamento financiero realiza un informe y emite a consejo politécnico, consejo politécnico aprueba o no el documento si es que si envía un informe indicando el presupuesto asignado y envía al director departamental si es que no se le solicita al director departamental realice otra vez el presupuesto, ningún departamento puede trabajar sin un presupuesto

3.0 Procedimiento

Director departamental

1. Realiza la proforma de su unidad.

Departamento financiero

1. Analiza el presupuesto si existe
2. Asigna presupuesto

Consejo Politécnico

1. Aprueba o no el presupuesto de la unidad mas el informe de Departamento financiero.

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Presupuesto.- Puede ser para salarios, proyectos, necesidades, etc.

6.0 Documentos

No existe documentos

Figura IV.60 Procesamiento del proceso proforma

Para documentar el proceso este quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

ELABORACION DE PROFORMA PRESUPUESTARIAS

SERIAL: R02007	FECHA DE EMISIÓN:27/07/2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Aníbal Herrera

2.Area involucrada
Desarrollo

3. Fecha de reporte
27/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : X
-Sistemas: -
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Aníbal Herrera

2. Fecha de recepción
27/07/2012

3 Se trata de riesgo operativo

-Si: -
-No: -

4. Describir la acción tomada

El departamento financiero comunicará al Director del DESITEL que se ha realizado el ingreso o modificación de la información, el Director indicará al encargado del sistema que realice las respectivas correcciones.

Figura IV.61 Registro del proceso proforma

m. PROCESO: Culminación de malla curricular

- **Propósito:** Determinar el cumplimiento de requisitos previos al proceso de graduación.
- **Alcance:**

  El estudiante debe cumplir con los siguientes requerimientos:

  - Haber aprobado la malla curricular,
  - Presentar el informe de las prácticas pre-profesionales.
  - Cumplir con las obligaciones establecidas en la normativa institucional:

  La secretaria de la escuela enviará a Secretaria Académica institucional, la carpeta académica del estudiante con la documentación respectiva para realizar la auditoria; si cumple con lo estipulado, enviará un informe favorable a la secretaria de la escuela a la que pertenece el estudiante; caso contrario, solicitará a la secretaria de la escuela efectuar los correctivos recomendados por Auditoría, a fin de cumplir con los requerimientos exigidos.

  En las carpetas académicas de los estudiantes, debe constar la siguiente documentación:

  - Fotocopia documentos personales
  - Fotocopia titulo de bachiller
  - Certificado medico
  - Certificado inscripción
  - Certificado de la UISELG
  - Certificados de no adeudar a las diferentes dependencias de la institución

- Certificados de aprobación de los niveles de Inglés, Expresión Artística y Cultura Física
- Matrículas y pagos de primero al ultimo nivel
- Tres copias del record académico
- En caso de retiro de asignatura/s o reingreso dentro del periodo que corresponda, debe constar en la carpeta la solicitud autorizada
- En caso de convalidación de asignaturas, debe constar la resolución de Consejo Académico, Consejo Directivo y respaldos de documentos exigidos para este trámite.

- **Procesamiento:**

  Ing. Alex Tacurí: Encargado del Sistema Académico - OASIs.

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los archivos de actas y calificaciones.

  Secretaria Académica: Encargada de Velar por el desarrollo académico Institucional en el ámbito de pregrado y postgrado.

  Estudiante.

- **Referencias:**
  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis “Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL”.
  - Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**:

- Estatutos Politécnicos
- Reglamento de Régimen Académico 2009.

Los actores que intervienen en este proceso son:

Figura IV.62 Actores del proceso culminación malla

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Culminación de la malla curricular	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 1 de agosto del 2012 a partir de las 9 de la	Ninguna

Figura IV.63. Hoja de planificación del proceso culminación malla

			mañana	

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

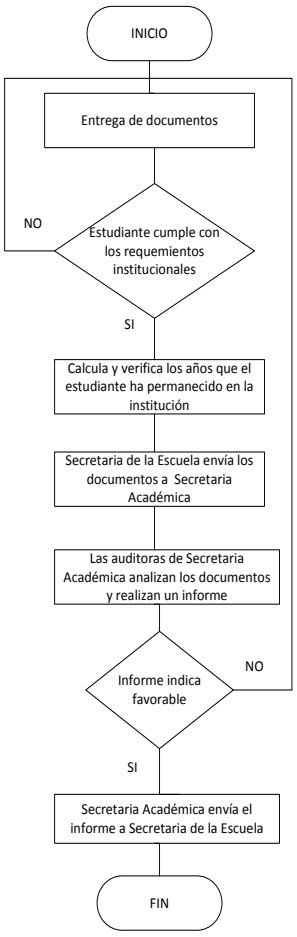


Figura IV.64 Flujograma del proceso culminación malla

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

	NOMBRE DEL PROCESO: Culminación de la malla curricular	**DOCUMENTO:** P02009
EMISIÓN: 1/08/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Alex Tacuri.

1.0 Propósito

Determinar el cumplimiento de requisitos previos al proceso de graduación.

2.0 Alcance

El estudiante debe cumplir con los siguientes requerimientos:

- Haber aprobado la malla curricular
- Presentar el informe de las practicas pre – profesionales
- Cumplir con las obligaciones establecidas en la normativa institucional.

La secretaría de la escuela enviará a secretaría académica institucional, la carpeta académica del estudiante con la documentación respectiva para realizar la auditoria; si cumple lo estipulado, enviará informe favorable a la secretaría de la escuela a la que pertenece el estudiante, caso contrario, solicitará a la secretaría de la escuela efectuar los correctivos recomendados por Auditoria, a fin de cumplir con los requerimientos exigidos.

- Fotocopia documentos personales
- Fotocopia titulo de bachiller
- Certificado medico
- Certificado inscripción
- Certificado de la UISELG
- Certificados de no adeudar a las diferentes dependencia de la institución
- Certificados de aprobación de los niveles de Inglés, expresión Artística y Cultura Física
- Matrículas y pagos de primero a ultimo nivel
- Tres copias del record académico
- En caso de retiro de asignatura/s o reingreso dentro del periodo que corresponda, debe constar en la carpeta la solicitud autorizada.
- En caso de convalidación de asignaturas, debe constar la resolución de Consejo Académico, Consejo Directivo y respaldos de documentos exigidos para este trámite.

3.0 Procedimiento

Secretaria de la escuela

1. Enviar la carpeta del estudiante

Secretaría Académica

2. Enviar informe favorable
3. Solicita efectuar correctivos de la documentación

Estudiante

1. Cumplir con los requerimientos

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

Presupuesto.- Puede ser para salarios, proyectos, necesidades, etc.

6.0 Documentos

- ✓ Estatutos Politécnicos
- ✓ Reglamento de Régimen Académico 2009

Figura IV.65 Procesamiento del proceso culminación malla

Este proceso quedará en los registros del Sistema de información de seguridad de Información del DESITEL bajo la Norma ISO 27001.

CULMINACION DE LA MALLA CURRICULAR

SERIAL: R02009	FECHA DE EMISIÓN:1/08/ 2012	FECHA DE MODFIFICACION:-	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Alex Tacuri

2.Area involucrada
Desarrollo

3. Fecha de reporte
27/07/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : X
-Sistemas: -
-Eventos externos:-
-Aspectos legales:-
-Actos Internos: -
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Alex Tacuri

2. Fecha de recepción
27/07/2012

3 Se trata de riesgo operativo
-Si: -
-No: -

4. Describir la acción tomada
En caso de que la información sea mal registrada se solicitará al Director del DESITEL que se realiza las debidas rectificaciones.

Figura IV.66 Registro del proceso culminación malla

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL DESITEL		
SERIAL: P00002	FECHA DE EMISIÓN:02/08/2012	FECHA DE MODFIFICACION:-	APROBACAION: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

Proceso de culminación de la malla curricular

ALCANCE: Informar las secretarias de todas las facultades el orden de los documentos para presentar la carpeta para la auditoria académica.

VIGENCIA: 6 meses al iniciar el periodo académico

POLITICA

Se deberá presentar las carpetas con el siguiente orden:

- Fotocopia documentos personales
- Fotocopia titulo de bachiller
- Certificado medico
- Certificado inscripción
- Certificado de la UISELG
- Certificados de no adeudar a las diferentes dependencia de la institución
- Certificados de aprobación de los niveles de Inglés, expresión Artística y Cultura Física
- Matrículas y pagos de primero a ultimo nivel
- Tres copias del record académico
- En caso de retiro de asignatura/s o reingreso dentro del periodo que corresponda, debe constar en la carpeta la solicitud autorizada.
- En caso de convalidación de asignaturas, debe constar la resolución de

	Consejo Académico, Consejo Directivo y respaldos de documentos exigidos para este trámite.

En base al análisis del se ha mostrado que necesita la declaración de una política para este proceso.

n. PROCESO: Matriculación de tesis

- **Propósito:** Control de las matriculaciones de las tesis en la ESPOCH.
- **Alcance:** El estudiante politécnico deberá cumplir requisitos(estar matriculado en la materia de diseño de tesis o haber culminado la malla curricular) si este fuera el caso el estudiante deberá escoger un director de tesis, tema de tesis, deberá desarrollar el anteproyecto de tesis, si el director lo aprueba se enviará a CIFIE, el mismo que envía una resolución aprobando (que no exista otra tesis con el mismo nombre), el tema de tesis e indicando el tribunal, el estudiante organizará con los profesores asignados el día de la defensa del anteproyecto, Ese día los profesores harán los cambios respectivos y emitirán una nota cada uno sobre la defensa del tema de tesis, el estudiante entregará en secretaria del vicedecanato el anteproyecto corregido si existieron cambios y las notas, secretaria del vicedecanato enviará al CIFIE, el mismo que aprobará y emitirá la resolución para indicar el orden de matricula de la tesis, el estudiante se acercará a su respectiva escuela donde la secretaria entregará la orden de pago para la matrícula y el estudiante deberá cancelar en la tesorería de la institución y entregar nuevamente a la secretaria de la escuela quien registrará en el sistema la matricula de la tesis, la fecha que fue emitida la resolución será la que indica que empieza a transcurrir el plazo de tiempo de elaboración de la tesis.

Figura 4.67. Política del proceso culminación malla

- **Procesamiento:**

  Ing. Alex Tacuri: Encargado del Sistema Académico.

  Director de Tesis: Encargado del tema de tesis del estudiante.

  Secretaria de la Escuela: Encargada de la documentación de los estudiantes y de los archivos de actas y calificaciones.

  Secretaria Vicedecanato: Encargado de planificación, convalidación y trámites administrativos de los estudiantes.

  Estudiante.

- **Referencias:**

  - Punto E. Flujograma Matricial Normativos Propuesta de la Metodología para documentar los procesos. Tesis "Implementación de la Norma ISO 27001 para la Gestión en Seguridad de Información. Caso práctico DESITEL".
  - Microsoft Visio 2010. Formas de diagrama SDL.

- **Documentos**:

  - Estatutos Politécnicos
  - Reglamento de Régimen Académico 2009.

Los actores que intervienen en este proceso son:

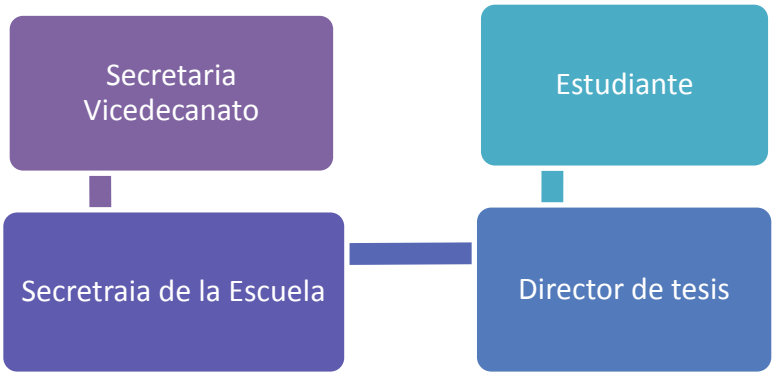


Figura IV.68 Actores del proceso matriculación

Con la utilización de las hojas para planificar precederemos a la reunión al encargado del proceso de creación de cuentas de correo.

	HOJA DE PLANIFICACIÓN PARA LEVANTAMIENTO DE PROCESOS			
Proceso a documentar	**Alcance**	**Actores de intervienen**	**Convocatoria para reunión**	**Observaciones**
Matriculación de tesis	Recolección de la información necesaria del proceso	Técnico Encargado del proceso	La reunión se realizó el día 8 de agosto del 2012 a partir de las 9 de la mañana	Ninguna

Figura IV.69 Hoja de planificación del proceso matriculación

Para la arquitectura del procesamiento procedemos a realizar el flujograma matricial normativo.

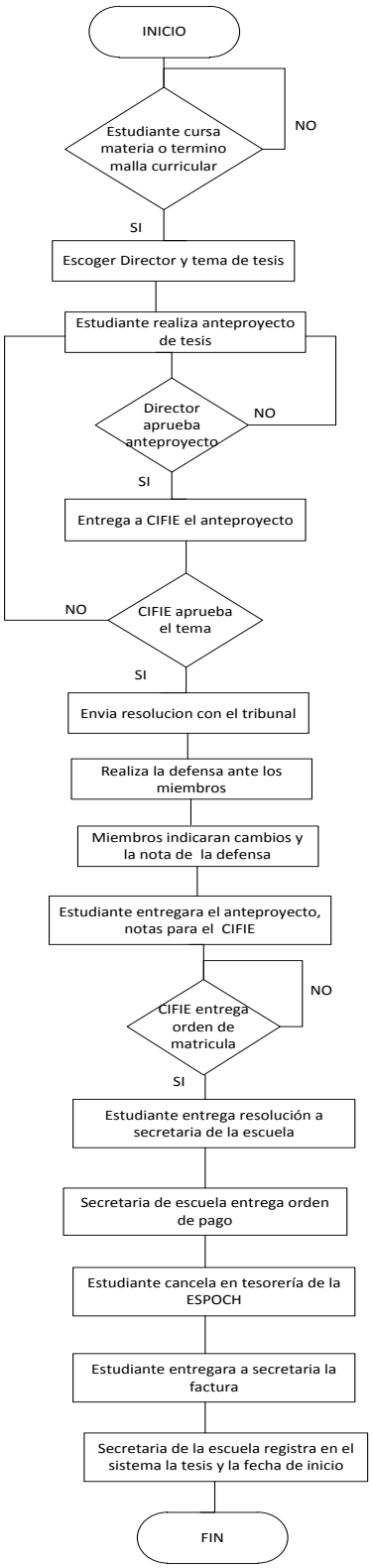


Figura 4.70. Flujograma del proceso matriculación

	NOMBRE DEL PROCESO: Matriculación de tesis	**DOCUMENTO:** P020012
EMISIÓN: 8/08/2012	GENERADO POR: Tesista	APROBACIÓN Y REVISADO POR: Ing. Alex Tacuri.

1.0 Propósito

Controlar los registros de notas de los docentes al sistema Académico de la ESPOCH.

2.0 Alcance

El estudiante politécnico deberá cumplir requisitos(estar matriculado en la materia de diseño de tesis o haber culminado la malla curricular) si este fuera el caso el estudiante deberá escoger un director de tesis, tema de tesis, deberá desarrollar el anteproyecto de tesis, si el director lo aprueba se enviará a CIFIE, el mismo que envía una resolución aprobando(que no exista otra tesis con el mismo nombre), el tema de tesis e indicando el tribunal, el estudiante organizará con los profesores asignados el día de la defensa del anteproyecto, Ese día los profesores harán los cambios respectivos y emitirán una nota cada uno sobre la defensa del tema de tesis, el estudiante entregará en secretaria del vicedecanato el anteproyecto corregido si existieron cambios y las notas, secretaria del vicedecanato enviará al CIFIE, el mismo que aprobará y emitirá la resolución para indicar el orden de matricula de la tesis, el estudiante se acercara a su respectiva escuela donde la secretaria entregará la orden de pago para la matrícula y el estudiante deberá cancelar en la tesorería de la institución y entregar nuevamente a la secretaria de la escuela quien registrará en el sistema la matricula de la tesis, la fecha que fue emitida la resolución será la que indica que empieza a transcurrir el plazo de tiempo de elaboración de la tesis

3.0 Procedimiento

Director de tesis

1. Subir las notas al sistema académico
2. Debe imprimir las actas de notas
3. Debe entregar en secretaria las notas impresas
4. Realiza oficio al director si no alcanzó a entregar

Secretaría Escuela

1. Recibe las notas de los profesores
2. Entrega orden de pago al estudiante
3. Recibe la factura de el pago
4. Registra en el sistema la tesis y la fecha de inicio

Secretaria Vicedecanato

1. Entrega a CIFIE el anteproyecto del estudiante
2. Entrega a CIFIE la notas y cambios de la defensa del anteproyecto

Estudiante

1. Escoge director de tesis y tema de tesis
2. Realizar anteproyecto de tesis
3. Realiza defensa ante los miembros
4. Entrega resolución en secretaria de la escuela
5. Cancela en tesorería el valor indicado

CIFIE

1. Aprueba tema de tesis y director de tesis y asigna miembros
2. Envía resoluciones con los miembros del tribunal
3. Analiza y emite fecha de matriculación de tema de tesis

Miembros del tribunal

1. Indican los cambios a realizar de la tesis
2. Colocan una nota por la defensa del anteproyecto

4.0 Referencias

Punto E. flujograma matricial normativo propuesta de la metodología para documentar los proceso. Tesis "Implementación de la Norma ISO 27001 para la gestión de seguridad de información. Caso práctico DESITEL"

5.0 Definiciones

CIFIE.- Centro de investigación de la Facultad De Informática Y Electrónica

6.0 Documentos

- ✓ Estatutos Politécnicos
- ✓ Reglamento de Régimen Académico 2009

Figura IV.71 Procesamiento del proceso de matriculación de tesis

Para la validación del flujograma matricial constará la firma de responsabilidad del encargado del proceso con esto quedará constancia de la validez del documento este se encuentra en el **ANEXO III**: **(**Flujogramas Validados**)**

Una vez analizado el proceso de matriculación de tesis realizaremos de la documentación del proceso en el formato establecido para el mismo:

MATRICULACIÓN DE TESIS			
SERIAL: R020012	FECHA DE EMISIÓN:8/08/ 2012	FECHA DE MODFIFICACIÓN: -	APROBACIÓN: SI
ELABORADO POR: Tesista	REVISADO Y APROBADO POR: Dr. Carlos Buenaño		NÚMERO DE PÁGINA:1 de 1

DETECCIÓN DE INCIDENTES

1. Nombre del Informante
Ing. Alex Tacuri

2.Area involucrada
Desarrollo

3. Fecha de reporte
8/08/2012

4. Lugar del Incidente
Área de Desarrollo del DESITEL

5. Tipo de Incidente

-Personas: X
-Procesos : X
-Sistemas: -
-Eventos externos:-
-Aspectos legales: -
-Actos Internos: X
-Prácticas laborales:-
-Daño a activos:-
-Incumplimiento a normas: -

TÉCNICO INFORMÁTICO

1. Nombre del Supervisor o encargado
Ing. Alex Tacuri

2. Fecha de recepción
8/08/2012

3 Se trata de riesgo operativo

-Si: -
-No: -

4. Describir la acción tomada

El Director de escuela solicitará al Director del DESITEL mediante resolución que realiza los cambios correctivos en el sistema mediante un oficio. El director del DESITEL indicará al encargado del Sistema que haga los cambios.

Figura IV.72 Registro del proceso de matriculación de tesis

4.3 ANALISIS DE RESULTADOS

Para la tabulación de los resultados se analizan los datos obtenidos al realizar la encuesta en el DESITEL frente a la implantación de la norma ISO 27001 en el levantamiento de procesos, para ello nos guiamos en tres parámetros importantes en el Sistema de Seguridad de Información.

- Confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.
- Integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Para ellos realizamos un análisis del Departamento de sistemas y telemática **antes** de la implementación de la norma ISO 27001 para la gestión de seguridad de información, y **posteriormente** una vez que se ha empezado a utilizar las políticas y manuales de la gestión de seguridad.

Para ello realizamos encuestas que nos ayuda a la recolección de la información. **Anexo IV.I** (Encuestas de la situación anterior), **Anexo IV.II** (Encuestas de la situación con el uso de la Norma ISO en la Gestión de seguridad).

Los datos obtenidos están descritos en la siguiente tabla la cual esta presentada de forma porcentual

El tema de investigación posee un paradigma Critico- Propositivo por que se diagnóstica y analiza la situación actual del DESITEL y se plantea una alternativa de solución para respaldar la información existente.

POBLACION Y MUESTRA

POBLACION

El estudio que se ha realizado en el Departamento De Sistemas Y Telemática De La Escuela Superior Politécnica De Chimborazo, posee 11 profesionales informáticos que manejan los procesos.

MUESTRA

En este caso nuestro universo será la misma cantidad que nuestra población ya que no sobrepasa las 30 personas.

- ✓ El número de encuestados esta representado por N: **N=11**

- ✓ El valor que en nuestras filas será un total de 11 ya que las preguntas pueden tener un valor de 11 como máximo y se pueden distribuir entre las 3 opciones:

  11 100%|
  x ? = **(X * 100)/11 =**

- ✓ Por lo tanto la fórmula porcentual de las columnas para cada pregunta será la sumatoria de las preguntas, ya que el máximo de cada pregunta es 11 la sumatoria es de 44 y la formula será:

  44 100%
  ∑(X) ? = **(∑(X) * 100)/44 =**

- ✓ Y por último para encontrar el valor porcentual general del total será de 44 por las 3 opciones de respuesta que es 132.

  132 100%
  ∑ (X, Y, Z) ? = **(∑ (X, Y, Z) * 100)/132**

TABLA IV.II
VALORES PORCENTUALES DE LAS ENCUESTAS

Indicador / Pregunta		Antes			%	Después			%
		Si(X)	No(Y)	Par(Z)		Si	No	Par	
Disponibilidad	1	0	63,6	36,4	100	81,8	0	18,2	100
	3	0	72,7	27,3	100	90,9	0	9,1	100
	10	18,2	54,5	27,3	100	90,9	9,1	0	100
	11	0	90,9	9,1	100	100	0	0	100
Total disponibilidad		4,55	70,4	25	100	90,9	2,3	6,8	100
Integridad	4	72.7	9,1	18,2	100	90,9	0	9,1	100
	5	90,9	0	9,1	100	90,9	0	9,1	100
	6	81,8	9,1	9,1	100	90,9	0	1	100
	9	90,9	0	9,1	100	100	0	0	100
Total integridad		84,1	4,5	11,4	100	93,2	0	6,8	100
Confidencialidad	2	18,2	63,6	18,2	100	9,1	81,8	9,1	100
	7	72,7	0	27,3	100	90,9	0	9,1	100
	8	0	45,5	54,5	100	63,6	0	36,4	100
Total confidencialidad		30,3	36,4	33,3	100	54,5	27,3	18,2	100
TOTAL		**39,6**	**37,2**	**23,2**	**100**	**79,5**	**9,9**	**10,6**	**100**

Elaborado por: Lucia Guevara

ANALISIS DE LOS RESULTADOS POR INDICADOR

DISPONIBILIDAD:

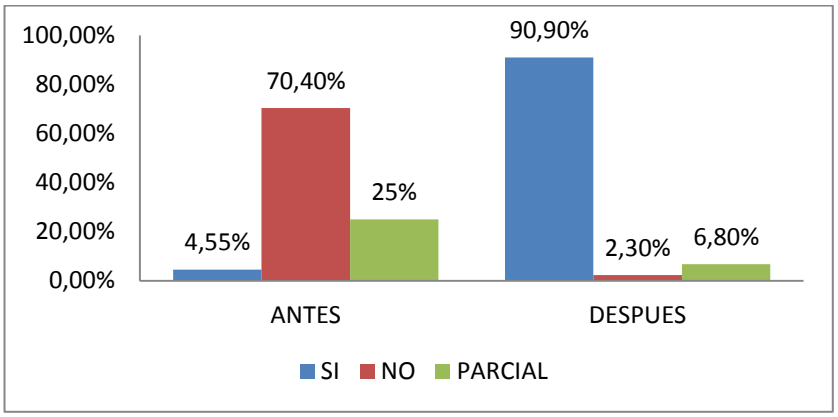


Figura IV.73 Gráfico de resultados indicador de disponibilidad

Al obtener los datos nos muestra que en el indicador de disponibilidad ha existido un incremento en la gestión de la seguridad de la información de 86,35% es decir que la información estará al alcance de quien la necesite.

INTEGRIDAD:

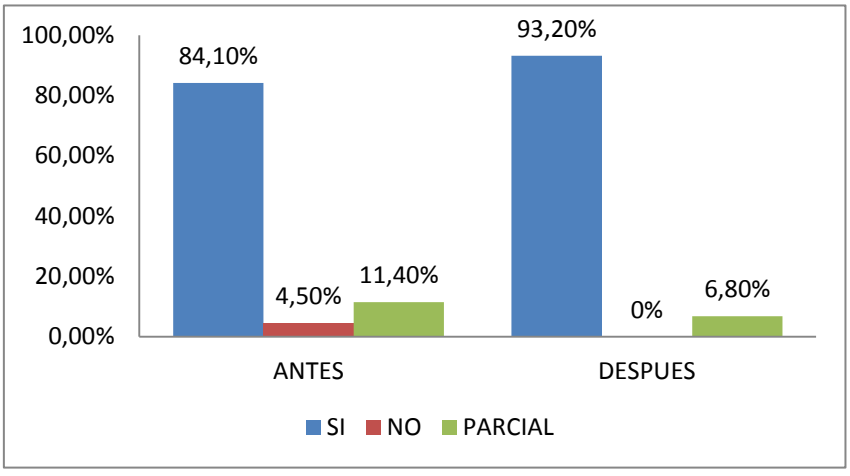


Figura IV.74 Gráfico de resultados indicador de integridad

Al obtener los datos nos muestra que en el indicador de integridad ha existido un incremento en la gestión de la seguridad de la información de casi un 10% es decir que ha existido un incremento en la creación de procesos exactos en la gestión de la seguridad de la información.

CONFIDENCIABILIDAD:

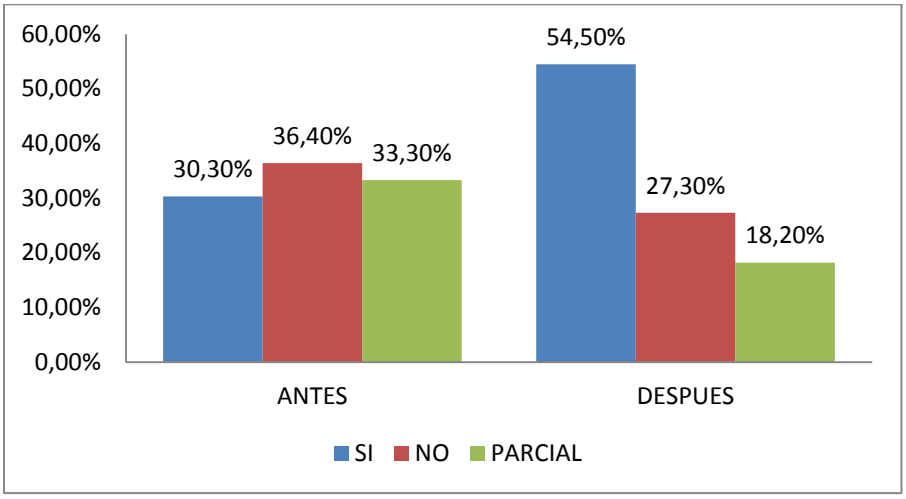


Figura IV.75 Gráfico de resultados indicador de confidencialidad

Al obtener los datos nos muestra que en el indicador de confidencialidad ha existido un incremento en la gestión de la seguridad de la información de casi un 25% es decir que ha existido un incremento en la seguridad de la información y su acceso a personas solo del personal y que no ha existidos salida de esta información que pueda perjudicar al Departamento de Sistemas y Telemática.

ANÁLISIS DE LAS DE LA INVESTIGACIÓN:

TABLA IV.III
VALORES PORCENTUALES TOTALES

MOMENTOS	OPCIONES		
	SI	NO	PARCIAL
ANTES	39,60%	37,20%	23,20%
DESPUES	79,50	9,90%	10,60%

Elaborado por: Lucia Guevara

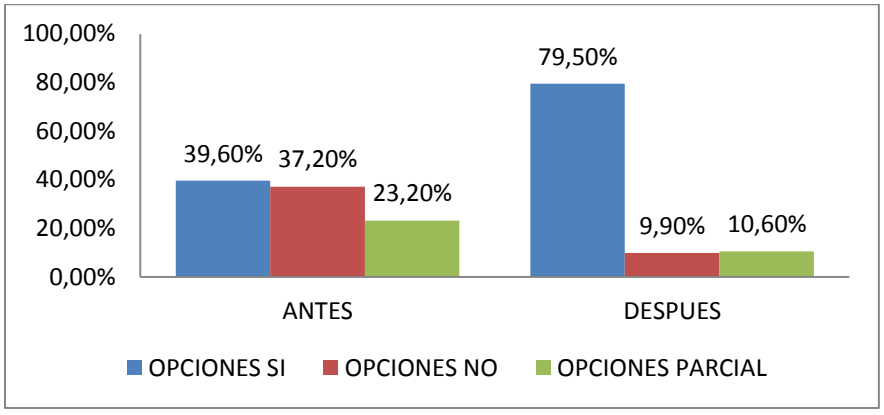


Figura IV.76 Gráfico de resultados generales de la investigación

INCREMENTO = 79,50 – 39,60 = El incremento es de **40%**

Al obtener los resultados que nos muestra la tabla general mediante el gráfico podemos observar el incremento del 40% que ha existido en la mejora de la seguridad de la información con el uso de políticas y manuales para la gestión de la información con las Norma ISO 27001.

4.4 COMPROBACION DE HIPOTESIS GENERAL

a) Modelo Lógico

H_1 (Hipótesis Alterna**)**

El cumplimiento de políticas y manuales basados en la Norma ISO 27001, **permitirán** incrementar la gestión de seguridad en la información (SGSI) en el DESITEL.

H_0 (Hipótesis Nula**)**

El cumplimiento de políticas y manuales basados en la Norma ISO 27001, **no permitirán** incrementar la gestión de seguridad en la información (SGSI) en el DESITEL

b) Modelo Estadístico

$H_1 > H_0$

$H_1 \neq H_0$

- **Nivel de Significación**

  95% de confianza = 5% de error ⇒ 0,05

- **Zona de rechazo de la Hipótesis**

  Nula (H_0)

- **Fórmula para el cálculo JI-CUADRADO**

$$X^2 = \frac{(A_1 - D_1)^2}{D_1} + \frac{(A_2 - D_2)^2}{D_2} + \frac{(A_3 - D_3)^2}{D_3} = \sum_{J=1}^{K} (A_J - D_J)^2 \ / \ D_J$$

Donde: x es la letra de ji y x^2 se lee ji- cuadrado.

X^2 = ji cuadrado

A = porcentaje antes de

D = porcentaje después de.

J= el NÚMERO de opciones que se tiene

INTERPRETACION DE RESULTADOS

VARIABLES

- ✓ INDEPENDIENTE

  Cumplimiento de las políticas y manuales basados en la Norma ISO 27001

- ✓ DEPENDIENTE

  Gestión De La Seguridad De La Información (SGSI)

TABLA DE CONTINGENCIA

En la siguiente tabla nos muestra las frecuencias observadas y las frecuencias esperadas, esta tabla esta sujeta a la hipótesis planteada.

Indicador 1 = Disponibilidad Indicador 2 = Integridad

Indicador 3 = Confidencialidad

TABLA IV.IV
Frecuencias Obtenidas

VARIABLE DEPENDIENTE		VARIABLE INDEPENDIENTE						
		PREGUNTA	SIN ESTANDAR			CON ESTANDAR		
			SI	NO	PARCIAL	SI	NO	PARCIAL
H_0 No incrementa la gestión de seguridad de la información	I1	**1**	0	7	0	0	0	0
		3	0	8	0	10	0	0
		10	0	6	3	0	0	0
		11	0	10	0	0	0	0
	I2	**4**	8	0	0	0	0	0
		5	10	0	1	0	0	0
		6	9	0	1	0	0	0
		9	10	0	0	1	0	0
	I3	**2**	2	0	2	0	0	0
		7	8	0	0	0	0	1
		8	0	5	0	0	0	0
H_1 Incrementa la gestión de seguridad de la información	I1	**1**	0	0	4	9	0	2
		3	0	0	3	0	0	1
		10	2	0	0	10	0	2
		11	0	0	1	11	0	0
	I2	**4**	0	1	2	10	0	1
		5	0	0	0	10	0	1
		6	0	1	0	10	0	1
		9	0	0	1	11	0	0
	I3	**2**	0	7	0	0	9	1
		7	0	0	3	10	0	0
		8	0	0	6	7	0	4

La matriz que tenemos en la tabla IV.IV es de 11 x 6, 11 verticalmente y 6 horizontalmente.

Resolvemos la ecuación de tabla final de total de la matriz:

Frecuencia Observada	**49**	**45**	**27**
Frecuencia Observada	**99**	**9**	**14**

$$X^2 = \frac{(A_1 - D_1)^2}{D_1} + \frac{(A_2 - D_2)^2}{D_2} + \frac{(A_3 - D_3)^2}{D_3} = \sum_{J=1}^{K} (A_J - D_J)^2 / D_J$$

$$\sum_{J=1}^{K} (A_J - D_J)^2 / D_J = 170.32$$

$Gl_V = N - 1 \Rightarrow 11 - 1 = 10$ $\qquad$ $Gl_H = N - 1 \Rightarrow 6 - 1 = 5$

$$\sigma = \sqrt{\frac{\sum_{J=1}^{K} (A_J - D_J)^2 / D_J}{k - 1}}$$

$\sqrt{170,3/10}=4.13$
$\sqrt{170.32/5}=5.83$

Valor crítico $X^2_{.99} = 2.76$ $\qquad$ **Valor crítico $X^2_{.99} = 3.36$**

Para el valor de critico de ji – cuadrado de $X^2_{.99}$ en horizontal y verticalmente difieren las frecuencias significativamente por lo tanto **rechazamos H_0 y aceptamos H_1.**

H_1 (Verticalmente) > = H_0 (Verticalmente)

4,12 > = 2,76

H_1 (Horizontalmente) > = H_0 (Horizontalmente)

5,83 > = 3,36

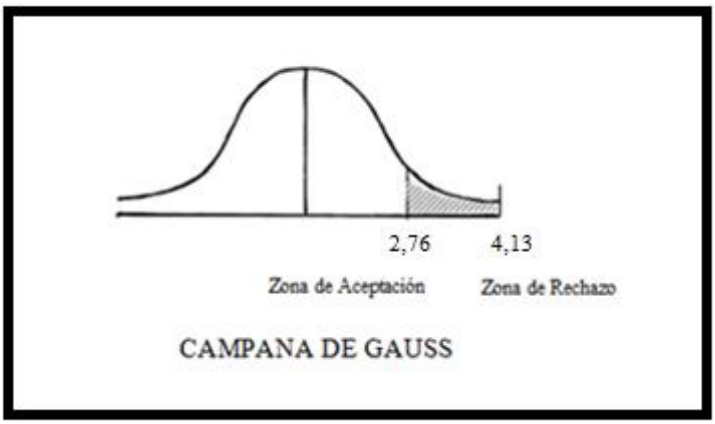


Figura IV.77 Campana de Gauss para el análisis

4.5 SOFTWARE UTILIZADO

SecuriaSGSI es un software libre el cual se puede obtener en www.securia.com libremente el código esta realizado en Java y la base de Datos en PostgreSql.

Las certificadoras recomienda el uso de este software para la gestión de documentos, gestión de incidentes, perfiles de usuarios, etc. Posee dos partes la partes I de el cliente, y la Parte II del administrador, es de muy fácil uso e instalación **Anexo V (**Manual de Usuario de Securia**).**

CONCLUSIONES

1. El análisis realizado sobre la metodología para la seguridad de la información permite gestionar las mejoras en la seguridad de la información del Departamento.

2. El estudio de la Norma ISO 27001 ha permitido el conocimiento de seguridad de información, sus problemas y los medios de protección además cubre con el vacío generado por la inexistencia de un método de documentación para los procesos críticos que maneja el DESITEL.

3. Mediante la recopilación de los activos involucrados en los sistemas de información perteneciente al DESITEL se pudo constatar la situación actual y posteriormente con el uso de la metodología de procesos se ha notado una mejora de 40% en la organización de la seguridad de la información en el DESITEL.

4. El uso de la Norma ISO 27001 en la organización de la seguridad de la información ayudará de forma interna al personal del DESITEL a mejorar las autorizaciones, acuerdos de confidencialidad y disponibilidad de la información de los procesos que manejan.

5. Con el uso del software facilitará el manejo de los documentos y el registro de incidentes que se desarrollan en el DESITEL, para la toma correcta de decisiones por parte del encargado del SGSI.

RECOMENDACIONES

1. Para una buena gestión de seguridad de la información es recomendable el cumplimiento de las políticas y documentación por parte del personal involucrado en el manejo de la Información.

2. Se considere que cualquier organización sin importar su tamaño requiere de una metodología para sus procesos para garantizar la comerciabilidad, integridad y disponibilidad de si información.

3. La puesta en práctica de la metodología de los procesos para que se garantice la seguridad por parte de los encargados de los procesos.

4. Se recomienda el uso de las políticas y documentos para que siempre quede constancia de cualquier eventualidad que suceda con la información que maneja el Departamento.

5. Se recomienda a los profesionales informáticos el uso de la documentación para que siempre este respaldada la información de la cual están encargados, en caso de cualquier tipo de suceso o auditoría de la información.

RESUMEN

Implementación de la Norma ISO 27001 para la Gestión En Seguridad De Información, caso práctico "DESITEL" Departamento de Sistemas y Telemática de la Escuela Superior Politécnica de Chimborazo.

Utilizando el método inductivo para la observación de la situación actual, la clasificación y análisis de los procesos que maneja el DESITEL, el método deductivo nos permite comprobar que la implementación de la Norma ISO mejorara la gestión de seguridad de la información. Para el desarrollo se utilizó una computadora portátil Toshiba, con Windows 7, 640 en Disco.

Para la metodología propuesta para la gestión de seguridad en información en los proceso se utilizo herramientas como Microsoft Visio 2010 para el diseño de Flujogramas normativos, Microsoft Excel para la tabulación de datos.

Una vez aplicado la metodología con el uso de la Norma ISO 27001 en la gestión en seguridad de la información se obtuvo un **40%** de incremento, analizado por los tres indicadores propuestos: en disponibilidad se obtuvo el 86,35%, en integridad se obtuvo el 10% y confidencialidad se obtuvo 25%.

Concluyo que la utilización de la Norma ISO 27001 mejora la gestión de seguridad de la información del Departamento de Sistemas y Telemática de la Escuela Superior Politécnica de Chimborazo.

Se recomienda la utilización de estas políticas y documentos para el respaldo de la información que se maneja el Departamento de Sistemas y Telemática de la Escuela Superior Politécnica de Chimborazo para que se garantice el incremento en la gestión en seguridad de la información.

SUMMARY

Implementation of the Standard ISO 27001 in the information Security Management. Case “DESITEL”.

The inductive method was used in order to diagnose the current situation, the classification and analysis of the procedures managed by DESITEL. The fact that the implementation of the standard ISO will improve the information security was proved by using the deductive method. In development of this project a Toshiba Laptop with Windows 7 and 640 in disk was used.

In order to carry out the proposed mythology to the information security management, tools such as Microsoft Visio 2010 for the design of flowcharts and Microsoft Excel 2010 for the data tabulation were used.

Once the methodology with the Standard ISO 27001 was appilied to the information security management a 40% of increment was reached. This was analyzed with the three proposed indicators; availability 86.35%, integrity 10% and confidentiality 25%.

The author stands the standard ISO 27001 improves the information security management in the Telematics and Systems Department of the Polytechnic Superior School of Chimborazo.

It is recommended to use these polices and documents to create a backup of the information in the Telematics and Systems Department of the Polytechnic Superior School of Chimborazo in order to guarantee the improvement of the information of the information security management.

ANEXO I. Activos y su Propietario

SISTEMA DE POSTGRADO Y EDUCACIÓN CONTINUA		
Esta Virtualizado SI [ ] NO [X]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	GlassFish 3.1	Ing. Aníbal Herrera
Lenguaje de Programación Frameworks	Java 1.7 Jsp 2.0	
Base de Datos	PostreSql 8.4	
Proceso de Backup	Script	
Consideraciones Adicionales (Clúster, Firewall,etc) Algoritmo de identificación de ataques en base a Ips.		

SISTEMA ACADÉMICO OASIS		
Esta Virtualizado Si [ˇ] NO [ ]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	IIS 6.0	Ing. Alex Tacuri
Lenguaje de Programación Frameworks	C# .Net 1.1	
Base de Datos	Sql Server 2008	
Proceso de Backup	Cintas, Script	

SISTEMA DE EDUCACIÓN VIRTUAL		
Esta Virtualizado SI [ ] NO [ ]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Apache 2.2	Ing. Gustavo Hidalgo
Lenguaje de Programación Frameworks	Php 5.3, Java Jdk 6.3	
Base de Datos	MySql 5.7	
Proceso de Backup	Script, Linux diario	
Consideraciones Adicionales (Clúster, Firewall, etc.) Firewall de Linux.		
Consideraciones Adicionales(Clúster, Firewall,etc) Cluster SI, Firewall SI, https		

SISTEMA DE BIBLIOTECA		
Esta Virtualizado Si .. NO		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Windows 2003 Server	Ing. Eduardo Tenelanda
Lenguaje de Programación Frameworks	.Net ASP	
Base de Datos	SQL Server 2000	
Proceso de Backup	SQL Server 2000	
Consideraciones Adicionales(Clúster, Firewall,etc)		

SISTEMA MEDICO		
Esta Virtualizado Si [ ] NO [ ]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	IIS 6.0	Ing. Alex Tacuri
Lenguaje de Programación Frameworks	C# .Net1.1	
Base de Datos	SQL Server 2008	
Proceso de Backup	Cintas, Scripts	
Consideraciones Adicionales (Clúster, Firewall SI, etc.)		

SISTEMA DE CONSULTA DE GASTOS DE SERVICIOS ACADEMICOS EDUCACIONALES COMPLEMENTARIOS		
Esta Virtualizado SI [ ] NO [x]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Asterisk 1.6.2.12	Ing. Gonzalo Allauca
Lenguaje de Programación Frameworks	PHP 5.1.6	
Base de Datos	Crond	
Proceso de Backup	Automatizado Crond	
Consideraciones Adicionales(Clúster, Firewall,etc)		

SISTEMA live@edu		
Esta Virtualizado Si ˅ NO		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Administración de Servicios Web, Base de Datos y Actualización de funcionalidades	Microsoft	Ing. Gonzalo Allauca
Implementación de Funcionalidades como creación automática de cuentas y listas de correo académicas y administrativas	CELULAS.NET	
Soporte	Ing. Gonzalo Allauca	
Consideraciones Adicionales(Clúster, Firewall,etc)		

SISTEMA DE ENCUESTAS INSTITUCIONAL		
Esta Virtualizado Si [v] NO [ ]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	IIS 6.0	Ing. Daniel Layedra
Lenguaje de Programación Frameworks	.NET 2 ASP	
Base de Datos	SQL Server 2005, en 172.30.60.91	
Proceso de Backup	Tares Programadas, Script	
Consideraciones Adicionales(Clúster, Firewall,etc)		

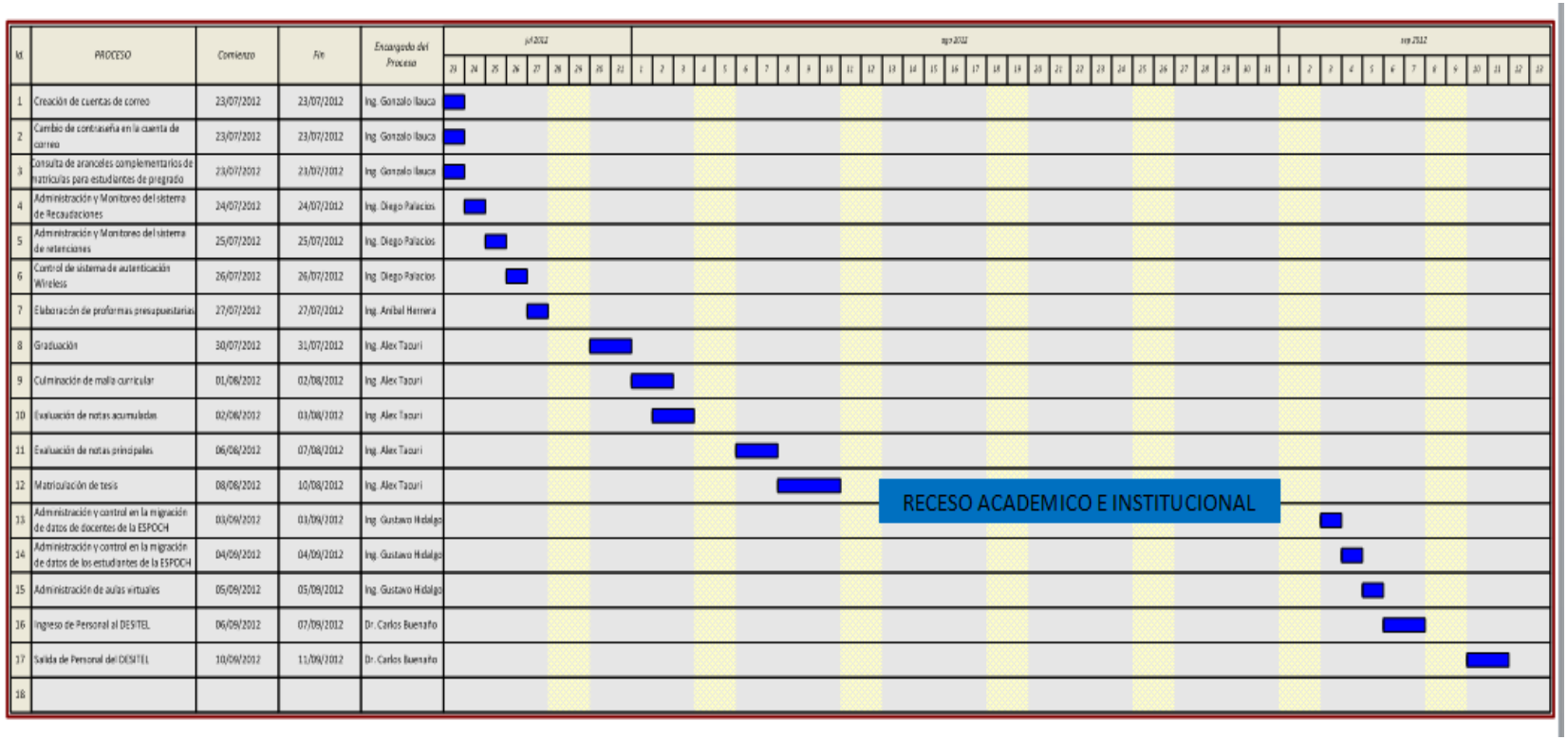
SISTEMA DE RECURSOS HUMANOS		
Esta Virtualizado Si ✓ NO		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Apache	Tglo. Iván Camacho
Lenguaje de Programación Frameworks	PHP	
Base de Datos	Mysql	
Proceso de Backup	Script	
Consideraciones Adicionales(Clúster, Firewall,etc)		

SISTEMA FINANCIERO		
Esta Virtualizado Si [ ] NO [v]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Escritorio	Ing. Diego Palacios
Lenguaje de Programación Frameworks	Java, J2SE, JDK 1.6	
Base de Datos	PostgreSql 8.4	
Proceso de Backup	Tareas programadas diarias c/4 horas	
Consideraciones Adicionales (Clúster, Firewall, Datacenter, etc.)		

SISTEMA ADMISIONES		
Esta Virtualizado Si [ ] NO [x]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Apache 2.2	Ing. Gustavo Hidalgo
Lenguaje de Programación Frameworks	Php 5.3 JDK 6.3	
Base de Datos	MySQL 5.7.11	
Proceso de Backup	Script Linux diario	
Consideraciones Adicionales (Clúster, Firewall, IPTables, etc.)		

SISTEMA DSPACE		
Esta Virtualizado Si [ ] NO [x]		
	SOFTWARE Y VERSIÓN	PROPIETARIO
Servidor web	Tomcat 5	Ing. Aníbal Herrera
Lenguaje de Programación Frameworks	Java 1.7 JSP 2.0	
Base de Datos	PostgreSQL 8.1	
Proceso de Backup	Script	
Consideraciones Adicionales (Clúster, Firewall, etc.)		

ANEXO II. Diagrama de Elaboración De Procesos



Id.	PROCESO	Comienzo	Fin	Encargado del Proceso
1	Creación de cuentas de correo	23/07/2012	23/07/2012	Ing. Gonzalo Ilauca
2	Cambio de contraseña en la cuenta de correo	23/07/2012	23/07/2012	Ing. Gonzalo Ilauca
3	Consulta de aranceles complementarios de matrículas para estudiantes de pregrado	23/07/2012	23/07/2012	Ing. Gonzalo Ilauca
4	Administración y Monitoreo del sistema de Recaudaciones	24/07/2012	24/07/2012	Ing. Diego Palacios
5	Administración y Monitoreo del sistema de retenciones	25/07/2012	25/07/2012	Ing. Diego Palacios
6	Control de sistema de autenticación Wireless	26/07/2012	26/07/2012	Ing. Diego Palacios
7	Elaboración de proformas presupuestarias	27/07/2012	27/07/2012	Ing. Aníbal Herrera
8	Graduación	30/07/2012	31/07/2012	Ing. Alex Tacuri
9	Culminación de malla curricular	01/08/2012	02/08/2012	Ing. Alex Tacuri
10	Evaluación de notas acumuladas	02/08/2012	03/08/2012	Ing. Alex Tacuri
11	Evaluación de notas principales	06/08/2012	07/08/2012	Ing. Alex Tacuri
12	Matriculación de tesis	08/08/2012	10/08/2012	Ing. Alex Tacuri
13	Administración y control en la migración de datos de docentes de la ESPOCH	03/09/2012	03/09/2012	Ing. Gustavo Hidalgo
14	Administración y control en la migración de datos de los estudiantes de la ESPOCH	04/09/2012	04/09/2012	Ing. Gustavo Hidalgo
15	Administración de aulas virtuales	05/09/2012	05/09/2012	Ing. Gustavo Hidalgo
16	Ingreso de Personal al DESITEL	06/09/2012	07/09/2012	Dr. Carlos Buenaño
17	Salida de Personal del DESITEL	10/09/2012	11/09/2012	Dr. Carlos Buenaño
18				

ANEXO IV.I Encuesta

ENCUESTA DIRIGIDA AL PERSONAL DEL DESITEL

Para conocer el manejo de la información en elDepartamento De Sistemas Y Telemática se solicita responder la siguiente encuesta, y con la colaboración de personal estableceremos la situación actual del DESITEL.

OBJETIVO: Determinar la situación actual del DESITEL sin la implementación de la Norma ISO 27001 en el sistema de seguridad de información.

N°	PREGUNTA	SI	NO	PARCIAL
1	¿Los procesos que se manejan actualmente poseen una documentación detallada y disponible en cualquier momento?			
2	¿Existe información que se filtra hacia fuera del departamento?			
3	¿Esta disponible en su totalidad todo tipo de información necesaria para todos los usuarios de los sistemas autorizados?			
4	¿Existe todas las seguridades para el ingreso de los usuarios autorizados?			
5	¿Existe un control periódico acerca de los datos almacenados de los sistemas?			
6	¿Se realiza actualización de software para el buen funcionamiento de los sistemas?			
7	¿Existe aun registro de las personas autorizadas para realizar respaldos de los sistemas?			
8	¿Presenta credenciales la persona que necesita información de un sistema?			
9	¿Esta implementado un algoritmo de seguridad que permita sacar automáticamente los respaldos de la información?			
10	¿Al realizar cambios en los sistemas se documenta la información del nuevo proceso?			
11	¿Conoce usted si el departamento cuenta con una Política de seguridad de la información?			
Elaborado por: Lucia Guevara Espinosa				

ANEXO IV.II Encuesta

ENCUESTA DIRIGIDA AL PERSONAL DEL DESITEL

Una vez realizado el trabajo de tesis en el Departamento de Sistemas y telemática y además con la colaboración de la información brindada por su personal sobre la implantación de la norma ISO 27001 en la gestión de la seguridad de la información se solicita responder la siguiente encuesta.

OBJETIVO: Determinar si el cumplimiento de políticas y manuales basados en la Norma ISO 27001, permitirán incrementar la gestión de seguridad en la información (SGSI) en el DESITEL.

N°	PREGUNTA	SI	NO	PARCIAL
1	¿Los procesos que se manejan actualmente poseen una documentación detallada y disponible en cualquier momento?			
2	¿Existe información que se filtra hacia fuera del departamento?			
3	¿Esta disponible en su totalidad todo tipo de información necesaria para todos los usuarios de los sistemas autorizados?			
4	¿Existe todas las seguridades para el ingreso de los usuarios autorizados?			
5	¿Existe un control periódico acerca de los datos almacenados de los sistemas?			
6	¿Se realiza actualización de software y se encuentra documentadadicha actualización para el respaldo del sistema?			
7	¿Existe aun registro o documento de las personas autorizadas para realizar respaldos de los sistemas?			
8	¿Presenta credenciales la persona que necesita información de un sistema?			
9	¿Esta implementado un algoritmo de seguridad que permita sacar automáticamente los respaldos de la información?			
10	¿Al realizar cambios en los sistemas se documenta la información del nuevo proceso?			
11	¿Conoce usted si el departamento cuenta con una Política de seguridad de la información?			
Elaborado por: Lucia Guevara Espinosa				

BIBLIOGRAFIA

1. **ALEXANDER A., Diseño de un Sistema de Gestión de Seguridad.,** 2a. ed., Bogotá – Colombia., Alfa Omega., 2007., pp. 170-200

2. **MURRAY R. SPIEGEL., Shaum Estadística.,** 2a. ed., Madrid – España., 2005., pp. 700

3. **NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY.** Recommended Security Controls for Federal Information System NIST Special Publication., Vol.3.N°10., Buenos Aires –Argentina., 2007., pp. 35-60

4. **GAVILANES, V**., Elaboración de la Metodología para la Gestión de Seguridad de la Información. Escuela De Ingeniería en Sistemas. Facultad de Informática y Electrónica. Escuela Superior Politécnica de Chimborazo., Riobamba – Ecuador., **TESIS**., 2011., pp. 40-60

BIBLIOGRAFIA DE INTERNET

5. **BLOG, IMPLEMENTACIÓN ISO 27001**
   http://blog.iso27001standard.com/
   2012-06-15

6. **ISO 27000.ES, IMPLEMENTACIÓN ISO 27001**
   http://www.iso27000.es/sgsi.html
   2012-07-01

7. **WIKIPEDIA, MARCO TEÓRICO**
   http://es.wikipedia.org/wiki/ISO/IEC_27001
   2012-05-01

8. **BSIGROUP, MARCO TEÓRICO**
http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/
2012-05-05

9. **RICON INFORMATICO, MARCO TEÓRICO**
http://www.rinconinformatico.net/seguridad-informatica-norma-iso-27001/
2012-07-15

10. **GRUPO GOOGLE SGSI, MARCO TEÓRICO**
http://sgsi-iso27001.blogspot.com/2006/03/resumen-de-la-norma-iso-270012005.html
2012-07-28

11. **LA FLECHA, IMPLEMENTACIÓN ISO 27001**
http://www.laflecha.net/canale/seguridad/articulo/metodologia-de-implantacion-y-certificacion-de-iso27001/
2012-08-01

12. **AGEDUM, METODOLOGÍA DE PROCESO**
http://www.agedum.com/Dise%C3%B1oeimplementaci%C3%B3ndeunSGSI ISO27001/
2012-08-03