ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"ELABORAR UNA METODOLOGÍA APLICANDO LA NORMA ISO/IEC 27001 EN LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL DESITEL DE LA ESPOCH"

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TÍTULO DE

INGENIERA EN SISTEMAS INFORMÁTICOS

PRESENTADO POR:

VERÓNICA ISABEL GAVILANES PILCO

RIOBAMBA – ECUADOR

2011

AGRADECIMIENTO

Quiero agradecer con todo mi corazón a Dios Todopoderoso, por darme salud, vida y protección en toda la carrera estudiantil permitiéndome tomar decisiones adecuadas para culminar exitosamente y haber cumplido una etapa más de mi vida.

El reconocimiento más sincero a mis, maestros guías del presente trabajo, amigos y colaboradores por su cariño, comprensión y ayuda incondicional a lo largo de mis días.

DEDICATORIA

A mi familia en especial a mi Madre por ser fuente de inspiración, ejemplo de trabajo, sacrificio y constancia diaria para poder llegar a término exitosamente este increíble sueño que hoy se hace realidad.

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, VERÓNICA ISABEL GAVILANES PILCO 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”.

Verónica Isabel Gavilanes Pilco

INDICE DE ABREVIATURAS

BSI	British Standard Institute
COBIT	Information Systems and Audit Control Association
DESITEL	Departamento de Sistemas y Telemática
DOC	Documento
DPI	Derechos de propiedad intelectual
ESP	Especificación
ESPOCH	Escuela Superior Politécnica de Chimborazo
IEC	Comisión Electrotécnica Internacional
INEI	Instituto Nacional de Estadísticas e Informática
IPR	Derecho de Propiedad Intelectual
ISO	Organización Internacional de Normalización
ITIL	Provide best practices for IT service management
LFE	Legislación de Firma Electrónica
LSSI-CE	Ley de Servicios para la Sociedad de la Información y el Comercio Electrónico.
MAGESID	Metodología Aplicada a la Gestión de la Seguridad de la Información en el DESITEL.
PDCA	Plan(Planificar), Do(Hacer), Check (Verificar), Act (Actuar)
REF	Referencia
SGSI	Sistema de Gestión de Seguridad de la Información
SOA	Statement of Applicability (Documentos de aplicabilidad)
TI	Tecnologías de la Información
VFA	Verificación Automática de Firmas

INDICE GENERAL

CAPÍTULO I:MARCO REFERENCIAL

CAPÍTULO II:MARCO TEORICO

CAPÍTULO III:ESTRUCTURA DE UNA METODOLÓGIA PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

CAPÍTULO IV:DESARROLLO DE LA METODOLÓGIA PROPUESTA PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO V:SISTEMA INFORMÁTICO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Los sistemas de información y los datos almacenados son uno de los recursos más valiosos con los que puede contar cualquier organización. La necesidad imperante del flujo de información hace que aparezcan vulnerabilidades que ponen en riesgo la seguridad en los sistemas de información de una organización.

La seguridad de la información es un bien no fácilmente medible, cómo se puede evaluar entonces si la gestión de políticas de seguridad que estamos efectuando es o no eficiente, cuales serian las áreas que necesitan mejoras, o si se requieren crear nuevas políticas de seguridad para salvaguardar la información, podríamos simplemente especular del tema pero, si existiera alguna medida que nos ayude a solucionar este problema sin lugar a dudas sería una excelente herramienta para mejorar la gestión de seguridad de la información dentro del DESITEL.

El Departamento de Sistemas y Telemática y de la ESPOCH por estar en constante progreso y desarrollar volúmenes importantes de información hace uso de diferentes tecnologías de información, las cuales apoyan los procesos que se mantienen y que generan información sobre la que se trabaja internamente, es entonces necesario proteger este crítico y valioso activo, mediante mecanismos de seguridad eficientes y valederos, uno de ellos es el uso de una metodología adecuada para consolidar y actualizar las políticas de seguridad de la información existentes con el fin de crear un ambiente ideal para mantener activo los propósitos de progreso en el DESITEL.

Consta de cinco capítulos, en el primer capitulo se explica la problemática del trabajo como son: los antecedentes, justificación, objetivos a cumplir y la hipótesis.

En el segundo capítulo se presenta el sustento teórico permitiendo conocer la importancia de la información en las organizaciones y la seguridad física y lógica, la definición de un sistema de gestión de seguridad, conceptos de la norma ISO 27001, la utilidad de gestionar políticas de seguridad y un estudio de los sistemas de gestión de seguridad de la información.

En el tercer capítulo se detalla la estructura de la propuesta para la guía metodológica con la utilización de la norma ISO 27001, la cual explica el alcance y objetivos de la guía, apoyándose en el análisis y vulnerabilidades existentes en los activos involucrados en el mantenimiento y proceso de la información .

En el cuarto capítulo se desarrolla la propuesta metodológica para un Sistema de Gestión de Seguridad de la Información.

En el quinto capítulo se explica el diseño de un sistema informático, es dirigida al usuario y administrador del sistema para el análisis del cumplimiento de los controles desarrollados en la metodología elaborada según la norma ISO 27001.

Con la estructura del presente trabajo se muestra la elaboración de una guía metodológica usando la norma ISO 27001 para la implementación de un Sistema de Gestión de Seguridad de la Información garantizando la estructuración eficiente de la misma y enmarcada en la realidad actual del departamento, de esta manera el resultado obtenido es la metodología con sus 133 controles y además un software de soporte para el análisis del cumplimiento de los controles aquí detallados y con esto es necesario impulsar la utilización de este elemento que permitirá alcanzar niveles aceptables de seguridad de la información, en el DESITEL de la ESPOCH.

CAPÍTULO I

MARCO REFERENCIAL

En el presente capítulo se explica la problemática del trabajo como son: los antecedentes, justificación, objetivos a cumplir y la hipótesis.

1.1 ANTECEDENTES

La información es un valor económico que debe ser protegido, pero su seguridad en varias ocasiones (hasta en las grandes empresas) es delegada a un segundo plano. La seguridad muchas veces es un problema de las personas, debido a que no hacen siempre lo que se espera de ellas, ¿Razones? Delitos, malicia, curiosidad, falta de conocimiento, etc., El resultado es obvio, se siguen manteniendo altos niveles de riesgo frente a las amenazas que afectan la seguridad de la información.

Todos estos incidentes que amenazan la seguridad de la información requieren, cada día más, de sistemas de gestión acordes con el valor de la propia información y de los sistemas informáticos que los tratan. Las directrices, procedimientos y controles que se utilizan para la adecuada gestión de la seguridad de la información, se propondrá en la elaboración de una metodología para un Sistema de Gestión de

Seguridad de la Información (SGSI) en el DESITEL de la ESPOCH, debido a que es necesario constituir un elemento que aborde esta tarea de una forma metódica, documentada y basada en objetivos claros de seguridad.

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:

- ✓ **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 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.

De acuerdo a lo mencionado la base sobre la que se cimienta todo el edificio de la seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad.

1.2 PROBLEMATIZACION

En la actualidad la ESPOCH a través de su Data Center ubicado en el Departamento de Sistemas y Telemática posee 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 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.

1.3 JUSTIFICACION

Las organizaciones y su información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio, inundación, etc. Muchos sistemas de información no han sido diseñados para ser seguros.

La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados para lo cual la administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización.

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 como:

Tabla I. I: Beneficios del SGSI

Aspecto Organizacional	Compromiso: El registro de las actividades permite garantizar y demostrar la eficiencia de los esfuerzos desarrollados para asegurar la información en todos sus niveles y probar la diligencia razonable de sus administradores.
Aspecto Legal	Conformidad con requisitos legales: el registro permite demostrar que la organización observa todas las leyes y normativas aplicables al alcance.
Aspecto Funcional	Gestión de los riesgos: Obtención de un mejor conocimiento de los sistemas de información, sus debilidades y los medios de protección, garantiza también una mejor disponibilidad de los materiales y datos.
Aspecto Comercial	Credibilidad y confianza: los usuarios al constatar la importancia que la organización concede a la protección de la información deposita confianza en ella.
Aspecto Financiero	Reducción de los costes vinculados a los incidentes y posibilidad de disminución de los egresos.
Aspecto Humano	Mejora la sensibilización del personal hacia la seguridad y a sus responsabilidades en la organización.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Elaborar una Metodología aplicando la norma ISO/IEC 27001 en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el DESITEL de la ESPOCH.

1.4.2 OBJETIVOS ESPECÍFICOS

- Conocer las políticas y reglamentos de legislación informática aplicadas a la información.

- Analizar la norma ISO 27001 para la aplicación de un Sistema de Gestión de Seguridad de la Información (SGSI).

- Aplicar el ciclo PDCA (Plan, Do, Check, Act) para el adecuado manejo de la información y lograr un producto diferente que ayude a la seguridad de la información como lo permite la norma ISO 27001.

- Elaborar una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información usando ISO/IEC 27001 en el DESITEL de la ESPOCH.

- Desarrollar un sistema informático que ayudará a verificar el cumplimiento de los controles en base a los cuales se estructurará la metodología a elaborarse, el mismo que se lo realizará en forma de reporte para los usuarios del departamento.

1.5 HIPÓTESIS

La utilización de una guía metodológica usando la norma ISO 27001 para un Sistema de Gestión de Seguridad de la Información permitirá mejorar el nivel de Control de Seguridad de la Información en el DESITEL de la ESPOCH.

ANALISIS

CAPÍTULO II

MARCO TEÓRICO

A continuación se presenta el sustento teórico permitiendo conocer la importancia de la información en las organizaciones y la seguridad física y lógica, la definición de un sistema de gestión de seguridad, conceptos de la norma ISO 27001, la utilidad de gestionar políticas de seguridad para una entidad.

2.1 LA SEGURIDAD

La Seguridad de la Información protege a esta, de una amplia gama de amenazas, a fin de garantizar la continuidad institucional, para minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

Para comprender qué es la seguridad de la información, debemos conocer que la información en esta área es referida a los activos de información (es decir, los datos, pero también los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, trasmitir y destruir la información), que tienen un valor para la organización.

En las complejas organizaciones de hoy en día, se recogen, gestionan y transmiten multitud de datos a través de diferentes medios a mucha gente, y todas las acciones relacionadas con ello pueden necesitar protección.

2.2 Importancia de la Seguridad de la Información para la Organización

El manejo de la información es fundamental para cualquier empresa, con ello se puede lograr un alto nivel competitivo dentro del mercado y obtener mayores niveles de capacidad de desarrollo. El manejo de información permite identificar cuáles son las fortalezas con las que se cuenta y cuáles son las debilidades y sectores vulnerables como organización.

La seguridad de la información, recalca su importancia como la protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de funcionamiento de la organización.

Estos parámetros básicos de la seguridad se definen como:

- ✓ **Confidencialidad**

  A la información sólo pueden acceder las personas autorizadas para ello.

- ✓ **Integridad**

  La información ha de estar completa y correcta en todo momento.

- ✓ **Disponibilidad**

  La información está lista para acceder a ella o utilizarse cuando se necesita.

- ✓ **Autenticidad**

  La información es lo que dice ser o el transmisor de la información es quien dice ser.

- ✓ **Trazabilidad**

  Poder asegurar en todo momento quién hizo qué y cuándo lo hizo.

2.3 Beneficios de la Seguridad de la Información

Existen numerosas e importantes razones para afrontar el desarrollo de una metodología para la implantación de un Sistema de Gestión de Seguridad de la Información:

- ✓ **Reducción de costes.** Al detectar los principales focos de fallos y errores, y eliminarlos o reducirlos hasta donde es posible, se evitan costosos incidentes de seguridad.

- ✓ **Optimizar los recursos y las inversiones en tecnología.** Habrá una motivación de negocio detrás de estas decisiones, por lo que la dirección podrá comprenderlas y apoyarlas de manera más consciente.

- ✓ **Protección de la organización.** Con una metodología que garantice una adecuada estructura para un SGSI se evitan interrupciones en el flujo de procesos de la organización, ya que se está asegurando de una manera eficaz la protección de la misma en base a políticas adecuadas.

- ✓ **Mejora de la competitividad.** Cualquier mejora en la gestión de la organización redunda en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza en la organización, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

- ✓ **Cumplimiento legal y reglamentario.** Gestionando de manera coordinada la seguridad tenemos un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

- ✓ **Mantener y mejorar la imagen corporativa.** Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y servicios.

2.4 Que es un SGSI

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. Se entiende por información todo aquel conjunto de datos organizados 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.), y su origen (de la propia organización o de fuentes externas).

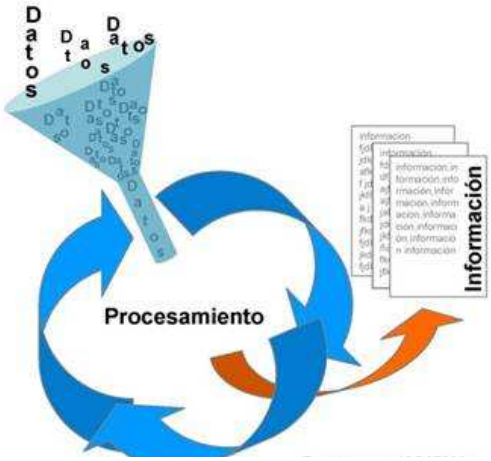


Fig.II.1. Organización de la información en un (SGSI)

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

De una manera más estricta una metodología para, un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que deberá incorporar:

- ✓ La política.
- ✓ La estructura organizativa.
- ✓ Los procedimientos.
- ✓ Los controles necesarios y

Para implantar la gestión de la seguridad de la información.

2.5 Para qué sirve un SGSI

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de la información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización.

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

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una metodología sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

2.6 Que consideraciones se debe incluir para un SGSI

Una metodología para un Sistema de Gestión de la Seguridad de la Información incluye lo siguiente:

Fig.II.2. Documentos para un (SGSI)

✓ **Documentos de Nivel 1**

Manual de seguridad: elaborado con la dirección, determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

✓ **Documentos de Nivel 2**

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información en base a una metodología concreta.

✓ **Documentos de Nivel 3**

Instrucciones y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

✓ **Documentos de Nivel 4**

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI.

2.7 Como se implementa un SGSI

Para establecer y gestionar una metodología adecuada para la implementación de un Sistema de Gestión de Seguridad de la Información se debe garantizar la interpretación del ciclo continuo PDCA, óptimo en los sistemas de gestión de la calidad, y de esta manera poder incorporar estos aspectos en el desarrollo de la misma.

2.7.1 PLAN: Establecer el SGSI

Fig.II.3. Fase PLAN (SGSI)

Planificar y diseñar una metodología para un SGSI implica:

- ✓ Establecer el alcance del SGSI. Es el primer paso. Hay que decidir qué parte de la organización va a ser protegida, o toda la organización.

- ✓ Establecer las responsabilidades. Se asignará un responsable de seguridad, que coordine las tareas y esfuerzos en materia de seguridad.

- ✓ Definir política de seguridad. La política de la organización es la que va a sentar las bases de lo que se va a hacer, mostrará el compromiso de la dirección con el SGSI y servirá para coordinar responsabilidades y tareas.

2.7.2 DO (Hacer): Implementar y utilizar el SGSI

Fig.II.4. Fase DO (SGSI)

Algunas medidas de corte técnico requerirán poca documentación, pero otras más de índole organizativa, como son el caso de la gestión de la documentación o de los recursos humanos, necesitan ser documentadas.

Una tarea importante dentro de esta fase es la formación. Desde luego la formación e información continua al personal dentro del proyecto debe comenzar con el mismo, se debe involucrar a todos aquellos que se vean afectados por el SGSI tanto de forma directa como indirecta.

2.7.3 CHECK (Comprobar): Monitorizar y revisar el SGSI

Fig.II.5. Fase CHECK (SGSI)

Una vez puesto en marcha el plan de seguridad, se debe revisar periódicamente de manera que se detecten posibles desviaciones. Pueden haberse producido retrasos

en las acciones a tomar o bien haber surgido problemas que no fueron previstos y que hay que solucionar para continuar con el plan.

2.7.4 ACT (Actuar): Mantener y mejorar el SGSI

Fig.II.6. Fase ACT (SGSI)

Cuando mediante cualquiera de las actividades de comprobación realizadas o incluso durante la operativa habitual del SGSI se descubren no conformidades, reales o potenciales, deben tomarse medidas para solucionarlas. Hay maneras para ello:

- ✓ Adoptar acciones correctoras. Las decisiones de qué hacer y cómo deben estar basadas en una identificación precisa de la causa del problema para evitar malgastar recursos simplemente arreglando provisionalmente un incidente que volverá a repetirse si no se ataca la causa que lo originó.
- ✓ Adoptar acciones preventivas. Son aquellas que se toman para prevenir que ocurra algo no deseado. La gran ventaja de estas acciones es que evidentemente es más eficaz y sencillo prevenir los problemas que solucionarlos. De todos modos es fundamental también en este caso determinar cuál es la posible fuente de problemas con el objeto de eliminarla.
- ✓ Definir acciones de mejora. Las acciones de mejora no surgen de la necesidad de solucionar un problema sino de la dinámica del sistema de gestión, que impulsa a refinar procesos y superar objetivos continuamente.

2.8 Tareas de la gerencia en un SGSI

Uno de los componentes primordiales en la implantación exitosa de una metodología para Sistema de Gestión de Seguridad de la Información es la participación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar que una metodología para un SGSI es mera cuestión técnica o documentada relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

2.9 Compromiso con la Dirección

La Dirección tiene varias de las responsabilidades claves en la puesta en marcha y funcionamiento de la metodología para un SGSI. Es la Dirección la que debe:

- ✓ Aprobar la Política y los objetivos de seguridad.
- ✓ Aprobar los planes de formación y auditorías.
- ✓ Realizar la revisión del SGSI.

Demostrar su compromiso con la seguridad de la información para promover una cultura efectiva dentro de la organización.

2.10. Marco legal y jurídico de la seguridad

2.10.1 Normativas de la seguridad

Una norma es una solución única a un problema que se repite, lograda mediante la intervención de todos los interesados, tomando como base la ciencia, técnica y experiencia, considerando el interés general del país y el momento de su desarrollo.

A continuación se observa las leyes sobre las que para su creación se basa la norma ISO 27001.

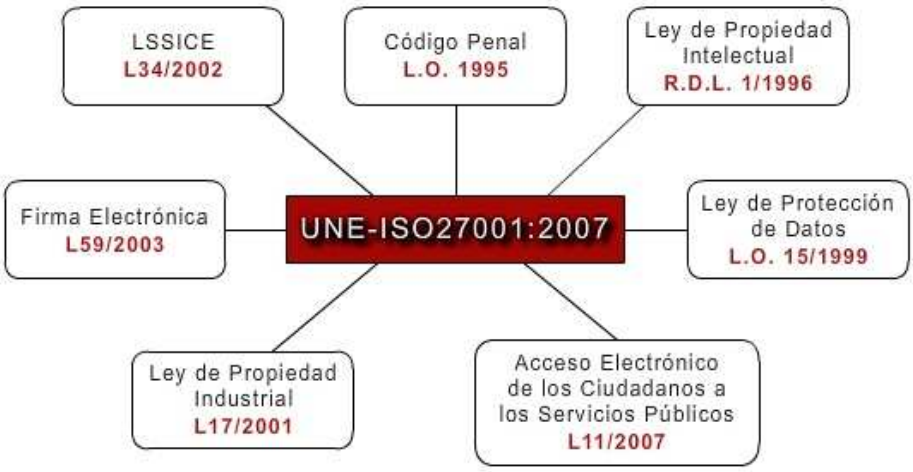


Fig.II.7. Normativas de Seguridad en las que se basa la Norma ISO-27001

2.10.2 Legislación Ecuatoriana

Las normativas de la legislación ecuatoriana se basan en medidas concretas que el reglamento obliga a cumplir y dependen fundamentalmente de la naturaleza de los datos.

- ✓ Derecho a la protección de datos (Art. 66 de la Constitución de la República).[1]

  "Aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular del derecho individual a la intimidad respecto del procesamiento manual o autónomo de datos".

- ✓ Vulnerabilidad de los Datos Personales en el Ecuador (Art. 62 de la Constitución de la República) Donde se garantiza el derecho a la intimidad personal y familiar.

Para poder controlar problemas de seguridad en la información existen leyes en nuestro país bajo el código Penal (Modificado por Ley99-38).[2]

[1] Tomado de la Constitución de la República
[2] Tomado del Código Penal

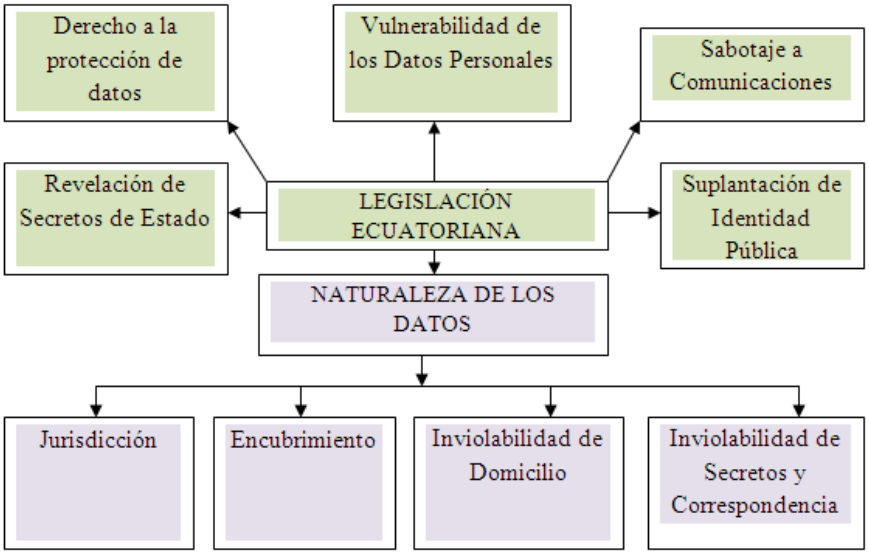


Fig.II.8 Legislación Ecuatoriana

- ✓ Art.5 : Jurisdicción
- ✓ Art.44: Encubrimiento (ocultar pruebas)
- ✓ Art.117: Revelación de Secretos de Estado
- ✓ Art.158: Sabotaje a Comunicaciones
- ✓ Art.191 a 196 : Inviolabilidad de Domicilio
- ✓ Art. 197 a 202 : Inviolabilidad de Secretos y Correspondencia
- ✓ Art. 236: Suplantación de Identidad Pública

2.11 Estándares de la Gestión de la Seguridad de la Información.

2.11.1 Estándares

- ✓ **COBIT** Information Systems and Audit Control Association
- ✓ **IT** governance and control framework
- ✓ **ITIL** -Provide best practices for IT service management
- ✓ **ISO** International Standards Organization

COBIT

Es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas.

ITIL

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (Information Technology Infrastructure Library), es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

ISO (International Standards Organization).

Tabla.II.II. – Organización del estándar ISO

ISO	DESCRIPCIÓN
ISO 27000	Proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
ISO 27001	CERTIFICACIÓN- Sistema de Gestión de Seguridad de la Información.
ISO 27002	Código de Mejores Prácticas de Gestión de Seguridad de la Información.
ISO 27003	Presenta información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases
ISO 27004	Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.
ISO 27005	Establece las directrices para la gestión del riesgo en la seguridad de la información

Que obtenemos con las normas ISO

- ✓ Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

- ✓ Reducción del riesgo de pérdida, robo o corrupción de información.
- ✓ El personal tiene acceso a la información a través de medidas de seguridad.
- ✓ Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- ✓ Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- ✓ Proporciona confianza y reglas claras a las personas de la organización.
- ✓ Aumenta la motivación y satisfacción del personal.

2.11.2 La organización ISO

ISO (Organización Internacional de Estándares) es una organización especializada en el desarrollo y difusión de los estándares. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (International Electrotechnical Commission), la organización que a nivel mundial prepara y publica estándares en el campo de electro - tecnología.

2.11.3 La familia de las normas.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

- ✓ ISO 27000 Sistemas de Gestión de Seguridad de la Información, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.

- ✓ ISO 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Es la norma con la cual serán certificados los SGSI de las organizaciones que lo deseen.

- ✓ ISO 27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

- ✓ ISO 27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.

- ✓ ISO 27005 Gestión del Riesgo en la Seguridad de la Información.

- ✓ ISO 27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información.

- ✓ ISO 27007. Guía para la realización de las auditorías de un SGSI.

- ✓ ISO 27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002.

2.11.4 La norma ISO 27001

ORÍGENES

La Norma fue publicada en el año 2007, pero tiene una larga historia antes de llegar a este punto.

Fig.II.9. Pilares de la Norma ISO 27001

En el año de 1995 el British Standard Institute (BSI) publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.

En vista de la gran aceptación de esta Norma, en 1998, el BSI pública la norma BS7799-2, Especificaciones para los sistemas de gestión de la seguridad de la información. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en el año 2002 y denominada ISO/IEC 17799 en el año 2005.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27001 y en octubre del 2007 la norma ISO 27001 se adopta también por IEC. Con la publicación de la ISO/IEC 27001, dejó de estar vigente la UNE 71502 y las empresas nacionales se certifican ahora únicamente con esta nueva norma (UNE-ISO/IEC 27001).

Contenido de la ISO/IEC 27001

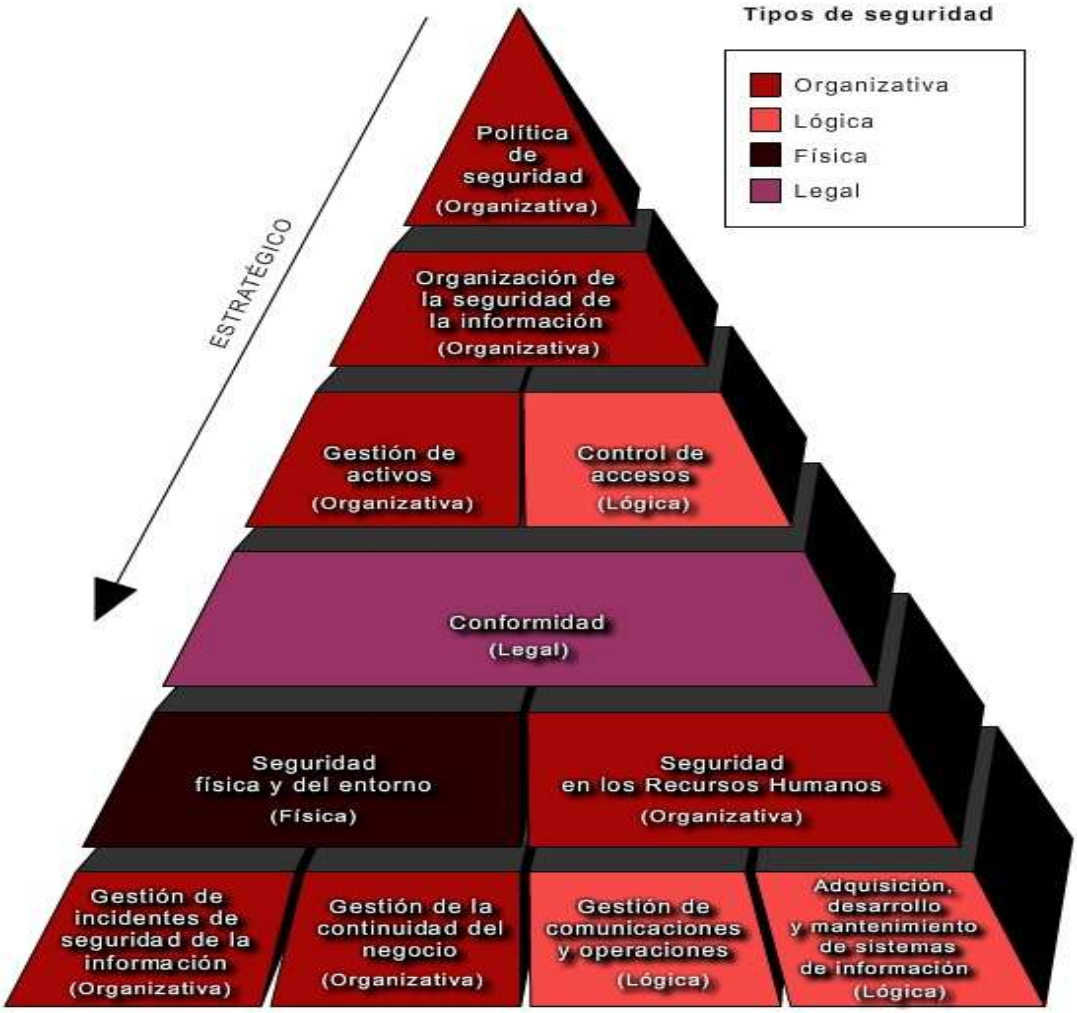


Fig.II.10. Contenido de la norma ISO 27001

La norma ISO/IEC 27001 da a conocer las pautas para elaborar una metodología para un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro del contexto de los riesgos identificados por la Organización.

Los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

La Norma ISO 27001 permite la elaboración de una metodología para:

- ✓ Los componentes del SGSI, es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.
- ✓ Cómo se debe implantar el SGSI.

- ✓ Define los controles que deberán ser adaptados a la realidad de una organización para proceder a la implantación de la metodología que se estime conveniente.

La ISO 27001 permite elaborar una metodología que adopte un proceso estructurado para implementar un SGSI.

CAPÍTULO III

ESTRUCTURA DE LA METODOLÓGIA MAGESID PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

A continuación se detalla la estructura de la propuesta para la metodológica MAGESID con la utilización de la norma ISO 27001, la cual explica el alcance y objetivos de la guía, apoyándose en el análisis y vulnerabilidades existentes en los activos involucrados en el mantenimiento y proceso de la información.

ESQUEMA GENERAL

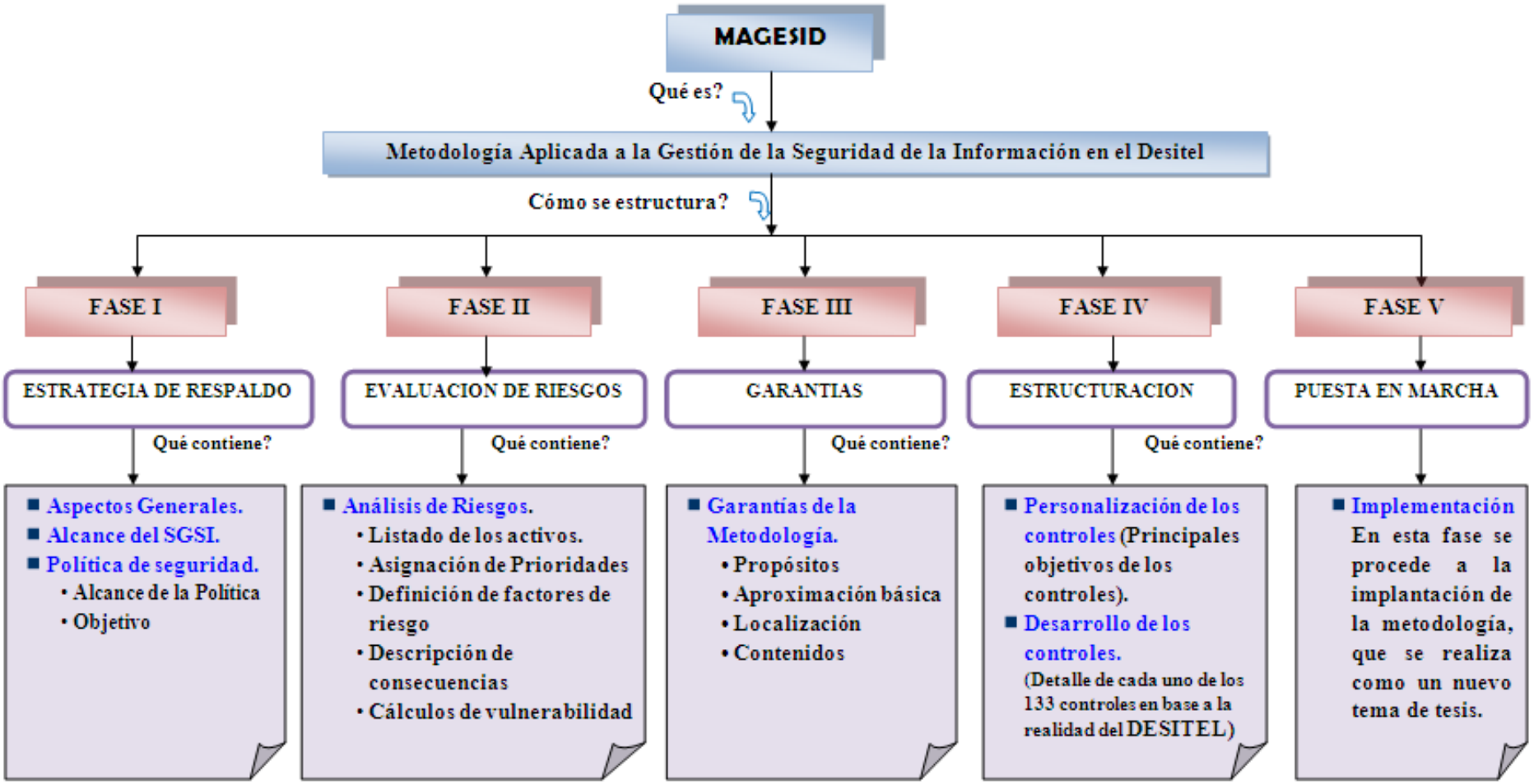


Fig. III.11. Esquema de la Metodología Propuesta

FASE I: ESTRATEGIAS DE RESPALDO

3. Aspectos Generales

En este apartado se especifican consideraciones generales acerca del propósito de la Metodología.

3.1 Alcance del SGSI

Para comenzar a diseñar una metodología para un SGSI en primer lugar hay que decidir qué se quiere proteger, es decir, el alcance que se le va a dar al sistema.

Según lo especificado por la Norma ISO 27001, los límites del SGSI deben estar definidos en términos de las características de la organización, localización, activos y tecnologías. Esto significa que hay que considerar qué parte de la organización va a quedar protegida por el SGSI, si es que no se pretende abarcarla toda.

No se debe olvidar que la implantación de este tipo de sistemas debe ayudar a los procesos propios de la empresa y no debe interferir en su desarrollo para que se lleven a cabo de la mejor manera posible, aunque inevitablemente la organización verá modificados algunos de sus hábitos sobre todo a nivel de gestión y del personal involucrado.

Una vez decidido si el alcance va a ser toda la organización o sólo una parte de ella, hay que definir claramente este alcance.

La definición del Alcance es, por tanto, uno de los puntos críticos en la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que su correcta definición hará que las tareas de implantación y los responsables estén correctamente determinados y que, de esta manera, dichas tareas así como el mantenimiento del sistema estén acordes con los recursos disponibles y las necesidades de la organización.

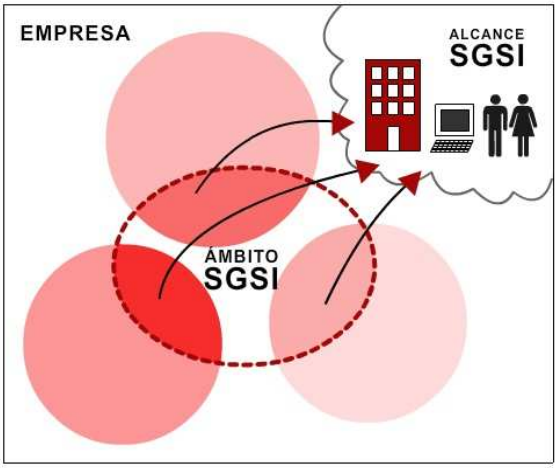


Fig.III.12. Alcance del SGSI

3.2 Política del SGSI

El objetivo de la Política de Seguridad es dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo a los requisitos del negocio. Es el punto de partida del diseño del SGSI, a partir del cual se desarrollan las actuaciones necesarias para implantar el SGSI. Es un requisito de la Norma ISO 27001 contar con este documento.

La Política de Seguridad la define la Dirección, estableciendo en ella de forma clara las líneas de actuación en esta área, que deben estar alineadas con los objetivos de negocio. El Documento que recoja la Política de Seguridad debe ser aprobado por la Dirección, publicado y comunicado a todos los empleados y terceras partes, tiene que ser del dominio público las intenciones y objetivos de la organización. Esto es fundamental para que el personal perciba la importancia del asunto y sea consciente de que no es una comunicación más dentro de la organización, sino que debe ser tomada en cuenta y puesta en práctica.

La Política debe ser un documento legible y comprensible para toda la audiencia a la que va dirigido, lo cual es más fácil de conseguir si es corto y preciso, enfocado a describir qué se quiere proteger en la organización y por qué.

Además de la declaración de principios, debe recogerse, en el mismo documento o en otro, una breve explicación de las políticas, principios, normas y requisitos de cumplimiento más importantes para la organización.

Esta política de seguridad de la información debe ser comunicada a todos los miembros de la empresa, y estar disponible para todos aquellos a los que va dirigida. Debe transmitirse el mensaje claro de que la seguridad es un asunto de todos y no solo de la dirección o del responsable de seguridad.

FASE II: EVALUACIÓN DE RIESGOS

3.3 Análisis de riesgos

3.3.1 Identificación de los activos de información

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Fig.III.13. Activos que se identifican en una organización

Para facilitar el manejo y mantenimiento del inventario los activos se pueden distinguir diferentes categorías de los mismos:

- ✓ **Datos**

Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.

- ✓ **Aplicaciones**

El software que se utiliza para la gestión de la información.

- ✓ **Personal**

En esta categoría se encuentra tanto el personal de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.

- ✓ **Tecnología**

Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)

- ✓ **Instalaciones**

Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.).

3.3.2 Inventario de Activos

Se debe recoger los activos más importantes e identificarlos de manera clara y sin ambigüedades.

Fig.III.14 Clasificación del Inventario de activos

El inventario de activos es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre. Esta información como mínimo es:

- ✓ **Identificación del activo**

Un código para ordenar y localizar los activos.

- ✓ **Tipo de activo**

A qué categoría de las anteriormente mencionadas pertenece el activo.

- ✓ **Descripción**

Una breve descripción del activo para identificarlo sin ambigüedades.

- ✓ **Propietario**

Quien es la persona a cargo del activo.

- ✓ **Localización**

Dónde está físicamente el activo. En el caso de información en formato electrónico, en qué equipo se encuentra.

3.3.3 Valoración de los activos

Una vez identificados los activos, el siguiente paso a realizar es valorarlos. Es decir, hay que estimar qué valor tienen para la organización, cual es su importancia para la misma.

Para calcular este valor, se considera cual puede ser el daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

3.3.4 Documentar el análisis de riesgos

El resultado debería ser una lista de los riesgos correspondientes a los posibles impactos en caso de que se materialicen las amenazas a las que están expuestos los activos.

Fig.III.15. Tratamiento del riesgo

Esto permite categorizar los riesgos e identificar cuales deberían ser tratados primero o más exhaustivamente. Se debe escoger, a la vista de los resultados, cual es el nivel de riesgo que la organización está dispuesta a tolerar, de manera que por debajo de ese nivel el riesgo es aceptable y por encima no lo será y se tomará alguna decisión al respecto.

3.3.5 Mitigación del riesgo

Las actividades a realizar son:

Fig.III.16. Mitigación del riesgo

1. Seleccionar los controles aptos para hacer frente a la vulnerabilidad presentada.
2. Implantar los controles para lo que deben desarrollarse procedimientos. Aunque sean controles tecnológicos deben desarrollarse para su instalación, uso y mantenimiento.
3. Verificar que los controles están correctamente implantados.
4. Establecer indicadores para saber en que medida la implantación de los controles seleccionados reduce el riesgo a un nivel aceptable.

3.3.6 Documentar la Gestión de Riesgos

La documentación de la gestión de riesgos se realiza mediante la **Declaración de Aplicabilidad** también conocida por sus siglas en inglés SOA (“Statement Of Applicability”).

FASE III: GARANTÍAS

3.4Garantías de la metodología

3.4.1 Propósitos

Se describe un propósito específico para la adaptación del contenido dentro de la realidad existente en el Desitel.

3.4.2 Aproximación básica

En este aspecto se describen los cambios a los que probablemente quedarán sometidos los procesos de la Organización, desde el momento en que se inicie con la implantación de la metodología.

3.4.3 Localización

Se especifica la ubicación física del lugar donde se encontrará la metodología elaborada.

3.4.4 Contenidos

Indica la base sobre la cual se estructura la metodología.

FASE IV: ESTRUCTURACIÓN

3.5 Personalización de Controles

En este parte de la metodología se describen los principales objetivos de cada uno de los controles como un resumen general.

3.6 Detalle de controles enmarcados en la realidad de la organización.

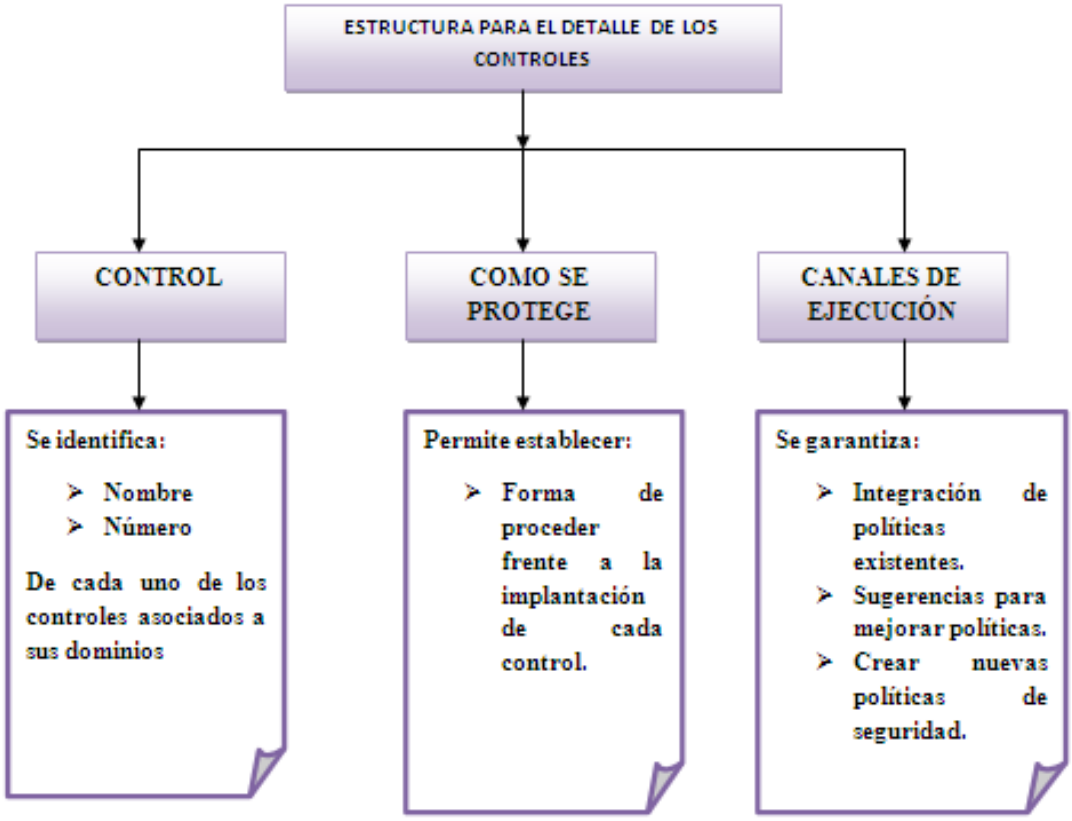


Fig. III.17 Estructura del Detalle de Controles

En este apartado se desarrollan los controles, se establecen caminos para proteger dichos controles; una vez que se opte por la decisión de implementarlos, junto a las garantías de cumplimiento se integra las sugerencias para la documentación necesaria que permitirá ejecutar de manera metódica, sistemática y valedera los procedimientos establecidos para un SGSI en el DESITEL.

CAPÍTULO IV

DESARROLLO DE LA METODOLOGÍA PROPUESTA "MAGESID" PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

A continuación se desarrolla la propuesta metodológica para un Sistema de Gestión de Seguridad de la Información en el DESITEL.

FASE I: ESTRATEGIA DE RESPALDO

4.1 Aspectos generales

El propósito de establecer la guía metodológica para un sistema de gestión de seguridad de la información, es proteger la información y los activos del Departamento de Sistemas y Telemática, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos; y las responsabilidades que debe asumir cada uno de los empleados mientras permanezcan en la institución para garantizar la seguridad de la información.

Estas políticas emergen como el instrumento para concienciar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de tal forma que permitan al DESITEL cumplir con su misión.

4.2 Alcance del SGSI.

La presente Metodología para el Sistema de Gestión de Seguridad de la Información cubrirá los aspectos de seguridad de los activos del Departamento de Sistemas y Telemática, adaptando los controles de la norma ISO 27001 en base a la realidad existente en la organización, con un análisis de riesgos, identificación de amenazas y vulnerabilidades de los activos físicos, lógicos y de servicios, incluyendo todo tipo de información del Departamento.

4.3 Política de Seguridad

4.3.1 Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información. Debe ser conocida y cumplida por todo el personal vinculado al departamento.

4.3.2 Objetivo

Proteger los recursos de la información del DESITEL y la tecnología utilizada para su procesamiento, frente a 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.

FASE II: EVALUACIÓN DE RIESGOS

4.3.3 Evaluación de Riesgos

El presente análisis de riesgos es desarrollado con el propósito de determinar cuál o cuales de los activos pertenecientes al DESITEL tienen mayor vulnerabilidad ante factores externos o internos que puedan afectarlos, identificando las causas potenciales que faciliten o impidan alcanzar los objetivos, calculando la probabilidad de su ocurrencia, evaluando sus probables efectos, y considerando el grado en que el riesgo pueda ser controlado, de esta manera se garantiza la adaptación efectiva y real en la integración de los controles de la norma ISO 27001.

Para generar esta información se desempeño las siguientes actividades:(Anexo V)

1. Listado de los activos del DESITEL: se evaluaron los distintos activos físicos y de software del departamento, generando un inventario de aquellos que son considerados como vitales para su desenvolvimiento seguro.
2. Asignación de prioridades a los activos: los activos son clasificados según el impacto que sufriría la ESPOCH si faltase o fallara tal activo.
3. Definición de factores de riesgo: acto seguido se lista los factores de riesgo relevantes a los que pueden verse sometidos cada uno de los activos.
4. Descripción de consecuencias: teniendo presente el listado anterior , se genera una descripción de las consecuencias que podría sufrir la ESPOCH si los activos son afectados por sus respectivos factores de riesgo, detallando la manera en que se protege al activo contra ese ataque en particular, y puntualizando en que grado son efectivas esas medidas.
5. Asignación de probabilidades de ocurrencia de los factores de riesgo: teniendo en cuenta los datos arriba mencionados fue posible estimar la probabilidad de ocurrencia que cada uno de los factores de riesgo representaba con respecto a los activos listados, considerando para esta estimación las medidas tomadas por el DESITEL.
6. Cálculo de niveles de vulnerabilidad: una vez identificados los riesgos se precede a su análisis. Con toda la información recolectada, se determina el nivel de vulnerabilidad que se asocia con cada activo listado.
7. Conclusiones: a partir de las actividades anteriormente descritas se puede evaluar la situación actual de los activos del Departamento en relación a los incidentes que pueden afectarla.
8. Consecuencias: luego de identificar, estimar y cuantificar los riesgos, los directivos del DESITEL deben determinar los objetivos específicos de control y con relación a ellos, establecer los procedimientos de control de forma que garantice su consistencia, para enfrentarlos de la manera más eficaz y económica posible con la utilización de los controles de la norma ISO 27001.

En general, aquellos riesgos cuya concreción esté estimada como de baja frecuencia, no justifican precauciones mayores. Por el contrario, los que se estiman de alta frecuencia deben merecer preferente atención. Entre estos extremos se encuentran casos que deben ser analizados cuidadosamente, aplicando elevadas dosis de buen juicio y sentido común.

A partir de la información antes descrita y al comprobar la necesidad de contar con una guía metodológica para la gestión de seguridad de la información usando la norma ISO 27001 detallamos lo siguiente:

FASE III: GARANTÍAS

4.4 Garantías de la Metodología

Una metodología de actividad empresarial es una herramienta analítica que tiene como fin gestionar la seguridad de la información. Para ello, se pone a disposición la guía donde se puede encontrar información diversa que facilita la puesta en marcha de un sistema de gestión de seguridad de la información.

¿Para qué sirve?

La guía metodológica será el instructivo o manual que deberá manejarse en el Departamento de Sistemas y Telemática de la ESPOCH, para de esta manera garantizar la seguridad de la información, tanto en confiabilidad, vulnerabilidad, veracidad, de esta manera se dispondrá de la información en los momentos y espacios requeridos evitando hechos lamentables que paralicen el desarrollo normal de las actividades.

Propósitos

El objetivo de la presente metodología es integrar la realidad existente en el DESITEL sobre la seguridad de la información y adaptar los controles de la norma ISO 27001 de forma que permita la interpretación clara y precisa de las políticas,

medidas y procedimientos definidos en la misma, con el objetivo de alcanzar niveles aceptables de seguridad.

Como metodología, tiene un carácter general, debiendo ser considerado como una guía de trabajo y no como un cuestionario que haya que seguir al pie de la letra, por lo que el equipo designado para su implementación desarrollará los aspectos que considere necesarios para desarrollar el Sistema de Gestión de Seguridad de la Información, de modo que aquellos aspectos que no correspondan a las necesidades de protección identificadas podrán ser excluidos y por supuesto, se adicionará cualquier elemento que se considere importante para los requerimientos de seguridad, con independencia de que no esté contemplado en este documento.

Aproximación básica

Esta metodología es la expresión del conjunto para integrar un SGSI a la organización de modo que no efecto el normal desenvolvimiento de los objetivos del departamento y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad de la informacion en el departamento, a través de los controles aquí detallados.

Localización

Departamento de Sistemas y Telemática (DESITEL) de la Escuela Superior Politécnica de Chimborazo (ESPOCH).

Contenidos

Basada en los tres conceptos fundamentales de confidencialidad, integridad y disponibilidad de la información, ya sea escrita, hablada o almacenada en un computador, la ISO 27001 define las mejores prácticas para manejar la seguridad de la información, en términos de procesos, no de tecnología.

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.

La metodología se basa en los siguientes dominios con sus respectivos objetivos y controles.

Tabla IV.III – Dominios de la Metodología MAGESID

Dominio		Objetivos de Control	Controles
1	Política de Seguridad	1	2
2	Organización de la seguridad de la información	2	11
3	Gestión de activos	2	5
4	Seguridad de los Recursos Humanos	3	9
5	Seguridad física y del entorno	2	13
6	Gestión de comunicaciones y operaciones	10	32
7	Control de acceso	7	25
8	Adquisición, Desarrollo y mantenimiento de sistemas.	6	16
9	Gestión de incidentes de seguridad	2	5
10	Gestión de continuidad del negocio	1	5
11	Cumplimiento	3	10
Totales:		39	133

FASE IV: ESTRUCTURACIÓN

4.4.1 Personalización de los controles.

A continuación los principales objetivos de cada uno de los dominios y sus controles:

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 desvió 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 veinticinco 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:

- ✓ Proteger y 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.

4.4.2 Detalle de los Controles

Una vez establecidos los principales objetivos de cada uno de los dominios asociados a los controles, se presenta los detalles de los controles organizados de la siguiente manera:

a) Control

En esta columna se identifica el número y nombre de cada control de acuerdo el dominio al que pertenece.

b) Cómo se protege

Permite establecer claramente la forma de proceder frente a la implantación de dicho control con la garantía de enmarcarse en el dominio respectivo basado en la realidad del departamento.

c) Canales de Ejecución y Comunicación, Garantías de Cumplimiento.

En este apartado a través de las sugerencias establecidas se pretende garantizar el cumplimiento efectivo del control, además es imprescindible respaldar los procedimientos con una documentación metódica que se la sugiere de acuerdo al control determinado tomando en cuenta todos las políticas de seguridad que posee el departamento, detallando criterios de mejoras de las presentes políticas y en los aspectos en los que se requiere se propone crear nuevas políticas de seguridad, además se establecen los canales de comunicación necesarios para la integración de todos los interesados en la implementación de un SGSI en el DESITEL, este aspecto permitirá comprobar el compromiso adquirido por la organización frente a la seguridad de la información junto a la dirigencia razonable de sus administradores.

Las actividades mencionadas se las ha realizado con la colaboración del Ing. Gonzalo Allauca y los integrantes del DESITEL para garantizar la estructuración adaptada a la realidad actual del Departamento.

A continuación el detalle de los controles establecidos para garantizar la seguridad de la información en el DESITEL.

4.4.2 Desarrollo de los controles

Tabla IV.IV Controles De La Metodología

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
POLITICA DE SEGURIDAD			
Políticas de seguridad de la información			
01	Documento de la política de seguridad de la información.	La Dirección debería definir y gestionar su aprobación para publicar un documento de la política de seguridad de la información a todos los empleados y las partes externas relevantes.	Dar a conocer a todos los integrantes del departamento la política de seguridad aprobada y vigente que se va emplear en la seguridad de la información. Posibles Documentos a elaborarse: • Política de Seguridad de la Información. • Formato de Procedimiento de comunicación de políticas de seguridad.
02	Revisión de la política de seguridad de la información	La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios funcionales o de gestión de la seguridad de la información significativos en el departamento) para garantizar que la seguridad es adecuada, eficaz y suficiente.	Ajustarse a los intervalos de tiempo planificados para la revisión o cambios que afectaron a la base de la evaluación inicial de riesgos, tales como los incidentes de seguridad, nuevas vulnerabilidades o cambios en la infraestructura organizativa y técnica. El proceso de revisión y evaluación consta de dos pasos distintos: **1. Planificación.** El coordinador del grupo de gestión de lanzamientos organiza el proceso de revisión. Esta persona se encarga de la programación de la revisión, la definición del papel de cada participante y determinar cómo los errores se pueden clasificar.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			2. Examen preliminar de la reunión (opcional) Esta reunión sirve para familiarizar a todos los miembros del departamento, con la revisión de la política de seguridad de la información y que se trate de reducir al mínimo el tiempo de preparación. Posibles Documentos a elaborarse: • Manual de planificación de revisión de la política de seguridad de la información con fechas de revisión adaptadas a las necesidades del departamento.
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
Organización interna			
03	Compromiso de la Dirección con la seguridad de la información.	Es responsabilidad del director del departamento respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización.	La persona encargada de la dirección no podrá ejercer adecuadamente su responsabilidad si no posee una eficiente capacitación sobre la seguridad de la información y poder brindar un soporte adecuado. Posibles Documentos a elaborarse: • Formato de Oficios para Asignación de Responsabilidades • Formato para Capacitación permanente.
04	Coordinación de la seguridad de la información.	Las actividades para la seguridad de la información deberían ser coordinadas por representantes que	Formar un grupo de gestión conformado por el director, técnicos coordinadores, usuarios finales

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
		posean cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización.	seleccionados, diseñadores de aplicaciones, y otros especialistas con el objetivo de establecer un marco de gestión para coordinar, fomentar y controlar el desarrollo de seguridad de la información dentro de la organización. Autorizar las iniciativas destinadas a mejorar la seguridad dentro de la organización. Posibles Documentos a elaborarse: • Informes de Análisis y aprobación de la política de seguridad de la información y las responsabilidades generales. • Manual Procedimiento para el control de cambios de gestión de la coordinación de la seguridad de la información. (Ej. Cambio de cualquier integrante del grupo de gestión, un nuevo estatuto institucional, etc.) • Registros de seguimiento de la coordinación de la seguridad de información.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
05	Asignación de responsabilidades relativas a la seguridad.	Definir y distribuir claramente todas las responsabilidades a los empleados (personal de apoyo y técnicos) del departamento para la seguridad de la información.	Emitir documentos formales que detallen el ámbito y nivel de responsabilidad sobre una tarea específica, un proceso o una actividad en la cual se utilice los activos físicos y lógicos del departamento (Anexo IV). Posibles Documentos a elaborarse: • Formato de Asignación de Responsabilidades y todo lo que ello implique.
06	Proceso de autorización de recursos para el tratamiento de la información.	Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información.	De acuerdo a la magnitud de la información y el valor de los activos se debe realizar el tratamiento de la información con herramientas adecuadas en base a un informe técnico detallado del personal que lo requiera. Posibles Documentos a elaborarse: • Manual de procesos de Autorización de recursos. • Formato de autorización de recursos.
07	Acuerdos de confidencialidad.	Se deberían identificar y revisar regularmente en los acuerdos de confidencialidad aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización.	Determinar claramente los acuerdos de confidencialidad al que están sometidos al pertenecer a una entidad que necesita la protección de su información. Posibles Documentos a elaborarse: • Formato de actas de confidencialidad

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
08	Contacto con las autoridades.	Se deberían mantener los contactos apropiados con las autoridades pertinentes.	Mantener registros de documentos físicos y/o digitales formales sobre la gestión de seguridad del departamento que ha sido informada a las autoridades. Posibles Documentos a elaborarse: • Registro o Bitácora de Documentos formales de contacto con las autoridades
09	Contacto con grupos de especial interés.	Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales.	El personal debe estar en constante preparación académica sobre la seguridad de la información, para obtener información actualizada y muy completa sobre aquellas amenazas publicadas a través Internet que están activas, y explica cómo evitarlas. Posibles Documentos a elaborarse: • Política de identificación de grupos especiales de interés.
10	Revisión independiente de la seguridad de la información.	Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información.	No descuidar por periodos largos de tiempo la estructuración de la seguridad de la información y el cumplimiento de la misma, de esta manera se evita retrasos en el cumplimiento de la planificación establecida y fundamentalmente definir ámbitos de independencia en la seguridad de la información.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a elaborarse: • Políticas de revisión independiente de la seguridad de información • Manual de procedimientos de revisión independiente de la seguridad de la información, en la cual se defina la autorización, responsabilidades, tiempos de cumplimiento y métodos de revisión con el único objetivo de asegurar la independencia de la revisión. • Formato Final del Informe de la revisión independiente realizada.
Terceros			
11	Identificación de los riesgos derivados del acceso de terceros	Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.	Identificar las partes terceras que no intervienen significativamente en el desarrollo del proyecto. Posibles Documentos a elaborarse: • Política de Identificación de terceros en el ámbito lógica como físico. ▪ Nivel de acceso que se le puede conceder. • Formato de riesgos derivados de la utilización de terceros.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
12	Tratamiento de la seguridad en la relación con los clientes.	Se deberían anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización.	Un cliente consume no genera por lo tanto solo debe enmarcarse en la forma de consumir no en su origen. Posibles Documentos a elaborarse: • Política de tratamiento de la seguridad en la relación con los clientes o Identificar clientes de acuerdo a los servicios prestados. • Determinar hasta que nivel de seguridad puede interactuar un cliente
13	Tratamiento de la seguridad en contratos con terceros.	Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.	Es necesario identificar las partes relevantes frente a la seguridad de la información, el momento de contratos con terceros. Posibles Documentos a elaborarse: • Política de tratamiento de la seguridad en contratos con terceros. o Control y cumplimiento de contratos con terceros.
GESTIÓN DE ACTIVOS			
Responsabilidad sobre los activos			
14	Inventario de activos.	Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.	No descartar ningún activo y lo más efectivo es revisar en varias ocasiones todos los activos existentes y comprobar su existencia.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a elaborarse: • Política de revisión de inventarios. • Formatos de Actas de entrega recepción
15	Responsable de los activos	Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización.	El director del departamento puede tomar todas las decisiones necesarias relativas a la información bajo su control a fin de mantener su integridad y su confidencialidad por lo tanto: • Entiende los principales riesgos involucrados en todos los usos internos de un tipo específico de información. • Especifica los métodos de control adicionales necesarias para proteger esta información. • Aprueba las solicitudes usuarios para acceder a la información. • Revisa la lista de control de acceso de los usuarios para determinar si los privilegios deben ser retirados. Posibles Documentos a elaborarse: • Manual de procedimiento para entrega de responsabilidades de activos. • Actas de Entrega recepción de activos y responsabilidades.
16	Uso aceptable de los activos.	Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.	El uso de un activo debe ser estrictamente lo necesario. Posibles Documentos a elaborarse: • Manual de uso de activos.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Manual de revisión del uso adecuado de los activos.
		Clasificación de la información.	
17	Directrices de clasificación.	La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.	Clasificación de la información de acuerdo a la importancia para el departamento. Posibles Documentos a elaborarse: • Política de Clasificación de la información o Parámetros de Clasificación de la información. o Asignación de prioridades a la información. • Formato de Clasificación de los activos.
18	Etiquetado y manipulado de la información.	Se debería desarrollar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización.	La información es vulnerable cuando su protección no es adecuada y esto se mejora con la clara identificación de la misma. Posibles Documentos a elaborarse: • Manual de etiquetado de la información
		SEGURIDAD DE LOS RECURSOS HUMANOS	
		Antes del empleo	
19	Funciones y responsabilidades.	Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.	Se debe establecer responsabilidades en base a jerarquías de trabajo para evitar complicaciones.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a elaborarse: • Documento de Jerarquías y responsabilidades y seguridad en el cumplimiento de su función. • Manual de Inserción y Ambientación de sus funciones.
20	Selección y política de personal.	Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.	Comprobación de referencias puede ser el método de detección más eficaz en un proceso de selección de personal. Verificación de referencias confirma la experiencia y la competencia de los candidatos, y proporciona una opinión de terceros sobre las aptitudes y actitudes de los solicitantes. Posibles Documentos a elaborarse: • Manual de selección de personal.* • Manual de comprobación de referencias. * ALTERNATIVA: Manual de Inserción y Ambientación de sus funciones.
21	Términos y condiciones de contratación	Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información.	La elección del acuerdo depende de las necesidades de las partes interesadas y sobre la relación de poder que existe entre ellos. Posibles Documentos a elaborarse: • Manual de contratación de personal

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			(REFERENCIA: Departamento de RRHH.) • Manual de contratación de contratistas y terceros (REFERENCIA: Sistema de Contratación Publica del Ecuador).
Durante el empleo			
22	Responsabilidades de la Dirección.	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización	Son responsabilidades ya definidas en base a las políticas de la seguridad de la información. Posibles Documentos a elaborarse: • Informes por periodos académicos respecto a la concordancia de personal vs responsabilidades departamentales. • Guiarse en las políticas de la seguridad de la información definida con la dirección.
23	Concienciación, formación y capacitación en seguridad de la información.	Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.	La capacitación debe ser constante de esto depende la proyección de mejora de la organización. Posibles Documentos a elaborarse: • Cronograma de capacitación a los empleados a intervalos de tiempo que se consideren necesarios sobre la seguridad de la información en base a sus responsabilidades.
24	Proceso disciplinario.	Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.	Las sanciones correctoras deben existir caso contrario no habrá una mejora continua.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a elaborarse: • Manual de sanciones a empleados que produzcan brechas en la seguridad. • (REF: Manual de Sanciones DEPT. RRHH institucional)
Cese del empleo o cambio de puesto de trabajo.			
25	Responsabilidad del cese o cambio.	Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas.	Este aspecto debe formar parte del acuerdo de trabajo pues claramente nos damos cuenta de la ventaja o desventaja que puede ocasionar un cambio en una responsabilidad determinada. Posibles Documentos a elaborarse: • Manual de cese o cambio de las responsabilidades del personal.
26	Devolución de activos	Todos los empleados, contratistas y terceros deberían devolver todos los activos de la organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo.	Por eso es importante el acuerdo de uso de los activos para que en la culminación de un empleo no existan inconvenientes que afecten a la organización. Posibles Documentos a elaborarse: • Formato de ACTAS ENTREGA RECEPCION.
27	Retirada de los derechos de acceso.	Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio.	Ningún empleado podrá acceder a la organización y su conjunto luego de haber terminado su función (Esto debe contar en la firma del contrato). Posibles Documentos a elaborarse:

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Formato de Retirada de acceso a activos (hardware o software). REFERENCIA: Manual de cese o cambio de las responsabilidades del personal
SEGURIDAD FÍSICA Y DEL ENTORNO			
Áreas seguras.			
28	Perímetro de seguridad física.	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.	El acceso al departamento debe contar con la seguridad física necesaria en base a políticas establecidas y a la importancia de la información. Posibles Documentos a elaborarse: • Manual de controles de entrada a áreas restringidas. **REFERENCIA:** SEGURIDADES EN EL DATACENTER IMPLEMENTADO
29	Controles físicos de entrada.	Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado.	Las entradas pueden convertirse en escapes, es necesario garantizar el acceso únicamente al personal autorizado. **REFERENCIA:** Manual de controles de entrada a áreas restringidas.
30	Seguridad de oficinas, despachos e instalaciones.	Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos.	La seguridad debe ser asignada de acuerdo a la estructura física del departamento. Posibles Documentos a elaborarse: • Manual de controles de entrada a oficinas, despachos e instalaciones.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
31	Protección contra las amenazas externas y de origen ambiental.	Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.	La ubicación de la información debe estar respaldada con varios escudos de protección para garantizar su seguridad. • Manual contra las amenazas externas y de origen ambiental.
32	Trabajo en áreas seguras.	Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras.	Un área segura de trabajo cuenta con controles de acceso a la misma.
33	Áreas de acceso público y de carga y descarga.	Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información.	El aislamiento de la información para el público en general debe ser estricto. AVISOS DE ACCESO A AREAS RESTRINGIDAS.
Seguridad de los equipos			
34	Emplazamiento y protección de equipos.	El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.	Se debe evitar el acceso no autorizado tomando las debidas precauciones en base a la ubicación de los equipos. Posibles Documentos a elaborarse: REF. Manual de acceso no autorizado.
35	Instalaciones de suministro	Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo.	Previo a la instalación de equipos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.
36	Seguridad del cableado.	Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.	Se debe etiquetar el cableado, las extensiones y los tableros de distribución eléctrica. Evitar los cableados sueltos o dispersos, estos deberán entubarse.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
37	Mantenimiento de los equipos.	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.	Es necesario establecer puntos centrales de corte de fluido eléctrico, a nivel de los pisos del DESITEL. Posibles Documentos a elaborarse: • Políticas de Mantenimiento de Recursos Hardware y Software. • Manual de Procedimiento para Mantenimiento de Hardware y Software.
38	Seguridad de los equipos fuera de las instalaciones.	Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos.	Se debe aplicar seguridad de acuerdo a la importancia de los equipos. Posibles Documentos a elaborarse: • Políticas de Seguridad para equipos fuera de las instalaciones.
39	Reutilización o retirada segura de equipos.	Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación.	Se debe considerar aspectos importantes en la eliminación de la información como: pérdidas irreparables, daños, etc. Posibles Documentos a elaborarse: • Políticas de reutilización o retirada segura de equipos. • Manual de Procedimiento para la reutilización o retirada segura de equipos.
40	Retirada de materiales de propiedad de la empresa.	No deberían sacarse equipos, información o software fuera del local sin una autorización.	Controlar los accesos a los activos a través de un registro de movimientos con periodos de tiempo.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles documentos a elaborarse • Manual de registro de movimientos de materiales fuera de la empresa. • Formato Actas entrega – recepción.
GESTIÓN DE COMUNICACIONES Y OPERACIONES			
Responsabilidades y procedimientos de operación.			
41	Documentación de los procedimientos de operación.	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.	Es necesario mantener informado a todo el personal de la documentación existente para mejorar el desempeño de la organización. Posibles Documentos a elaborarse: • Política de comunicación de procedimientos de operación. • Manual de procedimiento de comunicación de procedimientos de operación.
42	Gestión de cambios.	Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información.	Los cambios deben ser solo los necesarios a acoplados a la política vigente. Posibles Documentos a elaborarse: • Política de Gestión de Cambios • Manual de procedimiento de Gestión de Cambios. • Formatos para la gestión de cambios.
43	Segregación de tareas.	Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos	Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación, autorización, y concienciación a los usuarios respecto de su responsabilidad.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
		de la organización.	Posibles Documentos a elaborarse: • Políticas de Segregación de tareas.
44	Separación de los recursos de desarrollo, prueba y operación.	La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.	Los recursos deben ser asignados en base a la operación a realizarse Posibles Documentos a elaborarse: • Políticas de Separación de los recursos de desarrollo, prueba y operación. • Manual de Procedimiento para separación de recursos de desarrollo, prueba y operación (producción) de sistemas.
Gestión de la provisión de servicios por terceros.			
45	Provisión de servicios.	Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa.	Aquí es importante la distribución de responsabilidades para el manejo de situaciones externas. Posibles Documentos a elaborarse: • Política: Generación de Reportes por unidad de tiempo (definirla de acuerdo a la criticidad del servicio) sobre la provisión de servicios.
46	Supervisión y revisión de los servicios prestados por terceros.	Los servicios, informes y registros suministrados por terceros deberían ser monitoreados y revisados regularmente, y las auditorías se deberían realizar a intervalos regulares.	Se debe garantizar la prestación segura de los servicios de terceros con una clara identificación de su participación. Posibles Documentos a elaborarse: REFERENCIA: Política de Generación de

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Reportes por unidad de tiempo (definirla de acuerdo a la criticidad del servicio) sobre la provisión de servicios.
47	Gestión del cambio en los servicios prestados por terceros.	Se deberían gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes, en los procedimientos y los controles teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.	Los cambios se deben aceptar luego de una reevaluación de los riesgos. Posibles Documentos a elaborarse: • Política de Gestión de Cambios prestados por terceros • Manual de procedimiento de Gestión de cambios prestados por terceros. • Formatos para la gestión de cambios prestados por terceros.
Planificación y aceptación del sistema.			
48	Gestión de capacidades.	Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema.	La dirección debe monitorizar el uso y capacidades de los recursos así como la eficiencia en la utilización del personal. Posibles Documentos a elaborarse: • Política: Generación de Informes semestrales de gestión de capacidades.
49	Aceptación del sistema.	Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.	Definir los requerimientos mínimos acordes con la política de seguridad que garantice su aceptación y buen funcionamiento. Posibles Documentos a elaborarse: • Políticas de Establecimiento de criterios de aceptación para nuevos sistemas, actualizaciones y nuevas versiones.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Políticas de pruebas durante desarrollo y previo la aceptación • Manual de Procedimiento de Aceptación de nuevos sistemas .(ESTUDIO DE FACTIBILIDAD, Análisis Costo Beneficio Análisis de Riegos, Planificación Temporal) • Formato de Solicitud de Implementación de Nuevos Sistemas. • Formatos de Seguimiento y Aceptación de Nuevos Sistemas. • Formato de actualización de Nuevos Sistemas • Formato de producción de Nuevos Sistemas* *Ref: Manual de Procedimiento de Aceptación de nuevos sistemas .(ESTUDIO DE FACTIBILIDAD, Análisis Costo Beneficio Análisis de Riegos, Planificación Temporal)
Protección contra el código malicioso y descargable.			
50	Controles contra el código malicioso.	Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios.	El personal que tiene acceso a los servidores en forma mono usuaria, deberá encargarse de detectar y eliminar en los medios magnéticos u ópticos, la infección o contagio de código malicioso. Posibles Documentos a elaborarse: • Políticas de controles de detección,

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			prevención y recuperación contra el sw malicioso. • Manual de procedimiento para la concienciación de los usuarios. A tal efecto, utilizara los procedimientos establecidos por el DESITEL. El director del DESITEL designara por escrito, al personal responsable de realizar los procedimientos de prevención, detección, y eliminación de código malicioso.
51	Controles contra el código descargado.	Cuando se autoriza la utilización de código móvil, la configuración debería asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos móviles no autorizados.	No deben utilizarse unidades de almacenamientos provenientes del exterior del departamento. Posibles Documentos a elaborarse: • Política de uso de código descargado.
Copias de seguridad.			
52	Copias de seguridad de la información.	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación.	Se deben hacer copias permanentes de seguridad con periodos de tiempo establecidas por la dirección dependiendo de la criticidad de la información. Posibles documentos a elaborarse: • Políticas de copias de seguridad de la información. • Manual de controles de copias de seguridad.
Gestión de la seguridad de las redes.			

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
53	Controles de red.	Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.	Se debe evitar el acceso de usuarios de la intranet a redes externas sin el justificativo correspondiente (Ej. Red del Banco Pacifico – Sistema de Cobros en Línea), cualquier excepción deberá ser documentada y contar con el visto bueno de la dirección. Posibles documentos a elaborarse: • Política de acceso a redes externas. • Formato de Justificación al acceso a redes externas.
54	Seguridad de los servicios de red.	Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior.	• Acuerdos Internos: los podemos definir la asignación de responsabilidades de implementación de un servicio de red, que deberá ser plasmado con un informe técnico que describa todos los indicadores de funcionamiento del servicio de red implementado. • Acuerdo Externos: proveedores externos de servicios de red, en los que los indicadores de funcionamiento estarán plasmados en los contratos. Seguimiento y Monitoreo de los indicadores de servicio definidos en el acuerdo. Identificar claramente el acuerdo sobre los servicios de red. Posibles documentos a elaborarse: • Políticas de Seguridad de servicios de

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			red. • Manual de procedimiento para la implementación de servicios de red.
Manipulación de los soportes.			
55	Gestión de soportes extraíbles.	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.	En la medida más adecuada no deben utilizarse unidades de almacenamiento provenientes del exterior del departamento. Posibles Documentos a elaborarse: • Políticas de uso de soportes extraíbles. • Manual de procedimiento para el uso de soportes extraíbles.
56	Retirada de soportes.	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.	Registrar el soporte, su origen y la forma de retirarla. Posibles documentos a elaborarse: • Manual de procedimientos de retirada de soportes. • Formato de Informe de Retiro de Soportes
57	Procedimientos de manipulación de la información.	Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados.	La organización debe cuidar su información contra divulgaciones o usos no autorizados o inadecuados. Posibles documentos a elaborarse: • Políticas de Manipulación de la información. • Manual de Procedimiento para la entrega de información confidencial a terceros.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Sanciones: REFERENCIA: Política de Sanciones de RRHH.
58	Seguridad de la documentación del sistema.	Se debería proteger la documentación de los sistemas contra accesos no autorizados.	En base a la política de seguridad de la información debe mantenerse la Seguridad de la documentación del sistema. Posibles documentos a elaborarse: • Política de Seguridad de la documentación del sistema • Manual de procedimiento de acceso a terceros a la documentación del sistema. • Formato de ACTAS ENTREGA – RECEPCION.
Intercambio de información.			
59	Políticas y procedimientos de intercambio de información.	Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación.	La información debe ser manejada cuidadosamente, el intercambio de la misma debe ser analizado y autorizado. Posibles documentos a elaborarse: • Política de intercambio de la información.
60	Acuerdos de intercambio.	Se deberían establecer acuerdos para el intercambio de información y software entre la organización y las partes externas.	La información debe ser manejada cuidadosamente el intercambio de la misma debe ser analizada y autorizada y documentada. Posibles documentos a elaborarse: • Formato de acuerdos para el intercambio de información y software entre la

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			organización y las partes externas.
61	Soportes físicos en tránsito.	Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.	Evitar el cambio constante de medios que contengan información importante. Posibles documentos a elaborarse: • Política de transporte de la información fuera de los límites físicos de la organización. • Manual de Procedimiento de soportes físicos en tránsito. • Formato de Salida y Entrada de soportes físicos en tránsito.
62	Mensajería electrónica.	Se debería proteger adecuadamente la información contenida en la mensajería electrónica.	La mensajería electrónica en caso de existir no debe ser autorizada en los equipos donde consta la información relevante de la organización. Posibles documentos a elaborarse: • Políticas de Seguridad de Mensajería Electrónica.
63	Sistemas de información empresariales.	Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información del negocio.	Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre los sistemas de información. Posibles documentos a elaborarse: • Política de seguridad en la interconexión de sistemas de información del negocio.
Servicios de comercio electrónico.			

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
64	Comercio electrónico.	Se debería proteger la información involucrada en el comercio electrónico que pasa por redes públicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas.	Garantizar la seguridad del uso de redes públicas para evitar pérdidas considerables de la información. Ej. PAGOS ONLINE EN LA ESPOCH.
65	Transacciones en línea.	Se debería proteger la información implicada en las transacciones en línea para prevenir la transmisión incompleta, enrutamiento equivocado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.	Ej. PAGO DE ARANCELES ACADEMICOS Y DE OTROS SERVICIOS ONLINE. Posibles Documentos • Política de Transacciones en Línea entre instituciones o entre sistemas internos.
66	Información públicamente disponible.	Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas.	Se debe evitar el acceso público a la información relevante del departamento, con medidas puntuales de la integridad de la información. Posibles documentos a elaborarse: • Política de acceso publico a los sistemas de información.
		Supervisión.	
67	Registros de auditoría.	Se deberían producir y mantener durante un periodo establecido los registros de auditoría con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso.	Los registros de auditoría deben ser documentados con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información. Posibles documentos a elaborarse: • Política de Mantenimiento de Registros

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			de auditoría.
68	Supervisión del uso del sistema.	Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo.	Revisar regularmente los resultados de las actividades de monitoreo, para el efectivo cumplimiento. Posibles documentos a elaborarse: • Política de Supervisión del uso del sistema. • Manual de procedimiento para supervisión del uso del sistema. • Formato de Informe de Supervisión del uso del sistema.
69	Protección de la información de los registros.	Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados.	La protección de la información debe ser en base a las normas establecidas. Posibles documentos a elaborarse: • Política de protección de la información de los registros. Ej. Proteger un informe desfavorable o favorable respecto al funcionamiento de un determinado sistema en el cual se identifique responsable, y este documento se vuelva crítico.
70	Registros de administración y operación.	Se deberían registrar las actividades del administrador y de los operadores del sistema.	Se deben contar con registros periódicos dependiendo de la criticidad o de eventualidades para comprobar el desempeño de las partes involucradas.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles documentos a elaborarse: • Políticas de registros de administración y operación • Formato de Registro de administración y operación
71	Registro de fallos.	Se deberían registrar, analizar y tomar acciones apropiadas de las averías.	Frente a la presencia de fallos es necesario un registro adecuado para evitar inconvenientes futuros. Posibles documentos a elaborarse: • Política de Registro de Fallos • Manual de procedimiento para fallos • Formato de Informe de Fallos.
72	Sincronización del reloj.	Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo.	El tiempo debe ser coordinado y cronometrado. Posibles documentos a elaborarse: • Política de sincronización de relojes en los sistemas. • Manual de Procedimiento de sincronización de relojes de los sistemas.
CONTROL DE ACCESO			
Requisitos de negocio para el control de acceso			
73	Política de control de acceso.	Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.	Es recomendable que el acceso sea restringido al personal autorizado, contándose con registro de entradas y salidas de los visitantes. Posibles documentos a elaborarse:

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Política de Control de Acceso a todas las dependencias del Departamento.
Gestión de acceso de usuario.			
74	Registro de usuario.	Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.	Impedir el acceso no autorizado a los sistemas de información del departamento. Posibles documentos a elaborarse: **REF:** PUERTAS DE ACCESO AUTOMATICAS, cámara de seguridad (REGISTRO EN VIDEO).
75	Gestión de privilegios.	Se debería restringir y controlar la asignación y uso de los privilegios.	Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso, deberán ser notificados al administrador con el visto bueno del Director. Posibles documentos a elaborarse: • Política de Gestión de Privilegios. • Manual de procedimiento para asignación, eliminación y cambio de privilegios.
76	Gestión de contraseñas de usuario.	Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal.	La asignación de password debe ser realizada de forma individual, por lo que el uso de password compartidos debe ser notificado formalmente. Posibles documentos a elaborarse: • Política de gestión de contraseñas de usuario. • Manual de procedimiento para

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			asignación de contraseñas (para responsables y backups) y uso de las mismas.
77	Revisión de los derechos de acceso de usuario.	El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.	Se debe documentar con regularidad los derechos de acceso de los usuarios. Posibles documentos a elaborarse: • Política de revisión de derechos de acceso de usuario. • Manual de procedimiento para revisión de los derechos de acceso de usuario. • Formato de Informe de Revisión.
Responsabilidades de usuario.			
78	Uso de contraseñas.	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.	Se debe evitar que los password se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizada puedan descubrirlos.
79	Equipo de usuario desatendido.	Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada.	En este control se consideran desatendidos a los equipos que no son controlados frecuentemente pero poseen información relevante de la organización, por lo cual se debe tener garantías de seguridad para el acceso no autorizado.
80	Política de puesto de trabajo despejado y pantalla limpia.	Políticas para escritorios y monitores limpios de información.	Todos los usuarios deberán cumplir con la política de puesto de trabajo despejado y pantalla limpia.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
Control de acceso a la red.			
81	Política de uso de los servicios en red.	Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.	Para la utilización de los servicios en red, se debe contar con las garantías de accesos a los mismos, considerando jerarquías de autorización de acceso. Posibles Documentos a elaborarse: • Política de uso de los servicios de Red • Formato de Autorización de Acceso a los servicios de red.
82	Autenticación de usuario para conexiones externas.	Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios.	De acuerdo a las políticas de la organización se debe contar con métodos de autenticación de acceso remoto de conexiones externas. Posibles documentos a elaborarse: • Política de autenticación para conexiones externas. Ej. Escritorio Remoto, SSH, TELNET, etc
83	Identificación de los equipos en las redes.	Se debería considerar la identificación automática de los equipos como un medio de autenticación de conexiones procedentes de lugares y equipos específicos.	Para garantizar la seguridad en este punto se debe obtener como seguridad un registro de los equipos conectadas a la red Posibles documentos a elaborarse: • Política de Identificación de los equipos en las redes. • Formato de Inventario de equipos identificados.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
84	Protección de los puertos de diagnóstico y configuración remotos.	Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico.	Se debe proteger los puertos de diagnóstico y configuración remotos con un control de acceso a los mismos. Posibles documentos a elaborarse: Política de protección de puertos de diagnostico y configuración remotos. **SUG:** Revisión de Logs y/o uso de software especifico.
85	Segregación de las redes.	Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes.	La segregación de usuarios depende de la jerarquía de utilización de las redes y de la importancia de la información. Posibles Documentos a elaborarse: • Política de Segregación de las redes. REF: Gestión de VLANs.
86	Control de la conexión a la red.	En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la política de control de accesos y necesidad de uso de las aplicaciones de negocio.	El control de conexiones se debe realizar en base a la política de control de accesos y necesidad de conexión a la red Posibles documentos a elaborarse: • Política de de Control de conexión a la red. • Formato de Informe de conexión inadecuada a la red.
87	Control de encaminamiento (routing) de red.	Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones	Verificar la política de control de acceso de las conexiones de los ordenadores a través de un registro permanente de routing.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
		de negocio.	Posibles Documentos a elaborarse: • Informe de Control de Encaminamiento (routing) de red. Por. ejm: Control de Acceso entre VLANS definido. SUG: Utilizar software especifico.
Control de acceso al sistema operativo.			
88	Procedimientos seguros de inicio de sesión.	Debería controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión.	Se debe incorporar controles de acceso autorizados. Posibles documentos a elaborarse: • Política de procedimientos seguros de conexión al SO.
89	Identificación y autenticación de usuario.	Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario.	Se debe evitar que las contraseñas se encuentren de forma legible en cualquier medio impreso o dejarlos en un lugar donde personas no autorizada puedan descubrirlos. Posibles Documentos a elaborarse: • Política de Identificación y Autenticación de usuario al SO.
90	Sistema de gestión de contraseñas.	Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas.	La forma de gestionar la creación de contraseñas dependen de la organización pero deben enmarcarse en estándares de seguridad como: Combinaciones de letras y números, longitud de la contraseña, etc.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a elaborarse: • Política de Gestión de Contraseñas al Sistema Operativo.
91	Uso de los recursos del sistema.	Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones.	La garantía de seguridad depende de los controles del sistema y de sus aplicaciones mediante la restricción de programas que no son de utilidad. Posibles Documentos a elaborarse: • Formato de Inventario de los recursos su funcionalidad, sus configuraciones y oros.
92	Desconexión automática de sesión.	Se deberían desconectar las sesiones tras un determinado periodo de inactividad.	Se debe contar con control de desconexión de las sesiones de acuerdo a las necesidades de inactividad de los equipos. Posibles Documentos a elaborarse: • Política de Control de Desconexión automática de sesión del SO.
93	Limitación del tiempo de conexión.	Se deberían utilizar limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo.	Frente a las aplicaciones de alto riesgo se debe otorgar controles de accesos según la necesidad. Posibles Documentos a elaborarse: • Política de Limitación del Tiempo de Conexión al SO.
Control de acceso a las aplicaciones y a la información.			
94	Restricción del acceso a la información.	Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.	Se debe asignar prioridades de acceso a la información en base a la política de control de accesos definida.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a elaborarse: REF: Política del Dominio de Control de Acceso
95	Aislamiento de sistemas sensibles.	Los sistemas sensibles deberían disponer de un entorno informático dedicado (propio).	Los sistemas deben contar con un tratamiento apropiado de acuerdo a la importancia de los mismos. Posibles Documentos a elaborarse: • Política de Aislamiento de sistemas sensibles. • Manual de Procedimiento de Aislamiento de sistemas sensibles.
Ordenadores portátiles y teletrabajo.			
96	Ordenadores portátiles y comunicaciones móviles.	Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.	La protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones debe ser documentada por la dirección. Posibles Documentos a elaborarse: • Política de acceso a ordenadores portátiles y acceso a sus comunicaciones móviles.
97	Teletrabajo.	Se debería desarrollar e implantar una política, planes operacionales y procedimientos para las actividades de teletrabajo.	En el caso de existir con un plan operacional de teletrabajo. Ej. Turnos de Monitorización del DataCenter y las aplicaciones fuera de horario de trabajo y fuera de la institución. Posibles Documentos a elaborarse: • Política de Control de Acceso de Teletrabajo.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Formato de Informes de Teletrabajo. •
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
Requisitos de seguridad de los sistemas de información.			
98	Análisis y especificación de los requisitos de seguridad.	Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad.	Se debería especificar conjuntamente entre los jefes y técnicos tanto de las dependencias requirentes como del DESITEL, los requerimientos de seguridad necesarios, y se deberán verificar y validar (SRS)los mismos por parte de los jefes de los departamentos a través de la firma de documentos en los cuales se detallen fechas, involucrados, responsabilidades y requerimientos, tanto para las demandas de nuevos sistemas de información o mejoras de los sistemas ya existentes y garantizar que no se pierden recursos. REF: política de aceptación de nuevos sistemas de información o mejoras de los sistemas ya existentes. Posibles Documentos a elaborarse: • Actas de Reuniones para Análisis y especificación de los requisitos de seguridad. • SRS de requisitos de seguridad.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
Tratamiento correcto de las aplicaciones.			
99	Validación de los datos de entrada.	Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados.	Establecer grupos o personal, métodos y técnicas de validación de datos de entrada Posibles Documentos a elaborarse: • Política de validación de datos de ingreso. • Manual de Procedimiento de Validación de datos de entrada • Formato de Informe de Validación de datos de entrada.
100	Control del procesamiento interno.	Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas.	Establecer grupos o personal, métodos y técnicas para el control de procesamiento interno. Posibles Documentos a elaborarse: • Política de validación control del procesamiento interno (SRS) • Manual de Procedimiento de Control del procesamiento interno. • Formato de Informes de Control del procesamiento interno.
101	Integridad de los mensajes.	Se deberían identificar los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, e identificar e implantar los controles apropiados.	Se deben identificar los requisitos para asegurar la autenticidad y protección de la integridad de los mensajes Establecer grupos o personal, métodos y técnicas para el control de procesamiento interno. Posibles Documentos a elaborarse: • Política de validación Integridad de los mensajes. (SRS) • Manual de Procedimiento de Integridad

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			de los mensajes. • Formato de Informes de Integridad de los mensajes.
102	Validación de los datos de salida.	Se deberían validar los datos de salida de las aplicaciones para garantizar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.	Los datos de salida de las aplicaciones deben validarse de acuerdo a la complejidad de la aplicación. Establecer grupos o personal, métodos y técnicas para la validación de los datos de salida. Posibles Documentos a elaborarse: • Política de Validación de los datos de salida. (SRS) • Manual de Procedimiento de Validación de los datos de salida. • Formato de Informes de Validación de los datos de salida.
Controles criptográficos.			
103	Política de uso de los controles criptográficos.	Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información.	De acuerdo a la necesidad se podría contar con controles criptográficos para el tratamiento de la información. Posibles Documentos a elaborarse. • Política de uso de los controles criptográficos. Ej. md5 modificado, https, firma digitales, otros.
104	Gestión de claves.	Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la Organización.	La asignación de claves debe realizarse es base a la complejidad de técnicas criptográficas.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Posibles Documentos a Generar. • Política de Gestión de claves para controles criptográficos. • Manual de Procedimiento para gestión de claves de controles criptográficos.
		Seguridad de los archivos de sistema.	
105	Control del software en explotación.	Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos	Los sistemas que estén operando deben cumplir con controles de software para su correcta manipulación. Posibles Documentos a Generar: • Política de Control de software en explotación • Manual de Procedimiento para el control de software en explotación • Formatos de Informes de Control del Software en Explotación
106	Protección de los datos de prueba del sistema.	Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas.	Se debe contar con un equipo especial para la prueba del sistema. Posibles Documentos a elaborarse: • Política de protección de los datos de prueba del sistema • Manual de Procedimiento de Protección de los datos de prueba de sistemas. • Formatos de Confidencialidad de datos de prueba del sistema

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Ejemplo de Casos. Solicitudes de Bases de Datos para implementación de tesis, solicitud de cuentas de mail.
107	Control de acceso al código fuente de los programas.	Se debería restringir el acceso al código fuente de los programas.	El control de acceso al código fuente debe ser en base a la importancia, privacidad y autenticidad del código. Posibles Documentos a elaborarse: • Política de Control de acceso al código fuente de los programas. Ejemplos. Accesos Extranet: de hackers, cracker a través de sitios web. Acceso Intranet: Claves Compartidas de Servidores, Copias en PC personales de uso compartido, Robos de PC.
Seguridad en los procesos de desarrollo y soporte.			
108	Procedimientos de control de cambios.	Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios.	El SRS generado para un cambio debe estar con firma de responsabilidad de los jefes de los departamentos o dependencias involucradas, en este caso el Director del DESITEL y el jefe del departamento requirente, estas autoridades a su vez controlaran las responsabilidades operativas de los técnicos operativos. Posibles Documentos a elaborarse:

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Política de control de cambios
109	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización	Debido a los cambios que se generen en la revisión técnica de las aplicaciones, es crucial garantizar su eficiencia. Posibles Documentos a elaborarse: • Política de revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo • Manual de Procedimiento para efectuar cambios en el sistema operativo. Ejemplos. • Yum upgrade (en Linux) • Instalación servipacks en Windows • Otros
110	Restricciones a los cambios en los paquetes de software.	Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados.	Los cambios en los paquetes de software se deben evitar en lo posible, pues en su creación se establecen requerimiento con su tiempo de duración. Posibles Documentos a elaborarse: • Política de Restricciones a los cambios de paquetes de software • Manual de Procedimiento de restricciones de los cambios de paquetes de software

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			Ejemplo: • Actualizar la versión del apache en Linux • Cambiar únicamente si verificamos vulnerabilidades o si es necesario en el funcionamiento de las nuevas versiones de software
111	Fugas de información.	Se debería prevenir las posibilidades de fuga de información.	La fuga de información no es más que: • Llevar o acceder a la información sin autorización. • Inutilización de la misma. Posibles Documentos a elaborarse: • Política para evitar la fuga de información. • Manual de Procedimiento en caso de fuga de información.
112	Externalización del desarrollo de software.	Se debería supervisar y monitorizar el desarrollo del software subcontratado por la Organización.	El director del Departamento debe ser el encargado de supervisar el desarrollo del software generado fuera de la Organización. Posibles Documentos a elaborarse: • Política de Externalizacion del desarrollo de software. • Manual de Procedimiento para recepción de software desarrollado externamente.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
		Gestión de la vulnerabilidad técnica.	
113	Control de las vulnerabilidades técnicas.	Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados.	Se debe realizar una capacitación de todo el personal oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando y evitar daños futuros. Posibles Documentos a elaborarse: • Política de Control de Vulnerabilidades. • Manual de Procedimiento para el control de vulnerabilidades técnicas. • Manual de Procedimiento para el tratamiento de vulnerabilidades identificadas.
		GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
		Notificación de eventos y puntos débiles de seguridad de la información.	
114	Notificación de los eventos de seguridad de la información.	Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados.	La comunicación de un fallo de seguridad debe ser realizada lo más rápido posible a las instancias pertinentes y de acuerdo a la complejidad de la información para canalizar soluciones optimas. Documentos Posibles a elaborarse: • Política de Notificación de los eventos de fallo en la seguridad de la información • Manual de Procedimiento de notificación de los eventos de fallo en la seguridad de la información.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			• Formato de Notificación.
115	Notificación de puntos débiles de seguridad.	Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.	Cuando se encuentren puntos débiles en la seguridad de la información, a través de un informe adecuado se debe notificar para garantizar la integridad del funcionamiento del sistema y de la información del mismo. Documentos Posibles a elaborarse: • Política de Notificación de puntos débiles de seguridad • Manual Procedimiento de Notificación de puntos débiles de seguridad. • Formato de Notificación
Gestión de incidentes y mejoras de seguridad de la información.			
116	Responsabilidades y procedimientos.	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.	La respuesta frente a un incidente en la seguridad de la información, se la debe realizar en base a un procedimiento involucrado donde se definan responsables y formas de enfrentar el problema. Documentos Posibles a elaborarse. • Política de Responsabilidad y Procedimientos en la gestión de incidentes. • Manual de Responsabilidades y procedimiento de la gestión de incidentes.

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
117	Aprendizaje de los incidentes de seguridad de la información.	Debería existir un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información.	Los incidentes de seguridad de la información, deben ser almacenados mediante un informe para en tiempos posteriores analizar su evolución. Documentos Posibles a elaborarse. • Formato de Informes de Incidentes de seguridad de la información. • Bitácora de Incidentes y Soluciones. (Aplicar algún tipo de Codificación).
118	Recopilación de evidencias.	Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada conforme a las reglas para la evidencia establecidas en la jurisdicción relevante.	En base a la política de sanciones determinada por el departamento después de un incidente en la seguridad de información la evidencia debe ser guardada, para proceder de acuerdo a las políticas vigentes. Posibles Documentos a elaborarse: • Procedimiento Técnico: Análisis Forense. • Procedimiento Legal: Departamento de RRHH, y Unidad de Procuraduría
GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
Aspectos de seguridad de la información en la gestión de la continuidad del negocio.			
119	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	Se debería desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la	La continuidad del negocio no es más que el **cumplimiento de las políticas de seguridad vigente** y por lo tanto se debe sugerir mejoras en el desarrollo de la política de seguridad de la

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
		continuidad del negocio.	información para mantener resultados óptimos.
120	Continuidad del negocio y evaluación de riesgos.	Se deberían identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.	La evaluación me permitirá atacar las causas y manejar los efectos de manera que podamos a futuro tratar de evitar los eventos y minimizar su impacto para garantizar la continuidad del negocio Posibles Documentos a elaborarse: • Manual de Procedimiento de Evaluación de Eventos. • Formatos de Informes, Bitácora de Evaluaciones.
121	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempo requerido, tras la interrupción o fallo de los procesos críticos de negocio.	El plan de continuidad deberá incluir el análisis de los procesos que componen la organización, qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas. Posibles Documentos a elaborarse: • Guía de desarrollo del plan de

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			continuidad. • Plan de Continuidad para aseguramiento de la información.
122	Marco de referencia para la planificación de la continuidad del negocio.	Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.	Un Plan de Continuidad de Negocio, a diferencia de una Plan de Contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las operaciones de negocio críticas necesarias para continuar en funcionamiento después de un incidente no planificado. Posibles Documentos a elaborarse: • Formato de referencia para la continuidad del negocio.
123	Pruebas, mantenimiento y reevaluación de planes de continuidad.	Se deberían dar el seguimiento adecuado para CONTROLAR, VALIDAR VERIFICAR Y REEVALUAR los planes de continuidad regularmente para garantizar su consistencia.	Los planes de continuidad deben ser analizados luego de un periodo considerable de tiempo para garantizar la sostenibilidad de la metodología y políticas establecidas en la organización. Posibles Documentos a elaborarse: • Formato para la reevaluación del plan de continuidad.
CUMPLIMIENTO			
Cumplimiento de los requisitos legales.			
124	Identificación de la legislación aplicable.	Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Organización para cumplir con estos requisitos, deberían ser explícitamente definidos,	De acuerdo a la política establecida se debe gestionar el cumplimiento de las reglas establecidas para garantizar que no existan demoras en el desarrollo de la seguridad de la

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
		documentados y actualizados para cada uno de los sistemas de información y la Organización.	información. Posibles Documentos a elaborarse: • Política de Cumplimiento de reglas. • Manual de Procedimiento de sanción por incumplimiento de reglas.
125	Derechos de propiedad intelectual (DPI).	Se deberían implantar procedimientos adecuados que garanticen el cumplimento de la legislación, regulaciones y requisitos contractuales para el uso de material con posibles derechos de propiedad intelectual asociados y para el uso de productos software propietario.	Los derechos de propiedad intelectual deben ser respetados en base a la ley vigente. Art 55 CP. Patentar software institucional. Mantener Actualizado el Inventario de Software Utilizado y Licenciado por la ESPOCH.(CONTRATO DE LCAMPUS AGREEMENT) Posibles Documentos a elaborarse: • Política de Patente y Licenciamiento del uso de Software en la ESPOCH. • Manual de Procedimiento de Patente y Licenciamiento de Software Propietario. • Formato de Inventario del uso Software Propietario en la institución. • Formato de Solicitud de Patente de Software Institucional.
126	Protección de los documentos de la organización.	Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio.	El activo más importante de la organización es la información por lo tanto la protección de los documentos relacionados a esta se la debe realizar en base a políticas definidas. Posibles Documentos a elaborarse: • Política de protección de los documentos

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
			de la organización. • Manual de Procedimiento por perdida, destrucción o falsificación de documentos. • Formato de Notificación de Perdida, Destrucción o Falsificación de Documentos
127	Protección de datos y privacidad de la información de carácter personal.	Se debería garantizar la protección y privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales.	Si la organización no requiere información relevante de carácter personal, no es necesario acceder a ella. Posibles Documentos a elaborarse: • Política protección de datos y privacidad de la información de carácter personal.
128	Prevención del uso indebido de recursos de tratamiento de la información.	Se debería disuadir a los usuarios del uso de los recursos dedicados al tratamiento de la información para propósitos no autorizados.	Los recursos de tratamiento de la información deben ser de uso estricto y mantener un control del uso de los activos según su importancia. Posibles Documentos a elaborarse: • Política de Prevención del uso indebido de recursos de tratamiento de la información. • Manual de procedimiento de notificación del uso indebido de recursos de tratamiento de la información.
129	Regulación de los controles criptográficos.	Se deberían utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes.	Se deben implantar los algoritmos criptográficos en base a las consideraciones del DESITEL.
Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.			
130	Cumplimiento de las políticas y	Los directivos se deberían asegurar que todos los	Los documentos elaborados (políticas y normas

#	Control	¿Cómo se protege?	Canales de ejecución y comunicación Garantías de Cumplimiento
	normas de seguridad.	procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad.	de seguridad) deben cumplirse por lo cual la dirección debe proporcionar garantías de cumplimiento a través de políticas de sanciones establecidas si fuera necesario a quienes incumplan con el proceso y se observe demoras en las respuestas. Posibles Documentos a elaborarse: • Generación de Informes de Seguimiento del cumplimiento de las políticas y nomas de seguridad
131	Comprobación del cumplimiento técnico.	Se debería comprobar regularmente la conformidad de los sistemas de información con los estándares de implantación de la seguridad.	La gerencia debe asumir el proceso de desarrollo de seguridad de la información con responsabilidad ya que de esto depende el progreso del personal involucrado. Posibles Documentos a elaborarse: • Registro de Documentos sobre Reuniones, Autorizaciones, Seguimiento de las responsabilidades adquiridas
Consideraciones sobre las auditorías de los sistemas de información.			
132	Controles de auditoría de los sistemas de información.	Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio.	Una vez iniciado el proceso de elaboración de un SGSI se debe gestionar controles de auditoria para garantizar el análisis del desarrollo. Posibles Documentos a elaborarse: • Plan de Auditorias que deben constar en el Plan Estratégico del Departamento
133	Protección de las herramientas de auditoría de los sistemas de información.	Se deberían proteger los accesos a las herramientas de Auditoría de los Sistemas con el objeto prevenir posibles mal uso y daño de cualquier información.	Política de Protección de las herramientas de auditoría de los sistemas de información.

4.5 ANALISIS DE RESULTADOS

Para la tabulación de resultados se analizan los datos obtenidos de las consideraciones realizadas en el DESITEL frente a las políticas de seguridad estructuradas. Ver Anexo VIII.

Los resultados obtenidos se resumen en el siguiente cuadro:

Tabulación de datos

Tabla.IV.V. Tabulación de resultados

TABULACIÓN DE DATOS				
Ítem	ALTERNATIVAS			TOTAL
Nº	SI	NO	Parcialmente	
1	18	-	-	18
2	15	3	-	18
3	12	2	4	18
4	17	-	1	18
5	16	1	1	18
6	17	-	1	18
7	10	6	2	18
8	16	-	2	18
9	17	-	1	18
10	18	-	-	18

4.6 COMPROBACIÓN DE HIPOTESIS

HERRAMIENTA T - STUDENT

1. Planteamiento de la Hipótesis

a. Modelo lógico

H_1 (Hipótesis Alterna)

La utilización de una guía metodológica usando la norma ISO 27001 para el Sistema de Gestión de Seguridad de la Información permitirá mejorar el nivel de Control de Seguridad de la Información en el DESITEL de la ESPOCH.

H_0 (Hipótesis Nula)

La utilización de una guía metodológica usando la norma ISO 27001 para el Sistema de Gestión de Seguridad de la Información **no** permitirá mejorar el nivel de Control de Seguridad de la Información en el DESITEL de la ESPOCH.

b. Modelo estadístico

$H_1 > H_0$

$H_1 \neq H_0$

- ✓ **Nivel de Significación**

  95% de confianza = 5% de error $\Rightarrow$ 0.05

- ✓ **Zona de rechazo de la Hipótesis Nula (Ho)**

- ✓ **Fórmula para el Cálculo T de Student**

$$t = \frac{\bar{d}}{\frac{\sigma d}{\sqrt{N}}}$$

Donde:
t = valor estadístico del procedimiento.
$\bar{d}$= Valor promedio o media aritmética de las diferencias entre los momentos antes y después.
σd = desviación estándar de las diferencias entre los momentos antes y después.
N = tamaño de la muestra.

La media aritmética de las diferencias se obtiene de la manera siguiente:

$$\bar{d} = \frac{\Sigma d}{N}$$

La desviación estándar de las diferencias se logra como sigue:

$$\sigma d - \sqrt{\frac{\Sigma(d - \bar{d})^2}{N - 1}}$$

APLICACIÓN DE T-STUDENT[3]

Para la aplicación de la prueba T- Student se consideran los resultados obtenidos en el DESITEL frente al análisis de las mejoras de las políticas de seguridad.

Tabla IV.VI – Test de student

TEST DE STUDENT					
Nivel	**SI**	**NO**	**d**	**d - d**	**$(d - d)^2$**
1	18	0	18	4.8	23.04
2	15	3	12	-1.2	1.44
3	12	6	6	-7.2	51.84
4	17	1	16	2.8	7.84
5	16	2	14	0.8	0.64
6	17	1	16	2.8	7.84
7	10	8	2	-11.2	125.44
8	16	2	14	0.8	0.64
9	17	1	16	2.8	7.84
10	18	0	18	4.8	23.04
			Σd= 132 X= 13.2		**$\Sigma(d-d)^2$= 249.6**

[3] Anexo VIII

Cálculo de la prueba estadística

$$\bar{d} = \frac{\Sigma d}{N} = 132 / 10 = 13.2$$

$$\sigma d = \sqrt{\frac{\Sigma(d - \bar{d})^2}{N - 1}} = 249.6 / 9 = 5.26$$

$$t = \frac{\bar{d}}{\frac{\sigma d}{\sqrt{N}}} = 13.2 / 1.66 = 7.95$$

Margen de error admisible $\alpha = 0.05$

Grados de libertad $gl = 9$

Test de Student Hipótesis Alterna $t = 2.26$

Test de student Hipótesis Nula $t_0 = 7.95$

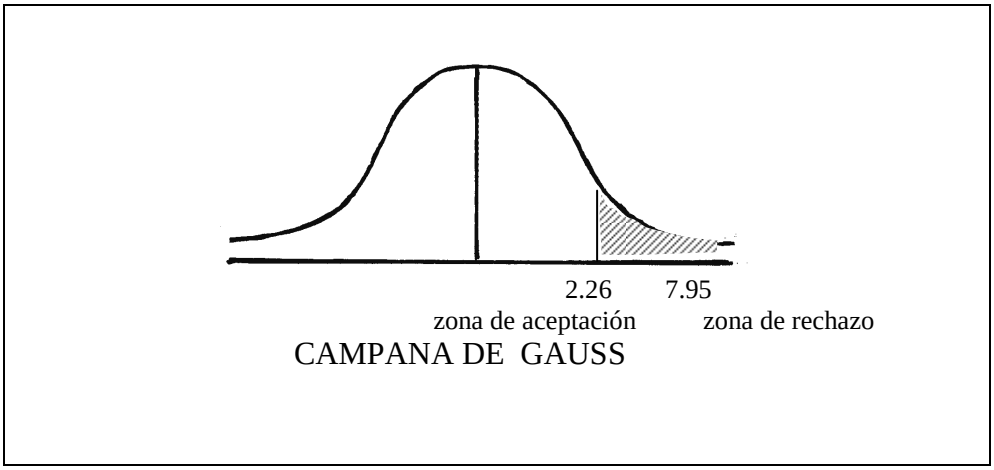


Fig.IV.18 Campana de Gauss

El valor obtenido de t (7.95) se compara con los valores críticos de la distribución t (tabla), y se observa que a una probabilidad de 0.05 le corresponde 2.26 de t. Por tanto, el cálculo tiene una probabilidad menor que 0.05.

Como to es de 7.95, con 9 grados de libertad, tiene un valor de probabilidad menor que 0.05, entonces se acepta H**1** y se rechaza Ho.

Debido a que to > tt se rechaza Ho.

2. Regla de decisión

$$R\ (H_1): \quad t = 2.26$$

$$R\ (H_0): \quad t_0 = 7.95$$

Entonces: $t\ (H1) \geq t\ (Ho)$

$2.26 < 7.95$

3. Decisión estadística

La Hipótesis Alterna (H1), tiene nueve grados de libertad y el valor esperado del test de student es igual a 2.26, mientras que la zona de aceptación del test de student de la Hipótesis Nula (Ho), llega hasta el valor de 7.95 según el análisis estadístico, lógicamente, se rechaza la Hipótesis Nula y se acepta la Hipótesis Alterna, que dice: "La utilización de una guía metodológica usando la norma ISO 27001 para el Sistema de Gestión de Seguridad de la Información permitirá mejorar el nivel de Control de Seguridad de la Información en el DESITEL."

CAPÍTULO V

SISTEMA INFORMÁTICO

En el presente capitulo se explica el diseño de un sistema informático, que es dirigido al usuario y administrador del sistema para el análisis del cumplimiento de los controles desarrollados en la metodología elaborada MAGESID según la norma ISO 27001.

FASE DE ANÁLISIS

5.1 DEFINICIÓN DE LOS CASOS DE USOS.

Una técnica excelente que permite mejorar la comprensión de los requerimientos es la creación de los casos de uso, es decir, descripciones narrativas de los procesos del dominio.

Caso de uso 1: MÓDULO DE SEGURIDAD.

Tabla V.VII: Caso de Uso Módulo De Seguridad

CASO DE USO: Seguridad de la aplicación.	
ACTORES:	Administrador.
TIPO:	Esencial primario.
PROPÓSITO :	Permitir que la aplicación sea manipulada solo por personal autorizado por el administrador.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador ingresa a la aplicación y éste puede crear o eliminar usuarios, cambios de contraseña, para permitir el acceso solo a personal autorizado, el sistema solicita una clave si es correcta permitirá ingresar si no se denegara el acceso.

Caso de uso 2: MÓDULO DE INGRESO DE DATOS AL SISTEMA.

Tabla V.VIII: Caso De Uso Módulo De Ingreso De Datos.

CASO DE USO:	Ingreso de datos.
ACTORES:	Administrador.
TIPO:	Esencial primario.
PROPÓSITO:	Permitir el ingreso de dominios, controles de la metodología, ingreso de usuarios del sistema.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador ingresa al sistema para su administración.
REFERENCIAS:	Ninguno.
CURSO TÍPICO DE EVENTOS	
1. El administrador ingresa al sistema. 3. El administrador ingresa su contraseña. 5. El administrador escoge la opción de ingreso de datos, dependiendo de qué datos se va ingresar 7. El administrador ingresa datos. 9. El administrador sale de la opción	2. Sistema solicita contraseña. 4. El sistema valida contraseña y presenta OP de ingreso del menú. 6 El sistema pide los datos específicos. 8. El sistema Guarda los datos en la BD.
CURSOS ALTERNATIVOS	
R3: Contraseña mal ingresada.	

Caso de uso 3: MÓDULO DE REPORTE.

Tabla V.IX: Caso de Uso Módulo de reporte

CASO DE USO:	Reportes.
ACTORES:	Administrador.
TIPO:	Esencial primario.
PROPÓSITO:	Presentar al administrador registros de la ejecución de los controles de la metodología.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador del sistema solicita reportes.
REFERENCIAS:	Ninguna.
CURSO TÍPICO DE EVENTOS	
1. El administrador ingresa al sistema. 3. El administrador ingresa su Contraseña. 5. El administrador escoge la opción 7. El administrador escoge el reporte Deseado. 9. El administrador sale de la opción	2. Sistema solicita contraseña. 4. El sistema valida contraseña y presenta OP de ingreso del menú 6. El sistema presentalos reportes Para que el administrador tome decisiones. 8.El sistema valida e imprime Dicho reporte.
CURSOS ALTERNATIVOS	
R3: Contraseña mal ingresada R7: Reporte no deseado.	

Caso de uso 4: MÓDULO DE AYUDA

Tabla.V.X.: Caso de uso módulo de ayuda

CASO DE USO:	Ayuda.
ACTORES:	Administrador.
TIPO:	Esencial primario.
PROPÓSITO:	Despejar cualquier duda del funcionamiento del Sistema para la óptima utilización del sistema por el responsable de la administración.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador-usuario autorizados están dentro del sistema y poseen alguna inquietud, pueden interactuar con la ayuda.
REFERENCIAS:	Ninguna.
CURSO TÍPICO DE EVENTOS	
1.El administrador ingresa al sistema.	2. El sistema presenta la ayuda necesaria para la manipulación del Sistema
3. El administrador escoge la opción de ayuda 5. El administrador sale de la opción	4. El sistema presenta la ayuda
CURSOS ALTERNATIVOS	
R3: Contraseña mal ingresada	

5.2 DEFINIR LOS DIAGRAMAS DE CASOS DE USO

Los diagramas de casos de uso tienen como objetivo representar las relaciones del sistema con el personal que maneja la aplicación informática, se menciona los módulos que el sistema tendrá.

MÓDULO DE SEGURIDAD

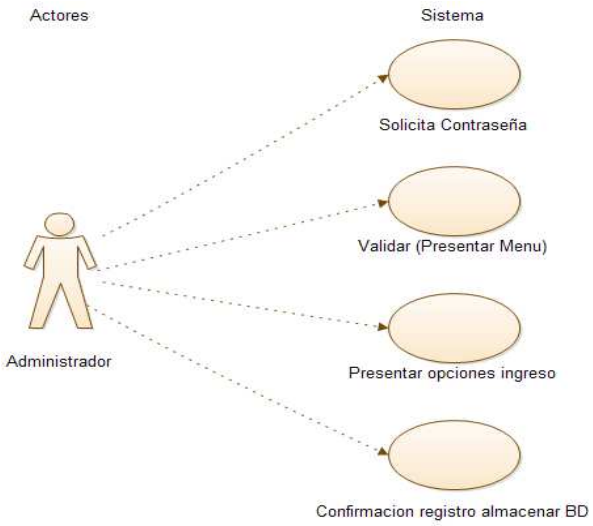


Fig.V.19. Diagramas de Casos de Uso Modulo de seguridad

MÓDULO DE INGRESO DE DATOS

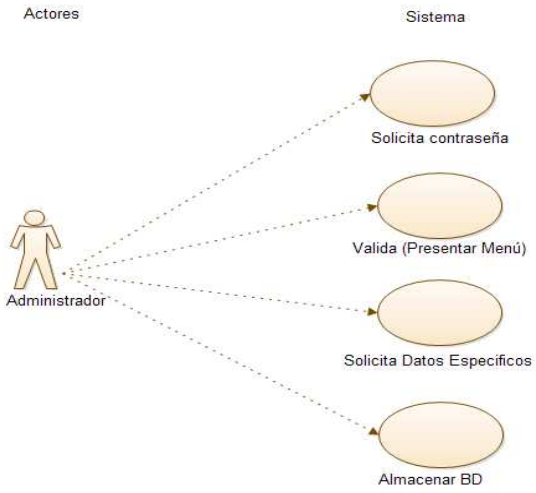


Fig.V.20 Diagrama Caso De Uso Modulo De Ingreso De Datos

MÓDULO DE REPORTES

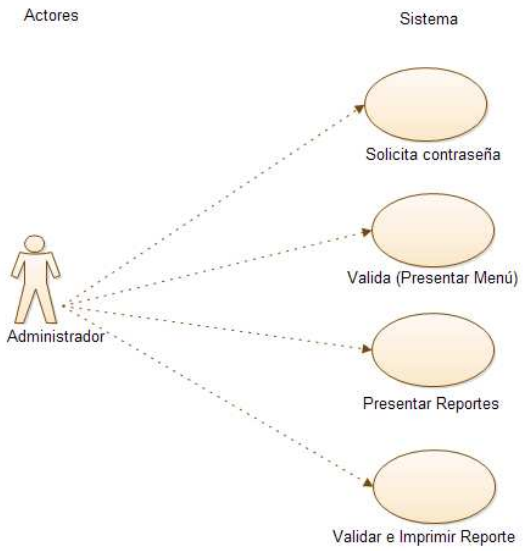


Fig.V.21. Diagrama Caso De Uso Modulo De Reportes

MÓDULO DE AYUDA

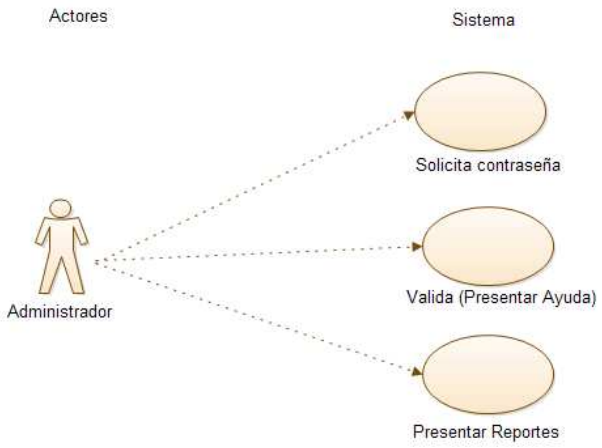


Fig.V.22. Diagrama Caso De Uso Modulo De Ayuda

5.3 DEFINIR Y REFINAR EL MODELO CONCEPTUAL.

El paso esencial de un análisis o investigación es descomponer el problema en conceptos u objetos individuales: un modelo conceptual es la representación de conceptos en un dominio del problema, lo ilustramos con un grupo de diagramas de estructura estática donde no se define ninguna operación.

La designación del modelo conceptual ofrece la ventaja de subrayar fuertemente una concentración en los conceptos del dominio, no en las entidades del SW.
Puede mostrarnos:

- ✓ Conceptos
- ✓ Atributos de conceptos
- ✓ Relaciones entre conceptos

5.3.1 IDENTIFICACIÓN DE CONCEPTOS.

En nuestro problema hemos identificado los siguientes conceptos:

Tabla.V.XI. Identificación de conceptos

CONCEPTOS
Dominios
Controles
Usuarios

5.3.2IDENTIFICACIÓN DE CARACTERÍSTICAS

Tabla.V.XII: Identificación de Características

Clase	Características	Comportamiento
Usuario	Nombre Clave Tipo	Insertar Eliminar Actualizar
Dominios	Nombre Tipo Numero	Insertar Eliminar
Controles	Nombre Tipo Numero	Insertar Actualizar Eliminar

5.3.3 IDENTIFICACIÓN DE RELACIONES.

El sistema desarrollado cuenta con varias clases y relaciones, se ha simplificado la abstracción de cada una de las clases y relaciones por lo cual las siguientes son las más óptimas para poder resolver el problema.

Tabla.V.XIII. Identificación de las relaciones

Usuario **Obtiene** Información
Usuario **Obtiene** controles de la metodología
Administrador **Realiza** Ingresos
Actividad **Contiene** Recursos
Controles se **Asigna** a Dominios
Dominios **Contiene** Controles

5.3.4 PRESENTACIÓN GRAFICA DEL MODELO CONCEPTUAL

5.4 DIAGRAMA DE SECUENCIA.

El diagrama de secuencia de un sistema es una representación que muestra, en determinado escenario de un caso de uso, los eventos generados por actores externos, su orden y los eventos internos del sistema. A todos los sistemas se les trata como una caja negra; los diagramas se centran en los eventos que trascienden las fronteras del sistema y que fluyen de los actores a los sistemas.

5.4.1 Módulo De Seguridad De La Aplicación

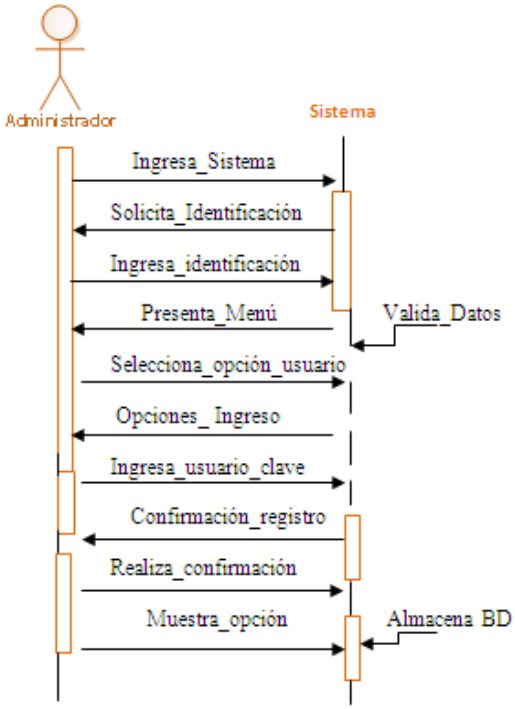


Fig.V.23. Diagrama de Secuencia Modulo De Seguridad

5.4.2 Módulo De Ingresos De Datos Al Sistema

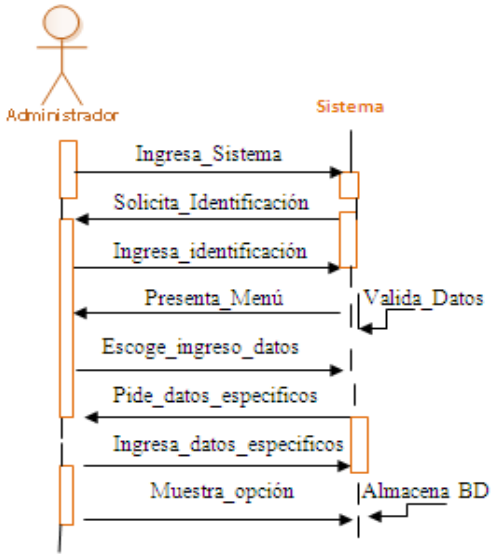


Fig.V.24. Diagrama de Secuencia modulo de Ingreso de dato

5.4.3 Módulo De Reporte

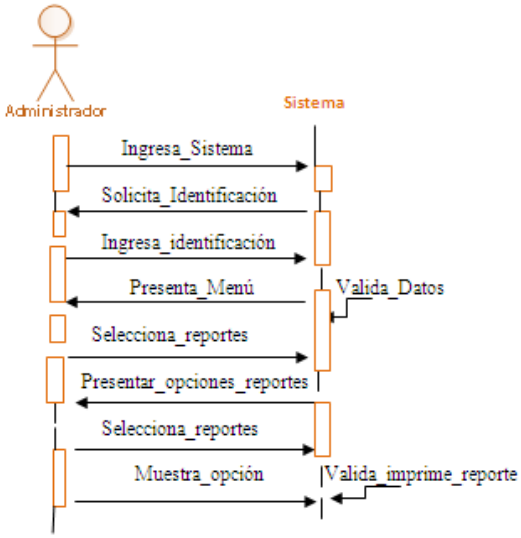


Fig.V.25. Diagrama de Secuencia Modulo de Ingreso de Reportes

5.4.4 Módulo De Ayuda

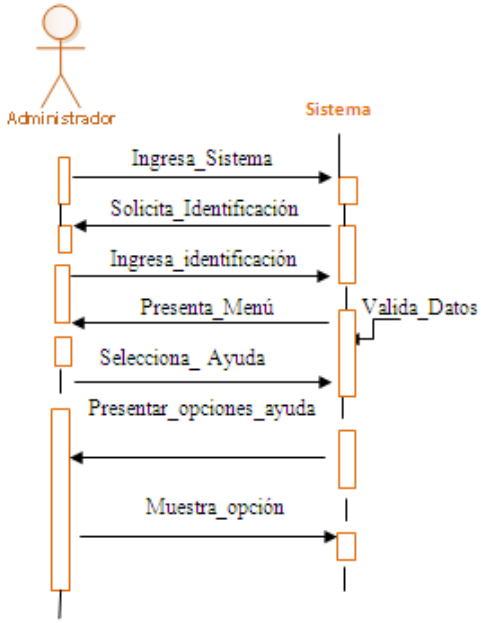


Fig.V.26. Diagrama de Secuencia Modulo de Ayuda

5.5 DICCIONARIO DE CLASES Y OBJETOS

Tabla.V.XIV: Diccionario de clases

CLASES Y OBJETOS	DESCPRIPCIÓN
Administrador	Persona encargada de la manipulación total del sistema, puede ingresar, actualizar, modificar o eliminar controles.
Usuario común	Persona que solo puede acceder a la página de información.
Metodología	Documento que contiene dominios y controles que deben ser cumplidos por los gestores del SGSI.

5.6 CONTRATOS DE OPERACIÓN.

Es un documento que describe, lo que se espera de una operación. Tiene una redacción en estilo declarativo, enfatizando en el qué más que en el cómo. Estos contratos de operación ayudan a describir los cambios en todos los estados por lo cual tienen que pasar nuestro sistema, cuando un agente externo invoca a una operación.

MÓDULO DE SEGURIDAD DE LA APLICACIÓN.

Tabla.V.XV.Contratos de Operación Seguridad

Nombre	Ingresar al sistema como administrador con su Nombre: string y Clave: string para realizar la configuración del modelo.
Responsabilidades	Ingresar al sistema de tal manera que se le presenten las opciones disponibles para realizar las operaciones que implican la configuración del sistema.
Referencias	
Casos de uso	Configuración de seguridad.
Excepciones	No se puede presentar las opción, si no ha ingresado correctamente, se presentará un mensaje de error.
Salida	Mensaje de haber ingresado correctamente.
Pre-Condición	El administrador debe estar activo.
Post-Condición	Actualiza la base de datos, con los datos configurados

MÓDULO DE INGRESO DE DATOS AL SISTEMA.

Tabla.V.XVI. Contrato De Operación Ingreso De Datos

Nombre	Ingresar al sistema como administrador con su Nombre: string y Clave: string para realizar el ingreso de datos.

Responsabilidades	Ingresar datos al sistema de los dominios y controles para almacenar en la base de datos.
Referencias cruzadas	
Casos de uso	Ingreso de datos.
Excepciones	No se puede ingresar datos si no es Administrador si no ha ingresado correctamente se le presentará un mensaje de error.
Salida	Mensaje de haber ingresado datos Correctamente.
Pre-Condición	El administrador o usuario debe estar activo.
Post-Condición	Actualiza la base de datos con los datos ingresados.

MÓDULO DE REPORTE

Tabla.V.XVII: Contrato De Operación De Reporte

Nombre	Ingresar al sistema como administrador o Usuario con su Nombre: string y Clave: string para obtener las opciones del sistema.
Responsabilidades	Ingresar al sistema de tal manera que pueda acceder a los reportes del sistema.
Referencias	
Casos de uso	Módulo de reporte.
Excepciones	Se puede Ingresar a la opción como administrador o usuario, se le presentará un mensaje de error si no tiene permisos
Pre-Condición	El administrador o usuario debe estar activo.

Post-Condición	Actualiza la base de datos con los datos Configurados.

MÓDULO DE AYUDA

Tabla.V.XVIII. Contrato de operación de Ayuda

Nombre	Ingresar al sistema como administrador o Usuario con su Nombre: string y Clave: string
Responsabilidades	Ingresar al sistema de tal manera que pueda acceder a la ayuda de la interacción y funcionalidad del sistema.
Referencias cruzadas	
Casos de uso	Modulo de ayuda.
Excepciones	Se puede ingresar a la opción como administrador o usuario, se le presentará un mensaje de error si no tiene permisos.
Pre-Condición	El administrador o usuario debe estar activo.
Post-Condición	Actualiza la base de datos con los datos configurados

5.7 DIAGRAMAS DE ESTADO.

Un diagrama de estado describe visualmente los estados y eventos más interesantes de un objeto, así como su comportamiento ante un evento. No es necesario que muestren todos los eventos posibles; si tiene lugar un evento que no está representado en el diagrama, se excluye siempre y cuando no sea relevante en el diagrama de estado.

Los diagramas de estado representan los estados por los que pasa un caso de uso o una clase, debido a la presencia de eventos que provocan un cambio de estado.

5.7.1 Módulo De Seguridad

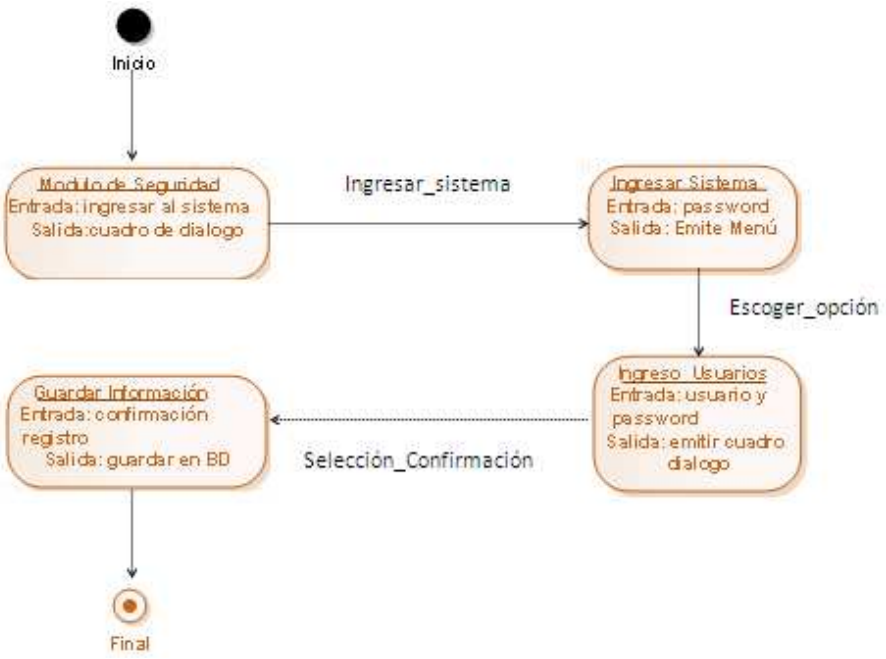


Fig.V.27. Diagrama De Estado Modulo De Seguridad

5.7.2 Módulo De Ingreso De Datos

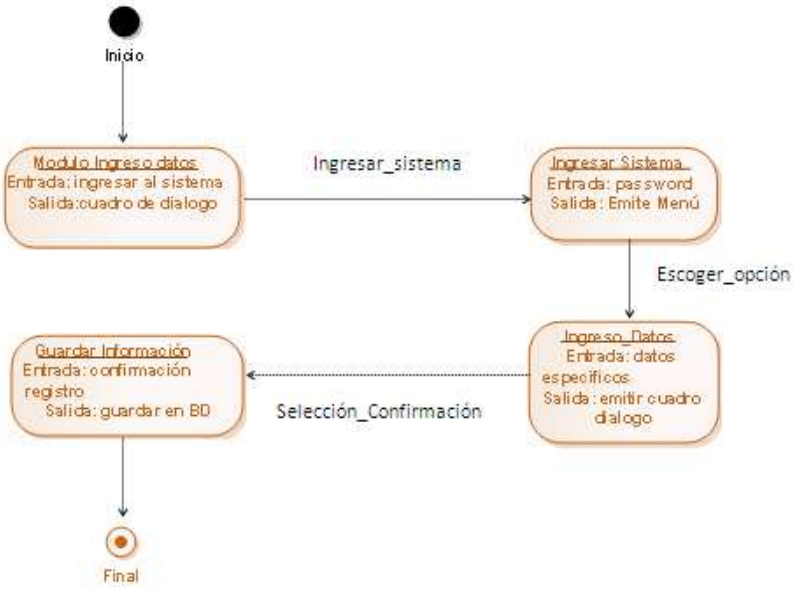


Fig.V.28. Diagrama De Estado Modulo De Ingreso

5.7.3 Módulo De Reporte

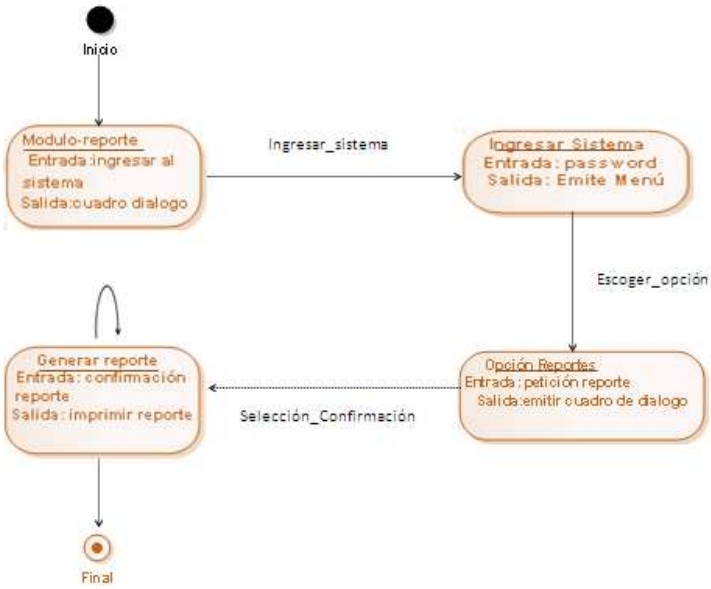


Fig.V.29. Diagrama De Estado Modulo De Reporte

5.7.4 Módulo De Ayuda

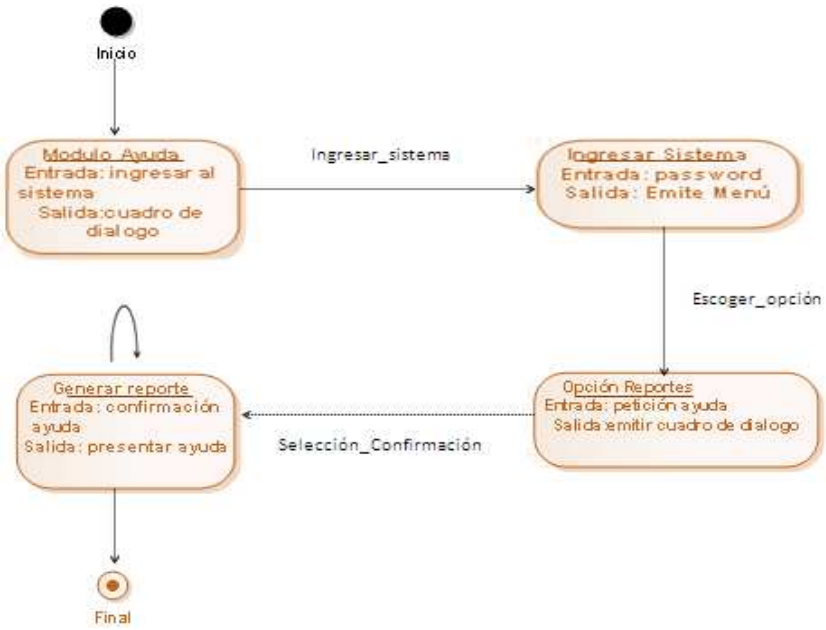


Fig.V.30. Diagrama De Estado Modulo De Ayuda

5.8 DIAGRAMA DE CALLES

Un diagrama de calles coordina todas las actividades que se realizan dentro del sistema, en este diagrama escribimos cada actor del sistema conjuntamente con las operaciones identificadas en los casos de uso, es decir que este nos ayuda a mejorar el comportamiento de nuestro sistema.

Fig.V.31. Diagrama De Calles Del Sistema

FASE DE DISEÑO

5.9 CASOS DE USOS REALES.

La definición de los casos de usos reales describe el diseño real según una tecnología concreta de entrada y de salida y su implementación. Si el caso de uso implica una interfaz de usuario, el caso de uso incluirá bocetos de las ventanas y detalles de la interacción a bajo nivel.

Caso de uso 1: MÓDULO DE SEGURIDAD.

Tabla.V.XIX Caso De Uso Módulo De Seguridad

CASO DE USO:	Seguridad de la aplicación.
ACTORES:	Administrador
TIPO:	Esencial primario.

PROPÓSITO:	Permitir que la aplicación sea manipulada solo por personal autorizado por el administrador.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador ingresa a la aplicación y éste puede crear o eliminar usuarios, cambios de contraseña, para permitir el acceso solo a personal autorizado, el sistema solicitará una clave si es correcta permitirá ingresar si no se denegara el acceso.
REFERENCIAS:	Ninguna.

CURSO TÍPICO DE EVENTOS	
1. El administrador ingresa al sistema. 3. El administrador ingresa su nombre y clave. 5. El administrador de la red escoge la opción de creación o eliminación	2. Sistema solicita contraseña. 4. El sistema valida nombre y clave y presenta OP de ingreso del menú 6. El sistema presentar opciones de ingreso datos específicos.
De usuarios, cambio de contraseñas del modelo del menú. 7. El administrador ingresa nombre de usuarios y su contraseña. 9. El asistente de jefe confirma el	8. El sistema pide la confirmación de registro. 10. El sistema almacena los datos a la BD.
CURSOS ALTERNATIVOS	
R3: Contraseña mal ingresada. R7: Datos mal ingresado.	

Caso de uso 2: MÓDULO DE INGRESO DE DATOS

Tabla.V.XX Caso De Uso Módulo De Ingreso de datos

CASO DE USO:	Ingreso de datos.
ACTORES:	Administrador.
TIPO:	Esencial primario.
PROPÓSITO:	Permitir el ingreso de controles, Políticas de seguridad con sus respectivos campos.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador ingresa al sistema e ingresa los datos Correspondientes.
REFERENCIAS:	Ninguno.
CURSO TÍPICO DE EVENTOS	
1 El administrador ingresa al Sistema. 3. El administrador ingresa su Nombre y clave. 5. El administrador escoge la opción de ingreso de datos, dependiendo de	2. Sistema solicita contraseña. 4. El sistema valida contraseña y presenta OP de ingreso del menú 6. El sistema pide los datos i específicos.
que datos se va ingresar 7. El administrador ingresa datos con sus respectivos campos.	8. El sistema Guarda los datos en la BD.
CURSOS ALTERNATIVOS	

R3: Contraseña mal ingresada. R7: Datos mal ingresados.

Caso de aso 3: MÓDULO DE REPORTES.

Tabla.V.XXI: Caso De Uso Módulo De Reportes

CASO DE USO:	Reportes.
ACTORES:	Administrador.
TIPO:	Esencial primario.
PROPÓSITO:	Presentar Datos y tomar decisiones de cumplimiento de los dominios y controles.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador solicita datos de reportes
REFERENCIAS:	Ninguna.
CURSO TÍPICO DE EVENTOS	
1 El administrador Sistema. 3. El administrador ingresa su Contraseña. 5. El administrador escoge la opción 7 El administrador escoge el reporte	2. Sistema solicita contraseña. 4. El sistema valida contraseña y presenta OP de ingreso del menú. 6. El sistema presenta los diferentes tipos de reportes para que el administrador pueda escoger. 8. El sistema debe validar e imprimir dicho reporte

CURSOS ALTERNATIVOS
R3: Contraseña mal ingresada

Caso de uso 4: MÓDULO DE AYUDA.

Tabla.V.XXII: Caso De Uso Módulo De Ayuda

CASO DE USO:	Ayuda
ACTORES:	Administrador
TIPO:	Esencial primario.
PROPÓSITO:	Despejar cualquier duda del funcionamiento del Sistema para la óptima utilización del sistema por el responsable de la administración.
DESCRIPCIÓN GENERAL:	La interacción comienza cuando el administrador, usuario autorizados están dentro del sistema y poseen alguna inquietud puede interactuar con la ayuda.
REFERENCIAS:	Ninguna.
CURSO TÍPICO DE EVENTOS	
I El administrador ingresa al Sistema. 3. El administrador ingresa su Contraseña. 5. El administrador escoge la opción de ayuda.	2. Sistema solicita contraseña. 4. El sistema valida contraseña y presenta OP de ingreso del menú. 6 El sistema presenta la ayuda necesaria para la manipulación del sistema.

CURSOS ALTERNATIVOS
R3: Contraseña mal ingresada.

5.9.1 DIAGRAMA CASOS DE USOS REALES.

Caso de uso 1: Módulo de Seguridad

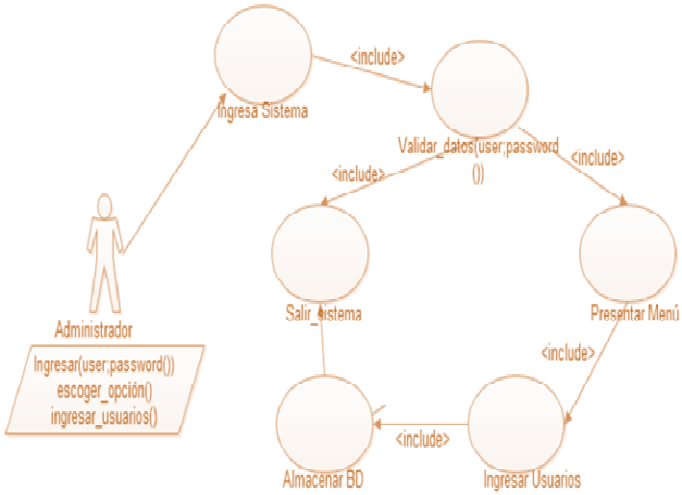


Fig.V.32. Caso de Uso real Módulo de seguridad

Caso de uso 2: Módulo de Ingreso de Datos.

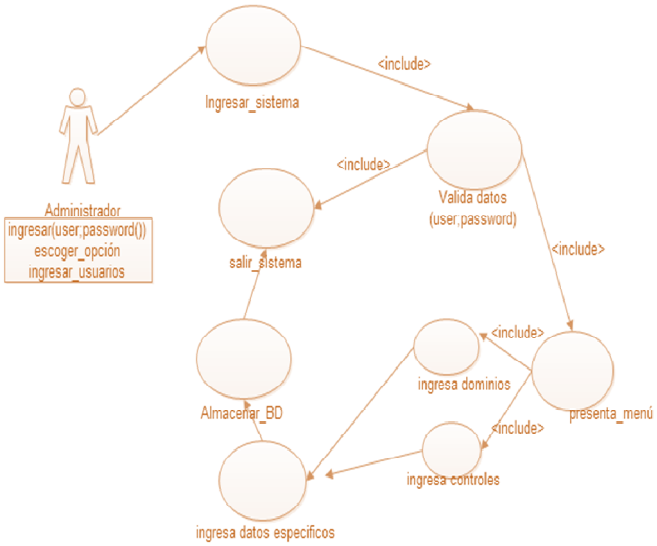


Fig.V.33. Caso de Uso real Módulo de ingreso de datos

Caso de uso 3: Módulo de Reporte

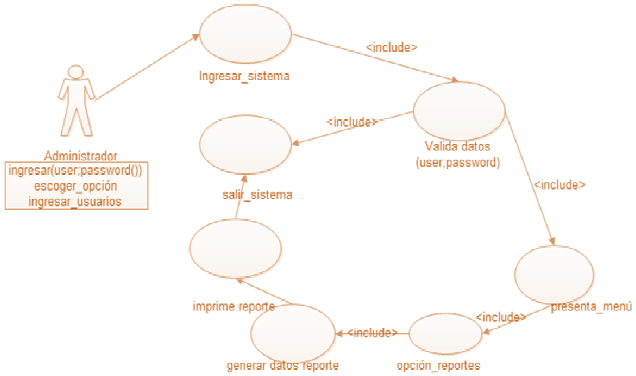


Fig.V.34. Caso de Uso real Módulo de reporte

Caso de uso 4: Módulo de Ayuda.

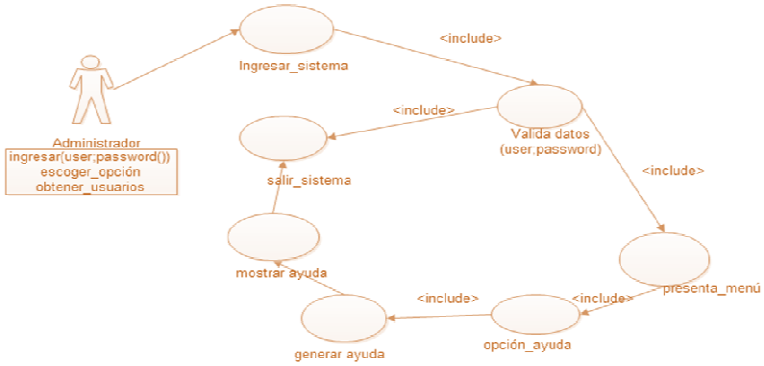


Fig.V.35. Caso de Uso real Módulo de Ayuda

5.10 DEFINIR FORMULARIOS PARA INTERFAZ DE USUARIO.

5.10.1 INFORME E INTERFAZ DE USUARIO.

El ser humano percibe el mundo a través de un sistema sensorial que comprendemos razonablemente bien. Cuando se considera una interfaz hombre máquina, predomina el sistema visual, táctil y auditivo.

La comunicación visual es el elemento clave de una interfaz amigable, aunque es necesario incluir elementos textuales porque la lectura es una actividad indispensable para el seguimiento de la información.

INTERFACES EXTERNAS.

Interfaces de Usuario:

Las interfaces del usuario están constituidas esencialmente por las ventanas, cuadros de diálogo, gráficos, hipertexto, etc., el propósito es crear un software con características de un programa visual y didáctico en cierto punto, dando lugar a los siguientes requerimientos que debe cumplir:

- ✓ Menús Interactivos (Cajas de diálogos y respuestas del sistema).
- ✓ Presentación de Mensajes de Error.
- ✓ Control a través de Teclado (Teclas de Función) y Mouse
- ✓ Gráficos.
- ✓ Hipervínculos de texto y gráficos.

ELEMENTOS DE FUNCIONALIDAD.

Botones de Radio.- Se denominan así, por la similitud a los botones de un radio de automóvil. Hay que tomar en cuenta que un solo botón puede ser escogido a la vez y solamente éste será tomado en cuenta, cada vez que se selecciona un botón, el anterior se deshabilita.

- ✓ Ingresar
- ✓ Guardar
- ✓ Actualizar
- ✓ Borrar
- ✓ Reportes

Caja de Diálogo.- Se trata de una porción de pantalla, en la cuál a más de escoger opciones, también permite ingresar texto. De ahí que se le califique como caja de diálogo.

Menú.- Listado de opciones, en el cual cada opción permite realizar una tarea específica. Logra un trabajo más interactivo con el usuario, y permite elegir la opción que le interese.

Elaboración de un lenguaje de presentación.- Se dará a conocer toda la información al usuario mediante Hint desplegables.

Representación de un Lenguaje de Acción.- Va desde el usuario al computador mediante un lenguaje de programación.

Elaboración de una Interfaz en Lenguaje Natural.- La interfaz es un punto ideal para la gente que trabaja con un computador. Además estas interfaces, permite que los usuarios interactúen con el sistema de una forma fácil y comprensible en un lenguaje familiar.

Elaboración de una Interfaz amigable con Áreas de Trabajo y Cajas de Diálogo.-

Busca a través de un menú y submenú y con un conjunto de íconos que trabaja en espacios o Área, para que el usuario interactúe estos se encontrarán debidamente balanceados.

5.10.2 INTERFACES DEL SISTEMA.

La primera pantalla de la aplicación es una ventana en la cual pide la identificación mediante el uso de la clave de acceso, dicha clave será proporcionada por el administrador.

5.11 DIAGRAMAS DE INTERACCIÓN

5.11.1 DIAGRAMA DE SECUENCIA

MÓDULO DE SEGURIDAD

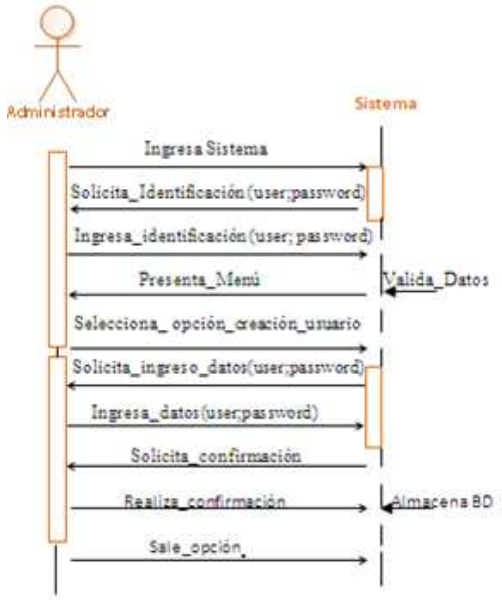


Figura.V.36. Diagrama De Secuencia Módulo De Seguridad

MÓDULO DE INGRESO

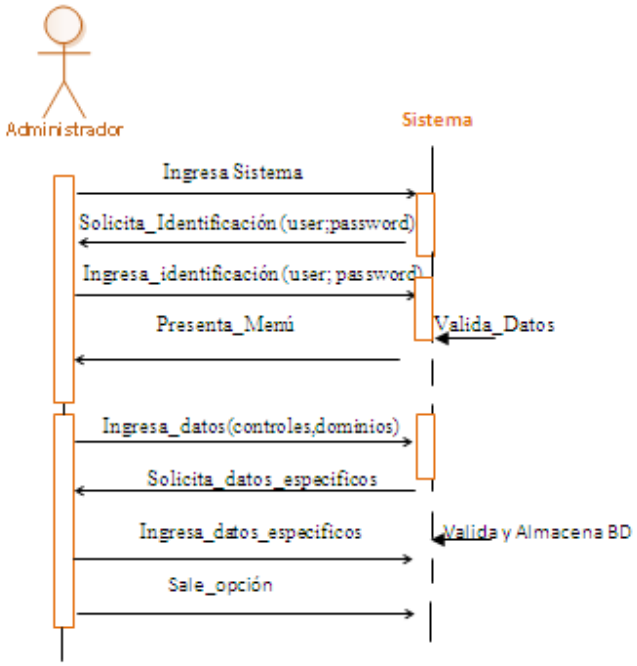


Fig.V.37. Diagrama De Secuencia Módulo De Ingreso

MÓDULO DE REPORTE

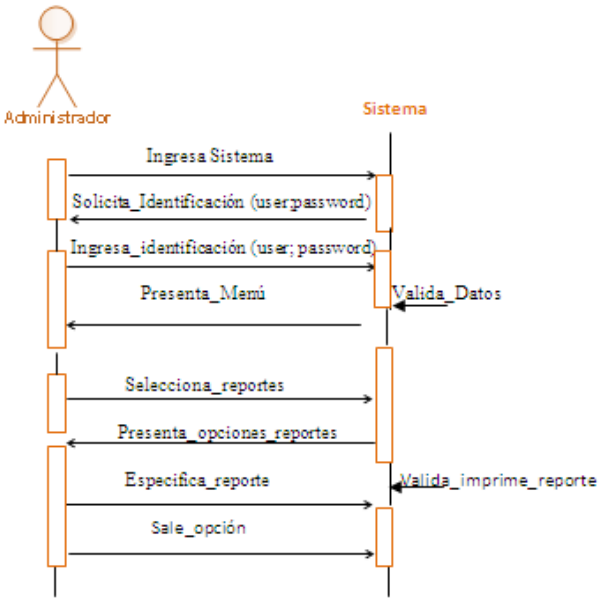


Fig.V.38. Diagrama De Secuencia Módulo De Reporte

MÓDULO DE AYUDA

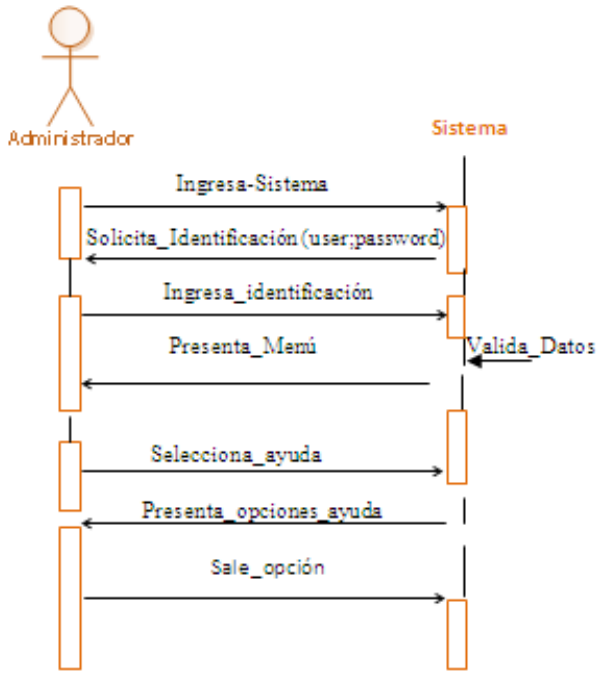


Fig.V.39. Diagrama De Secuencia Módulo De Ayuda

5.11.2 DIAGRAMAS DE COLABORACIÓN

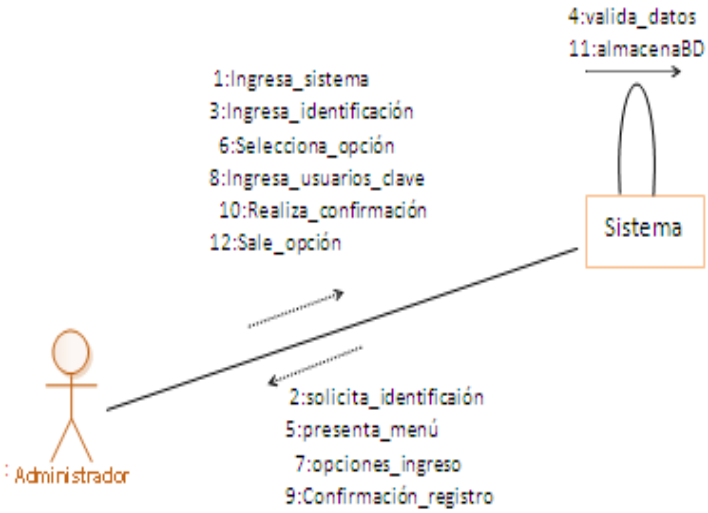


Fig.V.40. Diagrama de colaboración módulo de seguridad

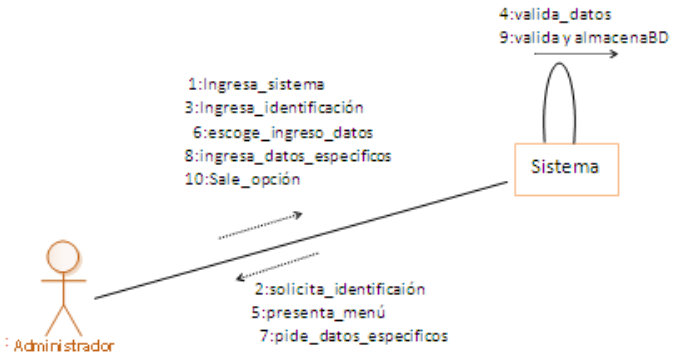


Fig.V.41. Diagrama De Colaboración Módulo De Ingreso

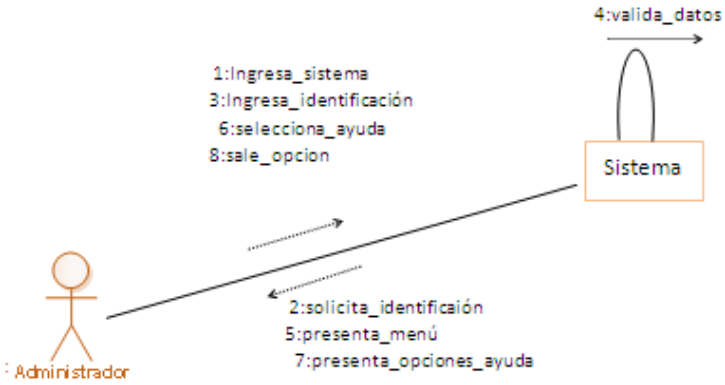


Fig.V.42. Diagrama De Colaboración Módulo De Ayuda

5.12 DIAGRAMA DE LA BASE DE DATOS

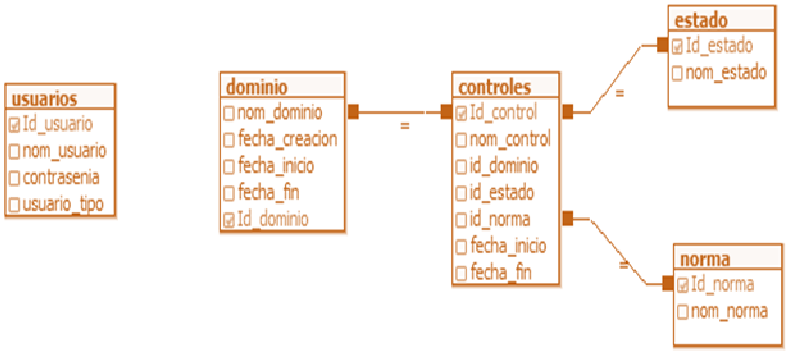


Fig.V.43. Diagrama de la base de datos

5.13 DISEÑO FÍSICO

5.13.1 DIAGRAMA DE COMPONENTES

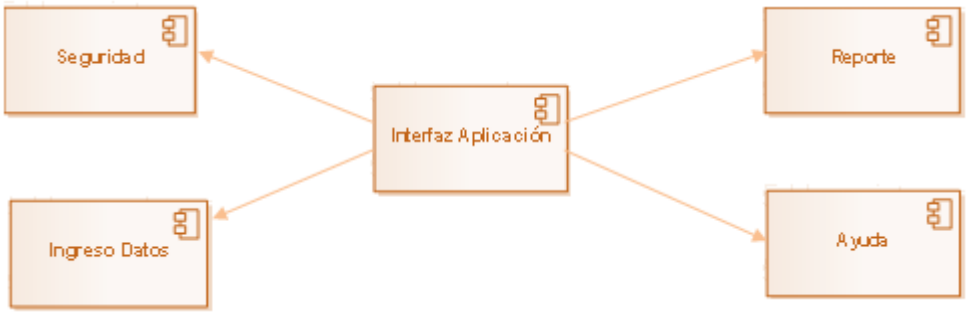


Fig.V.44. Diagrama de Componentes

5.14.2 DIAGRAMA DE DESPLIEGUE

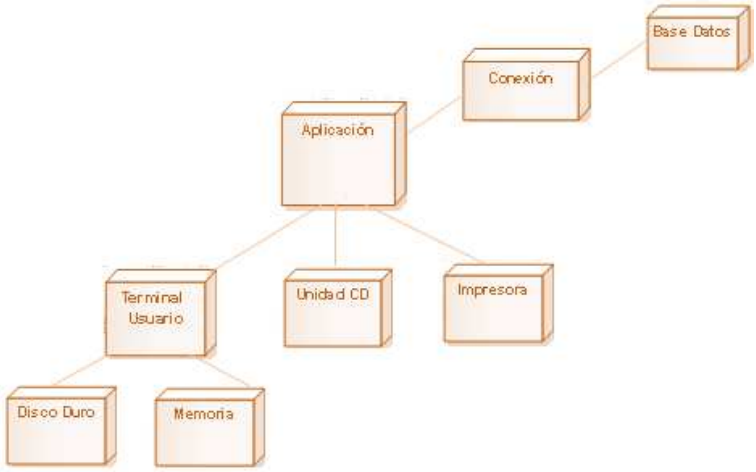


Fig.V.45. Diagrama de Despliegue.

CONCLUSIONES

1. El estudio realizado de políticas y reglamentos para la seguridad de la información permite visualizar con mayor claridad la importancia y el valor de la información para la Organización adaptados a la necesidad de protección de datos.

2. Mediante la recopilación de la información de los activos involucrados en los sistemas de información pertenecientes al DESITEL, se pudo constatar los problemas actuales de falencias en el mantenimiento, organización y la falta de una metodología de seguridad de la información basadas en normas que garanticen su seguridad.

3. El estudio de la Norma ISO 27001 ha permitido mejorar el conocimiento de los sistemas de seguridad de la información, sus problemas y los medios de protección además cubre el vacío que ha generado la inexistencia de un método documentado, sobre cómo proceder a implantar un Sistema de Gestión de Seguridad de la Información.

4. Al aplicar el ciclo (Plan, Do, Check, Act) en la elaboración inicial de la metodología se obtiene eficiencia en sus contenidos y se ha logrado determinar espacios de desarrollo para cada una de las actividades involucradas en la gestión de un SGSI, es decir que la metodología elaborada cubre estos aspectos durante todo el proceso de desarrollo.

5. A través de la creación de la metodología para un SGSI usando la norma ISO 27001, se pretende gestionar y concienciar el cumplimiento de la misma al personal del DESITEL para mejorar su compromiso con la seguridad de la información del departamento.

6. Por medio de la aplicación desarrollada se podrá analizar el cumplimiento de los elementos involucrados en la metodología elaborada según la norma ISO 27001, para la toma correcta de decisiones por parte de los gestores de un SGSI.

RECOMENDACIONES

1. Para llevar a cabo una buena gestión de la información es recomendable el compromiso de todo el personal involucrado en el funcionamiento y mantenimiento de los activos de la información en el DESITEL.

2. Toda organización grande o pequeña requiere de una metodología de Seguridad de Información acorde a sus necesidades para garantizar su confidencialidad, integridad y disponibilidad.

3. La puesta en práctica de la metodología requiere la autorización y colaboración de todas unidades operativas de las mismas sin diferenciar sean grandes o pequeñas.

4. Se recomienda poner en práctica el contenido de la metodología y los aspectos allí descritos para la gestión de la seguridad de la información, de esta manera se respalda el objetivo del trabajo que se convierte en los inicios del camino de certificación para el DESITEL bajo la Norma ISO 27001.

5. Es recomendable que una vez evaluada la gestión de seguridad del DESITEL se implemente las medidas necesarias para subir el nivel de eficiencia del mismo y mantener altos niveles de seguridad de la información, este aspecto es motivo de una nueva investigación

6. Se recomienda que el DESITEL dentro de su Orgánico Funcional, defina un área para la gestión de seguridades y pruebas del mantenimiento de la información.

RESUMEN

El objetivo de esta tesis es elaborar una Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en el DESITEL (Departamento de Sistemas y Telemática) de la ESPOCH.

Se utilizo la norma ISO 27001 por sus garantías de seguridad en disponibilidad, integridad, privacidad, legalidad de la información, lo cual permitió determinar los pasos necesarios de la seguridad física, lógica, organizativa y legal para la elaboración de la metodología.

Se utilizaron técnicas como encuestas, entrevistas a los empleados del departamento y observaciones directas a los activos de la información.
Con estas herramientas se pudo identificar los activos en riesgo y vulnerabilidades, determinando las políticas que se deben mejorar para garantizar la seguridad de la información en el departamento.

Esto permitió la concienciación del personal del DESITEL para proporcionar disponibilidad en la elaboración de la metodología, y poder contar con un instrumento que permita minimizar el nivel de vulnerabilidad en la seguridad de la información y mejorar el control de calidad de la seguridad del activo elite del departamento la información.

Mediante la metodología desarrollada para la implementación de un Sistema de Gestión de Seguridad de la información se puede concluir que garantiza, el cumplimiento de las buenas prácticas sugeridas por la Norma ISO 27001 para la seguridad de la información.

Se recomienda que la metodología sea implantada en su totalidad para lograr mejoras en la seguridad de la información y encaminarse en el proceso de certificación de seguridad bajo la norma ISO 27001.

SUMARY

The objective of this thesis is to elaborate a Methodology to implement a system of security Management of information (SGSI) in DESITEL (System and Technology Department at the ESPOCH.

The ISO 27001 norm was used by its security guarantees in availability, integrity, privacy, legality of the information, these permitted to determine the necessary steps for the logical, organizational, legal and physical security for the elaboration of the methodology.

Techniques like surveys, interviews to the employees of the department were used, and also direct observations to the information.

With these tools, it was possible to identify the assets in risks and vulnerabilities, determining the politics that should be improved to guarantee the security of the information in the department.

This, permitted that the personnel of DEDITEL becomes aware to give availability in the elaboration of the methodology, to have available an instrument that permits to minimize the level of vulnerability in the security of information and to improve the quality control in the security of the elite asset at the department, the information.

By means of the developed methodology for the implementation of a system of security management of the information, it is possible to conclude that it guarantees the fulfillment of the good practices suggested by ISO Norm 27001 for the information security.

It is advisable that the methodology can be implanted totally to get improvement in the security of information and to guide in the process of certification of security under the ISO Norm 27001.

GLOSARIO

Activo (Ingles: Asset) En relación con la seguridad de la información se refiere a cualquier información o sistema relacionado con el tratamiento que tenga valor para la misma.

Amenaza (Ingles: threat) Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o la organización.

Autenticación (Ingles: Authentication) Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Confidencialidad (Ingles: Confidenciality) Acceso a la información por parte únicamente de quienes estén autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel del riesgo asumido.

Directrices: Una directriz se dice de aquello que marca las condiciones en que se genera algo.

Disponibilidad (Ingles: Availability) Acceso de la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados en el momento que lo requiera.

Documentos: Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.

Garantizar: Proceso que asegura y protege contra algún riesgo o necesidad.

Gestión: Acción y efecto de administrar.

Información: Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.

Integridad (Ingles: Integrity) Mantenimiento de la información de forma completa y exacta y sus métodos de proceso.

ISO Organización Internacional de Normalización con dese en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

Normas: Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.

Organizar: Establecer o reformar algo para lograr un fin, coordinando las personas y los medios adecuados.

Reglamento: Colección ordenada de reglas o preceptos, que por la autoridad competente se da para la ejecución de una ley o para el régimen de una corporación, una dependencia o un servicio.

Respaldos: Apoyo, protección, garantía.

Seguridad: Se puede entender como un objetivo y un fin que el hombre anhela constantemente como una necesidad primaria.

Servicio: Organización y personal destinados a cuidar intereses o satisfacer necesidades del público o de alguna entidad oficial o privada.

Sistema: Conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí.

Tecnología: Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico.

ANEXOS

Anexo I

MANUAL DE USUARIO DEL SISTEMA PROPUESTO

Introducción

La importancia de gestionar la seguridad de la información en el DESITEL de la ESPOCH, radica principalmente en la calidad de servicio que se brinda a la comunidad politécnica, debido a que para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización, es por esto que se ha desarrollado una metodología basada en la norma ISO 27001 y una aplicación para el análisis del cumplimiento de la misma.

Generalidades del Sistema

- ✓ Desarrollo con Interfaz Gráfica.
- ✓ Software Web
- ✓ Cuenta con cuatro tipos de módulos para el DESITEL de la ESPOCH.

Seguridades

Se contará con dos usuarios que deberán acceder al sistema, el usuario común puede acceder a la página informativa y listar el estado de los dominios y controles; el usuario administrador puede acceder mediante el uso de la clave de acceso, el sistema brindará diferentes opciones de acuerdo al tipo de usuario.

¿Cómo esta organizado este manual?

Este manual contiene información completa del manejo correcto del sistema propuesto, por lo que le recomendamos leer detenidamente y completamente el contenido de este manual. Tendremos toda la información que se encuentra en el sistema con el fin de que el usuario pueda tener una completa visión del software antes de iniciar con su utilización, clasificando la información de forma progresiva para que se siga paso a paso, iniciando con los requerimientos para la instalación.

Sistema Operativo: Microsoft Windows Professional, XP, Windows 7 Ultimate,

Aplicaciones: Browser Internet Explorer.

Procesador:

Velocidad:

Memoria RAM: 512 MB mínimo, 1 GB recomendado

Disco Duro: 1GB libre mínimo, 2GB libres en el disco recomendado.

Monitor: SVGA

Descripción del software

El sistema se encuentra desarrollado totalmente visual con páginas dinámicas, a continuación describiremos cada una de estas.

El usuario tiene un portal informativo a través del cual puede revisar detenidamente temas como: SGSI, la Norma ISO 27001.

- SGSI (Sistema de Gestión de seguridad de la información): presenta temas importantes en los que usuario debe involucrarse para comprender los fundamentos de la metodología elaborada.

  - ✓ Que es un SGSI.
  - ✓ Para que sirve.
  - ✓ Como de implementa
  - ✓ Que incluye un SGSI

Cada tema es importante para comprender el porque de la elaboración de la metodología, se recomienda leer.

- Norma ISO 27001: presenta temas para un conocimiento claro de los objetivos de la norma ISO 27001.

  - ✓ Que es la norma ISO 27001.
  - ✓ Orígenes de la norma ISO 27001.
  - ✓ Contenido de la norma ISO 27001.
  - ✓ Estructura de la norma ISO 27001.

- Modulo de Dominios y Controles que contempla la metodología elaborada según ISO 27001.

COD	NOMBRE CONTROL	DOMINIO	ESTADO	NORMA ISO	FECHA INICIO	FECHA FIN
1	Documento	Politica	activo	Cumple	1969-01-31	1969-01-31
3	Compromiso	Organización	activo	No	1969-01-31	1969-01-31
4	CoordinaciÃ³n	Organización	activo	Cumple	1969-12-31	1969-12-31
5	AsignaciÃ³n	Organización	activo	Cumple	1969-12-31	1969-12-31
6	Proceso	Organización	pasivo	Cumple	1969-12-31	1969-12-31
7	Acuerdos	Organización	critico	No	1969-12-31	1969-12-31
8	Contacto	Organización	activo	Cumple	null	null
9	Contacto	Organización	pasivo	Cumple	null	null
10	Revisión	Organización	critico	Cumple	null	null
11	Identificación	Organización	activo	Cumple	null	null
12	Tratamiento	Organización	pasivo	Cumple	null	null
13	Tratamiento	Organización	critico	Cumple	null	null
14	Inventario	Gestión	activo	Cumple	null	null
15	Responsable	Gestión	pasivo	Cumple	null	null
16	Uso	Gestión	critico	Cumple	null	null
17	Directrices	Gestión	critico	Cumple	null	null

En este modulo de acuerdo al tipo de usuario de podrá Listar, Eliminar, Actualizar, Modificar dominios con sus respectivos controles asignados.

En el caso del usuario administrador podrá Listar, Eliminar, Actualizar, Modificar y agregarle un estado al control según su análisis. Además podrá obtener reportes de acuerdo a la necesidad de verificación

El usuario común solo podrá listar los dominios y controles.

- Ayuda: presenta un manual de ayuda para poder navegar por el sistema.

Recomendaciones:

- ✓ Leer detalladamente las instrucciones del presente manual.
- ✓ Acceder a las opciones del sistema; leyendo detalladamente los datos que se solicitan.
- ✓ Tener conectada la impresora para imprimir el cumplimiento de los controles en el caso de requerirlos.
- ✓ El uso de las claves debe ser confidencial para un mejor control de la seguridad.
- ✓ De debe tener un control adecuado con los equipos en los que se encuentren instalados los programas.

Anexo II

CÓDIGO DEL SISTEMA

BASE DE DATOS

TABLAS

```
-- Table: controles
-- DROP TABLE controles;
CREATE TABLE controles
(
  "Id_control" bigserial NOT NULL,
nom_control character varying(100),
id_dominio bigint,
id_estado bigint,
  id_norma bigint,
fecha_inicio timestamp without time zone,
fecha_fin timestamp without time zone,
  CONSTRAINT pk_id_control PRIMARY KEY ("Id_control"),
  CONSTRAINT fk_id_dominio FOREIGN KEY (id_dominio)
  REFERENCES dominio ("Id_dominio") MATCH SIMPLE
  ON UPDATE NO ACTION ON DELETE NO ACTION
)
WITH (
  OIDS=FALSE
);
ALTER TABLE controles OWNER TO postgres;

-- Table: dominio
-- DROP TABLE dominio;
CREATE TABLE dominio
(
nom_dominio character varying(100) NOT NULL,
fecha_creacion timestamp without time zone,
fecha_inicio timestamp without time zone,
fecha_fin timestamp without time zone,
  "Id_dominio" bigserial NOT NULL,
  CONSTRAINT pk_id_dominio PRIMARY KEY ("Id_dominio")
)
WITH (
  OIDS=FALSE
);
ALTER TABLE dominio OWNER TO postgres;



-- Table: estado
-- DROP TABLE estado;
CREATE TABLE estado
(
  "Id_estado" bigserial NOT NULL,
  nom_estado character varying(30),
  CONSTRAINT pk_id_estado PRIMARY KEY ("Id_estado")
)
WITH (
  OIDS=FALSE
```

```
);
ALTER TABLE estado OWNER TO postgres;
-- Table: norma
-- DROP TABLE norma;
CREATE TABLE norma
(
  "Id_norma" bigserial NOT NULL,
nom_norma character varying(30),
  CONSTRAINT pk_id_norma PRIMARY KEY ("Id_norma")
)
WITH (
  OIDS=FALSE
);
ALTER TABLE norma OWNER TO postgres;



-- Table: usuarios
-- DROP TABLE usuarios;
CREATE TABLE usuarios
(
  "Id_usuario" bigserial NOT NULL,
nom_usuario character varying(20),
contrasenia character varying(20),
usuario_tipo integer,
  CONSTRAINT pk_id_usuario PRIMARY KEY ("Id_usuario")
)
WITH (
  OIDS=FALSE
);
ALTER TABLE usuarios OWNER TO postgres;
```

FUNCIONES PARA LAS TABLAS

```
-- Function: "fa_Control"(character varying, bigint, bigint, timestamp without time zone, timestamp without time zone, bigint, bigint)

-- DROP FUNCTION "fa_Control"(character varying, bigint, bigint, timestamp without time zone, timestamp without time zone, bigint, bigint);

CREATE OR REPLACE FUNCTION "fa_Control"("pNOMBRE_CONTROL" character varying, "pID_DOMINIO" bigint, "pID_ESTADO" bigint, "pFECHA_INICIO" timestamp without time zone, "pFECHA_FIN" timestamp without time zone, "pID_NORMA" bigint, "pID_CONTROL" bigint)
  RETURNS boolean AS
$BODY$declare band boolean;
begin
UPDATE public."controles" SET "nom_control"=$1, "id_dominio"=$2, "id_estado"=$3,"fecha_inicio"=$4,"fecha_fin"=$5,"id_norma"=$6,"Id_control"=$7 WHERE "Id_control"=$7;
band=true;
return band;
end;$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100;
```

```
ALTER FUNCTION "fa_Control"(character varying, bigint, bigint, timestamp without time zone, timestamp without time zone, bigint, bigint) OWNER TO postgres;

-- Function: fa_dominio(character varying, timestamp without time zone, timestamp without time zone, timestamp without time zone, integer)

-- DROP FUNCTION fa_dominio(character varying, timestamp without time zone, timestamp without time zone, timestamp without time zone, integer);

CREATE OR REPLACE FUNCTION fa_dominio("pNOMBRE_DOMINIO" character varying, "pFECHA_CREACION" timestamp without time zone, "pFECHA_INICIO" timestamp without time zone, "pFECHA_FINAL" timestamp without time zone, "pID_DOMINIO" integer)
  RETURNS boolean AS
$BODY$declare band boolean;
begin
UPDATE public."dominio" SET "nom_dominio"="pNOMBRE_DOMINIO", "fecha_creacion"=$2, "fecha_inicio"=$3, "fecha_fin"=$4  WHERE "Id_dominio"=$5;
band=true;
return band;
end;$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100;
ALTER FUNCTION fa_dominio(character varying, timestamp without time zone, timestamp without time zone, timestamp without time zone, integer) OWNER TO postgres;

-- Function: "fa_Usuario"(character varying, character varying, integer, integer)

-- DROP FUNCTION "fa_Usuario"(character varying, character varying, integer, integer);

CREATE OR REPLACE FUNCTION "fa_Usuario"("pNOM_USUARIO" character varying, "pCONTRASENIA" character varying, "pUSUARIO_TIPO" integer, "pID_USUARIO" integer)
  RETURNS boolean AS
$BODY$declare band boolean;
begin
UPDATE public."usuarios" SET   "nom_usuario"=$1, "contrasenia"=$2,"usuario_tipo"=$3 WHERE "Id_usuario"=$4;
band=true;
return band;
end;$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100;
ALTER FUNCTION "fa_Usuario"(character varying, character varying, integer, integer) OWNER TO postgres;
-- Function: fa_estado(character varying, bigint)
-- DROP FUNCTION fa_estado(character varying, bigint);
CREATE OR REPLACE FUNCTION fa_estado("pNOMBRE_ESTADO" character varying, "pID_ESTADO" bigint)
  RETURNS boolean AS
$BODY$declare band boolean;
begin
UPDATE public."estado" SET "nom_estado"=$1 WHERE "id_estado"=$2;
band=true;
return band;
end;$BODY$
  LANGUAGE plpgsql VOLATILE
```

```
  COST 100;
ALTER FUNCTION fa_estado(character varying, bigint) OWNER TO postgres;

-- Function: fc_obtener_todos_control()

-- DROP FUNCTION fc_obtener_todos_control();

CREATE OR REPLACE FUNCTION fc_obtener_todos_control(OUT "pID_CONTROL" bigint, OUT "pNOMBRE_CONTROL" character varying, OUT "pID_DOMINIO" bigint, OUT "pID_ESTADO" bigint, OUT "pFECHA_INICIO" timestamp without time zone, OUT "pFECHA_FIN" timestamp without time zone, OUT "pID_NORMA" bigint)
  RETURNS SETOF record AS
$BODY$begin
return query SELECT "Id_control", "nom_control", "id_dominio", "id_estado", "fecha_inicio", "fecha_fin", "id_norma"

from public."controles";
end;
$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100
  ROWS 1000;
ALTER FUNCTION fc_obtener_todos_control() OWNER TO postgres;

-- Function: fc_obtener_todos_dominio()

-- DROP FUNCTION fc_obtener_todos_dominio();

CREATE OR REPLACE FUNCTION fc_obtener_todos_dominio(OUT "pNOM_DOMINIO" character varying, OUT "pFECHA_CREACION" timestamp without time zone, OUT "pFECHA_INICIO" timestamp without time zone, OUT "pFECHA_FIN" timestamp without time zone, OUT "pID_DOMINIO" bigint)
  RETURNS SETOF record AS
$BODY$begin
return query SELECT "nom_dominio", "fecha_creacion", "fecha_inicio", "fecha_fin", "Id_dominio"

from public."dominio";
end;
$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100
  ROWS 1000;
ALTER FUNCTION fc_obtener_todos_dominio() OWNER TO postgres;

-- Function: fi_control(character varying, bigint, bigint, timestamp without time zone, timestamp without time zone, bigint)

-- DROP FUNCTION fi_control(character varying, bigint, bigint, timestamp without time zone, timestamp without time zone, bigint);

CREATE OR REPLACE FUNCTION fi_control("pNOMBRE_CONTROL" character varying, "pID_DOMINIO" bigint, "pID_ESTADO" bigint, "pFECHA_INICIO" timestamp without time zone, "pFECHA_FIN" timestamp without time zone, "pID_NORMA" bigint)
  RETURNS boolean AS
$BODY$
```

```
DECLARE BANDERA BOOLEAN;
BEGIN
INSERT INTO "public"."controles"("nom_control", "id_dominio", "id_estado", "fecha_inicio", "fecha_fin", "id_norma")
VALUES ($1,$2,$3,$4,$5,$6);
BANDERA = TRUE;
RETURN BANDERA;
END;
$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100;
ALTER FUNCTION fi_control(character varying, bigint, bigint, timestamp without time zone, timestamp without time zone, bigint) OWNER TO postgres;

-- Function: fi_dominio(character varying, timestamp without time zone, timestamp without time zone, timestamp without time zone)

-- DROP FUNCTION fi_dominio(character varying, timestamp without time zone, timestamp without time zone, timestamp without time zone);

CREATE OR REPLACE FUNCTION fi_dominio("pNOM_DOMINIO" character varying, "pFECHA_CREACION" timestamp without time zone, "pFECHA_INICIO" timestamp without time zone, "pFECHA_FINAL" timestamp without time zone)
  RETURNS boolean AS
$BODY$
DECLARE BANDERA BOOLEAN;
BEGIN
INSERT INTO "public"."dominio"("nom_dominio", "fecha_creacion", "fecha_inicio", "fecha_fin")
VALUES ($1,$2,$3,$4);
BANDERA = TRUE;
RETURN BANDERA;
END;
$BODY$
  LANGUAGE plpgsql VOLATILE
  COST 100;
ALTER FUNCTION fi_dominio(character varying, timestamp without time zone, timestamp without time zone, timestamp without time zone) OWNER TO postgres;
```

CODIGO DE LA INTERFAZ

CONEXION

```
package AccesoADatos;
import java.sql.*;
import java.util.*;

/**
 *
 * @author root
 */
public class Conexion {
public  String driver;
            public  String url;
            public  String user;
            public String pass;

            public Conexion(){
            }
```

```
        public String getDriver(){
                return this.driver;
        }

        public String getUrl(){
                return this.url;
        }
        public String getUser(){
                return this.user;
        }

        public void setUser(String user){
                this.user=user;
        }

        public void setPassword(String pass){
                this.pass=pass;
        }

        public  Conexion(String pdriver, String pURL, String pusuario,String pclave ){
                this.driver=pdriver;
    this.url=pURL;
    this.user=pusuario;
    this.pass= pclave;
        }


public ResultSet ejecutaPrepared(PreparedStatement prStm) throws Exception
    {
   ResultSet rts=null;
try {
rts =prStm.executeQuery();

    } catch (SQLException exConec) {
throw  new Exception(exConec.getMessage());
    }
return rts;
    }


public PreparedStatement creaPreparedSmt(String sql) throws Exception
    {
     PreparedStatement prStm=null;
try {
Class.forName(this.driver);
      //  System.out.println("OK al cargar");
try {
        Connection con = DriverManager.getConnection(this.url,this.user,this.pass);
        // System.out.println("Conectado a Oracle");
prStm = con.prepareStatement(sql);

      } catch (SQLException exConec) {
throw  new Exception(exConec.getMessage());
        }
```

```
        }
catch (ClassNotFoundException exCarga) {
throw  new Exception(exCarga.getMessage());
       }
return prStm;
       }

public boolean  ejecutaPreparedTransaccion(ArrayList<Comando> lstComandos) throws Exception
       {
boolean respuesta=false;
Class.forName(this.driver);
          Connection con = DriverManager.getConnection(this.url,this.user,this.pass);
try {

if (con.getAutoCommit()) {
con.setAutoCommit(false);
}
for (Comando comando : lstComandos) {
                PreparedStatement ptrs = con.prepareStatement(comando.getSetenciaSql());
for (Parametro parametro : comando.getLstParametros()) {
ptrs.setObject(parametro.getPosicion(), parametro.getValor());
}
                ResultSet rst = ptrs.executeQuery();
if (rst.next()) {
                   String bandera = rst.getString(1);
respuesta = bandera.equals("t")?true:false;
                }
             }
con.commit();
          }
catch (SQLException exConec) {
con.rollback();
throw  new Exception(exConec.getMessage());
       }
return respuesta;
       }

public int ejecutaPreparedTransaccionFactura(ArrayList<Comando> lstComandos) throws
Exception
       {
int respuesta=-1;
boolean respuestaItems=false;
int respuestaEncabezado=-1;
Class.forName(this.driver);
          Connection con = DriverManager.getConnection(this.url,this.user,this.pass);
try {

if (con.getAutoCommit()) {
con.setAutoCommit(false);
}
             Comando encabezado= lstComandos.get(0);
             PreparedStatement ptrsencabezado = con.prepareStatement(encabezado.getSetenciaSql());
for (Parametro parametro : encabezado.getLstParametros()) {
ptrsencabezado.setObject(parametro.getPosicion(), parametro.getValor());
             }
```

```
            ResultSet rstencabezado = ptrsencabezado.executeQuery();
if (rstencabezado.next()) {
respuestaEncabezado = rstencabezado.getInt(1);
            }


            //
int p=0;
p=lstComandos.size();

for (int j = 1; j < p; j++){
            Comando items= lstComandos.get(j);
            PreparedStatement ptrsItems = con.prepareStatement(items.getSetenciaSql());
for (Parametro parametro : items.getLstParametros()) {
if(parametro.getPosicion()==2)
                {
parametro.setValor((Object)respuestaEncabezado);
                }
else
                {}
ptrsItems.setObject(parametro.getPosicion(), parametro.getValor());
            }
            ResultSet rstitems = ptrsItems.executeQuery();
if (rstitems.next()) {

                    String bandera = rstitems.getString(1);
respuestaItems = bandera.equals("t")?true:false;
//respuestaItems = rstitems.getInt(1);
            }

            }
if((respuestaEncabezado>0)&&(respuestaItems==true))
                //&& (respuestaPagoEfectivo==true)&& (respuestaPagoTarjeta==true)
             {
respuesta= respuestaEncabezado;
             }
rstencabezado.close();
con.commit();
con.close();
          }
catch (SQLException exConec) {
con.rollback();
throw  new Exception(exConec.getMessage());
       }
return respuesta;
       }
}
```

DIRECCIONAMIENTO

```
package AccesoADatos;

/**
 *
 * @author root
 */
```

```
public class Global {
public static final  String url="jdbc:postgresql://localhost:5432/dbguiametodologica";
public static final  String user="postgres";
public static final  String pass="123456";
public static final  String driver="org.postgresql.Driver";
}
```

REGLAS DE NEGOCIO

```
package ReglasNegocio;
import java.sql.Timestamp;
import AccesoADatos.*;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.util.*;
/**
 *
 * @author RHCN
 */
public class controles {
private Integer Id_control;
private String nom_control;
private Integer Id_dominio;
private String nom_dominio;
private Integer Id_estado;
private String nom_estado;
private java.sql.Timestamp  fecha_inicio;
private java.sql.Timestamp fecha_fin;
private Integer Id_norma;
private String nom_norma;

public controles() {
   }

public controles(Integer Id_control, String nom_control, Integer Id_dominio, Integer Id_estado,Timestamp fecha_inicio, Timestamp fecha_fin, Integer Id_norma) {
this.Id_control = Id_control;
       this.nom_control = nom_control;
       this.Id_dominio = Id_dominio;
this.Id_estado = Id_estado;
       this.fecha_inicio = fecha_inicio;
       this.fecha_fin = fecha_fin;
       this.Id_norma = Id_norma;
}

public Integer getId_control() {
return Id_control;
   }

public void setId_control(Integer Id_control) {
       this.Id_control = Id_control;
   }

public Integer getId_dominio() {
return Id_dominio;
```

```
    }

public void setId_dominio(Integer Id_dominio) {
        this.Id_dominio = Id_dominio;
}

public Integer getId_estado() {
return Id_estado;
    }

public void setId_estado(Integer Id_estado) {
        this.Id_estado = Id_estado;
}

public String getNom_control() {
return nom_control;
    }

public void setNom_control(String nom_control) {
        this.nom_control = nom_control;
    }
        /**
     * @return the Id_norma
     */
public Integer getId_norma() {
return Id_norma;
    }

    /**
     * @param Id_norma the Id_norma to set
*/
public void setId_norma(Integer Id_norma) {
        this.Id_norma = Id_norma;
    }

    /**
     * @return the fecha_inicio
     */
public java.sql.Timestamp getFecha_inicio() {
return fecha_inicio;
    }

    /**
     * @param fecha_inicio the fecha_inicio to set
     */
public void setFecha_inicio(java.sql.Timestamp fecha_inicio) {
        this.fecha_inicio = fecha_inicio;
    }

    /**
     * @return the fecha_fin
     */
public java.sql.Timestamp getFecha_fin() {
return fecha_fin;
    }
```

```
    /**
     * @param fecha_fin the fecha_fin to set
     */
public void setFecha_fin(java.sql.Timestamp fecha_fin) {
        this.fecha_fin = fecha_fin;
}
    /**
   * @return the nom_dominio
   */
public String getNom_dominio() {
return nom_dominio;
  }

  /**
   * @param nom_dominio the nom_dominio to set
   */
public void setNom_dominio(String nom_dominio) {
    this.nom_dominio = nom_dominio;
  }

  /**
   * @return the nom_estado
   */
public String getNom_estado() {
return nom_estado;
  }

  /**
   * @param nom_estado the nom_estado to set
   */
public void setNom_estado(String nom_estado) {
this.nom_estado = nom_estado;
}

  /**
   * @return the nom_norma
   */
public String getNom_norma() {
return nom_norma;
  }

  /**
   * @param nom_norma the nom_norma to set
   */
public void setNom_norma(String nom_norma) {
    this.nom_norma = nom_norma;
  }
    /*
     * ACTUALIZAR
     */
   //LISTO
public static boolean  Actualizar_Controles(controles control) throws Exception
    {
boolean respuesta=false;
```

```
try
      {
            Conexion conn=new Conexion(Global.driver,Global.url,Global.user,Global.pass);
            ArrayList<Comando> comandos = new ArrayList<Comando>();
            Comando cmd = new Comando();
cmd.setSetenciaSql("select \"public\".\"fa_Control\"(?,?,?,?,?,?,?)");
            ArrayList<Parametro> parametros = new ArrayList<Parametro>();
parametros.add(new Parametro(1, control.getNom_control()));
            parametros.add(new Parametro(2, control.getId_dominio()));
            parametros.add(new Parametro(3, control.getId_estado()));
            parametros.add(new Parametro(4, control.getFecha_inicio() ));
            parametros.add(new Parametro(5, control.getFecha_fin()));
            parametros.add(new Parametro(6, control.getId_norma()));
            parametros.add(new Parametro(7, control.getId_control()));
            cmd.setLstParametros(parametros);
            comandos.add(cmd);
            respuesta =   conn.ejecutaPreparedTransaccion(comandos);
} catch (SQLException exConec) {
throw  new Exception(exConec.getMessage());
       }
return respuesta;
   }

   //LISTO
public static boolean  Eliminar_Control(int cont) throws Exception
   {
boolean respuesta = false;
try
      {
            Conexion con = new Conexion(Global.driver,Global.url,Global.user,Global.pass);
            ArrayList<Comando> comandos = new ArrayList<Comando>();
            Comando cmd = new Comando();
cmd.setSetenciaSql("select \"public\".\"fe_control\"(?)");
            ArrayList<Parametro> parametros = new ArrayList<Parametro>();
parametros.add(new Parametro(1, cont));
cmd.setLstParametros(parametros);
            comandos.add(cmd);
            respuesta =   con.ejecutaPreparedTransaccion(comandos);
      } catch (SQLException exConec) {
throw  new Exception(exConec.getMessage());
       }
return respuesta;
   }
```

DOMINIO

```
/*
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
*/

package ReglasNegocio;

import java.sql.Timestamp;
import AccesoADatos.*;
```

```
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.util.*;
/**
 *
 * @author RHCN
 */
public class dominio {

private Integer Id_dominio;
public String nom_dominio;
private java.sql.Timestamp fecha_creacion;
private java.sql.Timestamp  fecha_inicio;
private java.sql.Timestamp fecha_fin;

    public dominio() {
    }

    public dominio(Integer Id_dominio, String nom_dominio, Timestamp fecha_creacion, Timestamp
fecha_inicio, Timestamp fecha_fin) {
this.Id_dominio = Id_dominio;
        this.nom_dominio = nom_dominio;
this.fecha_creacion = fecha_creacion;
        this.fecha_inicio = fecha_inicio;
        this.fecha_fin = fecha_fin;
}

    public Integer getId_dominio() {
        return Id_dominio;
    }

    public void setId_dominio(Integer Id_dominio) {
        this.Id_dominio = Id_dominio;
}

    public Timestamp getFecha_creacion() {
        return fecha_creacion;
    }

    public void setFecha_creacion(Timestamp fecha_creacion) {
        this.fecha_creacion = fecha_creacion;
    }

    public Timestamp getFecha_fin() {
        return fecha_fin;
    }

    public void setFecha_fin(Timestamp fecha_fin) {
        this.fecha_fin = fecha_fin;
    }

    public Timestamp getFecha_inicio() {
        return fecha_inicio;
    }
```

```
    public void setFecha_inicio(Timestamp fecha_inicio) {
        this.fecha_inicio = fecha_inicio;
}

    public String getNom_dominio() {
        return nom_dominio;
    }

    public void setNom_dominio(String nom_dominio) {
        this.nom_dominio = nom_dominio;
    }

//LISTO
    public static boolean Insertar_dominio(dominio dominios)throws Exception
    {
        boolean respuesta=false;
        try
        {

            Conexion conn=new Conexion(Global.driver,Global.url,Global.user,Global.pass);
            ArrayList<Comando> comandos = new ArrayList<Comando>();
            Comando cmd = new Comando();
            cmd.setSetenciaSql("select \"public\".\"fi_dominio\"(?,?,?,?)");
            ArrayList<Parametro> parametros = new ArrayList<Parametro>();

            parametros.add(new Parametro(1, dominios.getNom_dominio()));
parametros.add(new Parametro(2, dominios.getFecha_creacion()));
            parametros.add(new Parametro(3, dominios.getFecha_inicio()));
            parametros.add(new Parametro(4, dominios.getFecha_fin()));
            cmd.setLstParametros(parametros);
            comandos.add(cmd);
            respuesta =   conn.ejecutaPreparedTransaccion(comandos);
        } catch (SQLException exConec) {
throw  new Exception(exConec.getMessage());
}
         return respuesta;
    }
```

Anexo III

ENCUESTA DIRIGIDA A LOS EMPLEADOS DEL DESITEL

Luego del trabajo realizado como tesis y al valorar la colaboración de los empleados del DESITEL, además del conocimiento impartido sobre el contenido de la metodología elaborada según ISO 27001, se les solicita responder el siguiente cuestionario.

OBJETIVO: Determinar el grado de aceptación de la metodología elaborada según ISO 27001 y la eficacia en sus contenidos, para impulsar su utilización.

#	PREGUNTA	Si	No	Parcialmente
1	¿Cree usted que las normas de seguridad contribuyen a mejorar y conservar la información del DESITEL?			
2	¿Considera necesario contar con una guía metodológica para garantizar la protección de la información?			
3	¿Considera que la estructura de la política de Seguridad establecida en el DESITEL mejorará su organización al utilizar la metodología elaborada según ISO 27001?			
4	¿La Organización en seguridad informática alcanzará mejoras en su estructuración al utilizar la metodología elaborada según ISO 27001?			
5	¿La Gestión de activos para el DESITEL mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?			
6	¿La Seguridad de los Recursos Humanos del Departamento mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?			
7	¿La Seguridad física y del entorno del departamento mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?			
8	¿El Control de acceso a toda la información mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?			
9	¿La Adquisición, Desarrollo y mantenimiento de sistemas mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?			
10	¿La Gestión de comunicaciones y operaciones mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?			
Elaborado por : Verónica Gavilanes P.				

Anexo IV

INVENTARIO DE APLICACIONES Y SOFWARE OPERATIVO EN SERVIDORES DEL DESITEL

SERVIDORES CARACTERISTICAS HW

Servidores HP.

- 2 DISCOS DUROS SCSI (200 gigas cada/uno)
- Procesador XEON 2.4 Ghz
- RAM 2GIGAS.

Servidores IBM.

- 2 DISCOS DUROS SCSI (40 gigas cada/uno)
- Procesador AMD 550MHz
- RAM 2GIGAS.

1. SERVIDOR DE CORREO (HP)

APLICACIÓN: http://webmail.espoch.edu.ec

SOFTWARE – VERSIONES:

- CENTOS 4.3
- MySQL Versión 5.0.27
- Apache versión 2.0.52
- PHP versión 5.1.6
- SpamAssassin versión 3.1.8
- Postfix versión 2.3.2

2. SERVIDOR DNS INTERNO (IBM)

Servicio De Red: DNS EXTERNO - BIND versión 9.3.3

3. SERVIDOR PROXY (IBM)

Servicios De Gestión de Red

- PROXY - DANSGUARDIAN
- DNS INTERNO (LAN)
- DHCP

Servicios Web

- CENTER-WIRELESS (http://center.espoch.edu.ec)

- RECURSOS HUMANOS (http://recursos.espoch.edu.ec)

- APPOCH (http://appoch.edu.ec)

- ANTARES (http://antares.espoch.edu.ec)

- Bienestar Politécnico (http://becas.espoch.edu.ec)

- Seguro de Cesantía (http://cesantia.espoch.edu.ec)

- LIBRERÍA (http://libreria.espoch.edu.ec)

- OTRAS APLICACIONES WEB TEMPORALES DE EVENTOS

SOFTWARE – VERSIONES:

- CENTOS 5.0

- MySQL Versión 5.0.22

- Apache versión 2.2.3

- PHP versión 5.1.6

- BIND versión 9.3.3

- DHCP versión 3.0.5

- SQUID versión 2.6

4. SERVIDOR WEB 2 (IBM)

APLICACIONES:

- PORTAL - ESPOCH (http:/www.espoch.edu.ec).

- ACADEMIA CISCO (http:/cisco.espoch.edu.ec).

SOFTWARE – VERSIONES:

- CENTOS 5.0

- MySQL Versión 5.0.22

- Apache versión 2.2.3

- PHP versión 5.1.6

5. SERVIDOR WEB 3 (HP)

APLICACIONES:

- E-VIRTUAL (http://evirtual.espoch.edu.ec).

SOFTWARE – VERSIONES:

- CENTOS 4.3
- MySQL Versión 5.0.22
- Apache versión 2.2.3
- PHP versión 5.1.6

6. SERVIDOR WEB 4 (HP)

APLICACIONES:

- SALUD ELECTRONICA (http://medicina.espoch.edu.ec).
- TELEFONIA IP. (http://telefonicaip.espoch.edu.ec)

SOFTWARE – VERSIONES:

Windows Server 2003

- SQLServer 2000
- Internet Information Server 6
- .NET 2003

7. SISTEMA ACADEMICO

Servidores:

- 1 Servidor de Base Datos (IBM)
- 3 Servidores de Aplicaciones (cluster) 1HP – 2 (IBM)

SOFTWARE – VERSIONES:

Windows Server 2003

- SQLServer 2000
- Internet Information Server 6
- .NET 2003

Anexo V

Análisis de los Activos y factores de riesgo

Presentamos los distintos activos reconocidos en el DESITEL de la ESPOCH, asignando un valor a la importancia que tienen en la institución, ponderada en una escala del 1 al 10. Esta importancia es un valor subjetivo que refleja el nivel de impacto que puede tener la ESPOCH si un incidente afectaría a los activos, sin considerar las medidas de seguridad que existan sobre los mismos.

Importancia de 1 a10

#	Activos a proteger	Valor	Imp.
1	Servidores Web (Memoria, Disco duro. Procesador, Monitor, Mouse, Fuente de poder).	45400	10
2	Bases de datos.(MySQL, SQL Server)	600	9
3	Servicios (Sistema académico. Antares. Evaluación Institucional, Sistema de recursos Humanos, Sistema de autenticación global E-mail).	42000	9
4	Software(Software de aplicación, programas fuente, sistemas operativos)	500	8
5	Backup o respaldos	3000	9

6	Dispositivos de red(Cableado , antenas, switch, hubs, módems, routers)	5700	7
7	Personal(Usuarios o empleados)	2500	6
8	Documentación de programas, hardware, sistemas, procedimientos administrativos, manuales, etc	3000	9
9	Insumos(cintas, cartuchos de tinta, toner, papel, formularios, etc)	150	6
	Total	102850	

A continuación se listan los factores de riesgo que pueden afectar a dichos activos, indicando la probabilidad de que estas contingencias ocurran, en una escala del 1 al 3.

Esta probabilidad es evaluada teniendo en cuenta las medidas de segundad existentes en el departamento de Sistemas y Telemática de la Espoch.

Probabilidad de 1 a 3

#	Factores de Riesgo	Probabilidad
1	Acceso no autorizado a datos	3

2	Acceso no autorizado a los laboratorios	2
3	Aplicaciones sin licencia	1
4	Ausencia o falta de segmentación	2
5	Complejidad en el diseño de las redes	1
6	Condiciones de trabajo adversas	3
7	Copia no autorizada de la información a un medio de datos	3
8	Corte de luz o variaciones de voltaje	2
9	Craking de password	2
10	Daño o destrucción de cables	1
11	Destrucción negligente de datos	3
12	E- mail bombing y spamming	1
13	Error de configuración en los servidores	2
14	Errores de software	2
15	Errores en las funciones de encriptación	2

16	Falla de Base de datos	3
17	Falla del sistema	2
18	Falta de autenticación	2
19	Falta de espacio de almacenamiento	2
20	Incendios	3
21	Ingreso de polvo	2
22	Interferencias	2
23	Inundaciones o filtración de agua	2
24	Limite de vida útil de equipos	1
25	Mal mantenimiento de los servidores	1
26	Mala administración de cuentas de usuario	1
27	Mala integridad de los datos resguardados	1
28	Suspensión de servicios Web	1
29	Perdida de backups	2

30	Riesgo por el personal de limpieza o personal externo	1
31	Robo de dispositivos o equipos	1
32	Rótulos inadecuados en los medios de datos	1
33	Sabotaje	1
34	Software desactualizado	1
35	Spoofing y sniffing	1
36	Transporte inseguro de archivos	1
37	Usurpación de usuarios	1
38	Utilización de claves o password simples por los usuarios	1
39	Virus	2

POSIBLES CONSECUENCIAS Y MEDIDAS EXISTENTES

En el presente cuadro se listan los activos del DESITEL, los factores de riesgos que los afectan directamente y las consecuencias que puede acarrear la ocurrencia de estos factores. Se agrega información referida a las medidas que ha tomado la ESPOCH para mitigar estas consecuencias. Por último mediante un análisis se ha evaluado estas medidas, indicando si son **deficientes, mejorables o eficientes.**

Activo	**Factor de Riesgo**	**Consecuencias?**	**Como se protege?**	**Es efectiva**
S E R V I D	Acceso no autorizado a los laboratorios	Robo, modificación de la información	Seguridad física, puertas protegidas	e
	Corte de luz, o variaciones de voltaje.	Daño de los equipos o parte de ellos	UPS, estabilizador, disposición de un pozo a tierra, generador de luz	m
	Incendios	Daño total o parcial de los equipos por el fuego o altas temperaturas	Equipos contra incendio (extintores, fuentes de agua) capacitación del personal.	m

O R E S	Inundaciones o filtración de agua	Daño total o parcial de los equipos por el agua	Seguridad física y buen diseño del edificio	e
	Limite de vida útil, maquinas obsoletas	Deterioro en la performance del sistema	Equipamiento actual y asesoramiento permanente	m
	Mal mantenimiento de los servidores	Interrupciones en el funcionamiento del sistema	Mantenimiento interno y permanente	m
	Robo de dispositivos o equipos	Perdida de equipamiento o información	Controles de accesos físicos, guardias de seguridad, alarmas	e

Activo	**Factor de Riesgo**	**Consecuencias?**	**Como se protege?**	**Es efectiva**
B	Acceso no autorizado a los	Robo, modificación de la	Seguridad lógica y firewall	m

A S E S D E D D T	datos	información		
	Copia no autorizada de un medio de datos	Divulgación de información	Desabilitación de puertos y controles lógicos	m
	Errores de software	Inconsistencias en los datos	Controles internos y backup de los datos.	m
	Falla de base de datos	Inconsistencias en los datos	Controles internos y backup de los datos.	m
	Falta de espacio de almacenamiento	Falla en la aplicación	Recursos abundantes de almacenamiento	e
	Mala integridad de los datos	Inconsistencias y redundancia de datos	Controles en las aplicaciones desarrolladas	e

O S	Perdida de confidencialidad en datos privados y de sistema	Divulgación de información	Controles físicos y controles de accesos lógicos a datos críticos	m
	Virus	Perdida, modificación o divulgación de datos, perdida de tiempo, y productividad.	Herramientas antivirus y firewall	m

Activo	**Factor de Riesgo**	**Consecuencias?**	**Como se protege?**	**Es efectiva**
S E R	Negación de servicio Web	Servicio inactivo	Responsable por cada servicio	m
	Utilización de claves o password simples por los usuarios	Fácil descubrimiento de claves	Capacitación a los usuarios con políticas de buenas password	m

V I C I O S	Usurpación de usuarios	Cambio o robo de información	Capacitación en la confidencialidad de la informacion	e
	Craking de password	Modificación o divulgación de información	Utilización de algoritmos complejos	e
	Transporte inseguro de archivos	Divulgación de información	Chequeo permanente de puertos, herramientas de monitoreo de datos	m

Activo	**Factor de riesgo**	**Consecuencias?**	**Como se protege?**	**Es efectiva**
S	Acceso no autorizado a los servidores	Mala administración en las cuentas de usuario o divulgación de claves	Permisos mínimos necesarios para el desempeño de sus funciones	m

Activo	**Factor de riesgo**	**Consecuencias?**	**Como se protege?**	**Es efectiva**
O F T W A R E	Error de configuración en los servidores	Mal funcionamiento de los servidores	Existen herramientas de análisis y personal de mantenimiento	m
	Falla del sistema	Posibles demoras en el desarrollo de las funciones	Backup y sistemas de respaldo	m
	Mala administración de control de acceso.	Divulgación y modificación de información.	Controles de accesos lógicos, reforzando en datos críticos.	e

Activo	**Factor de riesgo**	**Consecuencias?**	**Como se protege?**	**Es efectiva**
B A C K U P	Copia no autorizada a un medio de datos	Robo de información	Controles de seguridad física y controles de accesos lógicos a los servidores	e
	Falta de espacio de almacenamiento	Falla en la generación del backup	Existencia de discos redundantes para la copia	e
	Perdida de backups	Falta de datos, incapacidad de restaurarlos y divulgación de la información	Backups redundantes	d
	Rótulos inadecuados en los medios de datos	Errores durante la restauración de datos	Rótulos capaces de diferenciar cada medio de datos como único.	m

Activo	Factor de riesgo	Consecuencias?	Como se protege?	Es efectiva
D O C U M E N	Borrado, modificación o revelación desautorizada de información	Documentación incorrecta	Actualización permanente de políticas de seguridad	m
	Descripción de archivos inadecuada	Documentación incorrecta	Formatos bien estructurados para las diferentes funciones	m
				m

T A C I O N	Documentación insuficiente o faltante, funciones no documentadas	Entorpecimiento de la administración y uso del sistema	Actualización permanente de la documentación de los procesos	
	Robo de documentos	Divulgación de información	Controles de acceso físico a datos	m

CALCULO DE NIVELES DE VULNERABILIDAD

En este cuadro se calculan los niveles de vulnerabilidad (o niveles de riesgo) en los que incurre cada activo antes mencionado. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y la probabilidad de ocurrencia de estos riesgos. Para realizar dicho cálculo se desarrollaron las siguientes operaciones:

PROBABILIDAD DE OCURRENCIA: representan la probabilidad de que ocurran los factores de riesgo mencionados, en una escala del 1 al 3. Esta probabilidad fue evaluada teniendo en cuenta las medidas de seguridad existentes en el DESITEL.

PROBABILIDAD DEL RIESGO: se calcula el porcentaje de probabilidad de que ocurra un determinado factor de riesgo, con respecto a la cantidad de factores de riesgo intervinientes para dicho activo.

NIVEL DE VULNERABILIDAD

En este momento interviene el nivel de importancia, multiplicando a la probabilidad del riesgo. De esta forma se obtiene el nivel de vulnerabilidad de cada activo con respecto a un factor de riesgo.

Nivel de Vulnerabilidad = (Nivel de Importancia)*(Probabilidad de Riesgo)

La suma de estos valores es el nivel de vulnerabilidad total que corresponde a cada activo.

Nivel de Vulnerabilidad Activo = $\sum$ (Nivel de vulnerabilidad)

#	Nombre del Activo	Probabilidad de ocurrencia	Nivel de Importancia.	Probabilidad de riesgo	Nivel de vulnerabilidad
1	Servidores Web	2	10	60	600
2	Bases de datos.	2	9	70	630

3	Servicios.	2	9	60	540
4	Software	2	8	70	560
5	Backus	3	9	80	720
6	Dispositivos de red	2	7	40	280
7	Personal	2	6	60	360
8	Documentación	3	9	70	630
9	Insumos	2	6	50	300
	Total	20	73	560	4620

Anexo VI

Control de la documentación

Para los documentos generados se debe documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

• Aprobar documentos apropiados antes de su emisión.

• Revisar y actualizar documentos cuando sea necesario y renovar su validez.

• Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.

• Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.

• Garantizar que los documentos se mantienen legibles y fácilmente identificables.

• Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.

• Garantizar que los documentos procedentes del exterior están identificados.

• Garantizar que la distribución de documentos está controlada.

• Prevenir la utilización de documentos obsoletos.

• Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

Los principales documentos a generar son

- Política de seguridad. Con las líneas generales que la organización desea seguir en seguridad.
- Inventario de activos. Con la descripción de los activos de información de la organización y su valoración para la misma.
- Análisis de riesgos. Con los valores de riesgo de cada uno de los activos.
- Documento de aplicabilidad. En el que se recoge para cada control de la Norma ISO 27001 si se aplica o no y la justificación para esa decisión.
- Procedimientos. Con la descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI.
- Registros. Son las evidencias de que se han realizado las tareas definidas para el SGSI. Son muy importantes de cara a poder medir la eficacia de las medidas implantadas así como a justificar las labores realizas frente a las auditorías del sistema (tanto internas como externas).
- Desarrollar los documentos para la implantación de los controles de acuerdo a las consideraciones necesarias.

Anexo VII

PROCESO DE CERTIFICACIÓN.

El proceso de certificación empieza con la elección de la empresa certificadora, en nuestro País es posible contar con tres compañías: BSI, BVQI, SGS. A la empresa certificadora debemos entregarles información que les permita estimar la duración de las fases de certificación, como puede ser: el alcance número de empleados en el SGSI, cantidad de activos, ubicaciones geográficas, si ya cuenta con otro sistema de gestión (ej. ISO 9001).

La certificación del SGSI bajo la norma ISO 27001:2005 consta de dos fases:

FASE I: Aquí se verifica el cumplimiento documental en base a una metodología que se adapte a la realidad de la empresa que solicita la certificación, y se puede detectar fallas medulares en la implementación. En esta fase el Auditor Externo debe emitir un informe favorable para continuar o no con la Auditoría de FASE II. Por lo general entre FASE I y FASE II no pude exceder más de 30 días, pero es el cliente quien propone las fechas exactas para llevar a cabo cada una de las FASES de la Auditoría.

FASE II: El objetivo de esta fase, es que la certificadora verifique objetivamente la implantación correcta del SGSI bajo todas las exigencias de la norma. El equipo de auditores mediante muestreo verificará el cumplimiento de todas o la mayoría de áreas dentro del alcance del SGSI.

Como auditado es necesario mantener a la mano todos los procedimientos, registros, formatos y acceso a sistemas que sirvan como evidencia del cumplimiento. El último día de la auditoría se lleva a cabo la reunión de cierre donde el Auditor Líder presenta el informe donde se especifica los hallazgos y se recomienda o no para la certificación.

Anexo VIII

INTERPRETACION DE RESULTADOS

VARIABLES

DEPENDIENTE

- ✓ Sistema de Gestión de Seguridad de la Información.

INDEPENDIENTE

- ✓ Guía Metodológica

OPERACIONALIZACIÓN DE LAS VARIABLES

Variable Dependiente: Sistema de Gestión de Seguridad

Conceptualización	Dimensión	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Es el conjunto de normas y reglas para administrar la información	Seguridad	Falta de seguridad	¿Cree que al conocer normas de seguridad se puede administrar la información? ¿Dentro de la norma ISO27001 se puede mantener segura la información?	Encuestas y Cuestionarios.

Variable Independiente: Guía Metodológica

Conceptualización	Dimensión	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Es el tratado en que se dan preceptos para orientar de forma metódica la seguridad de la información.	Metodología	Desconoce técnicas para respaldar la información Falta de Directrices	¿Existe una metodología para el Sistema de Gestión de seguridad en el DESITEL? ¿Al contar con una guía metodológica de gestión de seguridad, la información está protegida?	Encuestas y Cuestionarios.

MÉTODO CIENTÍFICO

El tema de Investigación se encuentra dentro del paradigma Crítico – Propositivo, porque se diagnostica y analiza el Sistema de Seguridad de la Información existente en el DESITEL y se formula una alternativa de solución a la falta de seguridad existente.

POBLACIÓN Y MUESTRA

POBLACIÓN

El presente estudio se realiza en el Departamento de Telemática y Sistema de la Escuela Superior Politécnica de Chimborazo cuya población entre el Director departamental y empleados suman 18.

MUESTRA

La población o universo es de 18 integrantes, por lo tanto, se trabaja con la misma cantidad por ser pequeña y no sobrepasar los 30.

PRESENTACIÓN DE RESULTADOS

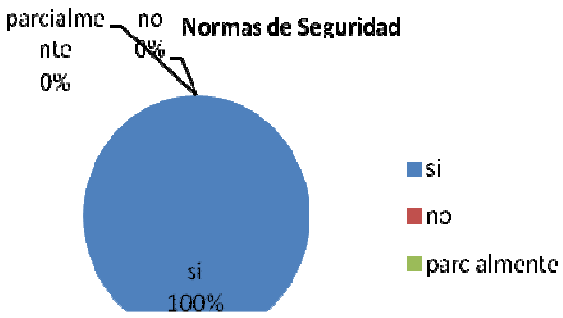
Una vez desarrollada la investigación se realiza el análisis respectivo, determinación de valores numéricos y su representación porcentualizada y gráfica de datos parciales y totales de las encuestas aplicadas.

RESPECTO A LAS ENCUESTAS DE EMPLEADOS

Pregunta 1 ¿Cree usted que las normas de seguridad contribuyen a mejorar y conservar la información del DESITEL?

CUADRO N° 01			
NORMAS DE SEGURIDAD			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
1	SI	18	100%
	NO	-	0%
	PARCIALMENTE	-	0%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 01



Análisis: El análisis demuestra que los 18 empleados encuestados que equivalente al 100% manifiestan que el conocimiento de las normas de seguridad contribuye a mejorar y conservar la información del DESITEL.

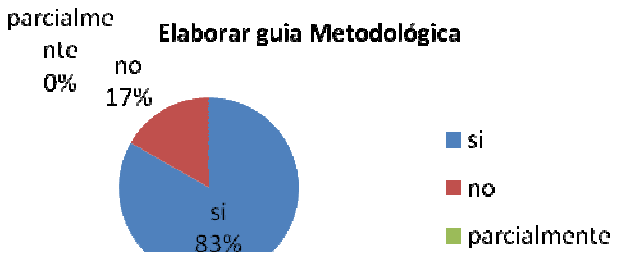
Interpretación: Del gráfico se deduce que hay aceptación por parte de los empleados del DESITEL en unificar los procesos para mejorar la seguridad de la información

Pregunta 2

¿Considera necesario contar con una guía metodológica para garantizar la protección de la información?

CUADRO N° 02			
Elaborar Metodología			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
2	SI	15	83%
	NO	3	17%
	PARCIALMENTE	-	0%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 02



Análisis: En base a los resultados obtenidos el 83% de los encuestados, expresan que contar con una metodología para garantizar la seguridad de la información servirá para garantizar el progreso de los objetivos del departamento

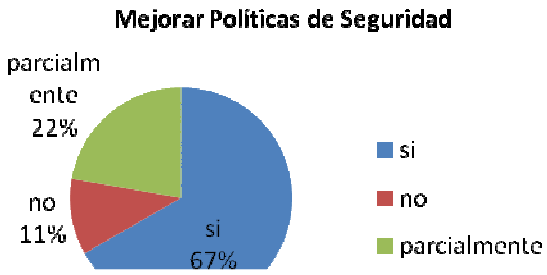
Interpretación: Existe aceptación para contar con metodología que se convierte el una herramienta de tratamiento a la seguridad de la información.

Pregunta 3

¿Considera que la estructura de la política de Seguridad establecida en el DESITEL mejorará su organización al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 03			
Mejorar la estructura de la organización			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
3	SI	12	67%
	NO	2	11%
	PARCIALMENTE	4	22%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 03



Análisis: El 67% de los encuestados manifiesta que al usar la metodología elaborada para la seguridad de la información en el DESITEL mejorará la estructura de la política de seguridad.

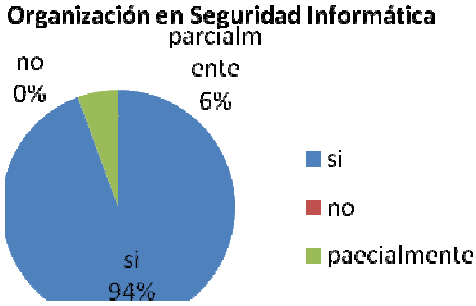
Interpretación: En base a la representación gráfica se indica que se tiene disponibilidad para la utilización de la metodología.

Pregunta 4

¿La Organización en seguridad informática alcanzará mejoras en su estructuración al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 04			
Organización de la Seguridad			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
4	SI	17	94%
	NO	-	0%
	PARCIALMENTE	1	6%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 04



Análisis: Con un porcentaje equivalente al 94% se concluye que la estructuración de la seguridad física del departamento alcanzará niveles eficientes de seguridad.

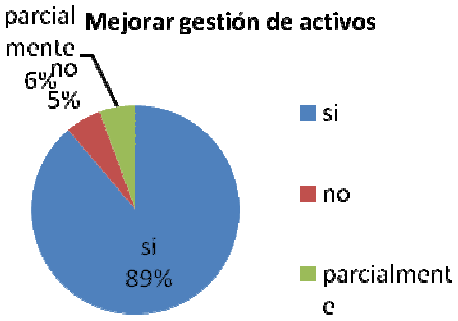
Interpretación: Del gráfico se deduce que los empleados al conocer la metodología elaborada, confían en que al utilizarla se mejorará la estructuración de la seguridad física del departamento

Pregunta 5

¿La Gestión de activos para el DESITEL mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 05			
Gestión de Activos			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
5	SI	16	89%
	NO	1	6%
	PARCIALMENTE	1	5%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 05



Análisis: El 89% de los encuestados aprueba la seguridad de la gestión de activos al utilizar la metodología elaborada.

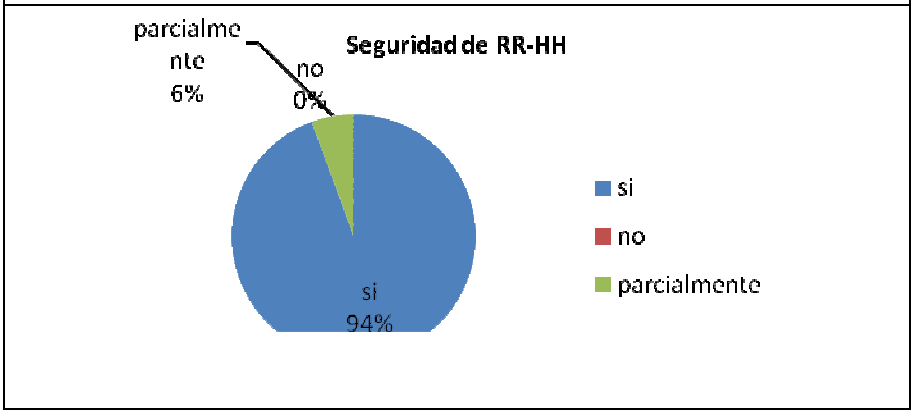
Interpretación: Del gráfico se deduce que al conocer la metodología elaborada aprueban sus contenidos en la seguridad de la gestión de activos.

Pregunta 6

¿La Seguridad de los Recursos Humanos del Departamento mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 06			
Seguridad de los RRHH			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
6	SI	17	94%
	NO	-	0%
	PARCIALMENTE	1	6%
TOTAL:		18	
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 06



Análisis: La seguridad de los RRHH garantiza un 94% de aceptación el conocer la estructuración de la metodología en este aspecto.

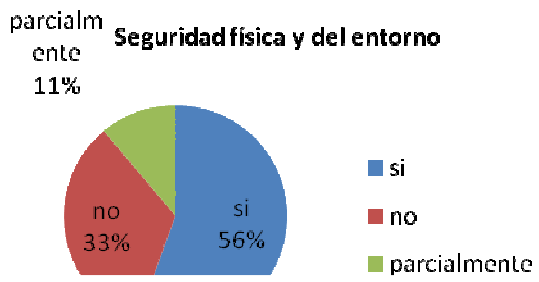
Interpretación: Por intermedio de la representación gráfica se deduce que, los empleados del DESITEL aprueban mejorar la seguridad de los RRHH a través de la utilización de la metodología elaborada.

Pregunta 7

¿La Seguridad física y del entorno del departamento mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 07			
Seguridad física y del entorno			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
7	SI	10	56%
	NO	6	33%
	PARCIALMENTE	2	11%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 07



Análisis: El 56% de los empleados manifiestan que se podrá mejorar la seguridad física del departamento.

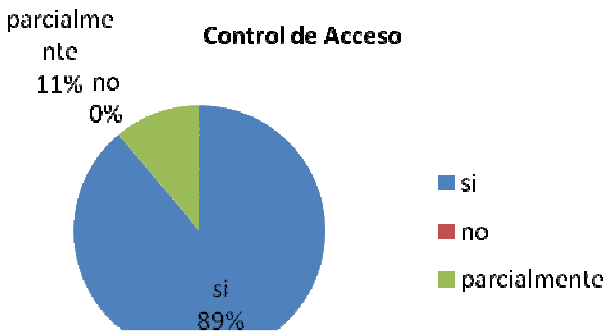
Interpretación: En base al gráfico se puede deducir los empleados en su mayoría piensan que se puede mejorar la seguridad física del departamento al cumplir con los controles para este aspecto de la metodología elaborada.

Pregunta 8

¿El Control de acceso a toda la información mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 08			
Control de Acceso			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
8	SI	16	89%
	NO	-	0%
	PARCIALMENTE	2	11%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 08

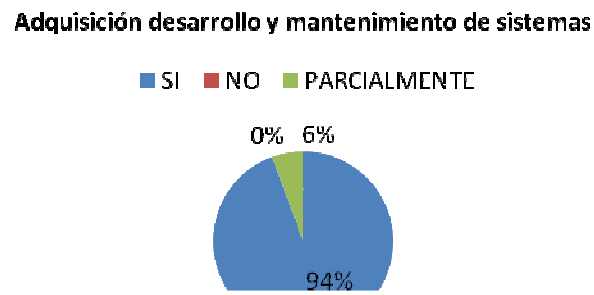


Pregunta 9

¿La Adquisición, Desarrollo y mantenimiento de sistemas mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 09			
Adquisición, Desarrollo y mantenimiento de sistemas			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
9	SI	17	94%
	NO	-	0%
	PARCIALMENTE	1	6%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 09



Pregunta 10

¿La Gestión de comunicaciones y operaciones mejorará los niveles de seguridad al utilizar la metodología elaborada según ISO 27001?

CUADRO N° 10			
Gestión de comunicaciones y operaciones			
ÍTEM	CATEGORÍA	FRECUENCIA	PORCENTAJE
10	SI	18	100%
	NO	-	0%
	PARCIALMENTE	-	0%
TOTAL:		18	100%
Fuente: Encuesta dirigida a Empleados Elaborado por: Gavilanes Verónica			

GRÁFICO # 10

BIBLIOGRAFÍA

· ALEXANDER A., Diseño de un Sistema de Gestión de Seguridad., Alfaomega., Bogota_Colombia,. 2007., pp170-200.

· BETARTE M. E. Corti, R. de la Fuente. Hacia una Implementación Exitosa de un SGSI. En Actas del 3º Congreso Iberoamericano de seguridad Informática (CIBSI'05), 2005., pp. 457–471.

· BRAVAL, E. Ingeniería de Software. 2ª Edición. Mexico: McGraw – Hill, 2002. Pp.425-470.

· COMISIÓN DE REGLAMENTOS TÉCNICOS. Norma Técnica Peruana NPT-ISO/ IEC 17799, .2007. 2ª .Edición.

· CORTI, M. Análisis y automatización de la implantación de SGSI en Empresas. Universidad de la República, Facultad de Ingeniería, 2008.

· FEDERAL OFFICE for Information security - Germany. BSI Standard 100-2 IT Grundschutz Methodology, 04 2009.

· INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques - Information security risk management (ISO/IEC 27005:2008), 2005.

· National Institute Of Standards and Technology. Recommended Security Controls for Federal Information Systemas NIST Special Publication 800-53. 2ª. Edición. 2007.

BIBLIOGRAFÍA DE INTERNET

- **Artículo de Seguridad Informática.**

  http://www.inforc.ec/inforc/imgs/favicon.ico

- **Modelo de seguridad informática basado en normas de gestión.**

  http://www.arcert.gov.ar/politica/modelo.html

- **Principio de políticas de seguridad de la información.**

  http://www.ssi.unc.edu.ar/Politicas/PoliticasSeguridad_4.html

- **Manual de seguridad de la información para usuarios.**

  http://www.seguridadinformacion.com/seguinfo.php