



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE INGENIERO EN SISTEMAS

TEMA: DESARROLLO DE UN MODELO DE SISTEMA DE  
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)  
BASADO EN LAS MEJORES PRÁCTICAS DE SEGURIDAD  
INFORMÁTICA PARA LA AGENCIA DE REGULACIÓN Y  
CONTROL HIDROCARBURÍFERO.

AUTORES: MONCAYO ZAMBRANO NÉSTOR RICARDO,  
GUAMÁN YUCAZA PAULINA PATRICIA

DIRECTOR: ING. DE LA TORRE ARTURO

SANGOLQUÍ

2016



DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN  
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

**CERTIFICACIÓN**

Certifico que el trabajo de titulación, "DESARROLLO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA PARA LA AGENCIA DE REGULACIÓN Y CONTROL HIDROCARBURÍFERO" realizado por los señores **GUAMÁN YUCAZA PAULINA PATRICIA Y MONCAYO ZAMBRANO NÉSTOR RICARDO**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores **GUAMÁN YUCAZA PAULINA PATRICIA Y MONCAYO ZAMBRANO NÉSTOR RICARDO** para que lo sustente públicamente.

Sangolquí, 15 de diciembre del 2015

Atentamente,



ING. ARTURO DE LA TORRE  
DIRECTOR



**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN  
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**AUTORÍA DE RESPONSABILIDAD**

Nosotros, **GUAMÁN YUCAZA PAULINA PATRICIA** con cédula de identidad N°1715924211 y **MONCAYO ZAMBRANO NÉSTOR RICARDO** con cédula de identidad N° 1711328870, declaramos que este trabajo de titulación "DESARROLLO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA PARA LA AGENCIA DE REGULACIÓN Y CONTROL HIDROCARBURÍFERO" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

**Sangolquí, 13 de Enero del 2016**

GUAMÁN YUCAZA PAULINA PATRICIA

C.C. 1715924211

MONCAYO ZAMBRANO NÉSTOR RICARDO

C.C. 1711328870




**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN  
CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**AUTORIZACIÓN**

Nosotros, **GUAMÁN YUCAZA PAULINA PATRICIA** y **MONCAYO ZAMBRANO NÉSTOR RICARDO**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "DESARROLLO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LAS MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA PARA LA AGENCIA DE REGULACIÓN Y CONTROL HIDROCARBURÍFERO" cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

**Sangolquí, 13 de Enero del 2016**

  
-----  
GUAMÁN YUCAZA PAULINA PATRICIA  
C.C. 1715924211

  
-----  
MONCAYO ZAMBRANO NÉSTOR RICARDO  
C.C. 1711328870

## DEDICATORIA

*Esta tesis la dedicamos a nuestras familias por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles.*

*Nos han dado todo lo que somos como personas, nuestros valores, nuestros principios, nuestro carácter, nuestro empeño, nuestra perseverancia, nuestro coraje para conseguir nuestros objetivos.*

*“La dicha de la vida consiste en tener siempre algo que hacer, alguien a quien amar y alguna cosa que esperar”.*

*Néstor y Paulina*

## AGRADECIMIENTO

*En primera instancia agradecemos a nuestros formadores, personas de gran sabiduría quienes se han esforzado por ayudarnos a llegar al punto en el que nos encontramos.*

*Sencillo no ha sido el proceso, pero gracias a las ganas de transmitirnos sus conocimientos y dedicación que los ha regido, hemos logrado importantes objetivos como culminar el desarrollo de nuestra tesis con éxito y obtener una afable titulación profesional.*

*Néstor y Paulina*

## ÍNDICE DE CONTENIDO

CARÁTULA	
CERTIFICACIÓN .....	..ii
AUTORIA DE RESPONSABILIDAD.....	..iii
AUTORIZACIÓN.....	..iv
DEDICATORIA .....	..v
AGRADECIMIENTO .....	..vi
INDICE .....	..vii
INDICE DE TABLAS.....	..xi
INDICE DE FIGURAS.....	..xii
RESUMEN.....	..xiii
SUMMARY .....	..xiv
<b>CAPÍTULO I</b>	<b>1</b>
<b>INTRODUCCIÓN</b>	
1.1 Descripción del Problema .....	3
1.2 Justificación .....	..4
1.3 Antecedentes.....	..5
1.4 Objetivos.....	6
1.4.1 Objetivo General .....	6
1.4.1 Objetivo Específicos .....	6
1.5 Alcance .....	7
1.6 Factibilidad .....	7
1.6.1 Factibilidad Técnica.....	7

1.6.2 Factibilidad Económica .....	9
1.6.3 Factibilidad Legal .....	10
1.6.4 Factibilidad Operacional .....	19
<b>CAPÍTULO II</b> .....	<b>20</b>
2.1 Las buenas prácticas de COBIT .....	20
2.1.1 Planificación y organización: .....	22
2.1.2 Adquisición e implementación: .....	23
2.1.3 Soporte y servicio: .....	23
2.1.4 Monitoreo: .....	24
2.1.5 Usuario: .....	24
2.1.6 Características:.....	25
2.1.7 Principios:.....	26
2.1.8 Requerimientos fiduciarios: .....	26
2.1.9 Requerimientos de seguridad:.....	27
2.2 Las buenas prácticas de ITIL .....	28
2.2.1 Gestión de servicios de tecnologías de la información.....	31
2.2.2 Las buenas prácticas de itil - mejores prácticas .....	32
2.2.3 Beneficios de las buenas prácticas de itil .....	33
2.2.4 Características de las buenas prácticas de itil.....	34
2.2.5 Las buenas prácticas de itil versión 2.0.....	35
2.2.6 Planeación para la implementación de la administración: .....	35
2.2.7 Administración de infraestructura: .....	36



2.2.8 Perspectiva del negocio: .....	36
2.2.9 Administración de aplicaciones: .....	36
2.2.10 Administración de seguridad:.....	36
2.2.11 Administración o gestión de servicios de ti: .....	37
2.2.12 Procesos de gestión de servicios.....	38
2.3 ISO/IEC 27001:2007.....	38
2.3.1 ISO 27001 .....	39
2.3.2 Sistema de gestión de la seguridad de la información .....	40
2.3.3 Controles .....	41
2.3.4 Política de seguridad. ....	42
2.3.5 Organización de la información de seguridad. ....	42
2.3.6 Administración de recursos .....	42
2.3.7 Seguridad de los recursos humanos. ....	43
2.3.8 Seguridad física y del entorno .....	43
2.3.9 ¿Quiénes la utilizan? .....	44
2.3.10 Beneficios .....	44
2.3.11 Implementación.....	45
<b>CAPÍTULO III</b> .....	<b>47</b>
3.1 Las Buenas Prácticas de COBIT .....	47
3.1.1 Administración de las tecnologías de la información .....	47
3.1.2 Control de las tecnologías de la información .....	50
3.1.3 Control de proveedores tecnológicos .....	54

3.2 Normas ISO 27001.....	55
3.2.1 Uso de la norma iso 27001.....	56
3.2.2 Administración y control de la seguridad de la información.....	62
3.2.3 Planes de continuidad de negocios.....	64
3.3 Las buenas prácticas de ITIL.....	65
3.3.1 Administración y control en la entrega de servicios tecnológicos.....	66
3.3.2 Gestión de la información.....	77
3.4 Análisis comparativo.....	77
3.5 Secuencia de los dominios de actividades.....	85
<b>CAPÍTULO IV</b>	<b>86</b>
Metodología con las mejores prácticas para la implementación del sgsi.....	87
4.1 Alinear la estrategia del servicio con la estrategia del negocio.....	89
4.2 Establecer la estrategia del servicio (políticas).....	105
4.3 Identificación del riesgo en la agencia.....	121
4.4 Planificación del tratamiento del riesgo.....	134
4.5 Implementación de los servicios prioritarios.....	135
4.6 Revisión periódica en la agencia.....	143
4.7 Planes de continuidad en la agencia.....	147
5.1 Conclusiones.....	188
5.2 Recomendaciones.....	189
Referencias.....	190
Bibliografía.....	191

## ÍNDICE DE TABLAS

Tabla 1. Presupuesto de la Realización de la Tesis.....	9
Tabla 2. Tabla de Planificación .....	78
Tabla 3. Tabla de Implementación .....	79
Tabla 4. Tabla de Servicios .....	80
Tabla 5. Tabla de Riesgos .....	81
Tabla 6. Tabla de Evaluación .....	82
Tabla 7. Tabla de Control.....	83
Tabla 8. Informe de Conformación del comité de seguridad .....	93
Tabla 9. Procedimiento para Definir la Información.....	151
Tabla 10. Protección de Registro de Información .....	156
Tabla 11. Tabla de Equipos de Seguridad Perimetral.....	163
Tabla 12. Licenciamiento y módulos de servicios del Sistema.....	165
Tabla 13. Licenciamiento y módulos de servicios del Sistema.....	166
Tabla 14. Licenciamiento del Sistema de registro y análisis del Sistema ...	167
Tabla 15: Planteamiento LAN .....	169
Tabla 16. Host de Administrativo .....	170
Tabla 17: Host Financiero .....	170
Tabla 18. Host Invitado.....	171
Tabla 19. Host.....	171
Tabla 20: Identificación de los Objetivos .....	172
Tabla 21. Diccionario de datos de la red institucional .....	173
Tabla 22. Tabla de Rutas Estáticas de Firewall .....	175

## ÍNDICE DE FIGURAS

Figura 1. Las buenas prácticas de ITIL .....	35
Figura 2. Procesos de Las buenas prácticas de COBIT .....	55
Figura 3. Fases de ISO 27000 .....	56
Figura 4: Autorización de la Máxima Autoridad.....	88
Figura 5. Compromiso de la máxima autoridad .....	90
Figura 6. Difusión del Esquema Gubernamental de Seguridad .....	91
Figura 7. Coordinación de la Gestión de la Seguridad de la Información.....	92
Figura 8. Designación del Oficial del Seguridad de la Información.....	95
Figura 9. Proceso de Autorización de nuevos Servicios de Procesamiento	96
Figura 10. Acuerdos de Confidencialidad .....	97
Figura 11: Modelo de Seguimiento de puesta en Marcha del EGSI.....	99
Figura 12. Memorando conformación de comité y oficial de seguridad.....	103
Figura 13. Acta de Reuniones.....	104
Figura 14. Planificación del Tratamiento del Riesgo .....	109
Figura 15. Tabla de permisos a usuarios en la Gestión de Privilegios.....	112
Figura 16: Matriz de Análisis de Riesgo Datos Solicitados .....	122
Figura 17: Matriz de Análisis de Riesgo de los Sistemas Informáticos.....	123
Figura 18: Matriz de Análisis de Riesgos del Personal.....	124
Figura 19: Análisis de Riesgo Promedio .....	125
Figura 20: Análisis factores de Riesgo .....	125
Figura 21: Fuente de valores.....	126

Figura 22. Uso Aceptable de Activos .....	129
Figura 23: Reglamento para el uso adecuado del servicio de internet .....	132
Figura 24. Reglamento del uso de acceso a Internet.....	133
Figura 25. Tratamiento del riesgo en el SGSI. ....	135
Figura 26. Implementación de Servicios Prioritarios .....	136
Figura 27. Revisión Periódica .....	143
Figura 28: Ficha de mantenimiento preventivo .....	147
Figura 29: Procedimiento de Algoritmo Cifrado .....	152
Figura 30. Registro de Fallas .....	158
Figura 31. Diagrama de red Situación Actual de la ARCH.....	162
Figura 33. Arquitectura del sistema de seguridad perimetral. ....	164
Figura 34. Licenciamiento y módulos de servicios del Sistema .....	166
Figura 35. Licenciamiento del Sistema de registro y análisis del Sistema..	167
Figura 36: Configuración de un Gateway para una LAN .....	168
Figura 37. Conexión remota .....	169
Figura 38. Servidor de Dominios .....	179
Figura 39. Tabla de permisos a usuarios .....	179
Figura 40: Servicio FTP .....	180
Figura 41: Configuración de un Proxy .....	181
Figura 42. Identificación de equipos conectados .....	182
Figura 43: servidor SNMP .....	182
Figura 44: Protocolo Https .....	183
Figura 45: Protocolo NTP.....	185

## **RESUMEN**

El desarrollo de un modelo de sistema de gestión de la seguridad de la información (SGSI) basado en las mejores prácticas de Seguridad Informática, se enfoca en la investigación del estado actual de los datos y la información que se encuentra en la Agencia de Regulación y Control Hidrocarburífero (ARCH) lo que permitió identificar riesgos a los cuales está expuesta la organización. Esta Metodología fue diseñada para asegurar los controles de seguridad de los activos de información, tomando como base la ISO / IEC 27001:2007 y el Acuerdo 166 de la Secretaría Nacional de la Administración Pública de la República del Ecuador. Esta propuesta de Metodología considera que las TIC son herramientas imprescindibles para el desempeño de institucional e interinstitucional, y como respuesta a la necesidad de gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, en base a los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante estos acuerdo se determinó que las entidades gubernamentales presten mayor atención a la protección de sus datos, con el fin de generar un resultado de confianza en la seguridad de la información de las instituciones públicas y así minimizar riesgos derivados de vulnerabilidades informáticas.

### **PALABRAS CLAVES**

- **SEGURIDAD DE LA INFORMACIÓN,**
- **ACTIVOS DE LA INFORMACIÓN,**
- **POLÍTICAS**
- **RIESGOS**

## **SUMMARY**

The development of a model for information security management system (ISMS) based on the best information security practices, focuses on the current state of research data and information found on the Agency for Regulation and Control Hydrocarbon (ARCH) which identified risks to which the organization is exposed. This methodology was designed to ensure security controls of information assets, based on the ISO / IEC 27001: 2007 and the Agreement 166 of the National Secretariat for Public Administration of the Republic of Ecuador. This proposed methodology considers that ICT is indispensable for the performance of institutional and inter-institutional tools, and in response to the need to manage in an efficient and effective information security in public entities, based on the issuance of Agreements Ministerial No. 804 and No. 837 of 29 July and 19 August 2011 respectively, by this agreement it is determined that government entities pay greater attention to the protection of their data.

### **KEYWORDS**

- **SECURITY OF THE INFORMATION,**
- **INFORMATION ASSETS,**
- **POLICIES**
- **RISKS**

## CAPÍTULO I

### 1. Introducción

Hoy en día el principal activo de la agencia ARCH es la información, los datos han pasado a ser elementos valiosos a nivel empresarial, pero a la vez vulnerables y/o violables. La posibilidad de interconectarse a nivel mundial a través de redes, se ha convertido en un mecanismo que ofrece a la agencia ARCH obtener mejoras tanto en productividad como en competitividad toda esta comunicación ha llevado consigo nuevas amenazas latentes para los sistemas de información y la protección de datos.

Adicionalmente hay que considerar que muchas instituciones públicas o privadas deben afrontar la Seguridad de forma metodológica con una planificación concreta, donde la visión es la mejora continua y la continuidad del negocio, todo esto conlleva a la necesidad de efectuar controles que garanticen de manera razonable la disponibilidad, confidencialidad e integridad de la información, como parte de esta protección la seguridad de la información involucra la implementación de estrategias y la instauración de políticas de seguridad para resguardar los procesos.

La elaboración de un modelo de SGSI se enfoca en la investigación continua para conocer el estado de la gestión de la seguridad de la



información en el ARCH e identificar los riesgos a los que están expuestos. Con este propósito, se pretende elaborar un modelo de sistema de gestión de la seguridad de la información (SGSI) el cual será diseñado para asegurar con controles de seguridad los activos de información, tomando como base la ISO/IEC 27001:2007 y el Acuerdo 166 de la Secretaría Nacional de la Administración Pública de la República del Ecuador.

La Secretaría Nacional de Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño de institucional e interinstitucional, y como respuesta a la necesidad gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación.

La comisión realizará un análisis de la situación respecto de la gestión de la Seguridad de la Información en las Instituciones de la Administración Pública Central, Dependiente e Institucional, llegando a determinar la necesidad de aplicar normas y procedimientos para seguridad de la información, e incorporar a la cultura y procesos institucionales la gestión permanente de la misma.

El Esquema Gubernamental de Seguridad de la Información (EGSI), está basado en la norma técnica ecuatoriana INEN ISO/IEC 27002 para Gestión

de la Seguridad de la Información y está dirigido a las Instituciones de la Administración Pública Central, Dependiente e Institucional.

El EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices.

La implementación del EGSI incrementará la seguridad de la información en las entidades públicas así como en la confianza de los ciudadanos en la Administración Pública.

## **1.1 Descripción del problema**

La Agencia de Regulación y Control Hidrocarburífero, ARCH, creada el 27 de julio del 2010 como una institución de derecho público, con personalidad jurídica, autonomía administrativa, técnica, económica, financiera y patrimonio propio, según cita el artículo 5 de la Ley Reformatoria a la Ley de Hidrocarburos y a la Ley de Régimen Tributario Interno, publicada en el Suplemento del Registro Oficial No. 244, ha experimentado un vertiginoso crecimiento tanto en su parte física como también en el manejo de su información lo cual ha provocado que se requiera de controles, políticas y normas para prevenir el acceso no autorizado, evitar

modificaciones de la información por parte de personal no autorizado y proporcionar acceso seguro en el momento en que se precisa.

En la actualidad en la Agencia de Regulación y Control Hidrocarburífero no se cuenta con controles que estandaricen o prevean las amenazas y vulnerabilidades para salvaguardar los datos de empresa por lo que se busca diseñar un mecanismo que logre regular, gestionar y mitigar al máximo los riesgos informáticos y establecer los requerimientos de la seguridad que nos permitan evitar pérdida de tiempo, dinero e información sensible para la institución.

## **1.2 Justificación**

Debido que en la Agencia de Regulación y Control Hidrocarburífero no existe al momento normas ni políticas que salvaguarden a la información tanto de las amenazas como vulnerabilidades, en el caso de que se presente un incidente no se cuenta con planes establecidos y definidos para la mitigación de riesgos, es importante que a través del desarrollo de este proyecto se recomiende algunas buenas prácticas para salvaguardar la información.

Y es por ello, que es vital para la organización tener una metodología que permita evaluar y administrar la seguridad de la información, todo esto debidamente documentado bajo las normas establecidas por las leyes del

Gobierno Ecuatoriano cumpliendo con disposiciones legales en el Acuerdo 166 de la Secretaría Nacional de la Administración Pública de la República del Ecuador.

### **1.3 Antecedentes**

Un sistema de gestión de la seguridad de la información (SGSI) (en inglés: information security management system, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para la agencia el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

La Agencia de Regulación y Control Hidrocarburífero, cumple con el control técnico de hidrocarburos, fiscalización de la comercialización de GLP y Gas natural así como el control técnico de la comercialización de derivados

del petróleo. Además mantiene trámites de infracciones y coactivas y la coordinación en general de la refinación e industrialización. Para todo ello no ha implementado un sistema de gestión de la seguridad de la información que sería de gran utilidad para la ARCH.

## **1.4 Objetivos**

### **1.4.1. Objetivo General**

Desarrollar un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) basado en las mejores prácticas de Seguridad Informática para la Agencia de Regulación y Control Hidrocarburífero.

### **1.4.1. Objetivos Específicos:**

- Analizar la situación actual de la ARCH dentro del concepto de seguridad informática.
- Desarrollar una metodología en la cual se apliquen las mejores prácticas de la norma ISO 27001:2007, las buenas prácticas de COBIT e las buenas prácticas de ITIL aplicables en la Agencia de Regulación y Control Hidrocarburífero.
- Analizar los riesgos informáticos de la institución
- Describir y documentar las políticas de seguridad de la información para mitigar el riesgo informático.

## **1.5 Alcance**

El desarrollo de este sistema de seguridad de la información aplicado a la Agencia de Regulación y Control Hidrocarburífero ayudará a prevenir la fuga de información, pérdida total y parcial de los servidores o sistemas computacionales, modificación y reutilización de datos y a implementar políticas de seguridad para la prevención de desastres.

## **1.6 Factibilidad**

### **1.6.1 Factibilidad Técnica**

Para la realización del presente proyecto se tiene el apoyo de la Dirección Informática del ARCH en cuanto a la facilidad de proporcionar información respecto a los elementos importantes y fundamentales que tiene el Centro de Datos de la Información y al levantamiento de los procesos como realmente se están realizando en la actualidad.

#### ➤ Tamaño del Producto

- Factores determinantes del Tamaño
  - Mercado
  - Disponibilidad de Recursos
  - Disponibilidad de Recursos Humanos
  - Disponibilidad de Materia Prima

- Capacidad del Proyecto
- Localización el Proyecto
  - Macro Localización
    - Justificación
    - Plano
  - Micro localización
    - Factores Locacionales
      - Medios de Transporte
      - Atractivos Turísticos
      - Estructura Impositiva y Legal
      - Factores Ambientales
      - Disponibilidad de Servicios Básicos
      - Posibilidad de Eliminación de Desechos
      - Disponibilidad de Infraestructura Física
- Ingeniería del Proyecto
  - Diagrama de Flujo
  - Proceso de producción, Organigrama
  - Requerimiento de Recurso Humano
  - Requerimiento de Activos, Materiales e Insumos
  - Estimación de Costos de Inversión
  - Calendario de Ejecución del Proyecto

## 1.6.2 Factibilidad Económica

A continuación se presenta el Presupuesto para el desarrollo de la Tesis, cuyo financiamiento estará a cargo de los postulantes, por lo que el trabajo es factible de realizarse, tal como se indica en la tabla 1.

**Tabla 1.**  
**Presupuesto de la Realización de la Tesis**

<b>PRESUPUESTO DE LA REALIZACIÓN DE LA TESIS</b>				
<b>1 INGRESOS</b>				
	<b>RUBRO</b>	<b>VALOR</b>	<b>UNIDADES</b>	<b>SUBTOTAL</b>
1.1	APORTE TESISISTAS	1200.00		1200.00
<b>TOTAL</b>				<b>1200.00</b>
<b>2 EGRESOS</b>				
	<b>2.1 PERSONAL</b>	<b>VALOR</b>	<b>UNIDADES</b>	<b>SUBTOTAL</b>
2.1.01	DEDICACION DEL TESISISTA (Medio Tiempo)		24 Semanas	58
<b>SUBTOTAL PERSONAL</b>				
	<b>2.2 RECURSOS FISICOS Y OTROS</b>	<b>VALOR</b>	<b>UNIDADES</b>	<b>SUBTOTAL</b>
2.2.01	MATERIAL BIBLIOG. Y DIDACT.	86.00		86.00
2.2.02	Gastos OFICINA Y COPIAS	456.00	6 Meses	456.00
2.2.07	EQUIPOS	600.00	6 Meses	600.00
<b>SUBTOTAL RECURSOS FÍSICOS Y OTROS</b>				<b>1200.00</b>
<b>TOTAL EGRESOS</b>				<b>1200.00</b>



### **1.6.3 Factibilidad Legal**

El tema a ser desarrollado se basa en la Norma ISO/ IEC 27001 y el Acuerdo 166 lo cual es solicitado por la SNAP de la República del Ecuador para las instituciones del estado.

#### **Sistema de la Gestión de la Seguridad de la Información**

**Acuerdo Ministerial 166**

**Registro Oficial Suplemento 88 de 25-Sep-2013**

Que, la Constitución de la República determina en el artículo 227 que la Administración Pública constituye un servicio a la colectividad que se rige por principios de eficacia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.

Que, el artículo 13 del Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva establece que la Secretaría Nacional de la Administración Pública es una entidad de derecho público, con personalidad jurídica y patrimonio propio, dotada de autonomía presupuestaria, financiera, económica y administrativa, encargada de establecer las políticas, metodologías de gestión e innovación institucional y herramientas necesarias para el mejoramiento de la eficiencia, calidad y transparencia de la gestión en las entidades y organismos de la Función Ejecutiva, con quienes coordinará las acciones que sean necesarias para la

correcta ejecución de dichos fines; así como también de realizar el control, seguimiento y evaluación de la gestión de los planes, programas, proyectos y procesos de las entidades y organismos de la Función Ejecutiva que se encuentran en ejecución; y, el control, seguimiento y evaluación de la calidad en la gestión de los mismos.

Que, mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

Que, es importante adoptar políticas, estrategias, normas, procesos, procedimientos, tecnologías y medios necesarios para mantener la seguridad en la información que se genera y custodia en diferentes medios y formatos de las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Que, la Administración Pública de forma integral y coordinada debe propender a minimizar o anular riesgos en la información así como proteger la infraestructura gubernamental, más aún si es estratégica, de los denominados ataques informáticos o cibernéticos.

Que, las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional e interinstitucional de la Administración Pública en tal virtud, deben cumplir con estándares de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información;

Que, la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación en referencia ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI), elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

Que, el artículo 15, letra i) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva establece como atribución del Secretario Nacional de la Administración Pública, impulsar proyectos de estandarización en procesos, calidad y tecnologías de la información y comunicación;

En uso de las facultades y atribuciones que le confiere el artículo 15, letra n) del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva. Acuerda:

Art. 1.- Disponer a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Art. 2.- Las entidades de la Administración Pública implementarán en un plazo de dieciocho (18) meses el Esquema Gubernamental de Seguridad de la Información (EGSI), que se adjunta a este acuerdo como Anexo 1, a excepción de las disposiciones o normas marcadas como prioritarias en dicho esquema, las cuales se implementarán en (6) meses desde la emisión del presente Acuerdo.

La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.

Art. 3.- Las entidades designarán, al interior de su institución, un Comité de Seguridad de la Información liderado con un Oficial de Seguridad de la Información, conforme lo establece el EGSI y cuya designación deberá

ser comunicada a la Secretaría Nacional de la Administración Pública, en el transcurso de treinta (30) días posteriores a la emisión del presente Acuerdo.

Art. 4.- La Secretaría Nacional de la Administración Pública coordinará y dará seguimiento a la implementación del EGSI en las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva. El seguimiento y control a la implementación de la EGSI se realizará mediante el Sistema de Gestión por Resultados (GPR) u otras herramientas que para el efecto implemente la Secretaría Nacional de la Administración Pública.

Art. 5.- La Secretaría Nacional de la Administración Pública realizará de forma ordinaria una revisión anual del EGSI en conformidad a las modificaciones de la norma INEN ISO/IEC 27002 que se generen y de forma extraordinaria o periódica cuando las circunstancias así lo ameriten, además definirá los procedimientos o metodologías para su actualización, implementación, seguimiento y control.

Art. 6.- Es responsabilidad de la máxima autoridad de cada entidad mantener la documentación de la implementación del EGSI debidamente organizada y registrada de acuerdo al procedimiento específico que para estos efectos establezca la Secretaría Nacional de la Administración Pública.

Art. 7.- Las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos de su institución, en base a la norma INEN ISO/IEC 27005 "Gestión del Riesgo en la Seguridad de la Información.

**Disposiciones Generales:**

Primera.- El EGSI podrá ser revisado periódicamente de acuerdo a las sugerencias u observaciones realizadas por las entidades de la Administración Pública Central, Institucional o que dependen de la Función Ejecutiva, las cuales deberán ser presentadas por escrito a la Secretaría Nacional de la Administración Pública.

Segunda.- Cualquier propuesta de inclusión de controles o directrices adicionales a los ya establecidos en el EGSI que se generen en la implementación del mismo, deberán ser comunicados a la Secretaría Nacional de la Administración Pública, previo a su aplicación; de igual manera, en caso de existir alguna excepción institucional respecto a la implementación del EGSI, ésta deberá ser justificada técnicamente y comunicada a la Secretaría Nacional de la Administración Pública, para su análisis y autorización.

Tercera.- Los Oficiales de Seguridad de la Información de los Comités de Gestión de Seguridad de la Información designados por las instituciones,

actuarán como contrapartes de la Secretaría Nacional de la Administración Pública en la implementación del EGSI y en la gestión de incidentes de seguridad de la información.

Cuarta.- Cualquier comunicación respecto a las disposiciones realizadas en el presente Acuerdo deberá ser informada directamente a la Subsecretaría de Gobierno Electrónico de la Secretaría Nacional de la Administración Pública.

#### **Disposiciones Transitorias:**

Primera.- Para efectivizar el control y seguimiento del EGSI institucional, la Secretaría Nacional de la Administración Pública en un plazo de quince (15) días creará un proyecto en el sistema GPR en el que se homogenice los hitos que deben de cumplir las instituciones para implementar el EGSI.

Segunda.- La Secretaría Nacional de la Administración Pública emitirá en el plazo de sesenta (60) días desde la emisión del presente Acuerdo los lineamientos específicos de registro y documentación de la implementación institucional del ESGI.

Tercera.- La Secretaría Nacional de la Administración Pública, además, en un plazo de noventa (90) días desde la emisión del presente

Acuerdo, definirá las metodologías o procedimientos para actualización, implementación, seguimiento y control del EGSI.

**Disposición Derogatoria:**

Deróguense los Acuerdo Ministeriales No. 804 de 29 de julio de 2011 y No. 837 de 19 de agosto de 2011.

**Disposición Final:**

Este Acuerdo entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado en el Palacio Nacional, a los 19 días del mes de septiembre de 2013.

f.) Cristian Castillo Peñaherrera, Secretario Nacional de la Administración Pública. Es fiel copia del original.- LO CERTIFICO. Quito, 20 de septiembre de 2013.

f.) Dra. Rafaela Hurtado Espinoza, Coordinadora General de Asesoría Jurídica, Secretaría Nacional de la Administración Pública.

Además de las leyes y normas de la gestión de los datos e información en el gobierno.

- Constitución de la República del Ecuador



- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley del Sistema Nacional de Registro de Datos Públicos
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública
- Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública
- Otras normas cuya materia trate sobre la gestión de los activos de información en las entidades de la Administración Pública

#### **1.6.4 Factibilidad Operacional**

La realización de esta tesis se basa en la investigación, es por eso que con las bases obtenidas a lo largo de la carrera y con el planteamiento descrito se pretende asegurar el éxito del trabajo, se cuenta con el apoyo de la Dirección de Tecnologías de la información de la Agencia de Regulación y

Control Hidrocarburífero. Los resultados obtenidos serán de gran apoyo y beneficio para la misma.

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **2.1 Las buenas prácticas de COBIT**

La evaluación de los requerimientos del negocio, los recursos y procesos Tecnologías de la Información, son puntos bastante importantes para el buen funcionamiento de la Agencia Nacional y para el aseguramiento de su supervivencia en el mercado.

“El modelo las buenas prácticas de COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de la agencia, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.” (Brito, 2004)

El modelo las buenas prácticas de COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de sus procesos de negocios y la seguridad Tecnologías de la Información y que abarca controles específicos de Tecnologías de la Información desde una perspectiva de negocios.

Las buenas prácticas de COBIT significa Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (Control Objectives for Information Systems and related Technology). El modelo es el resultado

de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association).

Fue lanzado en 1996, es una herramienta de gobierno de tecnologías que ha cambiado la forma en que trabajan los profesionales de tecnología.

Vinculando tecnología informática y prácticas de control, en el modelo las buenas prácticas de COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para los profesionales de control la gerencia, y los auditores.

Las buenas prácticas de COBIT se aplica a los sistemas de información de toda la agencia ARCH o institución del Estado, incluyendo los computadores personales y las redes.

Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere la agencia para lograr sus objetivos.

La estructura del modelo propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la calidad y seguridad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, sistemas, instalaciones,

entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

La adecuada implementación de un modelo las buenas prácticas de COBIT en la agencia y en la agencia, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, que aseguran que los procesos y recursos de información y tecnología que contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado.

El conjunto de lineamientos y estándares internacionales conocidos como las buenas prácticas de COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios principales, a saber:

### **2.1.1 Planificación y Organización:**

En este dominio cubre la estrategia, las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.

La consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas.

Se deberá establecerse la agencia y una infraestructura tecnológica apropiadas.

### **2.1.2 Adquisición e Implementación:**

En este dominio para llevar a cabo la estrategia de tecnologías de la información, las soluciones de tecnologías deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio.

Este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

### **2.1.3 Soporte y Servicio:**

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad.

Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios.

Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación en la mesa de servicios.

#### **2.1.4 Monitoreo:**

Todos los procesos necesitan ser evaluados constantemente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de datos e información, como de la tecnología que la respalda.

El objetivo de control facilita la generación y procesamiento de la información cumplan con las características de disponibilidad, efectividad, cumplimiento, eficiencia, confidencialidad, integridad, y confiabilidad de la información.

#### **2.1.5 Usuario:**

La Gerencia: para apoyar sus decisiones de inversión en Tecnologías de la Información y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de Tecnologías de la Información, su impacto en la organización y determinar el control mínimo requerido.

Los Responsables de Tecnologías de la Información: para identificar los controles que requieren en sus áreas. También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la Tecnologías de la Información en las empresas.

#### **2.1.6 Características:**

- Orientado al negocio.
- Alineado con estándares y regulaciones de facto.
- Basado en una revisión crítica y analítica de las tareas y actividades en Tecnologías de la Información.
- Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA)



### **2.1.7 Principios:**

El enfoque del control en Tecnologías de la Información se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI. Requerimientos de la información del negocio:

Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios: Requerimientos de Calidad: Calidad, Costo y Entrega.

### **2.1.8 Requerimientos Fiduciarios:**

Efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento de las leyes y regulaciones.

**EFFECTIVIDAD.-** La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

**EFICIENCIA.-** Se debe proveer información mediante el empleo óptimo de los recursos de forma más productiva y económica.

**CONFIABILIDAD.-** proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la agencia ARCH y cumplir con sus responsabilidades.

**CUMPLIMIENTO.-** de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la agencia ARCH.

### **2.1.9 Requerimientos de Seguridad:**

**CONFIDENCIALIDAD.-** Protección de la información sensible contra divulgación no autorizada.

**INTEGRIDAD.-** Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la agencia ARCH.

**DISPONIBILIDAD.-** accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

En las buenas prácticas de COBIT se establecen los siguientes recursos en Tecnologías de la Información necesarios para alcanzar los objetivos de negocio:

**DATOS.-** Todos los objetos de información se considera información interna y externa, estructurada o no, gráficas, sonidos, entre otros.

**APLICACIONES.-** Entendidas como sistemas de información, que integran procedimientos manuales y sistematizados.

**TECNOLOGÍA.-** Incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, entre otros.

**INSTALACIONES.-** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

**RECURSO HUMANO.-** Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información, o de procesos de Tecnología de Información.

**TECNOLOGÍAS DE INFORMACIÓN.-** Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información relacionada.

En esta sociedad global donde la información viaja a través del ciberespacio sin las restricciones de tiempo, distancia y velocidad esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las ciber amenazas y la guerra de información
- El costo de las inversiones actuales y futuras en información y en tecnología de información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos. Para muchas organizaciones, la información y la tecnología que la respalda, representan los activos más valiosos de la agencia ARCH, por lo que la gestión de los riesgos asociados de la Tecnología de Información, o Gobernabilidad de TI (IT Governance), ha ganado notoriedad en tiempos recientes como un aspecto clave de la gobernabilidad corporativa, dada su capacidad de proporcionar valor agregado al negocio, balanceando la relación entre el riesgo y el retorno de la inversión sobre TI y sus procesos. Estos aspectos se enfatizan en el Marco de referencia las buenas prácticas de COBIT, el cual se define como conjunto de Objetivos de Control para la Información y Tecnologías Relacionadas. (Ministerio de Costa Rica, 2015)

Bajo este escenario, una adecuada administración de los recursos de TI es fundamental para mejorar la calidad de los productos y servicios brindados por el área, lo que se reflejará en mejoras en los procesos que

respalda, y en el nivel de seguridad y control con el cual se trabaja, elevando su capacidad para satisfacer los objetivos de cumplimiento definidos en la estructura de control interno de la organización, reduciendo además los costos administrativos asociados al entorno informático.

Las buenas prácticas de COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios principales, a saber:

- Planificación y organización
- Adquisición e implantación
- Soporte y Servicios
- Monitoreo

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda.

En conjunto, estos dominios y los objetivos de control, facilitan que la generación y procesamiento de la información cumplan con las características de confidencialidad, integridad, disponibilidad, efectividad, eficiencia, cumplimiento y confiabilidad. Asimismo, se deben tomar en cuenta los recursos que proporciona la Tecnología de Información, tales como: datos, sistemas de aplicación, tecnología con diferentes plataformas, instalaciones y el recurso humano.

## **2.2 Las buenas prácticas de ITIL**

La Agencia y las instituciones hoy por hoy dependen de la Tecnología de Información la cual optimiza y mejorar los procesos del negocio brindando así un mejor servicio.

En muchos casos, los servicios de Tecnologías de la información se basan en modelos de negocios, mismos que no generan apoyo al negocio, es decir, son en ciertos casos el negocio mismo.

Al mismo tiempo las expectativas por la calidad, innovación y valor de Tecnologías de la información continúan acrecentándose. Mismo que conlleva a que las organizaciones de TI se enfoque hacia el negocio y el servicio.

### **2.2.1 Gestión de Servicios de Tecnologías de la Información**

Para realizar este cambio de en la vista de las áreas de Tecnologías de la información, es necesario ubicarse bajo el punto de vista de la calidad de los servicios que se prestan, y alinearse al objetivo estratégico de la organización.

Cuando los servicios de Tecnologías de la información son críticos, las actividades que se realizan deben ser ejecutadas en un orden establecido lo cual asegure que el equipo como tal de Tecnologías de la información suministre valor y entregue los servicios de forma sólida.

“La Gestión de servicios es un una disciplina de gestión basada en procesos que pretende alinear los servicios de TI con las necesidades de la organización, además brinda un orden determinado a las actividades de gestión”. (C, 2009) (Brito, 2004)

### **2.2.2 Las buenas prácticas de ITIL - Mejores Prácticas**

Las buenas prácticas de ITIL, (Information Technology Infrastructure Library) es una colección de documentos públicos, que basados en procesos y en un marco de mejores prácticas de la industria, permite la Gestión de Servicios de Tecnologías de la información con calidad y a un costo adecuado.

Las buenas prácticas de ITIL implica todos aquellos procesos que dentro de la ARCH deben ser ejecutados para la eficiente administración de la infraestructura de Tecnologías de la información, obteniendo una adecuada provisión de servicios a los funcionarios públicos presupuestado en el estado.

*“Desarrollada su 1er versión a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (las buenas prácticas de ITIL) se ha convertido en el estándar mundial de facto en la Gestión de Servicios Informáticos” (Osatis, Gestión de Servicios TI, 2013).*

Definición de buenas prácticas de ITIL es determinar para una adecuada Gestión de Servicios en las Tecnologías de Información es necesaria una mezcla sinérgica entre tres factores: Personas, Procesos y Tecnología.

### **2.2.3 Beneficios de las buenas prácticas de ITIL**

Los siguientes son algunos de los beneficios que debe tener una adecuada Gestión del Servicio en las Tecnologías de Información:

- Maximiza la calidad del servicio apoyando al negocio de forma expresa. Ofrece una visión clara de la capacidad del área tecnológica.
- Aumenta la satisfacción en el trabajo mediante una mayor comprensión de las expectativas y capacidades del servicio.
- Minimiza el ciclo de cambios y mejora los resultados de los procesos y proyectos tecnológica.
- Facilita la toma de decisiones de acuerdo con indicadores de Tecnologías de la información y de negocio



#### **2.2.4 Características de las buenas prácticas de ITIL**

Las siguientes son algunas de las características de las buenas prácticas de ITIL:

- Es un framework de procesos de Tecnologías de la información no propietario.
- Es independiente de los proveedores.
- Es independiente de la tecnología.
- Está basado en "Best Practices".

#### **Provee:**

- Una terminología estándar.
- Las interdependencias entre los procesos.
- Los lineamientos para la implementación.
- Los lineamientos para la definición de roles y responsabilidades de los procesos.
- Las bases para comparar la situación de la agencia ARCH frente a las mejores prácticas.

## 2.2.5 Las buenas prácticas de ITIL Versión 2.0

Las buenas prácticas de ITIL consta de varias publicaciones, las cuales se muestran en la siguiente figura; estas publicaciones permiten tener una relación entre la tecnología y el negocio, como se indica en la figura 1.

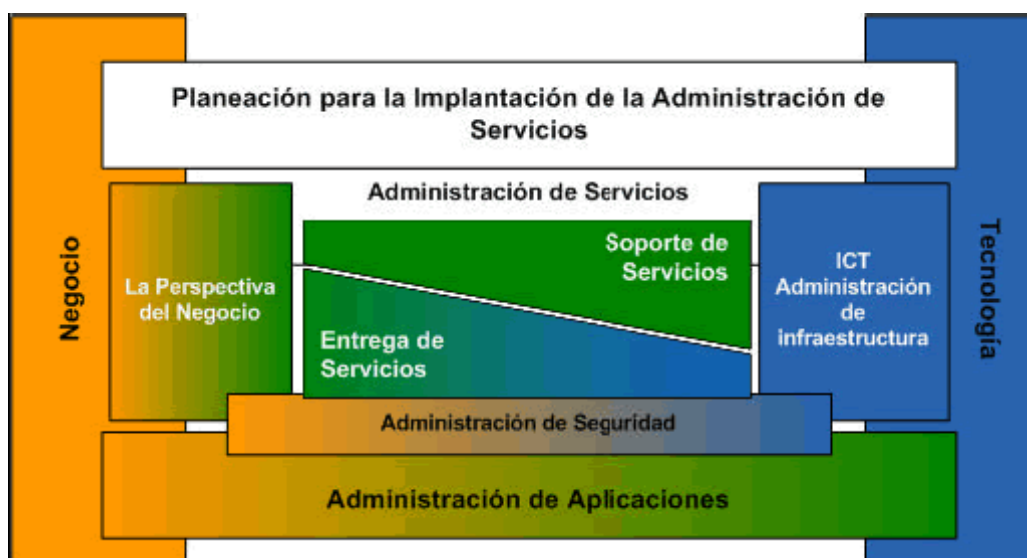


Figura 1. L(NASAudit, 2011)as buenas prácticas de ITIL

Fuente: Cruz, 2009, p. 28

## 2.2.6 Planeación para la Implementación de la Administración:

Esta publicación cubre los temas y actividades involucradas en planeación, implementación y mejora de los procesos de Administración de Servicios dentro de la agencia.

### **2.2.7 ICT Administración de Infraestructura:**

Abarca el tema de Tecnología de Información y Administración de la Infraestructura (ICTIM) y las relaciones con otras áreas, como la Administración de Servicios.

### **2.2.8 Perspectiva del Negocio:**

Tiene como objetivo familiarizarse con la administración del negocio con los componentes de Administración de Servicios, Administración de Aplicaciones y la Administración de la Infraestructura, los cuales son necesarios para soportar los procesos de negocio.

### **2.2.9 Administración de Aplicaciones:**

Trata el tema de la administración de las aplicaciones desde las necesidades del negocio hasta el ciclo de vida de la aplicación

### **2.2.10 Administración de Seguridad:**

Detalla el proceso de planeación y administración de un definido nivel de seguridad en la información y servicios.

## **2.2.11 Administración o Gestión de Servicios de TI:**

La gestión de Servicios Informáticos es abarcada por dos publicaciones:  
Entrega de Servicios y Soporte de Servicios.

### **2.2.11.1 Entrega de Servicios:**

Cubre los procesos necesarios para la planeación y entrega de la calidad de los servicios de TI. Estos procesos son:

- Administración de Niveles de Servicio
- Administración Financiera
- Administración de Capacidad
- Administración de la Continuidad de Servicios de TI
- Administración de la Disponibilidad

### **2.2.11.2 Soporte de Servicios:**

Proporciona los detalles de la función de Mesa de Servicio y los procesos necesarios para el soporte y mantenimiento de los servicios de TI. Estos procesos son:

- Administración de Incidentes
- Administración de Problemas
- Administración de Configuraciones

- Administración de Cambios
- Administración de Releases

### **2.2.12 Procesos de Gestión de Servicios**

La Gestión de Servicios de tecnologías organiza las actividades necesarias para administrar la entrega y soporte de servicios en procesos.

“Un proceso es una serie de actividades que a partir de una entrada obtienen una salida. El flujo de la información dentro y fuera de cada área de proceso indicará la calidad del proceso en particular”. (NASAAudit, 2011)

Existen puntos de monitoreo en el proceso para medir la calidad de los productos y provisión de los servicios. Los procesos pueden ser medidos por su efectividad y eficiencia, es decir, si el proceso alcanzó su objetivo y si se hizo un óptimo uso de los recursos para lograr ese objetivo.

Por lo que si el resultado de un proceso cumple con el estándar definido, entonces el proceso es efectivo, y si las actividades en el proceso están cumpliendo con el mínimos requerido esfuerzo y costo, entonces el proceso es eficiente.

## 2.3 ISO/IEC 27001:2007

La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la agencia. El hecho de disponer de la certificación según ISO/IEC 27001 le ayuda a gestionar y proteger sus activos de información.

### 2.3.1 ISO 27001

El estándar para la seguridad de la información **ISO/IEC 27001** (Information technology

- Security techniques
- Information security management systems
- Requirements) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido “Ciclo de Deming”: PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct.

- **Plan** (planificar): es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.

- **Do** (hacer): es una fase que envuelve la implantación y operación de los controles.
- **Check** (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Act** (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

### 2.3.2 Sistema de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es, como el nombre lo sugiere, un conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

El término se denomina en inglés "Information Security Management System" (ISMS).

“El concepto clave de un SGSI es para la agencia el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información”. (A, 2011) (A., 2009)

Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización así como los externos del entorno.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

### **2.3.3 Controles**

**Un “Control” es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable.**

Control abarca todo el conjunto de acciones, documentos, medidas a adoptar, procedimientos, medidas técnicas, entre otros.



#### **2.3.4 Política de seguridad.**

Política de seguridad se orienta al Nivel político o estratégico de la organización: El cual define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.

Plan de Seguridad se orienta al Nivel de planeamiento o táctico: Define el Cómo. Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

#### **2.3.5 Organización de la información de seguridad.**

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 de negocio.

#### **2.3.6 Administración de recursos**

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.

### **2.3.7 Seguridad de los recursos humanos.**

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.

### **2.3.8 Seguridad física y del entorno**

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 e 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.

### **2.3.9 ¿Quiénes la Utilizan?**

ISO/IEC 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información.

“ISO/IEC 27001 también es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida”. (A., 2009) (Institute, 2007)

### **2.3.10 Beneficios**

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.

- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001...).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

### **2.3.11 Implementación**

La implantación de ISO/IEC 27001 en la agencia es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiéndose por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido.

En general, es recomendable la ayuda de consultores externos. El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información que hayan realizado un curso de implantador de SGSI.

## **CAPÍTULO III**

### **Mejores Prácticas para el Desarrollo del Sistema de Gestión de la Seguridad de la Información.**

Las mejores prácticas y los estándares ayudan a posibilitar un gobierno eficaz de las actividades de TI.

“Incrementalmente, el uso de estándares y mejores prácticas tales como las buenas prácticas de ITIL, las buenas prácticas de COBIT e ISO/IEC 27000, está siendo conducido por requerimientos de negocio para mejoras de desempeño, transparencia y control sobre actividades de TI”. (Institute, 2007)

#### **3.1 Las buenas prácticas de COBIT**

##### **3.1.1 Administración de las Tecnologías de la Información**

Las buenas prácticas de COBIT básicamente presenta en gobierno de la gestión de tecnologías de la información en cinco dimensiones que son el alineamiento de las estrategias de tecnologías a las estrategias de negocio, no todas las gestiones de tecnologías de la información son fundadas en función de lo que el negocio necesita, a veces la gestión de la seguridad de la información de tecnologías de la información tiene un sesgo muy personal y suelen olvidar porque están ahí (las buenas prácticas de COBIT Gestión,

Control, Alineamiento y Monitoreo. (las buenas prácticas de COBIT 4.1, 2007).

Las buenas prácticas de COBIT tema en consideración los siguientes aspectos:

- 1.- Que la alineación de la estrategia de tecnologías de la información y la estrategia del negocio es lo primero que mide las buenas prácticas de COBIT.
- 2.- La Entrega de Valor, este consiste en la presentación de la calidad de trabajo.
- 3.- La administración de la tecnología y los recursos de humanos, nos permite saber que tan sólida es la base con la cual estamos trabajando, es decir, si se conoce las estrategias, los servicios debidamente garantizados con los procesos respectivos, y por otro lado no se tiene personal capacitado, no idónea, tecnología inadecuada para cubrir las necesidades; en este caso es necesario medir y saber que tan lejos se encuentra la dimensión de los recursos tecnológicos y humanos para llegar a cubrir las necesidades de la organización.
- 4.- Es la administración del riesgo; el riesgo tiene que ver con amenazas potenciales que existen, vulnerabilidades que los responsables de

seguridad y conocen por encontrarse trabajando en la agencia ARCH. La combinación que estas amenazas se materialicen a través de las vulnerabilidades, el impacto que generaría en forma directa o indirecta en el negocio.

A partir de la identificación de estos riesgos se procede a planificar como se hará frente a estas amenazas y así evitar que estos riesgos se materialicen y además estar preparados para ejecutar otro tipo de actividades en caso de ser necesarios, enmarcados en el plan de contingencias y mitigación, todo esto también se encuentra reflejado en un tablero de control diseño según lo que dice las buenas prácticas de COBIT.

5.- La Medición de la Performance, esto quiere decir que tan eficientes somos en toda la gestión y que tan mejores en un futuro y cómo hacer para lograrlo. Siguiendo el ejemplo de la movilidad vemos que tenemos el tablero con todos los indicadores que necesitamos y el Gobierno para poder aplicar acelerador y freno o hacer mover el volante para que la gestión vaya en la dirección correcta. Es aconsejable que todo proyecto de gestión de IT se realice mediciones y para ello es indispensable la utilización de las buenas prácticas de COBIT.



### 3.1.2 Control de las Tecnologías de la Información

**Objetivos de Control:** Integran en su contenido lo expuesto tanto en el resumen ejecutivo como en el marco de referencia.

El enfoque las buenas prácticas de COBIT propone 37 procesos organizados en 4 áreas funcionales

- Entrega y asistencia técnica
- Control
- Planeamiento y organización
- Aprendizaje e implementación

De los cuales los aplicables directamente al control de las Tecnologías de la Información son:

- **PLANEAR Y ORGANIZAR**

- **Gestionar la Seguridad**

**Establecer y mantener un SGSI (Sistema de Gestión de Seguridad de la Información).**

Se define las características, alcances y límites de lo que sería el Sistema de Gestión de Seguridad de Información (SGSI) y su la forma en que se debe implementar en la agencia ARCH. Se expresa a su vez que este sistema debe ir alineado a las Políticas de la agencia ARCH, contexto

organizacional y objetivos; esto va también con la alineación de este sistema con la gestión de seguridad general en la agencia ARCH y a su vez con los requerimientos de esta. También menciona de la importancia de la comunicación del sistema y su difusión por toda esta tanto la forma como los responsables.

### **Definir y administrar un plan de tratamiento de riesgos de la seguridad de la información**

Se menciona con alto detalle como el plan de seguridad de información va a manejar los riesgos en la agencia ARCH, con un plan estructurado que va alineado a los casos de negocio de la agencia ARCH.

Es importante resaltar el control de riesgos sea óptimo para esto debe estar asociada a los objetivos y recursos empresariales.

La norma describe de qué manera se proporcionara información para el correcto desarrollo de este plan.

### **Monitorear y revisar el SGSI.**

Es explícitamente lo referido al monitoreo y la revisión del Sistema de Gestión de Seguridad de Información.

Principalmente en la revisión periódica del SGSI para poder corregir aspectos importantes, para esto la importancia de recolectar y analizar información continuamente.

Las auditorías internas, así como la realización de exámenes para medir el grado de efectividad de SGSI actual.

Además se debe proporcionar información pertinente para el mantenimiento ya que esto nos ayudara a tener resultados correctos del seguimiento, también guardar acciones que podrían tener impacto en el rendimiento del SGSI en la agencia ARCH.

- **ADQUIRIR E IMPLEMENTAR**

- DSS05 Gestionar los servicios de seguridad**

- Proteger la información de la agencia ARCH para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.

- Gestionar el Entorno**

- Medidas de Protección contra factores de ambientales.

**Gestión de Instalaciones**

Gestión de Instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo

**Gestión del Acceso físico a los activos de tecnologías de la información**

Procedimientos para conceder, limitar, y revocar acceso a locales, edificios y áreas con equipos de conectividad de acuerdo con las necesidades del negocio, incluyendo emergencias. El acceso debe estar justificado, autorizado, registrado y supervisado.

- **SUPERVISAR, EVALUAR Y VALORAR**

**Supervisar, Evaluar y Valorar Rendimiento y conformidad**

Recolectar, validar y evaluar métricas y objetivos de negocio, de las TI y de procesos. Supervisar que los procesos se están realizando según el rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

**Supervisar, Evaluar y Valorar el Sistema de Control Interno**

Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e

ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.

### **Supervisar, Evaluar y Valorar LA conformidad con los Requerimientos externos.**

Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de las TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de las tecnologías de la información en el cumplimiento de la agencia ARCH general.

### **3.1.3 Control de Proveedores Tecnológicos**

#### **Gestionar los Proveedores**

**Identificar y evaluar las relaciones y contratos con proveedores**, en donde se necesita conocer las necesidades de los interesados

#### **Seleccionar proveedores**

Gestionar las relaciones y contratos con el proveedor

**Gestionar el Riesgo del proveedor**, es decir la capacidad del proveedor de brindar permanentemente el servicio.

## Monitorear el Desempeño y el cumplimiento del proveedor

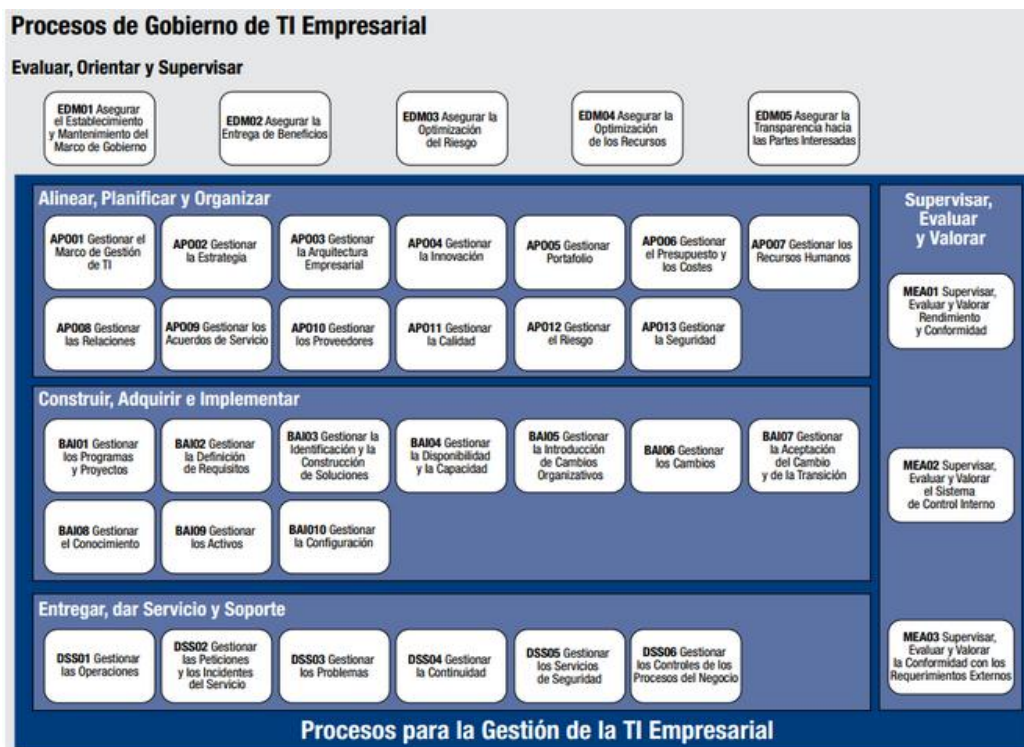


Figura 2. Procesos de Las buenas prácticas de COBIT

Fuente: las buenas prácticas de COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la agencia ARCH, Figura 31, 2012 ISACA.

### 3.2 NORMAS ISO 27001

Este grupo de normas permite es identificar las necesidades de integridad, disponibilidad y confidencialidad que la organización requiere para el manejo de su información. (Bsigroup.es, 2015)

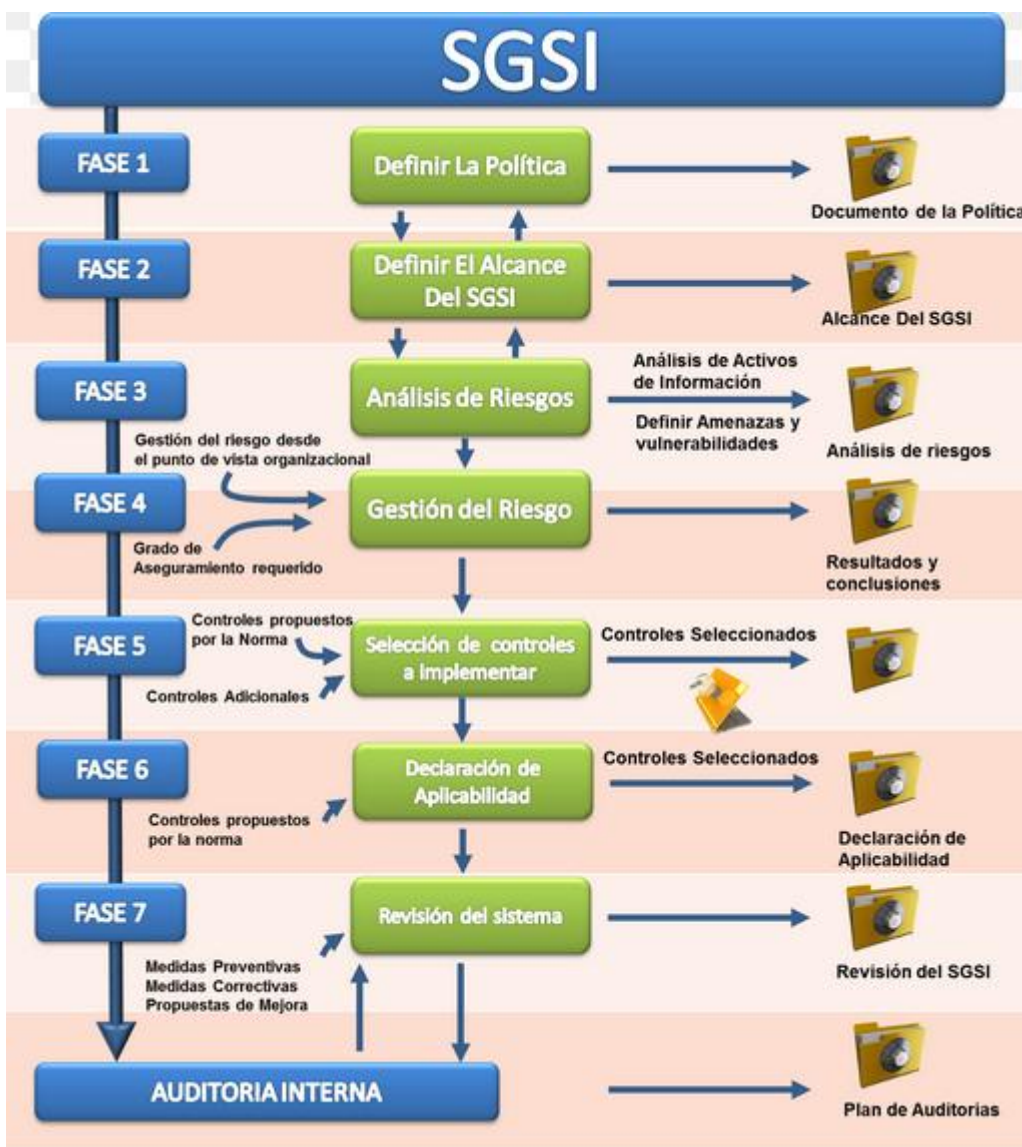


Figura 3. Fases de ISO 27000

Fuente: Seguridad de la Seguridad de la Información, 2005

### 3.2.1 Uso de la Norma ISO 27001

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de la agencia. La confidencialidad, integridad y disponibilidad de 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 y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, los ataques de denegación de servicio y el "hacking" son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

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

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar



parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

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

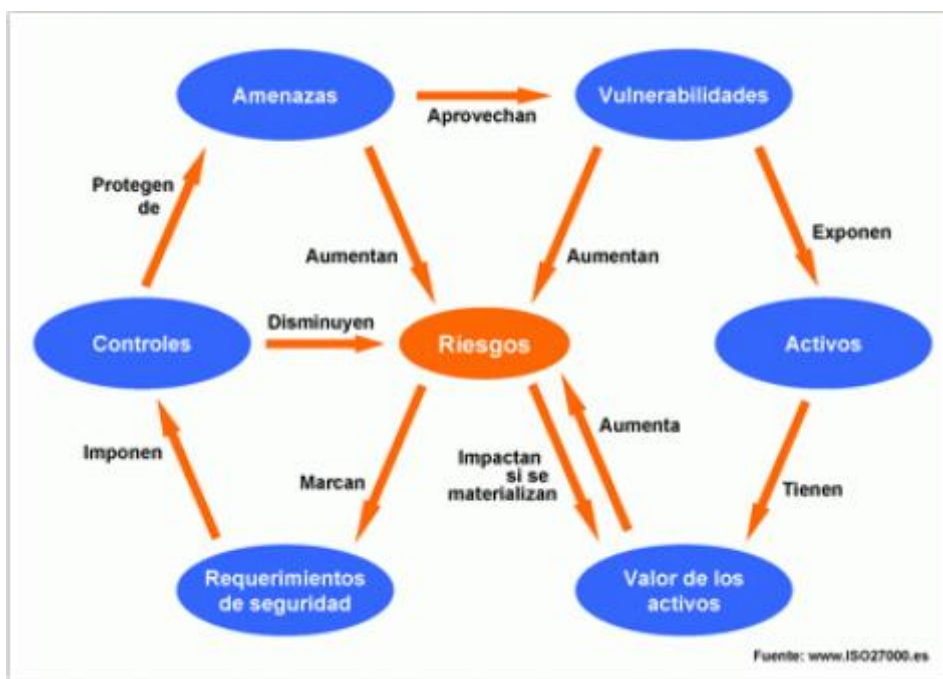


Figura 4. Riesgos

Fuente: ISO27000: 2013

## Beneficios

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001...).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal. (SGSI, 2015)

- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.



Figura 5. Costes vs. Beneficios

Fuente: ISO27000: 2013

### Documentación Mínima

- Política y objetivos de seguridad.
- Alcance del SGSI.
- Procedimientos y controles que apoyan el SGSI.
- Descripción de la metodología de evaluación del riesgo.
- Informe resultante de la evaluación del riesgo.

- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
- Registros.
- Declaración de aplicabilidad (SOA -Statement of Applicability-).
- Procedimiento de gestión de toda la documentación del SGSI.

**Las actividades más relevantes son:**

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.

- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

### **3.2.2 Administración y Control de la Seguridad de la Información**

Lo que se obtiene con la aplicación de esta norma es un plan de seguridad de la información acorde con las necesidades de la compañía, suele suceder en las compañías que tienen un responsable de seguridad de sistemas suelen colocar a las medidas de control de seguridad un sesgo muy personal donde si son gente que entiende que la confidencialidad es todo, va aplicar ciertas medidas de control que extreman la protección de la confidencialidad y por tanto degradan la funcionalidad de lo que la agencia ARCH necesita, ósea la seguridad aplicada a la compañía tiene que ver con el perfil profesional del personal del área de seguridad. (ISO.org, 2015)

La Confidencialidad es la restricción de cierta información que únicamente está autorizado para ser leído o entendido por algunas personas o entidades.

Existen diferentes niveles de confidencialidad como ser: información que es conocida por toda la compañía y los clientes, información que maneja cierto grupo, información que solo maneja un grupo reducido por lo general personas que se encuentran en la cúpula de la organización, información muy privada que ni siquiera la gestión de tecnologías sabe que existe simplemente lo supone. Para cada uno de estos grupos hay que aplicar diferentes medidas de control.

En lo referente a Integridad, si tenemos una base de datos que la soporte un sistema de emisión crítica, se optará por un motor de base de datos más sólidos con el fin de mantener la información completa y precisa.

Lo mismo pasa con la Disponibilidad, actualmente se puede encontrar conexión Wi- Fi o cableado estructurado, con el fin de buscar disponibilidad aplicado a toda la información en general. Esta norma certifica el plan de la seguridad de la información y nos permite dar evidencia de lo que decimos que hacemos realmente lo hacemos.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI, tal como se indica en la figura N° 6.



Figura 6. Ciclo de Vida

Fuente: ISO27000: 2013

### 3.2.3 Planes de Continuidad de Negocios

Los planes de Continuidad de Negocio se definen para el momento que falle el Sistema, no solo por si falla.

Un plan de continuidad es una respuesta prevista antes aquellas situaciones de riesgo que afectan de forma crítica a los servicios que ofrecen y que son los que le permiten la realización de sus actividades diarias y que deben ser las que se quiere proteger.

En éste se trata de obtener el mínimo tiempo de recuperación ante una determinada situación de riesgo así como la minimización de las consecuencias que estas acciones podrías llegar a provocar.

## **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**

De acuerdo a la norma, se toman en cuenta los siguientes puntos:

### **Continuidad de la seguridad de la información.**

Planificación de la continuidad de la seguridad de la información.

Implantación de la continuidad de la seguridad de la información.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

### **Redundancias.**

Disponibilidad de instalaciones para el procesamiento de la Información.

## **3.3 Las buenas prácticas de ITIL**

Se direcciona a brindar una perspectiva global del ciclo de un servicio el cual inicia con el diseño hasta detallar los procesos inmersos en la eficiente.



### 3.3.1 Administración y Control en la Entrega de Servicios

#### Tecnológicos

Las buenas prácticas de ITIL fue evolucionando en los últimos años, actualmente se cuenta con la versión 3, está separado en cinco fases que se podría interpretar como libros ordenados cronológicamente.

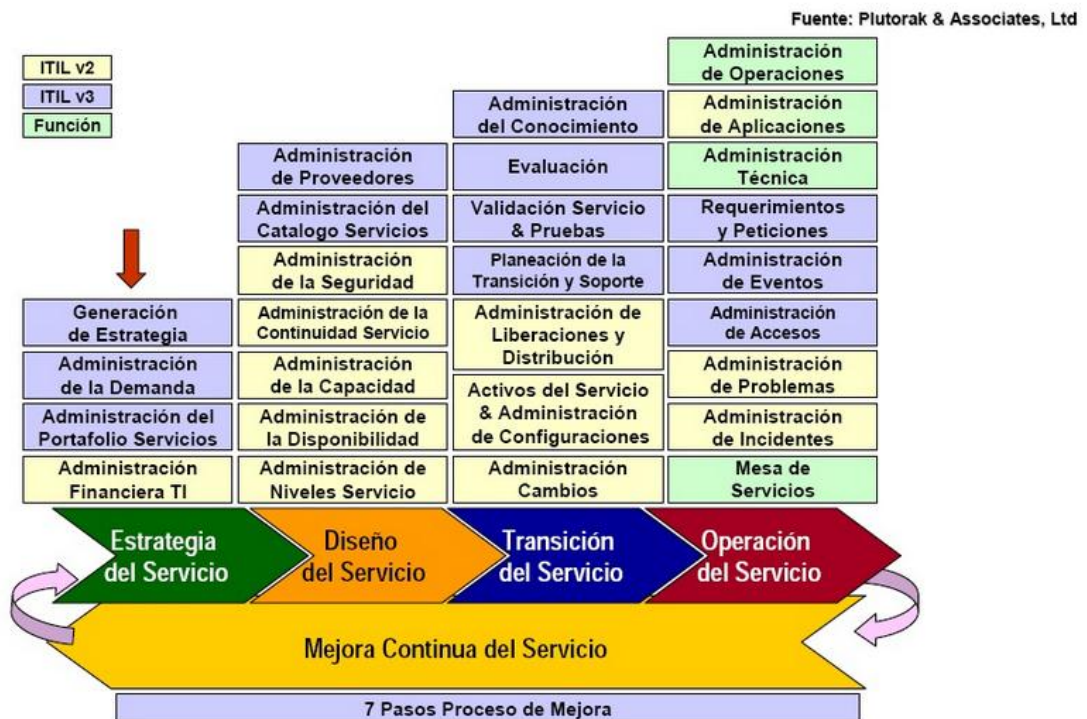


Figura 7. Procesos de las buenas prácticas de ITIL

Fuente: Héctor Acevedo Juárez, 2010

## **Estrategias de los Servicios de TI.**

La fase de Estrategia del Servicio es central al concepto de Ciclo de vida del servicio y tiene como principal objetivo convertir la Gestión del Servicio en un activo estratégico.

Para conseguir este objetivo es imprescindible determinar en primera instancia qué servicios deben ser prestados y por qué han de ser prestados desde la perspectiva del cliente y el mercado.

Una correcta Estrategia del Servicio debe:

- Servir de guía a la hora de establecer y priorizar objetivos y oportunidades.
- Conocer el mercado y los servicios de la competencia.
- Armonizar la oferta con la demanda de servicios.
- Proponer servicios diferenciados que aporten valor añadido al cliente.
- Gestionar los recursos y capacidades necesarios para prestar los servicios ofrecidos teniendo en cuenta los costes y riesgos asociados.
- Alinear los servicios ofrecidos con la estrategia de negocio.
- Elaborar planes que permitan un crecimiento sostenible.
- Crear casos de negocio para justificar inversiones estratégicas.

La fase de Estrategia del Servicio es el eje que permite que las fases de Diseño, Transición y Operación del servicio se ajusten a las políticas y visión estratégica del negocio.

Una correcta implementación de la estrategia del servicio va más allá del ámbito puramente tecnologías de la información y requiere un enfoque multidisciplinar que ayude a responder cuestiones tales como:

- ¿Qué servicios debemos ofrecer?
- ¿Cuál es su valor?
- ¿Cuáles son nuestros clientes potenciales?
- ¿Cuáles son los resultados esperados?
- ¿Qué servicios son prioritarios?
- ¿Qué inversiones son necesarias?
- ¿Cuál es el retorno a la inversión o ROI?
- ¿Qué servicios existen ya en el mercado que puedan representar una competencia directa?
- ¿Cómo podemos diferenciarnos de la competencia?

### **Diseño de Servicios de tecnologías de la información**

Es donde se define los servicios que se va ofertar, es decir el catálogo de servicios y mediante que procesos los vamos a soportar; para comprender mejor las diferencias de los dos primeros libros presentados a

donde se analiza el catálogo de servicios; por otro lado se encuentran los procesos que tienen;. Es decir, el servicio por un lado, proceso por otro lado. El Diseño del Servicio debe seguir las directrices establecidas en la fase de Estrategia y debe a su vez colaborar con ella para que los servicios diseñados:

- Se adecuen a las necesidades del mercado.
- Sean eficientes en costes y rentables.
- Cumplan los estándares de calidad adoptados.
- Aporten valor a clientes y usuarios.

El Diseño del Servicio debe tener en cuenta tanto los requisitos del servicio como los recursos y capacidades disponibles en la organización tecnologías de la información. Un desequilibrio entre ambos lados de la balanza puede resultar en servicios donde se vean comprometidas bien la funcionalidad o bien la garantía.

El proceso de diseño del servicio no es estanco y debe tener en cuenta que los procesos y actividades involucrados incumben a todas las fases del ciclo de vida.

Una correcta implementación del Diseño del Servicio debe ayudar a responder cuestiones tales como:

- ¿Cuáles son los requisitos y necesidades de nuestros clientes?

- ¿Cuáles son los recursos y capacidades necesarias para prestar los servicios propuestos?
- ¿Los servicios son seguros, ofrecen la disponibilidad necesaria y se garantiza la continuidad del servicio?
- ¿Son necesarias nuevas inversiones para prestar los servicios con los niveles de calidad propuestos?
- ¿Están todos los agentes involucrados correctamente informados sobre los objetivos y alcance de los nuevos servicios o de las modificaciones a realizar en los ya existentes?
- ¿Se necesita la colaboración de proveedores externos?

### **Transición de los Servicios de TI**

Es hacer que los productos y servicios definidos en la fase de Diseño del Servicio se integren en el entorno de producción y sean accesibles a los clientes y usuarios autorizados.

Sus principales objetivos se resumen en:

- Supervisar y dar soporte a todo el proceso de cambio del nuevo (o modificado) servicio.
- Garantizar que los nuevos servicios cumplen los requisitos y estándares de calidad estipulados en las fases de Estrategia y la de Diseño.

- Minimizar los riesgos intrínsecos asociados al cambio reduciendo el posible impacto sobre los servicios ya existentes.
- Mejorar la satisfacción del cliente respecto a los servicios prestados.
- Comunicar el cambio a todos los agentes implicados.

Para cumplir adecuadamente estos objetivos es necesario que durante la fase de Transición del Servicio:

- Se planifique todo el proceso de cambio.
- Se creen los entornos de pruebas y preproducción necesarios.
- Se realicen todas las pruebas necesarias para asegurar la adecuación del nuevo servicio a los requisitos predefinidos.
- Se establezcan planes de *roll-out* (despliegue) y *roll-back* (retorno a la última versión estable).
- Se cierre el proceso de cambio con una detallada revisión post-implementación.

Como resultado de una correcta Transición del Servicio:

- Los clientes disponen de servicios mejor alineados con sus necesidades de negocio.
- La implementación de nuevos servicios es más eficiente.
- Los servicios responden mejor a los cambios del mercado y a los requisitos de los clientes.
- Se controlan los riesgos y se dispone de planes de contingencia que eviten una degradación prolongada del servicio.

- Se mantienen correctamente actualizadas las bases de datos de configuración y activos del servicio.
- Se dispone de una Base de Conocimiento actualizada a disposición del personal responsable de la operación del servicio y sus usuarios.

### **Operación de los Servicios de TI**

Sin duda, la más crítica entre todas. La percepción que los clientes y usuarios tengan de la calidad de los servicios prestados depende en última instancia de una correcta organización y coordinación de todos los agentes involucrados.

Todas las otras fases del Ciclo de Vida del Servicio tienen como objetivo último que los servicios sean correctamente prestados aportando el valor y la utilidad requerida por el cliente con los niveles de calidad acordados. Es evidente que de nada sirve una correcta estrategia, diseño y transición del servicio si falla la “entrega”.

Por otro lado es prácticamente imposible que la fase de Mejora Continua del Servicio sea capaz de ofrecer soluciones y cambios sin toda la información recopilada durante la fase de operación.

Los principales objetivos de la fase de Operación del Servicio incluyen:

- Coordinar e implementar todos los procesos, actividades y funciones necesarias para la prestación de los servicios acordados con los niveles de calidad aprobados.
- Dar soporte a todos los usuarios del servicio.
- Gestionar la infraestructura tecnológica necesaria para la prestación del servicio.

Uno de los aspectos esenciales en la Operación del Servicio es la búsqueda de un equilibrio entre estabilidad y capacidad de respuesta.

La estabilidad es necesaria pues los clientes requieren disponibilidad y muestran resistencias al cambio. Por otro lado las necesidades de negocio cambian rápidamente y eso requiere habitualmente rapidez en las respuestas.

Normalmente los cambios correctamente planificados no tienen que afectar a la estabilidad del servicio pero esto requiere la colaboración de todos los agentes implicados en la Operación del Servicio que deben aportar el *feedback* necesario.

Para evitar los problemas de inestabilidad es conveniente adoptar una actitud proactiva que permita dar respuestas a las nuevas necesidades de negocio de una forma progresiva. La actitud reactiva provoca que los cambios sólo se implementen cuando la organización tecnológicas de la información se ve obligada a responder a estímulos externos lo que



usualmente provoca un estado de “urgencia” que no es conducente a una correcta planificación del cambio.

Es también esencial encontrar un correcto equilibrio entre los procesos de gestión internos orientados a gestionar y mantener la tecnología y recursos humanos necesarios para la prestación del servicio y las demandas externas de los clientes.

La organización tecnologías de la información no debe comprometerse en la prestación de servicios para los que carezca de capacidad tecnológica o los necesarios recursos humanos ni tampoco caer en el error de engordar en exceso la infraestructura tecnologías de la información encareciendo innecesariamente el coste de los servicios prestados.

Mejora de los Servicios de TI, hace referencia a que siempre se tiene que mejorar, este libro profesionaliza la forma de encarar la mejora, particularmente los procesos incluidos en cada libro, son los mismos de antes más otros nuevos, aparecen nuevos roles, nuevas funciones, cada libro toca tangencialmente uno o más procesos pero si el aspecto a destacar la cronología del avance de las buenas prácticas de ITIL. Para definir los roles es imprescindible acudir a las buenas prácticas de ITIL, los roles son combos de responsabilidades, las buenas prácticas de ITIL nos dice cuales responsabilidad es nuclear en un rol, cuales roles son compatibles para ser

ejecutados por la misma persona o grupo de personas y nos permite bajar al llano todo esto que es bastante abstracto de la gestión de tecnologías.

Efectivamente, los tiempos modernos nos exigen continuos cambios y éstos deben tener un solo objetivo en el campo de la gestión de servicios tecnologías de la información: ofrecer mejores servicios adaptados a las siempre cambiantes necesidades de nuestros clientes y todo ello mediante procesos internos optimizados que permitan mayores retornos a la inversión y mayor satisfacción del cliente.

Pero este objetivo de mejora sólo se puede alcanzar mediante la continua monitorización y medición de todas las actividades y procesos involucrados en la prestación de los servicios tecnologías de la información:

- **Conformidad:** los procesos se adecúan a los nuevos modelos y protocolos.
- **Calidad:** se cumplen los objetivos preestablecidos en plazo y forma.
- **Rendimiento:** los procesos son eficientes y rentables para la organización TI.
- **Valor:** los servicios ofrecen el valor esperado y se diferencian de los de la competencia.

Los principales objetivos de la fase de Mejora Continua del servicio se resumen en:

- Recomendar mejoras para todos los procesos y actividades involucrados en la gestión y prestación de los servicios tecnologías de la información.
- Monitorizar y analizar los parámetros de seguimiento de Niveles de Servicio y contrastarlos con los SLAs en vigor.
- Proponer mejoras que aumenten el ROI y VOI asociados a los servicios tecnologías de la información.
- Dar soporte a la fase de estrategia y diseño para la definición de nuevos servicios y procesos/ actividades asociados a los mismos.

Los resultados de esta fase del ciclo de vida han de verse reflejados en Planes de Mejora del Servicio que incorporen toda la información necesaria para:

- Mejorar la calidad de los servicios prestados.
- Incorporar nuevos servicios que se adapten mejor a los requisitos de los clientes y el mercado.
- Mejorar y hacer más eficientes los procesos internos de la organización tecnologías de la información.

### **3.3.2 Gestión de la Información**

De acuerdo a las fases descritas anteriormente, de las cuales se dividen en sub procesos en cada fase, se hace referencia específicamente a la Gestión de la Seguridad de la Información.

#### **Gestión de la Seguridad de la Información**

Con el advenimiento de las ubicuas redes de comunicación y, en especial, de Internet los problemas asociados a la seguridad de la información se han agravado considerablemente y nos afectan a todos.

La información es consustancial al negocio y su correcta gestión debe apoyarse en tres pilares fundamentales:

- **Confidencialidad:** la información debe ser sólo accesible a sus destinatarios predeterminados.
- **Integridad:** la información debe ser correcta y completa.
- **Disponibilidad:** debemos de tener acceso a la información cuando la necesitamos.

La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

### 3.4 Análisis Comparativo:

Tabla 2.

Tabla de Planificación

<u>las buenas prácticas de COBIT</u>		<u>las buenas prácticas de ITIL</u>		<u>ISO 27001</u>	
PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN
No aplica	No aplica	No aplica	No aplica	Alcance	El desarrollo de este sistema ayudará a prevenir la fuga de información, pérdida de total y parcial de los servidores o sistemas computacionales, modificación y reutilización de datos.
Gobierno de TI mediante estándares de mejores practicas	IT se encuentre alineado con las metas del negocio	Enfoque de procesos (planificación)	Determinar las diversas políticas, son sus objetivos, procesos y procedimientos para el ARCH.	Administración y Control en la Entrega de Servicios Tecnológicos	Para definir la estrategia del servicio, es decir hasta donde queremos llegar conjuntamente con su elaboración, transición y su respectivo funcionamiento.
No aplica	No aplica	Diseño de servicios de TI	Diseñar actuales e innovadores servicios que a su vez puede cambiar según el requerimiento solicitado en base a lo que existe, para de esta manera se consiga incrementar al catálogo de servicios y posteriormente el contorno de elaboración del servicio.	No aplica	No aplica
No aplica	No aplica	Diseño de soluciones de servicios	Es indispensable tener la agencia de los diferente elementos principales para el sistema que se va a realizar	No aplica	No aplica
<b>Justificación General.-</b> Procesos que ayudan a la planificación del SGSI					

Tabla 3.

Tabla de Implementación

<u>las buenas prácticas de COBIT</u>		<u>las buenas prácticas de ITIL</u>		<u>ISO 27001</u>	
PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN
Administración de Tecnologías de la Información	Alineación entre la Estrategia del y la Estrategia de TI. Resultado, la calidad de entrega del producto.	Administración y control en la entrega de servicios para SGSI	Implementar, de acuerdo las diferentes necesidades y requerimientos de los usuarios de la agencia y estar a la vanguardia e innovación así como también la calidad del servicio.	No aplica	No aplica
No aplica	No aplica	Gestione de la Información	Es necesario para que la información se encuentre de una forma segura.	No aplica	No aplica
No aplica	No aplica	Diseño de la arquitectura del servicio	Esencial que se mantenga todos los elementos primordiales para realizar el sistema, para poder interactuar entre ellos y con respectivo mercado al que va dirigido.	No aplica	No aplica
No aplica	No aplica	No aplica	No aplica	Planes de Continuidad del Negocio	Definir planes para cuando falle el sistema como la continuidad de la seguridad de la Información y las redundancias
<b>Justificación General.-</b> Procesos que ayudan a la implementación del sistema SGSI en el ARCH					

Tabla 4.

Tabla de Servicios

<u>las buenas prácticas de COBIT</u>		<u>las buenas prácticas de ITIL</u>		<u>ISO 27001</u>	
PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN
No aplica	No aplica	Diseño del Portafolio de Servicios	Sirve para la respectiva gestión del servicio mediante las diversas fases existentes en el ciclo de vida, y porque van a ir incluidas toda la seguridad del sistema de información ya que los servicios van a ir de la mano con la fase de mejoramiento.	No aplica	No aplica
No aplica	No aplica	Diseño de procesos	Se basa esta fase en el servicio que va brindar el sistema y sus respectivos proceso que están involucrados, ya que a su vez está totalmente explicado las funciones, actividades, organizaciones que va a tener el sistema.	No aplica	No aplica
No aplica	No aplica	Gestión del Catálogo de Servicios	Se podrá elaborar y también conservar un catálogo de los servicios brindados actualmente, ya que va a estar toda la información más importante.	No aplica	No aplica
No aplica	No aplica	Gestión de Niveles de Servicio	Responsable de acordar y garantizar los niveles de calidad de los servicios TI prestados.	No aplica	No aplica
<b>Justificación General.-</b> Procesos que describen los servicios que presentará el sistema en mención.					

Tabla 5.

Tabla de Riesgos

<u>las buenas prácticas de COBIT</u>		<u>las buenas prácticas de ITIL</u>		<u>ISO 27001</u>	
PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN
Gestión del Servicio de Seguridad	Revisar el entorno, factores ambientales, revisión de instalaciones, equipos, revisión del acceso físico a los Activos de TI.	No aplica	No aplica	No aplica	No aplica
No aplica	No aplica	No aplica	No aplica	Tratamiento del Riesgo	Se evitará los desastres, se realizará una fiscalización más eficaz.
<b>Justificación General.-</b> Procesos que nos ayudan a identificar los riesgos más importantes previo, durante, y después de la implementación SGSI.					



Tabla 6.

Tabla de Evaluación

<u>las buenas prácticas de COBIT</u>		<u>las buenas prácticas de ITIL</u>		<u>ISO 27001</u>	
PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN
Subministra lenguaje común	Permite comunicar sus metas, objetivos y resultados con Auditores, IT y otros profesionales.	No aplica	No aplica	No aplica	No aplica
Ejecutivos entienden y gestionan las inversiones en TI	Desarrollo de políticas claras y buenas prácticas para la gestión de IT y asegurar el cumplimiento, la continuidad, seguridad y privacidad.	Diseño de procesos	Se basa esta fase en el servicio que va brindar el sistema y sus respectivos proceso que están involucrados, ya que a su vez está totalmente explicado las funciones, actividades, organizaciones que va a tener el sistema.	No aplica	No aplica
Supervisar, evaluar y valorar	Es necesario gestionar el rendimiento y conformidad el sistema de control interno, la conformidad con requerimientos externos.	Diseño de métricas y sistemas de monitorización	Diseñar el sistema de exactitud y a su vez de su respectivo seguimiento	Enfoque a procesos (Medir)	Realizar evaluaciones al sistema, se pueda medir la respectiva utilidad que se le da a los procesos, e informar los resultados y de esta manera hacer correcciones y prevenir posteriores dificultades
No aplica	No aplica	Capacidad	Responsable de garantizar que organización TI dispone capacidad para prestar servicios acordados.	No aplica	No aplica
<b>Justificación General.-</b> Procesos que nos ayudan a evaluar o medir los elementos del sistema SGSI.					

Tabla 7.

Tabla de Control

<u>las buenas prácticas de COBIT</u>		<u>las buenas prácticas de ITIL</u>		<u>ISO 27001</u>	
PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN	PROCESO	DESCRIPCIÓN/ JUSTIFICACIÓN
Control de las Tecnologías de la información	Se definen Características, alcances, y como se debe implementar, la comunicación y difusión del sistema, el plan de tratamiento de riesgos, una revisión periódica de SGSI, auditorías internas, información sobre el mantenimiento.	No aplica	No aplica	Administración y control de la Seguridad de la Información	Control de las seguridades que se han tomado en cuenta debido a la confidencialidad, integridad y disponibilidad de la información.
Control Proveedores	Se necesita identificar las relaciones y contratos con proveedores, las relaciones y contratos con el proveedor, el riesgo con el proveedor, monitorear el desempeño y cumplimiento del proveedor	No aplica	No aplica	Gestión de Proveedores	Responsable de la relación con los proveedores y el cumplimiento de los UCs.
No aplica	No aplica	No aplica	No aplica	Gestión de la Continuidad de los Servicios TI	Responsable de establecer planes de contingencia que aseguren la continuidad del servicio en un tiempo predeterminado con el menor impacto posible en los servicios de carácter crítico.
<b>Justificación General.-</b> Procesos importantes que nos ayudan a realizar el control de elementos que requiere el sistema.					

### **3.5 Secuencia de los Dominios de Actividades**

#### **1. Alinear la Estrategia del Servicio con la Estrategia del Negocio**

Aquí se definirá como se va a alinear la propuesta SGSI con la Estrategia del Negocio es decir con la Agencia de Regulación y Control Hidrocarburífero, definiendo claramente su alcance de acuerdo a los recursos y el perímetro de la seguridad de la Información.

#### **2. Establecer la Estrategia del Servicio**

Se definen las respectivas políticas y los respectivos acuerdos de la institución que serán necesarios para la implementación del SGSI.

#### **3. Identificación de los Riesgos**

Identificar y evaluar los riesgos posibles con respecto a la seguridad de la información y de esta manera mitigarlos o minimizarlos.

#### **4. Planificación del tratamiento del Riesgo**

Una vez decididas las acciones a tomar, se debe realizar un análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía.

## **5. Implementación de los Servicios Prioritarios**

Aquí se definirán los Controles e implementaciones más importantes que necesita el ARCH

## **6. Planificación del Proceso de Cambio**

Aquí se controlará que los cambios no afecten los servicios entregados y se comunicará los cambios realizados, a toda la organización.

## **7. Revisión Periódica**

Se realizará una revisión de los procedimientos implementados periódicamente de los procesos a cada unidad competente.

## **8. Planes de Continuidad**

En los planes de continuidad se continuarán ejecutando procedimientos para que el SGSI continúe así como también las respectivas acciones correctivas y preventivas que se tomarán de acuerdo a los resultados.

**CAPÍTULO IV**  
**CASO PRÁCTICO AGENCIA DE REGULACIÓN Y CONTROL**  
**HIDROCARBURÍFERO (ARCH)**

La Agencia de Regulación y Control Hidrocarburífero ARCH, es un ente técnico – administrativo que se encarga de regular, controlar y fiscalizar las actividades Hidrocarburífero del Estado Ecuatoriano.

Consiente de su rol estratégico en la nueva era petrolera, la ARCH impulsa a la política pública Hidrocarburífero cumpliendo su misión reguladora y de control sobre procesos productivos y comerciales del petróleo y sus derivados.

Promueve la transparencia y excelencia en la gestión de empresas e instituciones reguladas, cuidando de los intereses ciudadanos desde la extracción petrolera hasta el consumo de sus derivados, además de vigilar el abastecimiento, calidad, cantidad y precio justo de los combustibles en beneficio de los ecuatorianos.

Vela por el Óptimo aprovechamiento de nuestros recursos Hidrocarburífero, a través de la regularización progresiva, el control y fiscalización del sector, al asegurar el buen funcionamiento de los mercados, la oportuna prestación de los servicios y la calidad de los productos y servicios conexos.

Así contribuye en el uso eficiente de los hidrocarburos en cada una de las fases de la industria, entregando una oportuna prestación de servicios y productos de calidad a la ciudadanía.

### **Metodología con las Mejores Prácticas para la Implementación del SGSI en la Agencia de Regulación y Control Hidrocarburífero**

Una de las principales características que debe poseer una empresa que busca un SGSI es establecer una metodología general para la implementación establecida en función de la norma ISO 27000.



El compromiso de la dirección es la base fundamental para iniciar el proyecto, el apoyo y la decisión de implementar el SGSI debe ser una decisión de la máxima autoridad de la ARCH.

La norma ISO 27000 establece los 26 compromisos que deben tener la dirección y la gestión de los recursos para lograr el funcionamiento del SGSI

Conjuntamente con las buenas prácticas de ITIL y Las buenas prácticas de COBIT lineamientos para aplicar buenas prácticas y mejoramiento de procesos, se deben reflejar los compromisos adquiridos, mediante las políticas, objetivos, planes, funciones y responsabilidades con respecto a la seguridad de la información.

De esta manera comunicar a la organización la importancia del cumplimiento de lo establecido; brindar los recursos necesarios; decidir criterios y niveles para aceptación de riesgo; asegurar que se realicen las auditorías internas y efectuar las revisiones del SGSI.

### CASO ARCH: Autorización Máxima Autoridad

MEMORANDO Nro. ...

Fecha:.....

**PARA:** Máxima Autoridad


**ASUNTO:** DIFUSION DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

De mi consideración:

De acuerdo al documento de la Política de la Seguridad de la Información Literal 1, se difundirá la política de Seguridad de la Información; y para dar cumplimiento al literal anteriormente mencionado, se solicita muy comedidamente a usted, como máxima autoridad de la Agencia de Regulación y Control Hidrocarburífero, autorizar los siguientes ítems:

- Realizar el Seguimiento y puesta en marcha de las normas de este documento
- Disponer la difusión, capacitación y sensibilización del contenido de este documento.
- Conformar oficialmente el Comité de Gestión de la Seguridad de la Información de la institución y designar a los integrantes. El comité de coordinación de la seguridad de la información involucrará la participación y cooperación de los cargos directivos de la institución. El comité deberá convocarse de forma periódica o cuando las circunstancias lo ameriten. Se deberá llevar registros y actas de las reuniones.

Atentamente,



**DIRECTOR DE TECNOLOGIAS DE LA INFORMACION**

**Figura 4: Autorización de la Máxima Autoridad**

**Fuente: ARCH**

#### **4.1 Alinear la estrategia del servicio con la estrategia del negocio en la Agencia de Regulación y Control Hidrocarburífero**

Como primera medida se debe establecer el alcance del Sistema de Gestión de la Seguridad de la Información, el mismo que se define de acuerdo a las características del ARCH, su organización, localización, activos y tecnología, de esta manera involucrar los procesos más importantes del negocio.

Se debe tomar en cuenta los requisitos legales y contractuales relacionados con la seguridad de la información.

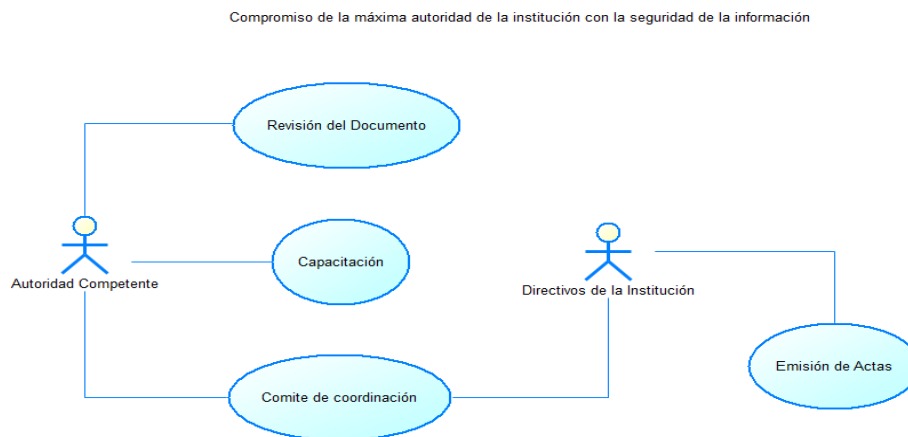
Para el caso de la Agencia de Regulación y Control Hidrocarburífero se enfoque en los procesos sobresalientes, tales como:

- Coordinación de Refinación e Industrialización
- Trámite de Infracciones y Coactivas
- Control Técnico de la Comercialización de Derivados
- Fiscalización de Comercialización de GPL y Gas Natural
- Control Técnico de Hidrocarburos
- Regulación y Normativa

##### **4.1.1. Compromiso de la máxima autoridad de la institución con la seguridad de la información**



## CASO DE USO: Compromiso de la Máxima Autoridad de la Institución con la Seguridad de la Información

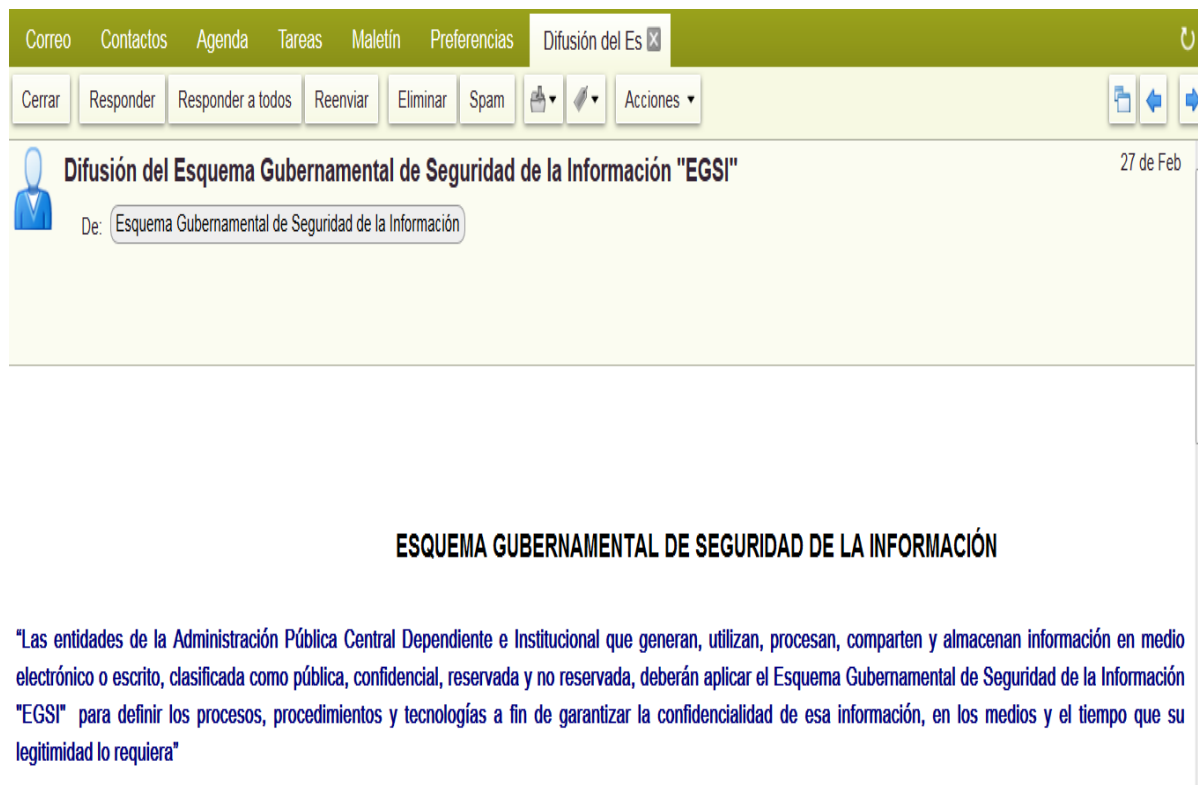


**Figura 5. Compromiso de la máxima autoridad**

**Fuente: ARCH**

El comité de coordinación de la seguridad de la información involucrará la participación y cooperación de los cargos directivos de la institución. El comité deberá convocarse de forma periódica o cuando las circunstancias lo ameriten. Se deberá llevar registros y actas de las reuniones.

## CASO ARCH: Difusión del Esquema Gubernamental de Seguridad de la Información



The screenshot shows an email client interface. At the top, there is a navigation bar with tabs for 'Correo', 'Contactos', 'Agenda', 'Tareas', 'Maletín', 'Preferencias', and 'Difusión del Es X'. Below this is a toolbar with buttons for 'Cerrar', 'Responder', 'Responder a todos', 'Reenviar', 'Eliminar', 'Spam', and 'Acciones'. The email header shows a profile icon, the subject 'Difusión del Esquema Gubernamental de Seguridad de la Información "EGSI"', and the date '27 de Feb'. The 'De:' field contains 'Esquema Gubernamental de Seguridad de la Información'. The main body of the email contains the following text:

**ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN**

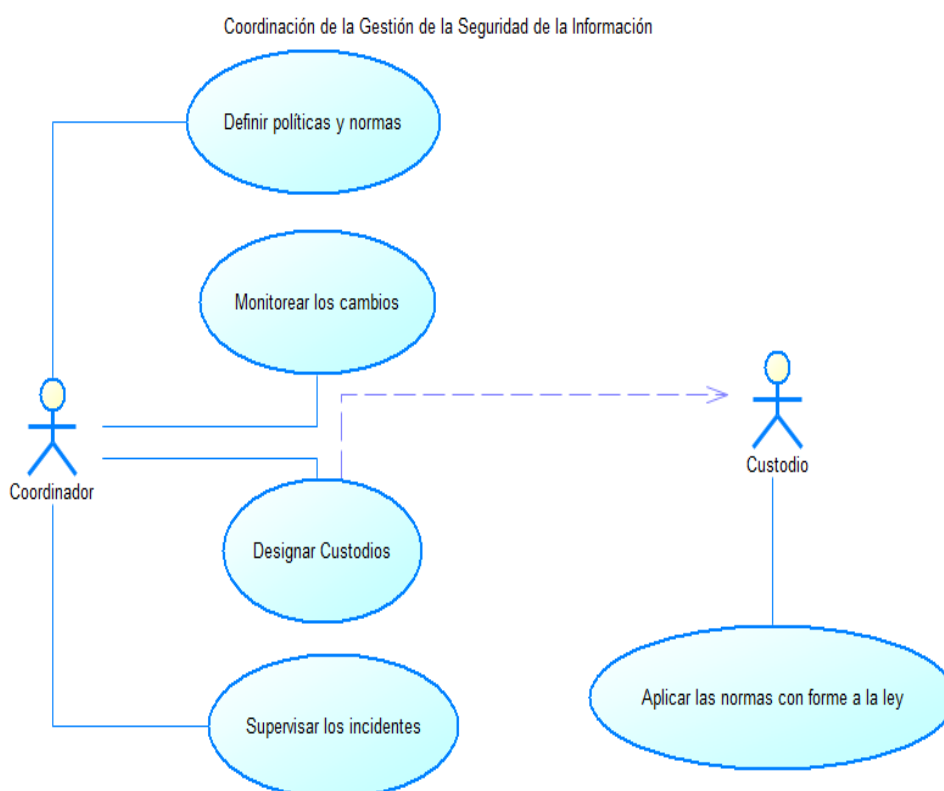
"Las entidades de la Administración Pública Central Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información "EGSI" para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad de esa información, en los medios y el tiempo que su legitimidad lo requiera"

Figura 6. Difusión del Esquema Gubernamental de Seguridad de la Información

Fuente: ARCH

#### 4.1.2. Coordinación de la Gestión de la Seguridad de la Información

##### CASO DE USO: Coordinación de la Gestión de la Seguridad de la Información



**Figura 7. Coordinación de la Gestión de la Seguridad de la Información**

**Fuente: ARCH**

La coordinación del Sistema de Gestión de Seguridad de la Información, estará a cargo del Comité de Gestión de Seguridad de la Información, que se encuentra conformado por:

Dirección de Recursos Humanos

Dirección Administrativa

Dirección de Auditoría Interna

Dirección de Tecnologías de la Información.

## CASO ARCH: Informa de Conformación del Comité de Seguridad

Tabla 8. Informe de Conformación del comité de seguridad

Fuente: ARCH

<b>Informe No.:</b>	<b>Año:</b>	<b>Mes:</b>	<b>Día:</b>
<b>Tema:</b> Comité de Gestión de Seguridad de la Información, elección de Oficial de Seguridad.	<b>Hora Inicial:</b>	<b>Hora Final:</b>	
<b>Lugar:</b> ARCH			
<b>DIRECCIONES PARTICIPANTES</b>		<b>TEMA</b>	
<ul style="list-style-type: none"> <li>• Dirección de Recursos Humanos</li> <li>• Dirección Administrativa</li> <li>• Dirección de Auditoría Interna</li> <li>• Dirección de Tecnologías de la Información.</li> </ul>		<b>Conformación del Comité de Seguridad de la Información y elección del Oficial de Seguridad de la Información.</b>	
<b>RESPONSABLES</b>			
<ul style="list-style-type: none"> <li>• Ing. ....</li> </ul>			
<b>GENERALIDADES DEL INFORME / DESARROLLO / CONCLUSIONES Y DECISIONES</b>			

**ANTECEDENTES:** En referencia a sumilla del Memorando No..... de fecha....., por parte de la Máxima Autoridad, y para la implementación del EGSI y conformación del "Comité de Seguridad de la Información" según la metodología establecida; el comité estará integrada al menos por :

- 1.- El Director Administrativo
- 2.- El Director de Recursos Humanos
- 3.- El Director del Área de Tecnologías de la Información,
- 4.- El Director de Auditoría Interna
- 5.- Y el Oficial de Seguridad de la Información

Se dispone la conformación del Comité de Gestión de la Seguridad de la Información y se procesa con la designación del Oficial de Seguridad, para los fines pertinentes.

Con fecha....., mediante memorando Nro.....

**OBJETIVO:** Conformar el comité de Seguridad de la Información y elegir el oficial de Seguridad de la Información, el mismo que tendrá responsabilidades detalladas en el plan desarrollado.


**ACTIVIDADES REALIZADAS:**





- Elección de oficial de Seguridad de la Información
- Conformación de Comité de Seguridad de la Información.

En virtud de lo antes expuesto queda elegido como Oficial de Seguridad de la Información al señor ..... con CI.....

Y conformación del comité de seguridad de la información a los señores:

Nombres..... CI.....Cargo.....

ASISTENTES	DIRECCION/ REPRESENTANTES	E-mail	FIRMA
Andrea Moscoso	Dirección Administrativa	Andrea.moscoso@arch.gob.ec	

Juan Rivadeneira	Dirección de Recursos Humanos	Juan.rivadenaire@arch.gob.ec	
Daniela Quirós	Dirección de Auditoría Interna	Daniela.quiros@arch.gob.ec	
Carlos Miranda	Dirección de Tecnologías de la Información	Carlos.miranda@arch.gob.ec	
Diego Martínez	Oficial de Seguridad de la Información.	Diego.martinez@arch.gob.ec	

#### 4.1.3 Asignación de responsabilidades para la seguridad de la información

El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:

#### CASO DE USO: Asignación de Responsabilidades para la Seguridad de la Información

Figura 8. Designación del Oficial del Seguridad de la Información

Fuente: ARCH

El responsable de Seguridad del Área de Tecnologías de la Información tendrá las siguientes responsabilidades:

- VER ANEXO 4.1.3.- Asignación de responsabilidades que debe cumplir el oficial de seguridad de la Información y el responsable del Área de Tecnologías de la Información.

#### 4.1.4 Proceso de autorización para nuevos servicios de procesamiento de la información.

##### CASO DE USO: Proceso de Autorización para nuevos Servicios de Procesamiento de la Institución.

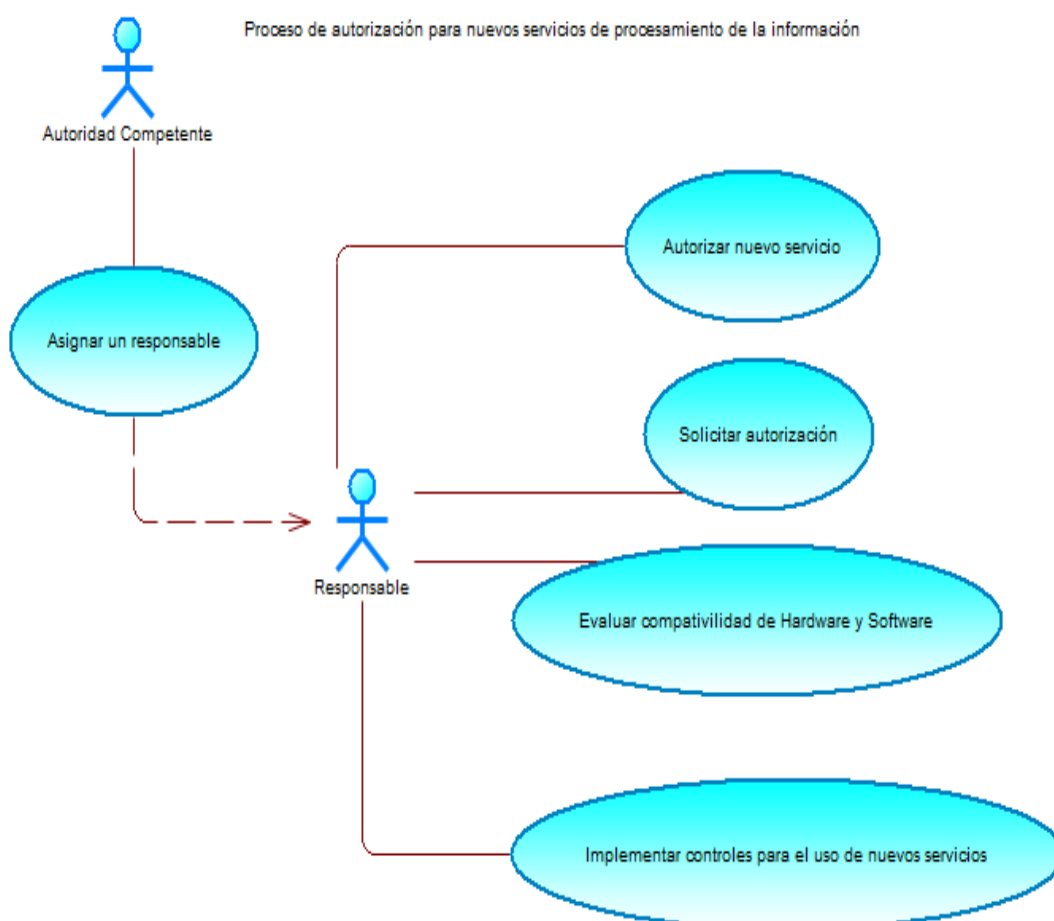


Figura 9. Proceso de Autorización de nuevos Servicios de Procesamiento de la Información

Fuente: ARCH

#### 4.1.5. Acuerdos sobre Confidencialidad

### CASO DE USO: Acuerdos sobre Confidencialidad

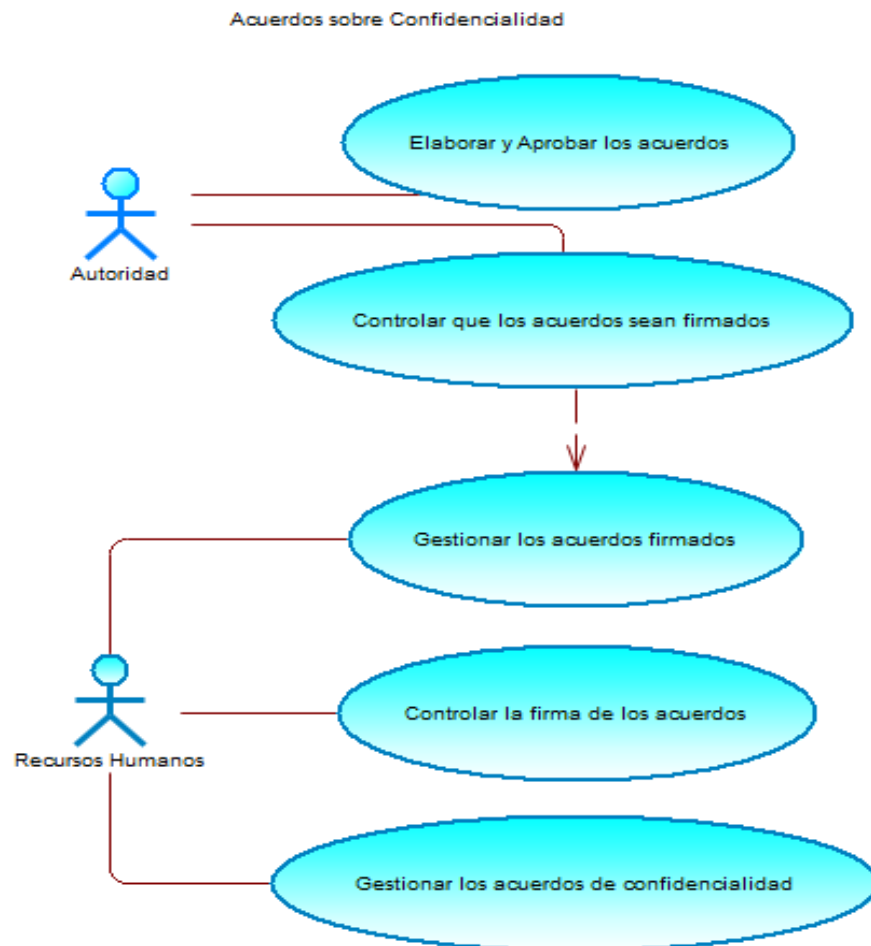


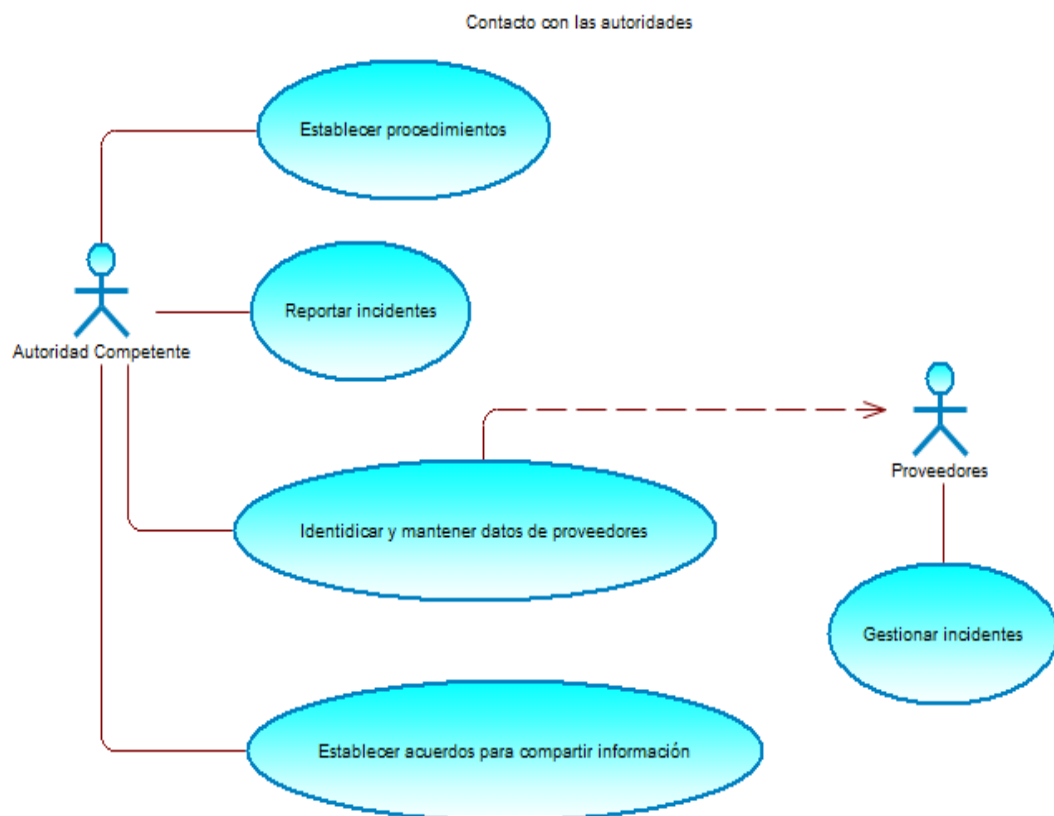
Figura 10. Acuerdos de Confidencialidad

Fuente: ARCH



#### 4.1.6 Contacto con las autoridades

### CASO DE USO: Contacto con las Autoridades



## CASO ARCH: Seguimiento de la puesta en marcha del EGSi



MEMORANDO Nro. ...

Fecha:.....

**PARA:** Máxima Autoridad

**ASUNTO:** AVANCE DE PROYECTO DE ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN

De mi consideración:

Con un atento y cordial saludo, y en base a la sumilla inserta del memorando Nro ..... referente a la Difusión de la Política de Seguridad de la Información, en la cual usted autoriza la implementación del Esquema Gubernamental de Seguridad de la Información "EGSI" y la conformación del Comité de Seguridad de la Información, el mismo que en reunión da a conocer el cumplimiento de la elección del oficial de la Seguridad de la Información, con lo cual se inicia el proceso de cada uno de los puntos que menciona el documento.

Con estos antecedentes, me permito informar el avance del proyecto mediante reporte adjunto con el .....% de hitos cumplidos por parte de la Agencia de Regulación y Control Hidrocarburífero, hasta la presente fecha, en espera de la revisión de los ítems y calidad de verificables.

Atentamente,

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

**Figura 11: Modelo de Seguimiento de puesta en Marcha del EGSi**

**Fuente: ARCH**

#### **4.1.7 Contactos con grupos de interés especiales**

- VER ANEXO 4.1.7.- Mantener un contacto con organizaciones públicas y privadas o grupos de interés especializados en seguridad de la información, intercambiar información y recibir reportes o alertas sobre ataques de vulnerabilidad de la información.

#### **4.1.8 Revisión independiente de la seguridad de la información**

- VER ANEXO 4.1.8.- Revisiones independientes de la gestión realizada para la seguridad de la información para identificar cambios de mejora y documentar y registrar todas las revisiones independientes.

#### **4.1.9 Identificación de los riesgos relacionados con las partes externas**

- VER ANEXO 4.1.9.- Evaluar los riesgos para la información que se relaciona con terceras personas, proceso de bloqueo mientras se firman acuerdos de confidencialidad, y garantizar que las partes externas estén conscientes de sus deberes y obligaciones.

Las partes externas se consideran las siguientes:

- Proveedores de servicios (ej., internet, proveedores de red, servicios telefónicos, servicios de mantenimiento, energía eléctrica, agua, entre otros);
- Servicios de seguridad;

- Contratación externa de proveedores de servicios y/u operaciones;
- Asesores y auditores externos;
- Limpieza, alimentación y otros servicios de soporte contratados externamente;
- Personal temporal (estudiantes, pasantes, funcionarios públicos externos);
- Ciudadanos/clientes.

#### **4.1.10 Consideraciones de la seguridad cuando se trata con ciudadanos o clientes**

VER ANEXO 4.1.10 Identificar requisitos de seguridad antes de facilitar servicios a ciudadanos o clientes de entidades gubernamentales que utilicen o procesen información de los mismos o de la entidad.

#### **4.1.11 Consideraciones de la seguridad en los acuerdos con terceras partes.**

Garantizar que exista un entendimiento adecuado en los acuerdos que se firmen entre la organización y la tercera parte con el objeto de cumplir los requisitos de la seguridad de la entidad. Refiérase a la norma INEN ISO/IEC para los aspectos claves a considerar en este control.

### **CASO ARCH: Consideraciones de la seguridad en los acuerdos con terceras partes**

- Dentro del ARCH, la máxima autoridad debe dar la autorización sobre la implementación y el seguimiento periódico sobre el avance de la implementación, mediante revisión de informes mensuales que deben ser entregados por el oficial de seguridad designado.
  
- Se deberá realizar la difusión, capacitación y sensibilización del documento, mediante charlas capacitaciones físicas o virtuales y mediante correo electrónico, a todo el personal que labora en la institución (ARCH), sobre la seguridad de la Información.
  
- Se realizará una respectiva reunión, para conformar el Comité de Seguridad de la Información, el mismo que estará integrado al menos por el director o su delegado de las siguientes áreas dentro del ARCH: Dirección Administrativa, Dirección de Talento Humano, Dirección de Tecnologías de la Información, Dirección de Auditoría Interna.

## MEMORANDO DE CONVOCATORIA DE CONFORMACIÓN DE COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y OFICIAL DE SEGURIDAD



MEMORANDO Nro. ...

Fecha:.....

**PARA:** Dirección de Recursos Humano  
Dirección Administrativa  
Dirección de Auditoría Interna

**ASUNTO:** COMITE DE GESTION DE LA SEGURIDAD DE LA INFORMACION DE LA AGENCIA DE REGULACION Y CONTROL DE HIDROCARBUROS.

De conformidad con el Memorando Nro. .... por parte de la máxima autoridad, y para dar cumplimiento a la implementación del Sistema Gestión de Seguridad la Información y de acuerdo a la metodología establecida, sobre la conformación del "Comité de Seguridad de la Información"; será integrado al menos por:

1. Director Administrativo
2. Director de Recursos Humanos
3. Director del Área de tecnologías de la Información
4. Director de Auditoría Interna
5. Y el Oficial de Seguridad de la Información

Con estos antecedentes, se convoca a una reunión el día....., a partir de las..... que se llevará a cabo en ....., con el fin de conformar el "Comité de Seguridad de la Información" y la designación del Oficial de seguridad de la Información, el mismo que tendrá las responsabilidades detalladas en la metodología a implementarse.


Atentamente,

**DIRECTOR DE TECNOLOGIAS DE LA INFORMACION**

**Figura 12. Memorando conformación de comité y oficial de seguridad de la información.**

**Fuente: ARCH**

## INFORME SOBRE LA CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

	DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN		
<b>Informe No.:</b>	<b>Año:</b>	<b>Mes:</b>	<b>Día:</b>
<b>Tema:</b> Comité de Gestión de Seguridad de la Información, elección de Oficial de Seguridad.		<b>Hora Inicial:</b>	<b>Hora Final:</b>
<b>Lugar:</b> ARCH			
<b>DIRECCIONES PARTICIPANTES</b>		<b>TEMA</b>	
<ul style="list-style-type: none"> <li>Dirección de Recursos Humanos</li> <li>Dirección Administrativa</li> <li>Dirección de Auditoría Interna</li> <li>Dirección de Tecnologías de la Información.</li> </ul>		<ul style="list-style-type: none"> <li>Conformación del Comité de Seguridad de la Información y elección del Oficial de Seguridad de la Información.</li> </ul>	
<b>RESPONSABLES</b>			
<ul style="list-style-type: none"> <li>Ing<sup>UMA</sup>.....</li> </ul>			
<b>GENERALIDADES DEL INFORME / DESARROLLO / CONCLUSIONES Y DECISIONES</b>			
<p><b>ANTECEDENTES:</b> En referencia a sumilla del Memorando No..... de fecha....., por parte de la Máxima Autoridad, y para la implementación del EGSI y conformación del "Comité de Seguridad de la Información" según la metodología establecida; el comité estará integrada al menos por:</p> <ol style="list-style-type: none"> <li>1.- El Director Administrativo</li> <li>2.- El Director de Recursos Humanos</li> <li>3.- El Director del Área de Tecnologías de la Información.</li> <li>4.- El Director de Auditoría Interna</li> <li>5.- Y el Oficial de Seguridad de la Información</li> </ol> <p>Se dispone la conformación del Comité de Gestión de la Seguridad de la Información uy se procesa con la designación del Oficial de Seguridad, para los fines pertinentes. Con fecha....., mediante memorando Nro.....</p> <p><b>OBJETIVO:</b> Conformar el comité de Seguridad de la Información y elegir el oficial de Seguridad de la Información, el mismo que tendrá responsabilidades detalladas en el plan desarrollado.</p> <ul style="list-style-type: none"> <li>Eleccion de oficial de Seguridad de la Información</li> <li>Conformacion de Comité de Seguridad de la Información.</li> </ul> <p>En virtud de lo antes expuesto queda elegido <b>ecomo</b> Oficial de Seguridad de la Información al señor..... con CI..... Y conformación del comité de seguridad de la información a los señores:</p> <p>Nombres..... CI..... Cargo.....</p>			






ASISTENTES	DIRECCION/ REPRESENTANTES	E-mail	FIRMA
Andrea Moscoso	Dirección Administrativa	Andrea.moscoso@arch.gob.ec	
Juan Rivadeneira	Dirección de Recursos Humanos	Juan.rivadeneira@arch.gob.ec	
Daniela Quiros	Dirección de Auditoría Interna	Daniela.quiros@arch.gob.ec	
Carlos Miranda	Dirección de Tecnologías de la Información	Carlos.miranda@arch.gob.ec	
Diego Martínez	Oficial de Seguridad de la Información.	Diego.martinez@arch.gob.ec	

Figura 13. Acta de Reuniones

Fuente: ARCH

## **4.2 Establecer la estrategia del servicio (políticas) en la Agencia de Regulación y Control Hidrocarburífero**

La política del SGSI, debe estar alineada con los objetivos organizacionales, es allí donde la alta dirección debe establecer un marco de referencia para posteriormente fijar objetivos específicos de control por cada proceso de la compañía, los cuales deben establecerse en conjunto con el líder de cada proceso.

La política del SGSI debe tener en cuenta el marco legal de la Agencia Nacional de Regulación y Control Hidrocarburífero:

- Estatuto Orgánico por Procesos N° 321 – Registro Oficial
- Registro Oficial Nro. 437
- Registro Oficial Nro. 436
- Resolución Conformación del Comité de Transparencia
- Plan Anual de Inversiones del 2015
- Documento Equipamiento de Laboratorio
- Reglamento de Higiene y seguridad DAF-CGTH-DM-06

Parte fundamental en la implementación de sistema es la divulgación de la política trazada a toda la compañía con el fin de que las decisiones en los diferentes niveles de la compañía estén siempre alineadas con lo que la alta dirección espera del sistema, adicional, dejar clara la correlación o impacto



de los objetivos genera mayor claridad de la razón de ser de los mismos y un mayor compromiso por parte de los responsables.

La gestión de riesgo en la seguridad de la información, inicia al establecer el contexto, este se refiere a la definición del alcance, límites y la política del SGSI, con el fin de asegurar que todos los activos de información de la organización se contemplen en el SGSI.

Es importante tener en consideración para los límites y criterios de aceptación de los riesgos: el tiempo, costo, recursos, impactos y requisitos legales para implementar los controles.

Al definir el contexto del SGSI, se realiza la valoración de los riesgos que involucra:

### **Política de seguridad de la información**

Documento de la Política de la Seguridad de la Información

a) La máxima autoridad de la institución dispondrá la implementación de este Esquema.

Gubernamental de Seguridad de la Información (EGSI) en su entidad.

b) Se difundirá la siguiente política de seguridad de la información como referencia.

Las entidades de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan

información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

En todo este documento esta marca significa que se trata de un control/directriz prioritario

Las entidades públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias.

#### **4.2.1. Revisión de la Política de Seguridad de la Información**

Para garantizar la vigencia de la política de seguridad de la información en la institución, esta deberá ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológica, económico, entre otros.

#### **4.2.2 Identificación de los Riesgos posibles en la institución**

La identificación del riesgo contempla inicialmente la determinación de los activos de información dentro del alcance del SGSI, teniendo en cuenta la ubicación, responsable y funciones.

De la misma manera se deben determinar las amenazas, vulnerabilidades e impactos en la organización, por las posibles pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

De acuerdo a lo anterior se realiza un inventario de activos relacionando cada proceso de la organización contemplado en el alcance del SGSI, los activos hacen referencia a: personal de la organización, imagen corporativa, información, sistemas de información, procesos, productos, aplicaciones y el entorno físico.

#### **4.2.3 Planificación del tratamiento del Riesgo**

La gestión de los riesgos es un proceso en el cual se implementan las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos analizados e identificados, de forma que las consecuencias que puedan generar sean eliminadas o, si esto no es posible, se puedan reducir lo máximo posible. Un resultado del análisis de riesgos es el criterio para

determinar los niveles de riesgo aceptables y en consecuencia, cuáles son los niveles inaceptables y que por lo tanto serán gestionados.

### CASO DE USO: Planificación del Tratamiento del Riesgo

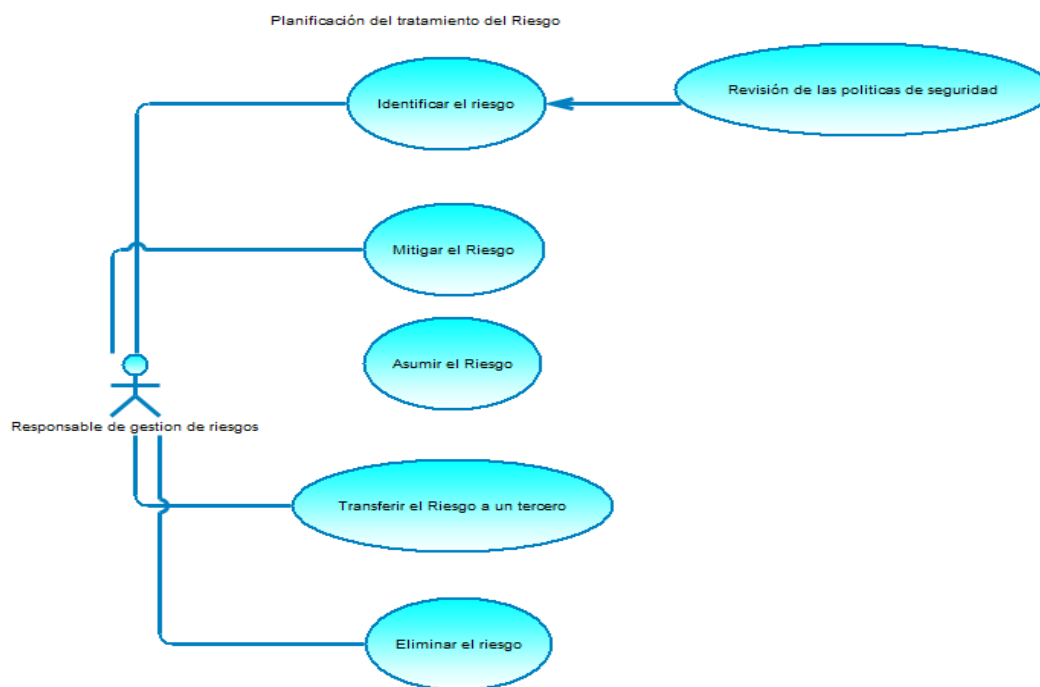


Figura 14. Planificación del Tratamiento del Riesgo

Fuente: ARCH

El objetivo es reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización.

Una vez se han analizados y se conocen los riesgos de la organización se determinara el tratamiento que deben recibir los activos y se deben tomar las acciones necesarias. Los cuatro tipos de tratamiento requieren de diferentes acciones:

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.
  
- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.
  
- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).
  
- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No habrá más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que en la agencia nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección.

#### **4.2.4. Política de Control de Acceso a los Sistemas de Información**

- a) Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
- b) Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
- c) Definir claramente los autorizadores de los permisos de acceso a la información.

#### **4.2.5. Registro de usuarios internos y externos de la institución**

Establecer un procedimiento formal, documentado y difundido, en el cual se evidencie detalladamente los pasos y responsables para:

- VER ANEXO 4.2.5.- Gestionar el administrador de accesos, documentos de requerimiento de accesos para personal interno o externo y documentos de confidencial para los mismos.

#### 4.2.6. Gestión de privilegios a usuarios

- VER ANEXO 4.2.6.- Controla la asignación de privilegios, mantiene y un cuadro de identificación y asignación de privilegios para los usuarios y que los activos de información tecnológica tengan niveles de acceso.

#### CASO ARCH: Permisos a Usuarios en la Gestión de Privilegios

Se puede usar el mismo servidor de dominios para gestionar los permisos que se puede asignar a los usuarios, como se muestra en la siguiente figura:

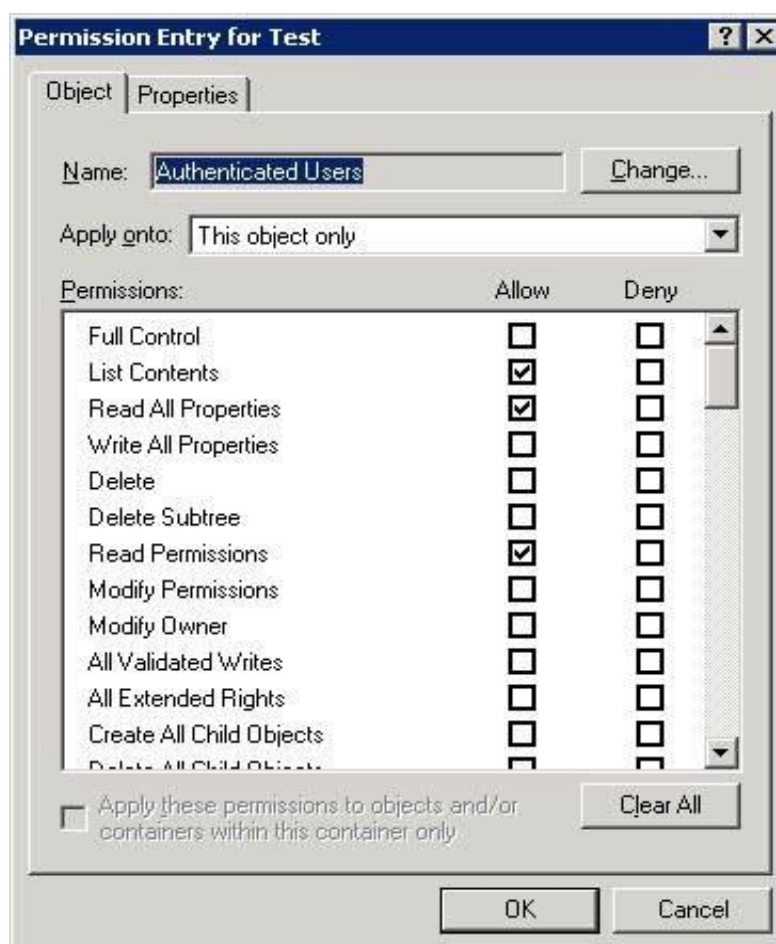


Figura 15. Tabla de permisos a usuarios en la Gestión de Privilegios

Fuente: ARCH

#### **4.2.7. Gestión de contraseñas para usuarios**

Establecer un proceso formal para la asignación y cambio de contraseñas, que contenga mínimo 8 caracteres entre letras, números, mayúsculas y minúsculas y caracteres especiales.

#### **4.2.8. Revisión de los derechos de acceso de los usuarios**

a) Realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 30 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.

b) Evidenciar los cambios sobre los derechos de acceso en archivos de log o registro de los sistemas, los cuales deben estar disponibles en caso que se requieran.

#### **4.2.9. Uso de contraseñas para usuarios internos y externos**

➤ VER ANEXO 4.2.9.- Responsabilidades sobre el uso de contraseñas para usuarios externos e internos, recomendaciones sobre las contraseñas deben tener ciertos caracteres, evitar contraseñas en blando y realizar un cambio periódico de las mismas.



#### **4.2.10. Equipo de usuario desatendido**

a) Implementar medidas para que, en un determinado tiempo (ej., no mayor a 10 minutos), si el usuario no está realizando ningún trabajo en el equipo, este se bloquee, y se desbloquee únicamente si el usuario ingresa nuevamente su clave.

#### **4.2.11. Política de puesto de trabajo despejado y pantalla limpia**

a) El Oficial de Seguridad de la Información deberá gestionar actividades periódicas una vez cada mes como mínimo para la revisión al contenido de las pantallas de los equipos, con el fin de que no se encuentren iconos y accesos innecesarios, y carpetas y archivos que deben ubicarse en la carpeta de documentos del usuario.

b) Mantener bajo llave la información sensible cajas fuertes o gabinetes, en especial cuando no estén en uso y no se encuentre personal en la oficina.

c) Desconectar de la red, servicio o sistema, las computadoras personales, terminales, impresoras asignadas a funciones críticas, cuando se encuentren desatendidas. Por ejemplo, haciendo uso de protectores de pantalla con clave.

d) Proteger los puntos de recepción de correo y fax cuando se encuentren desatendidas.

e) Bloquear las copadoras y disponer de un control de acceso especial para horario fuera de oficinas.

f) Retirar información sensible una vez que ha sido impresa.

- g) Retirar información sensible, como las claves, de sus escritorios y pantallas.
- h) Retirar los dispositivos removibles una vez que se hayan dejado de utilizar.
- i) Cifrar los discos duros de los computadores personales escritorio, portátiles, entre otros y otros dispositivos que se considere necesarios, de las máximas autoridades de la institución.

#### **4.2.12. Política de uso de los servicios de red**

- a) Levantar un registro de los servicios de red la institución.
- b) Identificar por cada servicio los grupos de usuarios que deben acceder.
- c) Definir los perfiles y roles para cada grupo de usuarios que tenga acceso a la red y sus servicios.
- d) Definir mecanismos de bloqueos para que sea restringido el acceso de equipos a la red.

#### **4.2.13. Autenticación de usuarios para conexiones externas**

- a) Generar mecanismos para asegurar la información transmitida por los canales de conexión remota, utilizando técnicas como encriptación de datos, implementación de redes privadas virtuales (VPN) y Servicio de Acceso Remoto (SAR) .

b) Realizar un mecanismo diferenciado para la autenticación de los usuarios que requieren conexiones remotas, que permita llevar control de registros logs y que tenga limitaciones de accesos en los segmentos de red.

#### **4.2.15. Protección de los puertos de configuración y diagnóstico remoto**

a) Establecer un procedimiento de soporte, en el cual se garantice que los puertos de diagnóstico y configuración sean sólo accesibles mediante un acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/ software que requiere el acceso.

b) Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.

#### **4.2.16. Separación en las redes**

➤ VER ANEXO 4.2.16.- Evaluación de riesgos para segmentos de red, redes de dominios lógicos, documentar segregaciones de red, configuraciones de puestas de enlace, controlar flujos de datos, etc.

#### **4.2.17. Control de conexión a las redes**

a) Restringir la capacidad de conexión de los usuarios, a través de puertas de enlace de red (gateway) que filtren el tráfico por medio de tablas o reglas predefinidas, conforme a los requerimientos de la institución.

b) Aplicar restricciones considerando:

- Mensajería
- Transferencia de archivos
- Acceso interactivo
- Acceso a las aplicaciones
- Horas del día y fechas de mayor carga

c) Incorporar controles para restringir la capacidad de conexión de los usuarios a redes compartidas especialmente de los usuarios externos a la institución.

#### **4.2.18. Control del enrutamiento en la red**

a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.

Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes

internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.

Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (ACL), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos de usuarios con salida libre y sin control, en base a las políticas de la institución.

#### **4.2.19. Procedimiento de registro de inicio seguro**

- VER ANEXO 4.2.19.- Autenticación de usuarios autorizados, proceso de registro de intentos fallidos o exitosos, restricción del tiempo de conexión, etc.

#### **4.2.20. Identificación y autenticación de usuarios**

- VER ANEXO 4.2.20.- Evidenciar las actividades de las personas responsables de administraciones críticas, las actividades regulares no deben ser realizadas desde cuentas privilegiadas, evitar uso de usuarios genéricos.

#### **4.2.21. Sistema de gestión de contraseñas**

- VER ANEXO 4.2.21.- Políticas de Acceso y buen uso de las contraseñas, cambio de contraseña en el primer registro, documentar el control de acceso para usuarios temporales, etc.

#### **4.2.22. Uso de las utilidades del sistema**

Restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles de un sistema en base a las siguientes directrices:

- VER ANEXO 4.2.22.- Restringir uso de programas en base al uso de procedimientos de identificación, autenticación para programas utilitarios y separación con el software de aplicaciones además de la limitación del uso de programas utilitarios.

#### **4.2.23. Tiempo de inactividad de la sesión**

- a) Suspende las sesiones inactivas después de un periodo definido de inactividad sin consideración de lugar dispositivo de acceso
- b) Parametrizar el tiempo de inactividad en los sistemas de procesamiento de información para suspender y cerrar sesiones.

#### **4.2.24. Limitación del tiempo de conexión**

- VER ANEXO 4.2.24.- Define restricciones en los tiempos de conexión para brindar seguridad adicional en las aplicaciones de alto riesgo.

#### **4.2.25. Control de acceso a las aplicaciones y a la información**

- VER ANEXO 4.2.25.- Controla el acceso de usuarios a la información y a las funciones del sistema de aplicación.

#### **4.2.26. Restricción de acceso a la información**

- VER ANEXO 4.2.26.- Controlar el acceso a las funciones de los sistemas, definir mecanismos de control para los derechos de acceso de los usuarios.

#### **4.2.27. Aislamiento de sistemas sensibles**

- VER ANEXO 4.2.27.- Identificar los sistemas sensibles y los riesgos que presentan cuando se ejecuta una aplicación o se encuentra compartiendo recursos.

#### **4.2.28. Computación y comunicaciones móviles**

- VER ANEXO 4.2.28.- Evitar exposición de equipos en sitios de alto riesgo, que la información sensible se encuentre en una partición diferente, que se defina un tiempo máximo que el equipo pueda estar sin conexión, etc.

#### **4.2.29. Trabajo remoto**

- VER ANEXO 4.2.29.- Se podrá autorizar una conexión en modo remoto, siempre que en la institución se apliquen las disposiciones de seguridad y los controles establecidos y evitar conexiones que no cumplan las respectivas medidas de seguridad.

#### **4.3 Identificación del riesgo en la Agencia de Regulación y Control Hidrocarburífero**

- VER ANEXO 4.3.- Inventariar los activos de información, sus responsables y el uso aceptable de los activos.





## Hoja de Sistemas e Infraestructura

Matriz de Análisis de Riesgo				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																																													
				Actos originados por la criminalidad común y motivación política											Sucesos de origen físico								Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones inadecuadas																										
Sistemas e Infraestructura	Clasificación			Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Altastracato (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de información, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software pirateado	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de dispositivos móviles	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Unidades portátiles con información sin cifrado	Transmisión no cifrada de datos críticos	Manejo inadecuado de contraseñas (incógnitas, no cambiar, compartirlas, etc.)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono											
	Acceso exclusivo	Acceso limitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)		Actos originados por la criminalidad común y motivación política	Sucesos de origen físico	Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones inadecuadas																																										
Programas de producción de datos	x	x	4	4	4	4	3	4	4	4	4	4	3	3	4	4	4	4	4	3	3	4	3	4	4	4	4	4	3	2	4	4	4	4	3	3	4	3	3	4	3								
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)	x	x	2	8	8	6	8	8	8	8	8	8	6	6	8	8	8	8	6	6	8	6	8	8	8	8	8	8	6	4	8	8	8	6	6	6	8	8	6	6	8	6							
Impresoras	x	x	3	12	12	9	12	12	12	12	12	12	9	9	12	12	12	12	9	9	12	9	12	12	12	12	12	12	9	6	12	12	12	9	9	9	12	9	9	12	9	9	12	9					
Memorias portátiles	x	x	3	12	12	9	12	12	12	12	12	12	9	9	12	12	12	12	9	9	12	9	12	12	12	12	12	12	9	6	12	12	12	9	9	9	12	9	9	12	9	9	12	9					
PBX (Sistema de telefonía convencional)	x	x	2	8	8	6	8	8	8	8	8	8	6	6	8	8	8	8	6	6	8	6	8	8	8	8	8	8	6	4	8	8	8	6	6	6	8	8	6	6	8	6	6	8	6				
Celulares	x	x	2	8	8	6	8	8	8	8	8	8	6	6	8	8	8	8	6	6	8	6	8	8	8	8	8	8	6	4	8	8	8	6	6	6	8	8	6	6	8	8	6	6	8	6			
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega)	x		1	4	4	3	4	4	4	4	4	4	3	3	4	4	4	4	4	3	3	4	3	4	4	4	4	4	3	2	4	4	4	3	3	3	4	3	3	4	3	3	4	3	3	4	3		
Vehículos	x	x	2	8	8	6	8	8	8	8	8	8	6	6	8	8	8	8	6	6	8	6	8	8	8	8	8	8	6	4	8	8	8	6	6	6	8	8	6	6	8	8	6	6	8	6	6	8	6

Figura 17: Matriz de Análisis de Riesgo de los Sistemas Informáticos

Fuente: ARCH

### Hoja de Personal

Matriz de Análisis de Riesgo				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																												
Personal	Clasificación			Actos originados por la criminalidad común y motivación política												Sucesos de origen físico						Sucesos derivados de la impericia										
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / deslave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados / software "pirateado"	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	
					4	4	3	4	4	4	4	4	4	4	3	3	4	4	4	4	4	4	3	3	4	3	4	4	4	4	4	4
Informática / Soporte técnico interno	x	x		4	16	16	12	16	16	16	16	16	16	12	12	16	16	16	16	12	12	16	12	16	16	16	16	16	16	12	8	16
Soporte técnico externo	x			3	12	12	9	12	12	12	12	12	9	9	12	12	12	12	12	9	9	12	9	12	12	12	12	12	12	9	6	12
Servicio de limpieza de planta	x	x		3	12	12	9	12	12	12	12	12	9	9	12	12	12	12	12	9	9	12	9	12	12	12	12	12	9	6	12	
Servicio de limpieza externo	x	x		2	8	8	6	8	8	8	8	8	6	6	8	8	8	8	8	6	6	8	6	8	8	8	8	8	6	4	8	
Servicio de mensajería de propio	x	x		3	12	12	9	12	12	12	12	12	9	9	12	12	12	12	12	9	9	12	9	12	12	12	12	12	9	6	12	
Servicio de mensajería de externo	x		x	2	8	8	6	8	8	8	8	8	6	6	8	8	8	8	8	6	6	8	6	8	8	8	8	6	4	8		

Figura 18: Matriz de Análisis de Riesgos del Personal

Fuente: ARCH

### Análisis de Riesgo promedio

		Probabilidad de Amenaza		
		Criminalidad y Político	Sucesos de origen físico	Negligencia y Institucional
Magnitud de Daño	Datos e Información	12,2	11,8	10,2
	Sistemas e Infraestructura	10,1	9,9	8,5
	Personal	10,7	10,4	8,9

Figura 19: Análisis de Riesgo Promedio

Fuente: ARCH

### Análisis de Factores de Riesgo

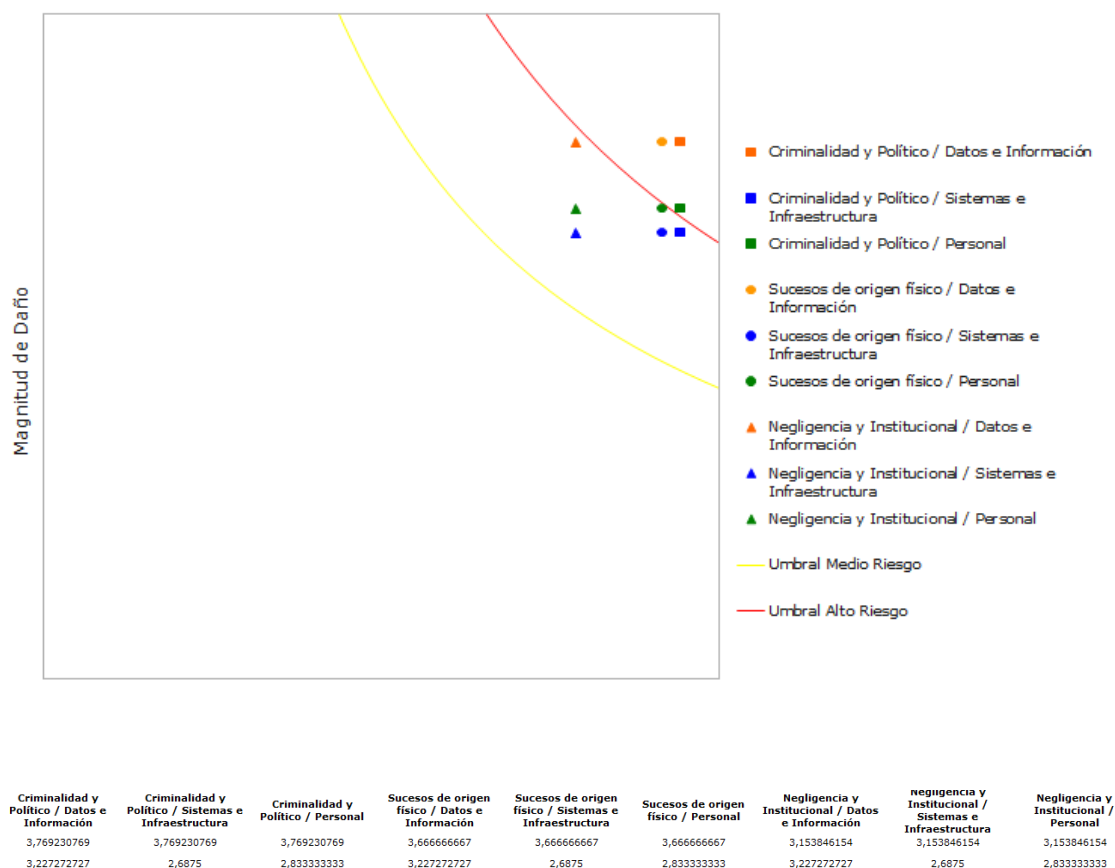


Figura 20: Análisis factores de Riesgo

Fuente: ARCH

Valoración	Escala	Valor_mi n	Valor_ma x	Lineas	Umbral Medio Riesgo	Umbral Alto Riesgo
Ninguna	1	1	3		7	10,5
Baja	2	4	6	x	Y	Y
Mediana	3	8	9	1,0	7,0	10,5
Alta	4	12	16	1,1	6,4	9,5
				1,2	5,8	8,8
				1,3	5,4	8,1
				1,4	5,0	7,5
				1,5	4,7	7,0
				1,6	4,4	6,6
				1,8	4,0	6,0
				1,8	3,9	5,8
				1,9	3,7	5,5
				2,0	3,5	5,3
				2,1	3,3	5,0
				2,2	3,2	4,8
				2,3	3,0	4,6
				2,4	2,9	4,4
				2,5	2,8	4,2
				2,6	2,7	4,0
				2,7	2,6	3,9
				2,8	2,5	3,8
				2,9	2,4	3,6
				3,0	2,3	3,5
				3,1	2,3	3,4
				3,2	2,2	3,3
				3,3	2,1	3,2
				3,4	2,1	3,1
				3,5	2,0	3,0
				3,6	1,9	2,9
				3,7	1,9	2,8
				3,8	1,8	2,8
				3,9	1,8	2,7
				4,0	1,8	2,6

Figura 21: Fuente de valores

Fuente: ARCH

## INTERPRETACIÓN DE RESULTADOS

La matriz de datos analizados está compuesta por el ingreso de tres hojas en las cuales se encuentran varios parámetros a ser evaluados, en la primera hoja **DATOS**, existen varios parámetros los cuales van a ser calificados con una ponderación de 1-20, de acuerdo a documentos

institucionales, base de datos, comunicaciones internas y externas que se encuentran en la columna de datos e información.

En la hoja de **SISTEMAS** de igual manera los puntos de calificación son determinados por actos originados por la criminalidad común y motivación política, sucesos de origen físico, sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales se cruza con la valoración con el sistema y la infraestructura.

En la hoja de **PERSONAL** los tres campos que se encuentra en la fila se cruza con los datos específicos del personal.

La magnitud de daño se cruza con la probabilidad de amenaza en donde se puede visualizar en el cuadro que los datos e información tienen una gran incidencia en el aspecto criminalidad y político con una valor promedio de 12,2 seguidos por el suceso de origen físico y por último el personal con criminalidad y político.

En la curva tenemos dos variables que se cruzan entre la magnitud de daño y probabilidad de amenaza, donde se puede visualizar que los tres puntos detallados anteriormente sobrepasan el umbral de color rojo a los cuales hay que tener mucho cuidado y que deben ser atacados con planes de contingencia para un menor impacto.

#### **4.3.1. Inventario de activos**

- Inventariar los activos primarios, en formatos físicos y/o electrónicos:
- Inventariar los activos de soporte de Hardware:
- Inventariar los activos de soporte de Software:
- Inventariar los activos referentes a la estructura organizacional:

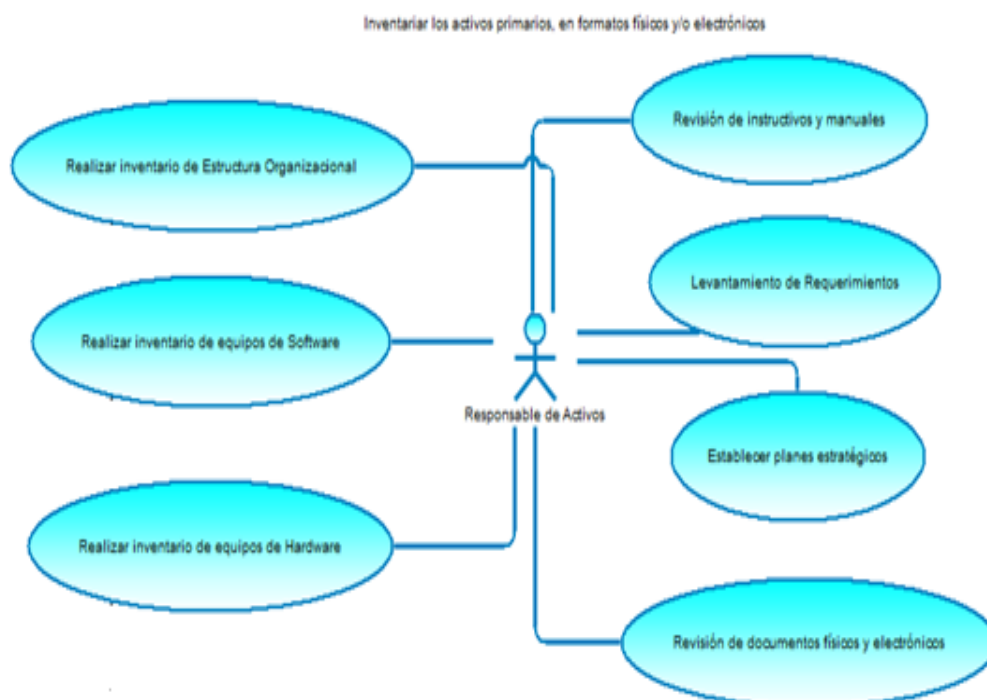
#### **4.3.2. Responsable de los activos**

a) Asignar los activos asociados (o grupos de activos) a un individuo que actuará como Responsable del Activo. Por ejemplo, debe haber un responsable de los computadores de escritorio, otro de los celulares, otro de los servidores del centro de datos, entre otros. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos. El Responsable del Activo tendrá las siguientes funciones:

- VER ANEXO 4.3.2.- Asignar los activos asociados (o grupos de activos) a un individuo que actuará como Responsable del Activo

b) Consolidar los inventarios de los activos a cargo del Responsable del Activo, por área o unidad organizativa.

### 4.3.3. Uso aceptable de los activos



**Figura 22. Uso Aceptable de Activos**

**Fuente: ARCH**

Reglamentar el uso de correo electrónico institucional:

- Este servicio debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- Cada persona es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- Todos los mensajes deben poder ser monitoreados y conservados permanentemente por parte de la institución.



- Toda cuenta de correo electrónico debe estar asociada a una única cuenta de usuario.
- La conservación de los mensajes se efectuará en carpetas personales, para archivar la información de acceso exclusivo del usuario y que no debe compartirse con otros usuarios. Debe definirse un límite de espacio máximo.
- Toda la información debe ser gestionado de forma centralizados y no en las estaciones de trabajo de los usuarios.
- Todo sistema debe contar con las facilidades automáticas que notifiquen al usuario cuando un mensaje enviado por él no es recibido correctamente por el destinatario, describiendo detalladamente el motivo del error.
- Deben utilizarse programas que monitoreen el accionar de virus informáticos tanto en mensajes como en archivos adjuntos, antes de su ejecución.
- Todo usuario es responsable por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos. En estos casos, no deben contestar dichos mensajes y deben enviar una copia al Oficial de Seguridad de la Información para que efectúe el seguimiento y la investigación necesaria.
- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.

- Todo usuario es responsable de la cantidad y tamaño de mensajes que envíe. Debe controlarse el envío no autorizado de correos masivos.



**e) Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios:**

- VER ANEXO 4.3.3.- Debido uso y acceso al internet y sus aplicaciones Identificando, documentando e implementando las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información

**f) Reglamentar el uso de los sistemas de video-conferencia:**

- VER ANEXO 4.3.3.- Debido uso y acceso a sistemas de videoconferencia, documentando e implementando las reglas sobre el uso aceptable de los activos asociados con los servicios de procesamiento de la información.

**REGLAMENTO PARA EL USO ADECUADO DEL SERVICIO DE INTERNET, SISTEMA  
DE VIDEOCONFERENCIA Y CORREO ELECTRONICO INSTITUCIONAL**

 GOBIERNO NACIONAL DE LA REPUBLICA DEL ECUADOR	<b>Procedimiento No. 1</b> REGLAMENTO DEL USO DEL SERVICIO DE INTERNET, SISTEMA DE VIDEOCONFERENCIA Y CORREO ELECTRONICO INSTITUCIONAL	 Agencia de Regulación y Control Hidrocarburiífero  <b>Código:</b>
---	--	--

**REGLAMENTO PARA EL USO ADECUADO DEL SERVICIO DE  
INTERNET, SISTEMA DE VIDEOCONFERENCIA Y CORREO  
ELECTRÓNICO INSTITUCIONAL**

**CAPITULO I**

**ASPECTOS GENERALES**

**Art. 1.- Objetivo**

El objeto de éste Reglamento para el uso adecuado del servicio de Internet, sistema de videoconferencia y correo electrónico institucional, es normar y optimizar la disponibilidad, uso y control en la navegación en sitios web del Internet, de la capacitación virtual y mensajería electrónica que se encuentran a disposición de las y los servidores públicos del ARCH.

**Art. 2.- Definiciones.-** Para efectos del presente Reglamento, se entenderá por:

- a) ARCH: Agencia de Regulación y Control Hidrocarburiífero
- b) DTI: Dirección de Tecnologías de la Información.
- c) Usuario: Servidor Público o persona autorizada del ARCH.
- d) Servidor Público: Serán servidoras o servidores públicos todas las personas que en cualquier forma o a cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro del sector público. (Definido en la LOSEP – Art. 4)
- e) Sistema de Videoconferencia: Plataforma tecnológica que permite a varios usuarios mantener una conversación virtual por medio de la transmisión en tiempo real de video, sonido y texto a través de Internet.
- f) Internet: Es la conexión vía cable o inalámbrica con la que las computadoras cuentan dentro de la red del ARCH para conectarse y visualizar las páginas web desde un navegador y acceder a otros servicios que ofrece esta red.
- g) Correo electrónico: Sistema de mensajería electrónica hacia otros usuarios vía Internet.

**Art. 3.- Régimen disciplinario.-** El incumplimiento en el presente Reglamento e instrucciones especiales, generará responsabilidad administrativa de acuerdo a lo prescrito en el Art. 42, inciso a) y Art. 43, literales a) y b) de la Ley Orgánica de Servicio Público.

El desconocimiento del presente reglamento, no exime de responsabilidad y sanciones a que se haga acreedor en término del presente documento que se establezcan.

**Figura 23: Reglamento para el uso adecuado del servicio de internet, sistema de  
videoconferencia y correo electrónico institucional**

**Fuente: ARCH**

#### 4.3.4. Directrices de clasificación de la información

- a) Clasificar la información como pública o confidencial.
- b) Elaborar y aprobar un catálogo de clasificación de la información. Se la deberá clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la institución.

#### 4.3.5. Etiquetado y manejo de la información

- VER ANEXO 4.3.5.-

### CASO ARCH: Reglamento Uso de Internet, correo electrónico y videoconferencia.

PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN"			
INFORME DE CUMPLIMIENTO DE HITOS			
ENTIDAD / (SIGLAS):		AGENCIA DE REGULACION Y CONTROL HIDROCARBURIFERO	
DENOMINACIÓN DEL HITO:		Identificación del Riesgo	
NUMERO DE HITO:		4.3	ES UN HITO PRIORITARIO? <i>Si</i>
No.	RESUMEN ACTIVIDADES REALIZADAS	VERIFICABLE INTERNO	
1	Se procede a elaborar los reglamentos y los procedimientos	Reglamentos y procedimientos	
PIE DE RESPONSABILIDAD			
FECHA ELABORACIÓN:			
NOMBRE y CÉDULA OFICIAL DE SEGURIDAD:		FIRMA:	
NOMBRE: C.I.			
NOMBRE Y CÉDULA RESPONSABLE DE SEGURIDAD DE TI:		FIRMA:	
NOMBRE: C.I.			

Figura 24. Reglamento del uso de acceso a Internet.

Fuente: ARCH

#### **4.4 Planificación del tratamiento del riesgo en la Agencia de Regulación y Control Hidrocarburífero**

Una vez decididas las acciones a tomar, se debe realizar un análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía.

##### **4.4.1 Mitigación del riesgo**

Una vez se han identificado los requisitos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, es conveniente seleccionar e implementar los controles para garantizar la reducción de los riesgos hasta un nivel aceptable. La selección de los controles de seguridad depende de las decisiones del laboratorio basadas en los criterios para la aceptación del riesgo y debería estar sujeta a toda la legislación y los reglamentos.

##### **4.4.2 Pasos para mitigar el riesgo:**

- VER ANEXO 4.4.2.- Seguir varios pasos necesarios para mitigar el riesgo, como selección de controles, diseño de procedimientos para implantar los controles, realizar una medición y seguimiento de los mismos.



**Figura 25. Tratamiento del riesgo en el SGSI.**

**Fuente: Poveda, J. Gestión y tratamiento de los riesgos, 2007.**

#### **4.5 Implementación de los Servicios Prioritarios en la Agencia de Regulación y Control Hidrocarburífero**

Aquí se definirán los Controles e implementaciones más importantes que necesita el ARCH.

El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad.

Establece el procedimiento más adecuado para etiquetar y manejar la información de acuerdo al medio físico o digital y su nivel de criticidad.

## CASO DE USO: Implementación de Servicios Prioritarios

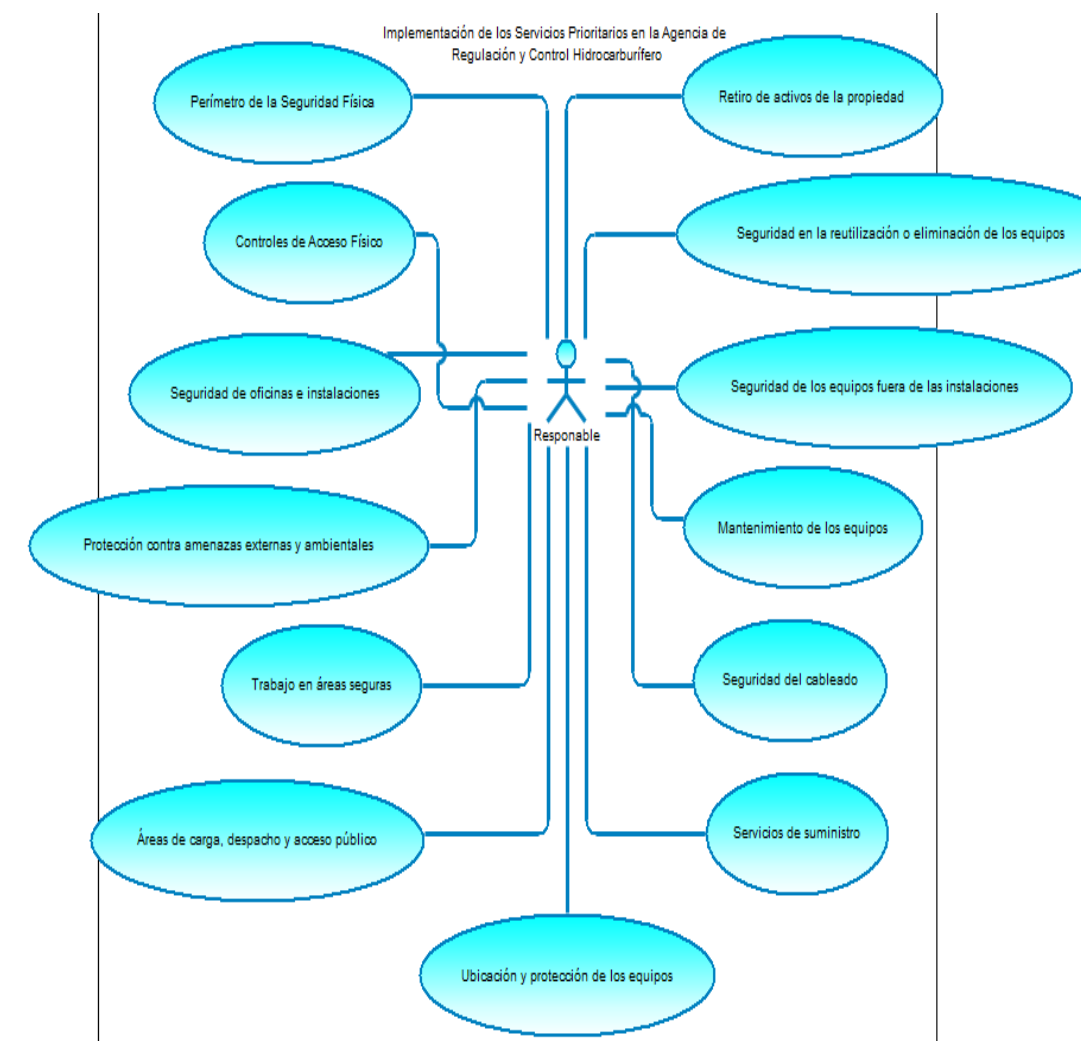


Figura 26. Implementación de Servicios Prioritarios

Fuente: ARCH

### 4.5.1. Perímetro de la seguridad física

- VER ANEXO 4.5.1.- Definir perímetros de seguridad, áreas de recepción, barreras físicas, alarmas, sistemas de vigilancia, etc.

#### **4.5.2. Controles de acceso físico**

- VER ANEXO 4.5.2.- Supervisar permanencia de los visitantes y establece límites de acceso.

#### **4.5.3. Seguridad de oficinas, recintos e instalaciones**

- VER ANEXO 4.5.3.- Estableces reglamentos y normas con relación a la seguridad en las oficinas, claves de acceso, señalamientos, etc.

#### **4.5.4. Protección contra amenazas externas y ambientales.**

- VER ANEXO 4.5.4.- ubicar equipos combustibles peligrosos a una distancia prudente, equipos contra incendios, instalaciones eléctricas, etc.

#### **4.5.5. Trabajo en áreas seguras**

- VER ANEXO 4.5.5.-  
Dar a conocer al personal las áreas seguras existentes, restringir al acceso de cámaras, equipos de audio y video sin la debida autorización



#### **4.5.6. Áreas de carga, despacho y acceso público**

- VER ANEXO 4.5.6.- Permitir únicamente a personal autorizado al área de carga, definir el área de carga y descarga y revisar el material que ingresa para evitar posibles amenazas.

#### **4.5.7. Ubicación y protección de los equipos**

- VER ANEXO 4.5.7.- Evitar accesos innecesarios a áreas restringidas, establecer directrices para no comer, beber o fumar cerca de áreas de procesamiento de información, etc.

#### **4.5.8. Servicios de suministro**

- VER ANEXO 4.5.8.- Implementar y documentar los servicios de electricidad, agua, calefacción, ventilación y aire acondicionado, Inspeccionar regularmente todos los sistemas de suministro, etc.

#### **4.5.9. Seguridad del cableado**

- VER ANEXO 4.5.9.- líneas de fuerza (energía) y de telecomunicaciones subterráneas protegidas, en cuanto sea posible, proteger cables, separar cables de energía con los de los demás, identificar y rotular de acuerdo a las normas, etc.

#### **4.5.10. Mantenimiento de los equipos**

- VER ANEXO 4.5.10.- mantenimientos periódicos a los equipos y dispositivos, únicamente con personal autorizado y calificado, registros de los mantenimientos, controles y planificaciones de los mantenimientos.

#### **4.5.11. Seguridad de los equipos fuera de las instalaciones**

- VER ANEXO 4.5.11.- Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución, controles de trabajo y cobertura de seguro.

#### **4.5.12. Seguridad en la reutilización o eliminación de los equipos**

- a) Destruir, borrar o sobrescribir los dispositivos que contienen información sensible utilizando técnicas que permitan la no recuperación de la información original.
  
- b) Evaluar los dispositivos deteriorados que contengan información sensible antes de enviar a reparación, borrar la información o determinar si se debería eliminar físicamente el dispositivo.

#### **4.5.13. Retiro de activos de la propiedad**

- a) Tener autorización previa para el retiro de cualquier equipo, información o software.
- b) Identificar a los empleados, contratistas y usuarios de terceras partes, que tienen la autorización para el retiro de activos de la institución.
- c) Establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de la devolución.
- d) Registrar cuando el equipo o activo sea retirado y cuando sea devuelto.

#### **4.6 Planificación del proceso de cambio en la Agencia de Regulación y Control Hidrocarburífero**

Aquí se controlará que los cambios no afecten los servicios entregados y se comunicará los cambios realizados, a toda la organización.

##### **4.6.1. Funciones y responsabilidades de los funcionarios**

- VER ANEXO 4.6.1.- Verificar a los candidatos, previa su contratación, solicitud del respectivo acceso y definición de las responsabilidades y competencias.

#### **4.6.2 Selección de Personal para ingreso a la Institución**

- VER ANEXO 4.6.2.- Se debe realizar todas las verificaciones necesarias y el cumplimiento de requisitos para realizar la selección de personal.

#### **4.6.3. Términos y condiciones laborales**

- VER ANEXO 4.6.3.- acuerdo de confidencialidad o no-divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información.

#### **4.6.4. Responsabilidades de la dirección a cargo del funcionario**

- VER ANEXO 4.6.4.- Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información.

#### **4.6.5. Educación, formación y sensibilización en seguridad de la información**

- a) Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información.

#### **4.6.6. Proceso disciplinario para los funcionarios**

- VER ANEXO 4.6.6.- tratamiento imparcial y correcto para los empleados que han cometido violaciones comprobadas a la seguridad de la información.

#### **4.6.7. Responsabilidades de terminación del contrato**

- VER ANEXO 4.6.7.- Comunicar oficialmente al personal las responsabilidades para la terminación de su relación laboral, recepción de documentación relacionada con las actividades que el funcionario vino desarrollando.

#### **4.6.8. Devolución de activos por parte de los funcionarios**

- VER ANEXO 4.6.8.- Formalizar el proceso de terminación del contrato, incluir la devolución de software, documentos corporativos y los equipos.

#### **4.6.9. Retiro de los privilegios de acceso**

Retirar los privilegios de acceso a los activos de información y a los servicios de procesamiento de información ej., sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, entre otros., inmediatamente luego de que se comunique formalmente al Oficial de

Seguridad de la Información formalmente la terminación de la relación laboral por parte del área correspondiente.

#### 4.7 Revisión periódica en la Agencia de Regulación y Control Hidrocarburífero

Se realizará una revisión de los procedimientos implementados periódicamente de los procesos a cada unidad competente.

#### CASO DE USO: Revisión Periódica

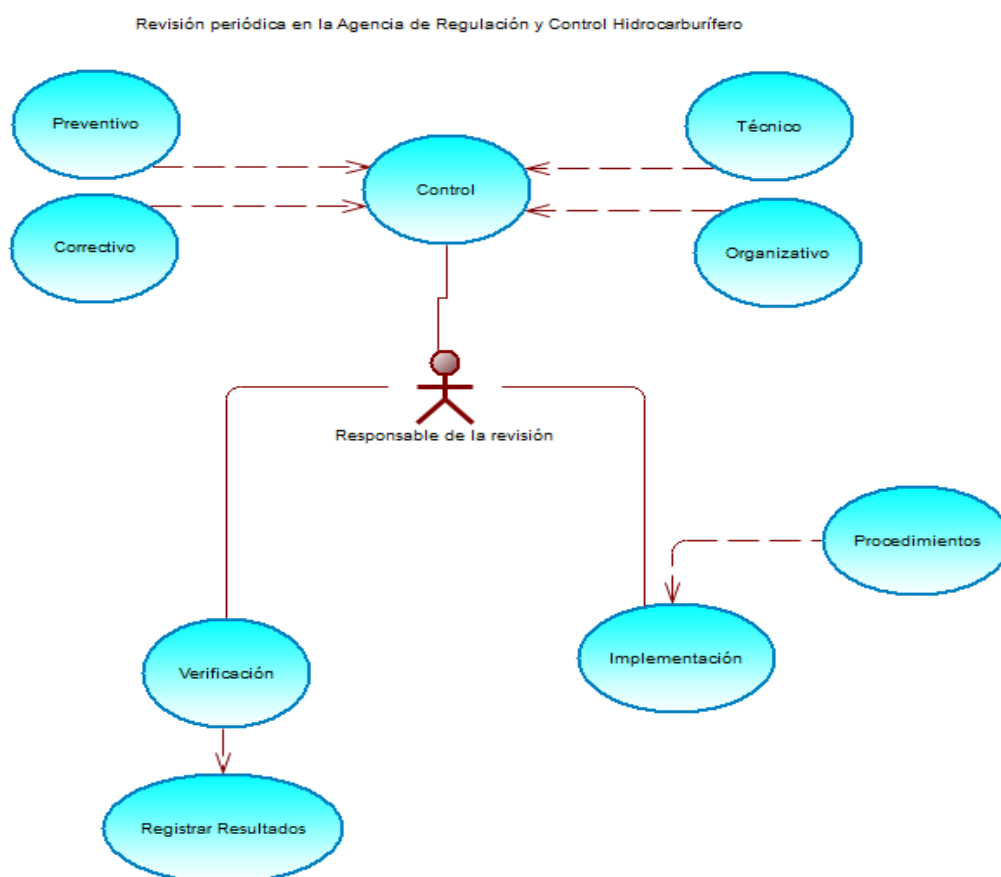


Figura 27. Revisión Periódica

Fuente: ARCH

## **Controles e Implementación para el ARCH**

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos. Existen dos grandes grupos de controles. Por un lado los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, y por otro los organizativos que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

Es muy importante conseguir un conjunto de controles que contenga controles de los dos tipos, ya que muchas medidas técnicas no pueden impedir que los usuarios de los sistemas cometan errores o dañen intencionadamente los activos y, al contrario, emitir muchas normas internas puede ser inútil si no hay una mínima seguridad técnica implantada.

Otra clasificación que se puede hacer de los controles para facilitar su selección es la de controles preventivos y correctivos. Los controles de tipo preventivo son aquellos que sirven para evitar incidentes de seguridad no deseados mientras que los correctivos son aquellos que se pondrán en marcha ante la ocurrencia de fallos o incidentes de seguridad.

Se deben tener en cuenta diferentes factores y restricciones en el momento de la selección de controles como son el costo de la implementación y mantenimiento del control, la disponibilidad, la ayuda que se debe brindar a los colaboradores para desempeñar el control y su aplicabilidad con respecto a los riesgos que se han detectado.

No todos los controles deben ser seleccionados, pero hay algunos que son requisito de la norma UNE/ISO-IEC 27001 tales como la Política de Seguridad o las auditorías internas.

#### **4.7.1.- Implementación de controles**

Seleccionados los controles pertinentes, debe definirse los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos, como por ejemplo la gestión de los recursos humanos. Pero incluso los de corte tecnológico pueden ser susceptibles de necesitar documentación, como por ejemplo la realización de copias de seguridad. Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Hay que contar también que si la organización no tiene procesos muy complejos puede ser posible que varios controles puedan agruparse en un único procedimiento.

No es necesario ni recomendable, desarrollar un procedimiento para cada control. La cantidad de documentación generada puede hacer



francamente difícil que se logren gestionar correctamente los controles. Por otro lado, los procedimientos deben ser lo más breves y claros posible. No deben incluir demasiadas instrucciones ni particularidades de la tarea a realizar.

El objetivo del procedimiento es contar con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

#### **4.7.2.- Verificación de Controles**

Una vez puestos en marcha, debe comprobarse periódicamente que los controles funcionan como se esperaba. Si no es así, deberán tomarse las acciones necesarias para corregir esa situación. Una herramienta fundamental del SGSI es la verificación de la eficacia de los controles implantados. Para ello deben establecerse objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los resultados de manera que se sepa si el control realmente protege los activos hasta el punto que la organización necesita.

El objetivo de rendimiento es contar con una herramienta que permita a cualquiera ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

### Ficha de mantenimiento preventivo


 Agencia de Regulación y Control Hidrocarburiífero		<b>SOPORTE TÉCNICO</b>	
MANTENIMIENTO PREVENTIVO Y PARQUE INFORMÁTICO			
USUARIO: _____		FECHA: _____	
AREA: _____		LUGAR: _____	
CI: _____		CORREO: _____	
<b>ESENCIALES</b>			
WIN RAR	<input type="checkbox"/>	ADOBE READER XI	<input type="checkbox"/>
FIREFOX (Version: Quipux)	<input type="checkbox"/>	GOOGLE CHROME	<input type="checkbox"/>
CCLEANER	<input type="checkbox"/>	SILVERLIGHT 5	<input type="checkbox"/>
<b>PLUGINS</b>			
FLASH PLAYER	<input type="checkbox"/>	JAVA 7	<input type="checkbox"/>
SHOCKWAVE	<input type="checkbox"/>	VLC	<input type="checkbox"/>
<b>MANTENIMIENTO SOFTWARE</b>			
TEMPORALES	<input type="checkbox"/>	ELIM. BARRAS HERR	<input type="checkbox"/>
ELIM. PROG P2P	<input type="checkbox"/>	REV FECHA Y HORA	<input type="checkbox"/>
CONFIG. TECLADO	<input type="checkbox"/>	DEFRAG. DISCO	<input type="checkbox"/>
ELIM. JUEGOS	<input type="checkbox"/>	ANTIVIRUS (ACTUALIZAR)	<input type="checkbox"/>
<b>MANTENIMIENTO FISICO</b>			
ARREGLO CABLES	<input type="checkbox"/>	LIMPIEZA INTERNA	<input type="checkbox"/>
<b>OPTIMIZACIÓN DE RECURSOS</b>			
CONFIG IMP B/N	<input type="checkbox"/>	IMP DOBLE CARA	<input type="checkbox"/>
PROT. PANTALLA 5	<input type="checkbox"/>	APAG. MONITOR 15 MIN	<input type="checkbox"/>
CONFIG SLEEP 30m	<input type="checkbox"/>	PASSWORD ADMIN	<input type="checkbox"/>
<b>PARQUE INFORMÁTICO</b>			
LEVANTAMIENTO INFO	<input type="checkbox"/>	RESPONSABLE: _____	
_____		_____	
USUARIO		RESPONSABLE	
OBSERVACIONES: _____			

Figura 28: Ficha de mantenimiento preventivo

Fuente: ARCH

#### 4.8 Planes de continuidad en la Agencia de Regulación y Control Hidrocarburiífero

En los planes de continuidad se continuarán ejecutando procedimientos para que el SGSI continúe así como también las respectivas

acciones correctivas y preventivas que se tomarán de acuerdo a los resultados

#### **4.8.1. Documentación de los procedimientos de Operación**

- VER ANEXO 4.8.1.-Procesamiento de manejo, respaldo, servicios de procesamientos de datos de información.

#### **4.8.2. Gestión del Cambio en equipos y software**

- VER ANEXO 4.8.2.- identificar, evaluar corregir, documentar los cambios realizados dentro de un equipo o software.

#### **4.8.3. Distribución de funciones de los funcionarios**

- VER ANEXO 4.8.3.- Las funciones y áreas de responsabilidad deben ser distribuidas para reducir oportunidades de modificación no autorizada.

#### **4.8.4. Separación de las instancias de Desarrollo, Pruebas, Capacitación y Producción.**

- VER ANEXO 4.8.4.- Definir y documentar los diferentes entornos, aislar los ambientes de desarrollo, pruebas, capacitación y producción.

#### **4.8.5. Presentación del Servicio Brindado**

- VER ANEXO 4.8.5.-Controles sobre definiciones del servicio y niveles de prestación del servicio

#### **4.8.6. Monitoreo y revisión de los servicios, por terceros.**

- VER ANEXO 4.8.6.- sistemas sensibles o críticos que convenga tener dentro o fuera de la institución, niveles de desempeño del servicio, repotes sobre el servicio.

#### **4.8.7. Gestión de los cambios en los servicios ofrecidos por terceros.**

- VER ANEXO 4.8.7.- Proceso de gestión de cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes.

#### **4.8.8. Gestión de la capacidad de recursos**

- VER ANEXO 4.8.8.- proyecciones de los requerimientos de capacidad futura de recursos para asegurar el desempeño de los servicios y sistemas informáticos.

#### **4.8.9. Aceptación del Sistema.**

- VER ANEXO 4.8.9.- que la instalación del nuevo sistema no afecte negativamente los sistemas existentes, procedimientos de recuperación y planes de contingencia.

#### **4.8.10. Controles contra código malicioso.**

- VER ANEXO 4.8.10.- Prohibir el uso de software no autorizado, procedimientos para evitar la descarga de archivos externos.

#### **4.8.11. Controles contra códigos móviles**

- VER ANEXO 4.8.11.- Bloquear códigos móviles no autorizados.

#### **4.8.12. Respaldo de la información.**

- VER ANEXO 4.8.12.- Determinar procedimientos para el resguardo de la información.

Resguardar los cambios en los servicios ofrecidos por terceros, en el desarrollo de aplicaciones, provisión de servicios de hardware, software, redes.

**Tabla 9. Procedimiento para Definir la Información que se debe Respaldar**

Elaborado por: Néstor y Paulina

N°	Actividad	DESCRIPCIÓN	RESPONSABLE	DOCUMENTO ENTREGABLE
<b>1. PROCEDIMIENTO PARA DEFINIR LA INFORMACIÓN QUE SE DEBE RESPALDAR</b>				
Inicio				
1	Determinar la información que será respaldada	Se debe determinar qué tipo de información se procesa o maneja dentro del ARCH, y cual se considera crítica para el proceso de respaldo (Aplicativos, Bases de Datos, Archivos de Log, Respaldo de Configuraciones, Sistemas Operativos, Información Confidencial, Archivos generados por Usuarios, etc.).	1. Técnico de DTI 2. Oficial de Seguridad 3. Propietario de la información	
2	Determinar a los usuarios cuya información se considera crítica	Se debe analizar cuáles son los usuarios cuya información se considera crítica y se debe respaldar.	1. Técnico de DTI 2. Oficial de Seguridad 3. Propietario de la información	Inventario* de la información considerada crítica para el proceso de respaldo (Aplicativos, Bases de Datos, Archivos de Log, Respaldo de Configuraciones, Sistema Operativo, Información Confidencial, Archivos generados por Usuarios, etc.).
Fin				
*El documento que se realice será confidencial y de uso exclusivo solo para la Dirección de Tecnologías de la Información.				

#### 4.8.13. Controles de las redes.

- VER ANEXO.- Separar el área de redes del área de operaciones, cuando la capacidad y recursos lo permitan

#### 4.8.14. Seguridad de los servicios de la red.

- VER ANEXO.- Incorporar tecnología para la seguridad de los servicios de red como la autenticación, encriptación y controles de conexión de red.

#### 4.8.15. Gestión de los medios removibles.

- VER ANEXO.- Establecer un procedimiento para la gestión de medios.

#### 4.8.16. Eliminación de los medios

- VER ANEXO.- Identificar los medios que requieran eliminación segura.

#### 4.8.17. Procedimientos para el manejo de la información

- VER ANEXO.- Establecer procedimientos para el manejo y etiquetado de todos los medios de acuerdo a su nivel de clasificación.

#### Algoritmo Cifrado que Garantiza la Integridad de Datos

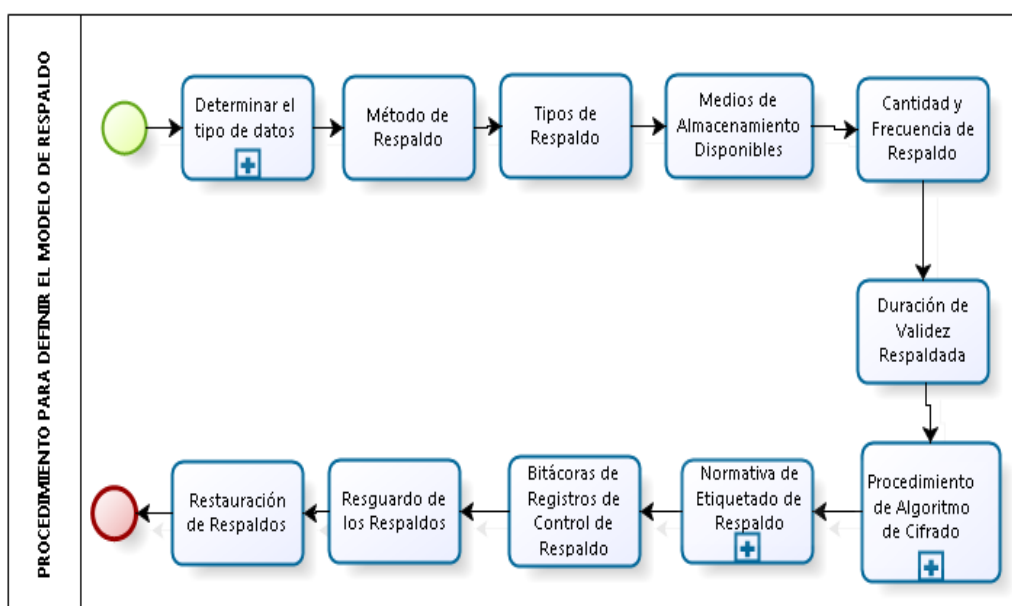


Figura 29: Procedimiento de Algoritmo Cifrado

Fuente: ARCH

#### **4.8.18. Seguridad de la documentación del sistema.**

- VER ANEXO.- Establecer procedimientos para proteger la información intercambiada contra la interpretación, copiado, modificación, enrutamiento y destrucción.

#### **4.8.19. Políticas y procedimientos para el intercambio de información.**

- VER ANEXO.- Establecer procedimientos para proteger la información intercambiada contra la interpretación, copiado, modificación, enrutamiento y destrucción.

#### **4.8.20. Acuerdos para el intercambio**

- VER ANEXO Definir procedimientos y responsabilidades para el control y notificación de transmisiones, envíos y recepciones.

#### **4.8.21. Medios físicos en tránsito**

- VER ANEXO.- Utilizar transporte confiable o servicios de mensajería.



#### **4.8.22. Mensajería electrónica**

VER ANEXO.- Establecer lineamientos para proteger los mensajes contra los accesos no autorizados, modificación o denegación de los servicios.

#### **4.8.23. Sistemas de información del negocio.**

VER ANEXO.- Proteger o tener en cuenta las vulnerabilidades conocidas en los sistemas administrativos, financieros, y demás sistemas informáticos donde la información es compartida.

#### **4.8.24. Transacciones en línea.**

VER ANEXO.- Definir procedimientos para el uso de certificados de firmas electrónicas por las partes implicadas en la transacción.

#### **4.8.25. Información disponible al público.**

VER ANEXO.- Establecer controles para que la información disponible al público se encuentre conforme a la normativa vigente.

#### **4.8.26. Registros de auditorías.**

- VER ANEXO.- Identificación de usuario, fecha hora de eventos clave, intentos rechazados o aceptados de acceso al sistema.

#### **4.8.27. Monitoreo de uso del sistema.**

- a) Registrar los accesos autorizados, incluyendo:
- b) Monitorear las operaciones privilegiadas, como
- c) Monitorear intentos de acceso no autorizados, como:
- d) Revisar alertas o fallas del sistema, como:
- e) Revisar cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

#### **4.8.28. Protección del registro de la información.**

- a) Proteger de alteraciones en todos los tipos de mensaje que se registren.
- b) Proteger archivos de registro que se editen o se eliminen.
- c) Precautelar la capacidad de almacenamiento que excede el archivo de registro.
- d) Realizar respaldos periódicos del registro del servicio.

Tabla 10.

## Protección de Registro de Información

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE REQUISITOS
	<b>Inicio</b>		
1	<b>Información que se debe respaldar</b>	Terminada la actividad 1 se tendrá la clasificación y el inventario de la información más importante que se debe respaldar (tanto a nivel de usuarios como a nivel de servicios/servidores)	
2	<b>Métodos de respaldos</b>	Se determina los métodos de respaldo para definir como los mismos serán obtenidos. <ul style="list-style-type: none"> <li>• Respalos en Caliente (en línea)</li> <li>• Respalos en Frío (Fuera de línea)</li> </ul>	1. Técnico de DTI 2. Propietario de la información 3. Actividad 1
3	<b>Tipos de respaldos</b>	Se analiza el tipo de respaldos que se aplicará a la información <ul style="list-style-type: none"> <li>• Respaldo Total</li> <li>• Respaldo Incremental</li> <li>• Respaldo Diferencial</li> </ul>	1. Técnico de DTI 2. Propietario de la información 3. Actividad 1
4	<b>Medios de almacenamiento disponibles</b>	Se analiza los medios de almacenamiento que se dispone como herramientas hardware y software para la automatización de respaldos, así como medios como Discos Duro Externo, Cintas, DVD, CD, etc.	1. Técnico de DTI 2. Propietario de la Información 3. Actividad 1
5	<b>Cantidad y Frecuencia de respaldo</b>	Se analiza la frecuencia (diaria, semanal, mensual) y cantidad de información que se respaldará (Kilobytes, Megabytes, Gigabytes, Terabytes)	1. Técnico de DTI 2. Propietario de la Información 3. Actividad 1
6	<b>Duración o validez de la</b>	Se establecerá el tiempo que la información tendrá validez y la duración que tendrá en el	1. Técnico de DTI 2. Propietario de la

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE REQUISITOS
	<b>información respaldada</b>	medio de almacenamiento al que se le asigne.	Información 3. Actividad 1
7	<b>Normativa de Etiquetado de RespalDOS</b>	Ver Procedimiento de Etiquetado de RespalDOS.	
8	<b>Bitácora de Registros y Control de respaldos</b>	Con los respaldos obtenidos se deberá realizar una bitácora que registre la información del proceso que se ha realizado (fecha, responsable, solicitante, medio usado, etc.).	1. Técnico de DTI 2. Propietario de la Información 3. Actividad 1
9	<b>Resguardo de los respaldos</b>	Para garantizar la seguridad física de los respaldos se definirá el lugar para su resguardo como el Centro de Datos, Cuartos de Almacenamiento, Archiveros/Armarios con Seguridad para el caso de los medios como CD, DVD, Cintas, etc.	1. Técnico de DTI 2. Propietario de la Información 3. Actividad 1
10	<b>Proceso de Restauración</b>	Ver Procedimiento de Restauración de la Información.	
11	<b>Fin</b>		

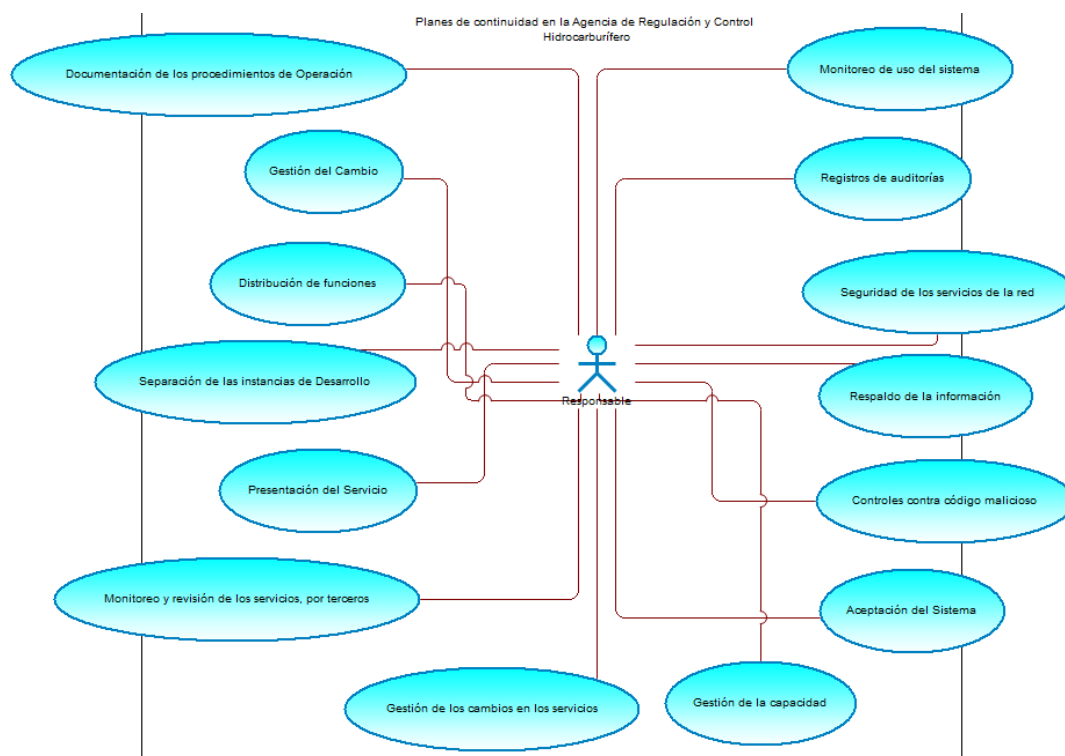
#### 4.8.29. Registros del administrador y del operador.

- a) Incluir al registro, la hora en la que ocurrió el evento.
- b) Incluir al registro, información sobre el evento.
- c) Incluir al registro, la cuenta de administrador y operador que estuvo involucrado.
- d) Añadir al registro, los procesos que estuvieron implicados.

### 4.8.30. Registro de fallas

- a) Revisar los registros de fallas o errores del sistema.
- b) Revisar las medidas correctivas para garantizar que no se hayan vulnerado los controles.
- c) Asegurar que el registro de fallas esté habilitado.

### CASO DE USO: Planes de Continuidad



**Figura 30. Registro de Fallas**

**Fuente: ARCH**

#### 4.8.31 Sincronización de relojes

a) Sincronizar los relojes de los sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local). En lo posible, se deberá sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.

b) Verificar y corregir cualquier variación significativa de los relojes sobretodo en sistemas de procesamiento donde el tiempo es un factor clave.

c) Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen representación diplomáticas del país, turistas extranjeros, entre otros).

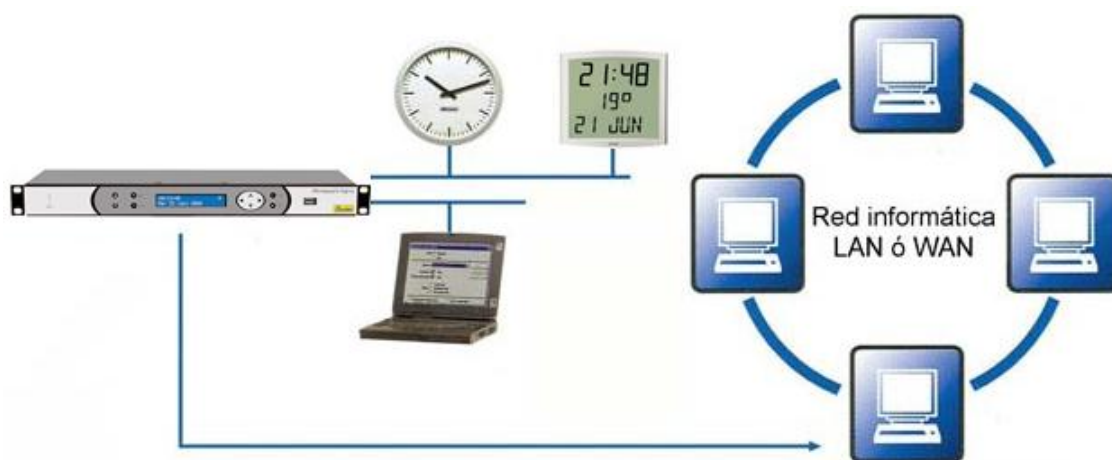


Figura 31. Modelo de Sincronización de Reloj

Fuente: Héctor Acevedo Juárez, 2010

## CASO COMPLETO: SEGURIDAD PERIMETRAL EN EL ARCH

### INFORME DE CUMPLIMIENTO DE HITOS

#### SISTEMA DE GOBIERNO POR RESULTADOS (GPR)

#### PROYECTO "IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN"

INFORME DE CUMPLIMIENTO DE HITOS		
<b>ENTIDAD / (SIGLAS):</b>	AGENCIA DE REGULACIÓN Y CONTROL HIDROCARBURÍFERO	
<b>DENOMINACIÓN DEL HITO:</b>	Disponer la implementación del EGSI en la institución por la máxima autoridad.	
<b>NÚMERO DE HITO:</b>	1.1.1.	<b>ES UN HITO PRIORITARIO?</b> SI
<b>RESUMEN ACTIVIDADES REALIZADAS</b>		<b>VERIFICABLE INTERNO</b>
<ul style="list-style-type: none"> <li>• Implicación de la Dirección.</li> <li>• Alcance del SGSI y política de seguridad.</li> <li>• Inventario de todos los activos de información.</li> <li>• Metodología de evaluación del riesgo.</li> <li>• Identificación de amenazas, vulnerabilidades e impactos.</li> <li>• Análisis y evaluación de riesgos.</li> <li>• Selección de controles para el tratamiento de riesgos.</li> <li>• Aprobación por parte de la dirección del riesgo residual.</li> <li>• Declaración de aplicabilidad.</li> <li>• Plan de tratamiento de riesgos.</li> <li>• Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.</li> </ul>		<p><i>Memorando No ARCH.CGGE.DTI-2014-1177-MEMO</i></p>

	<ul style="list-style-type: none"> <li>Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.</li> <li>Formación y concienciación en lo relativo a seguridad de la información a todo el personal.</li> <li>Monitorización constante y registro de todas las incidencias.</li> <li>Realización de auditorías internas.</li> <li>Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.</li> <li>Mejora continua del SGSI.</li> </ul>	
<b>PIE DE RESPONSABILIDAD</b>		
<b>FECHA ELABORACION:</b>	2015-08-25	
<b>NOMBRE y CEDULA OFICIAL DE SEGURIDAD:</b> IVAN PAREDES C.I.:171231805-2	<b>FIRMA:</b> 	
<b>NOMBRE Y CEDULA RESPONSABLE DE SEGURIDAD DE TI:</b> CHRISTIAN JIMENEZ C.I.:171320981-3	<b>FIRMA:</b> 	

Figura 32. Informe de Cumplimiento de Hitos

Fuente: EGS-ARCH

## LEVANTAMIENTO DE INFORMACIÓN

## MODELO DE LEVAMIENTO DE ELEMENTO ACTIVO

Lista y evaluación de dispositivos de red			
AGENCIA DE REGULACIÓN Y CONTROL HIDROCARBURÍFERO			
Número de versión 1.0		20120530	
#	Nombre dispositivo	Detalle del dispositivo	Valor
1	SWITCH CONECCION TLP	Dueño	ARCH
		Custodio	AREA TECNOLOGIAS
		Propietario	AREA TECNOLOGIAS
		Clasificación según el Departamento de TI	REDES-INFRAESTRUCTURA
		Activo ID	DRSWTCH1
		Número de serie	OLKJD
		Dirección IP	192.168.10.5
		Nombre host	SWITCH
		Localización	Primer Piso
		Aplicaciones / Requerimientos específicos del negocio	CAPA 3
		Contacto técnico [AS/AN]	AN (ADMINISTRADOR RED)
		Vendedor	HP
		Estado de mantenimiento	MEDIA
		Modelo	BORDE
		Programación de respaldos	Mensual
Localización del respaldo	MEDIO DIGITAL		
Criterio de confidencialidad	ALTO	A	
Criterio de integridad	MEDIO	M	
Criterio de disponibilidad	ALTO	A	

Figura 33. Modelo Levantamiento de Información Activos

Fuente: ARCH



## Diagrama de la Red

### Red Actual

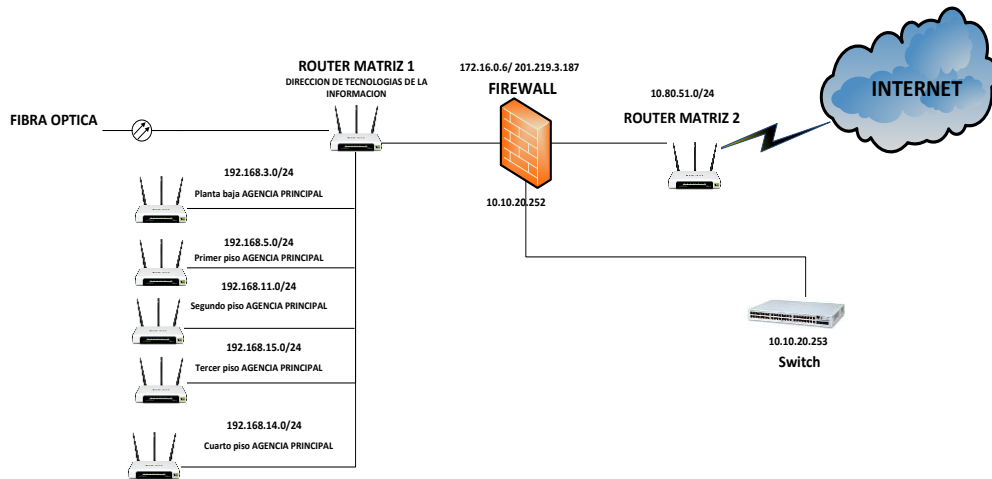


Figura 314. Diagrama de red Situación Actual de la ARCH

Fuente: ARCH

### Red Propuesta

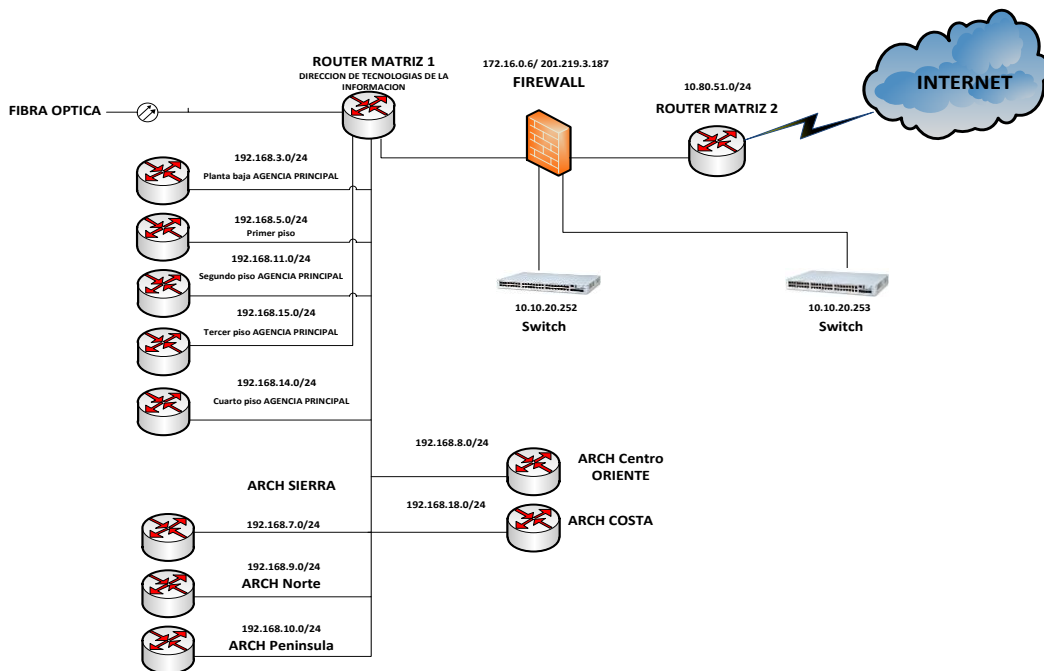


Figura 325. Diagrama de Red de la Propuesta para el ARCH

Fuente: ARCH

## Diccionario de Datos

### Perímetro de seguridad

Se procedió a realizar las verificaciones de la solución implementada para el sistema de seguridad perimetral; de la siguiente manera:

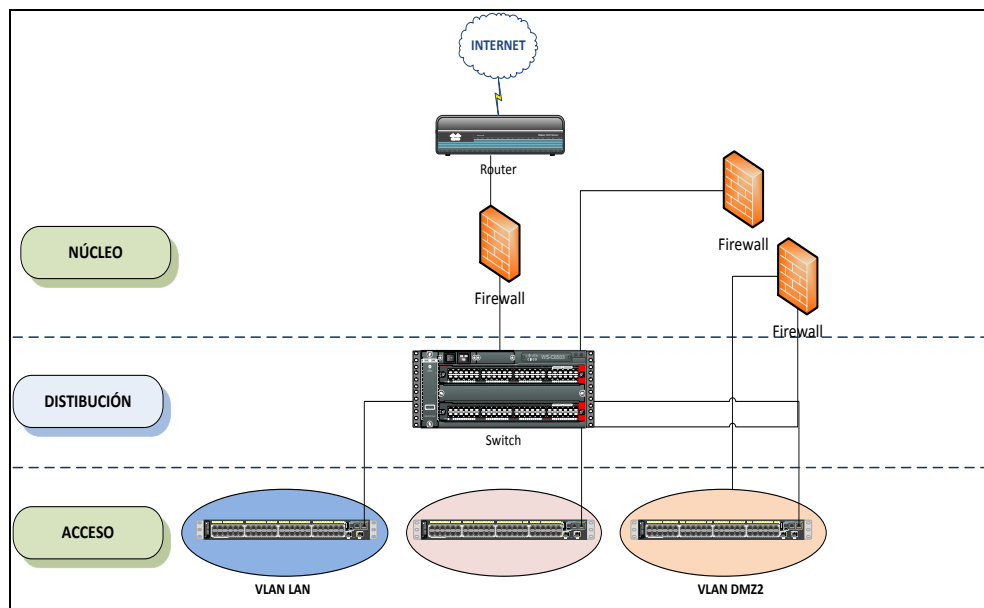
- En la tabla 11, se realiza el levantamiento del inventario de los equipos que integran la solución del sistema de seguridad perimetral de la institución.

**Tabla 11.**

**Tabla de Equipos de Seguridad Perimetral**

ITEM	EQUIPO
1	EQUIPO CONTROLADOR DE TRÁFICO DE CORREO
2	EQUIPO DE SEGURIDAD PERIMETRAL UTM
3	EQUIPO DE SEGURIDAD PERIMETRAL UTM
4	EQUIPO ANALIZADOR DE REGISTROS

- En la figura se identifica la implementación de la solución del sistema de seguridad perimetral basado en el modelo de tres capas que proporciona valor agregado a las conexiones y servicios de red.



**Figura 336. Arquitectura del sistema de seguridad perimetral.**

**Fuente: ARCH**

- Se procede a revisar el sistema de licenciamiento del equipo firewall y se verifica los módulos que se encuentran activados actualmente, como se indica en la tabla.

Tabla 12.

## Licenciamiento y módulos de servicios.

DESCRIPCIÓN	TIPO DE SOPORTE CONTRATADO	FECHA DE CADUCIDAD
<b>Contrato de Soporte</b>		
Hardware	Soporte 24 x 7 x 365	2015-08-04
Firmware	Soporte 24 x 7 x 365	2015-08-04
Soporte Mejorado	Soporte 24 x 7 x 365	2015-08-04
<b>Servicio</b>		
Siguiente Generación Firewall	IPS y Control de Aplicaciones	2015-08-04
ATP Services	AntiVirus / Filtro Web	2015-08-04
Otros Servicios	Análisis de Vulnerabilidades / Filtro de Email	2015-08-04
VPN	IPSEC / SSL	2015-08-04
WiFi y Controlador Switch	SSID / Control de Terminal	2015-08-04

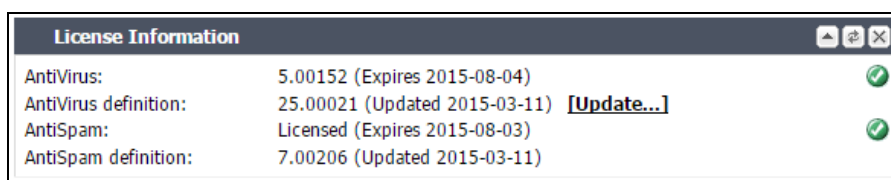
**Firewalls**

- Se procede a revisar el sistema de licenciamiento del equipo firewall y se verifica los módulos que se encuentran activados actualmente, como se indica en la tabla y figura.

Tabla 13.

Licenciamiento y módulos de servicios.

DESCRIPCIÓN	TIPO DE SOPORTE CONTRATADO	FECHA DE CADUCIDAD
Antivirus	Soporte 24 x 7 x 365 x	2015-08-04
AntiSpam	Soporte 24 x 7 x 365	2015-08-04



**Figura 34. Licenciamiento y módulos de servicios del Sistema de Antivirus y AntiSpam para el servicio de correo institucional.**

**Fuente: ARCH**

- Se procede a revisar el sistema de licenciamiento del equipo firewall y se verifica los módulos que se encuentran activados actualmente, como se indica en la tabla y figura.

Tabla 14.

## Licenciamiento del Sistema de registro.

DESCRIPCIÓN	TIPO DE SOPORTE CONTRATADO	FECHA DE CADUCIDAD
Total Numero de Dispositivos 2	Soporte 7 x 24 x 365	2015-08-04
Numero de Dispositivos permitidos 300	Soporte 7 x 24 x 365	2015-08-04

License Information	
Total Number of Devices	2
Number of Devices Allowed	300
GB/Day of Logs Allowed	15
GB/Day of Logs Used	1.19(7%) <a href="#">[Details]</a>

**Figura 35. Licenciamiento del Sistema de registro y análisis del Sistema de Seguridad Perimetral de la institución.**

**Fuente: ARCH**

- Dentro de los mecanismos de comunicación para asegurar la transmisión de la información a través de canales de conexión remota; se implementó el uso de redes privadas VPN para la comunicación con otras dependencias, utilizando técnicas de encriptación de datos como DES, 3DES, AES128, AES192 y AES256.

- Dentro de los mecanismos de verificación de acceso se dispone de los registros (log) que permite llevar el control de los accesos y segmentos de red referente a los accesos remotos. Mediante la aplicación de políticas de acceso a los sistemas de información; se identifican los NAT, dominios de red internas, externas e inalámbricas; debidamente separadas por el sistema firewall institucional.
- De igual manera se establecen las reglas para el enrutamiento de la red; de conformidad a las necesidades institucionales.

## Red LAN

### Configuración de un Gateway para una LAN

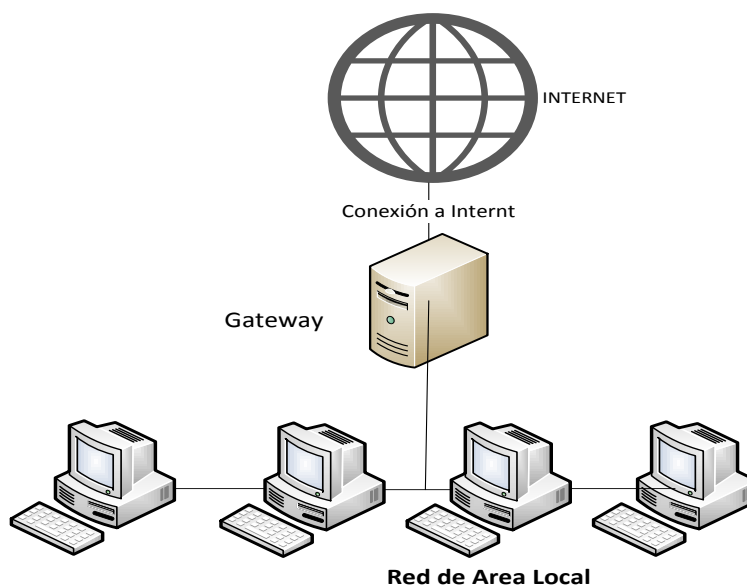


Figura 36: Configuración de un Gateway para una LAN

Fuente: ARCH

## Acceso Remoto

Ejemplo de una conexión de acceso remoto con un servidor de dominios

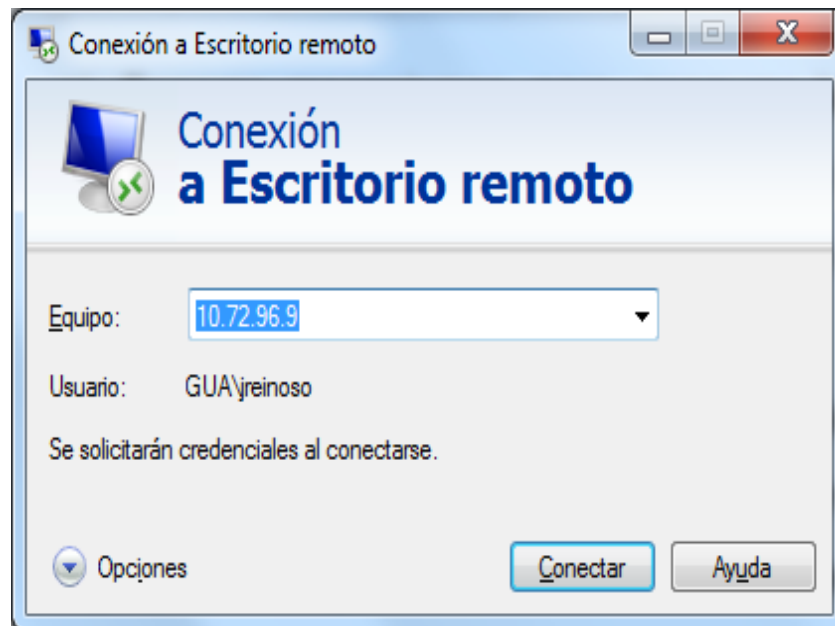


Figura 37. Conexión remota

Fuente: ARCH

## Procedimiento

### Planteamiento de las LAN

Tabla 15:

Planteamiento LAN

Nombre de red	Red
Red Financiero	192.168.5.0



Red de Administrativo	192.168.6.0
Red de Mercado	192.168.3.0
Red Invitado	192.168.4.0

### Definición de elementos

#### Hosts de Administrativo

Tabla 16.

##### Host de Administrativo

Dirección IP	Máscara de subred	Puerta de enlace
192.168.5.13	255.255.255.0	192.168.5.1
192.168.5.11	255.255.255.0	192.168.5.1
192.168.5.16	255.255.255.0	192.168.5.1

#### Hosts de Financiero

Tabla 17:

##### Host Financiero

Dirección IP	Máscara de subred	Puerta de enlace
192.168.3.12	255.255.255.0	192.168.3.1

## Host Invitado

Tabla 18.

### Host Invitado

Dirección IP	Máscara de subred	Puerta de enlace
192.168.3.10	<b>255.255.255.0</b>	<b>192.168.3.1</b>
192.168.3.20	<b>255.255.255.0</b>	<b>192.168.3.1</b>

## Hosts de Mercado

Tabla 19.

### Host

Dirección IP	Máscara de subred	Puerta de enlace
192.168.6.10	255.255.255.0	192.168.6.1
192.168.6.20	255.255.255.0	192.168.6.1
192.168.6.30	255.255.255.0	192.168.6.1
192.168.6.50	255.255.255.0	192.168.6.1
192.168.6.60	255.255.255.0	192.168.6.1
192.168.6.70	255.255.255.0	192.168.6.1
192.168.6.80	255.255.255.0	192.168.6.1

### Identificación de Objetos

**Tabla 20:**

**Identificación de los Objetivos**

	NOMBRE	DIRECCIÓN IP	DIRECCIÓN MAC	PUERTOS	
1	MXL3111BFP	172.16.2.60	A4-4E-31-C8-9E-4C	21	FTP
				515	IPMRESORA
				79	HUELLA DIGITAL
				83	FAX
2	ARCH-INT	172.16.1.87	A4-4E-31-B0-DB-20	80	WWW-HTTP
				135	LOC-SRV
				445	MICROSOFT-DS
				4400	PROXY+
3	CNU3469NBP	192.168.51.22 8	80-56-F2-73-0C-04	515	IMPRESORA
				4400	PROXY+
				21	FTP
				80	WWW-HTTP
4	MXL40711TS	172.16.2.173	A4-4E-31-CA-DB-34	21	FTP
				135	LOC-SRV
				80	WWW-HTTP
				4400	PROXY+
5	2CE2252LR0	192.168.50.78	80-56-F2-A7-05-EA	23	TELNET
				80	WWW-HTTP
				135	LOC-SRV
6	Admin-HP	192.168.50.78	80-56-F2-A6-F9-9E	445	MICROSOFT-DS
				21	FTP
				4400	PROXY+
				80	WWW-HTTP

7	MXL112012H	172.16.0.245	A4-43-31-B5-67-80	445	MICROSOFT-DS
				21	FTP
				4400	PROXY+
				80	WWW-HTTP

Tabla 21.

## Diccionario de datos de la red institucional

<b>Nombre:</b>	Rutas de la red Institucional	
<b>Descripción</b>	Contiene el listado de direcciones IP de la red Institucional	
<b>Campo</b>	<b>Dirección IP/mascara de red</b>	<b>Descripción</b>
ARCH Agencia Norte	192.168.9.0/24	Dirección IP del Router Correspondiente a la Agencia Norte
ARCH Agencia Sierra	192.168.7.0/24	Dirección IP del Router Correspondiente a la Agencia Sierra
ARCH Península	192.168.10.0/24	Dirección IP del Router Correspondiente a la Agencia Península
ARCH Centro Oriente	192.168.8.0/24	Dirección IP del Router Correspondiente a la Agencia Oriente
ARCH Costa	192.168.18.0/24	Dirección IP del Router Correspondiente a la Agencia Costa
ARCH Azuay	192.168.13.0/24	Dirección IP del Router correspondiente a la Agencia del Azuay
ARCH El Oro	192.168.5.0/24	Dirección IP del Router correspondiente a la Agencia de El Oro.
ARCH	192.168.6.0/24	Dirección IP del Router

Esmeraldas		correspondiente a la Agencia de El Esmeraldas.
ARCH Galápagos	192.168.20.0/24	Dirección IP del Router correspondiente a la Agencia de Galápagos.
ARCH Guayas	192.168.16.0/24	Dirección IP del Router correspondiente a la Agencia de Guayas.
ARCH Loja	192.168.3.0/24	Dirección IP del Router correspondiente a la Agencia de Loja.
ARCH Manabí	192.168.4.0/24	Dirección IP del Router correspondiente a la Agencia de El Oro.
ARCH Santo Domingo	192.168.13.0/24	Dirección IP del Router correspondiente a la Agencia de Santo Domingo.
ARCH Sucumbíos	192.168.17.0/24	Dirección IP del Router correspondiente a la Agencia de Sucumbíos.
ARCH Planta baja	192.168.3.0/24	Dirección IP del Router de la Agencia Principal correspondiente a la Planta Baja
ARCH Primer Piso	192.168.1.0/24	Dirección IP del Router de la Agencia Principal correspondiente al Primer Piso
ARCH Segundo Piso	192.168.11.0/24	Dirección IP del Router de la Agencia Principal correspondiente al Segundo Piso

ARCH Tercer Piso	192.168.15.0/24	Dirección IP del Router de la Agencia Principal correspondiente al Tercer Piso
ARCH Cuarto Piso	192.168.14.0/24	Dirección IP del Router de la Agencia Principal correspondiente al Cuarto Piso

**Tabla 22.****Tabla de Rutas Estáticas de Firewall**

<b>Nombre:</b>	Rutas estáticas de firewall Institucional	
<b>Descripción</b>	Contiene el listado de las rutas estáticas creadas en el firewall institucional	
<b>Campo</b>	<b>Dirección IP/mascara de red</b>	<b>Descripción</b>
Ruta hacia red de dependencia	192.168.0.0 255.255.248.0	Rutas de las redes de las dependencias del ARCH
Ruta a enlace de monitoreo	172.18.41.0 255.255.255.192	Rutas de enlaces de monitores
Ruta hacia red de dependencia	192.168.8.0 255.255.248.0	Rutas de las redes de las dependencias del ARCH
RUTA SISME VPN ...	192.168.14.8 255.255.255.255	Rustas enlaces Azuay
Ruta cloud	10.9.9.0 255.255.255.252	Ruta de enlaces al Cloud
Ruta SISME VPN	192.168.151.10 255.255.255.255 172.16.0.0 255.255.0.0	Rustas enlaces Centro Oriente

Ruta SISME VPN .	192.168.1.34 255.255.255.255	Rustas enlaces El Oro
Hacia la red wireless	192.168.50.0 255.255.254.0	Ruta a la Red Wirelles
RUTA SISME VPN .	192.168.1.35 255.255.255.255	Rustas enlaces Esmeraldas
Agencias	10.1.0.0 255.255.224.0	Ruta de enlaces a las Agencias
Ruta SISME VPN	192.168.100.10 255.255.255.255	Rustas enlaces Galápagos
Video	192.168.0.12 255.255.255.255	Rutas de Videoconferencias nivel Nacional
	10.121.1.0 255.255.255.255	
	10.20.30.0 255.255.255.0	
RUTA SISME VPN.	10.30.137.0 255.255.255.128	Enlaces Guayas
RUTA SISME VPN.	172.16.76.0 255.255.255.0	Enlaces Loja
RUTA SISME VPN.	192.168.55.0 255.255.255.224	Enlaces Manabí
RUTA SISME VPN.	172.16.8.84 255.255.255.255	Enlaces Agencia Norte
RUTA SISME PING	172.16.8.81 255.255.255.255	Enlaces Península
RUTA SISME VPN ...	192.168.14.5 255.255.255.255	Enlaces Santo Domingo de los Tsachillas
RUTA VPN PRUEBA SRV DES	192.168.20.21 255.255.255.255	Enlaces a CNT
RUTA VPN PRUEBA SRV PROD	192.168.12.75 255.255.255.255	Enlaces a CNT

RUTA VPN	192.168.37.31 255.255.255.255	Enlaces a Agencias
VPN SRV FTP	192.168.37.34 255.255.255.255	Enlaces a Sucumbíos
Ruta Externa	192.168.250.0 255.255.255.0	Ruta de red de Agencias

Reporte de interfaces de red creadas en el sistema firewall institucional.

- Mediante la creación de grupos de objetos, se brindan las de políticas de acceso a los sistemas de información y servicio de Internet de conformidad a las necesidades institucionales.

### **Tipos de Archivos que pueden Entrar en la Red**

Los tipos de archivos que maneja el ARCH es son: todos los archivos excepto los de .exe.

### **Problemas Identificados**

- No posee un plan de contingencia sobre los activos de información de la agencia ARCH.
- El personal de la ARCH, no posee un claro conocimiento sobre el debido uso y confidencialidad de la información.
- No se dispone de una adecuada evaluación de los riesgos.



## **Riesgos Asociados**

- Delegación de todas las responsabilidades en departamentos técnicos.
- Pérdida de Información importante de la agencia ARCH.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Falta de comunicación de los progresos al personal de la organización.
- Fuga de información sensible de la agencia ARCH o de los usuarios.

## **Registro de usuarios**

### **Servidor de Dominio**

Para la gestión de grupos de usuarios, lo recomendable es usar un servidor de dominio donde permite mantener una estructura jerárquica de la agencia ARCH como se muestra en la siguiente figura:



Figura 38. Servidor de Dominios

Fuente: ARCH

## Permisos a Usuarios

Se puede usar el mismo servidor de dominios para gestionar los permisos que se puede asignar a los usuarios, como se muestra en la siguiente figura:

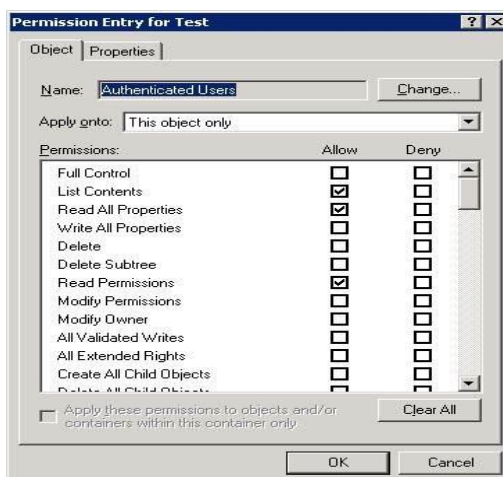


Figura 39. Tabla de permisos a usuarios

Fuente: ARCH

## Identificación de Equipos Conectados

Ejemplo para identificar los equipos conectados a una red a través de programa Advanced IP Scanner.

## Identificación de equipos conectados

### 4.2.15. Protección de los puertos de configuración y diagnóstico remoto

- a) Establecer un procedimiento de soporte, en el cual se garantice que los puertos de diagnóstico y configuración sean sólo accesibles mediante un acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware/ software que requiere el acceso.
- b) Los puertos, servicios (ej., ftp) que no se requieren por necesidades de la institución, deberán ser eliminados o deshabilitados.

## Servicios FTP

Ejemplo de un servicio ftp para compartir documentos

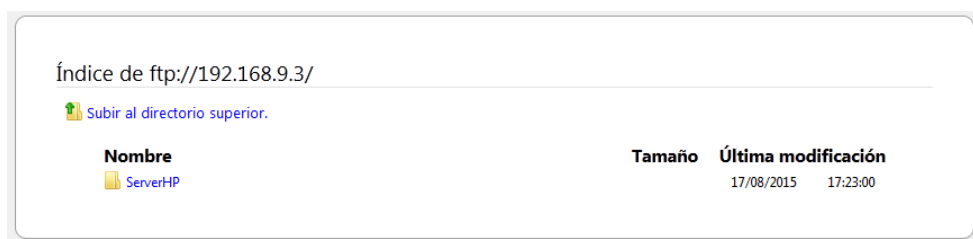


Figura 40: Servicio FTP

Fuente: ARCH

## 4.2.18. Control del enrutamiento en la red

a) Configurar políticas de control de acceso para el enrutamiento en la red, basándose en los requerimientos de la institución.

Las puertas de enlace de la seguridad (gateway) se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes internas y externas, si se emplean tecnologías proxy y/o de traducción de direcciones de red.

Las instituciones que utilizan proxys y quienes definen las listas de control de acceso (LCA), deben estar conscientes de los riesgos en los mecanismos empleados, a fin de que no existan usuarios o grupos.

### Configuración de un Proxy

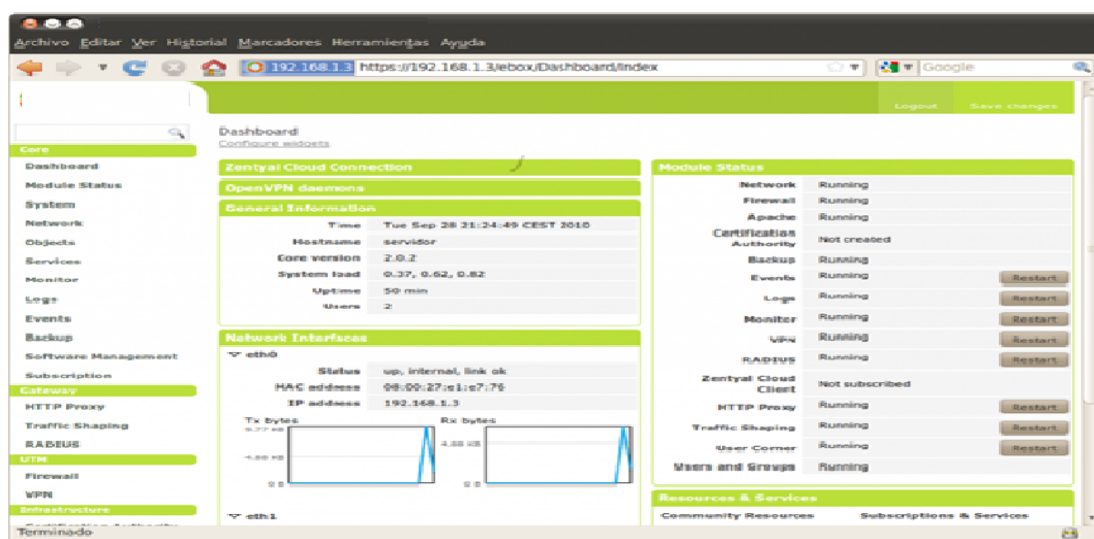


Figura 414: Configuración de un Proxy

Fuente: ARCH

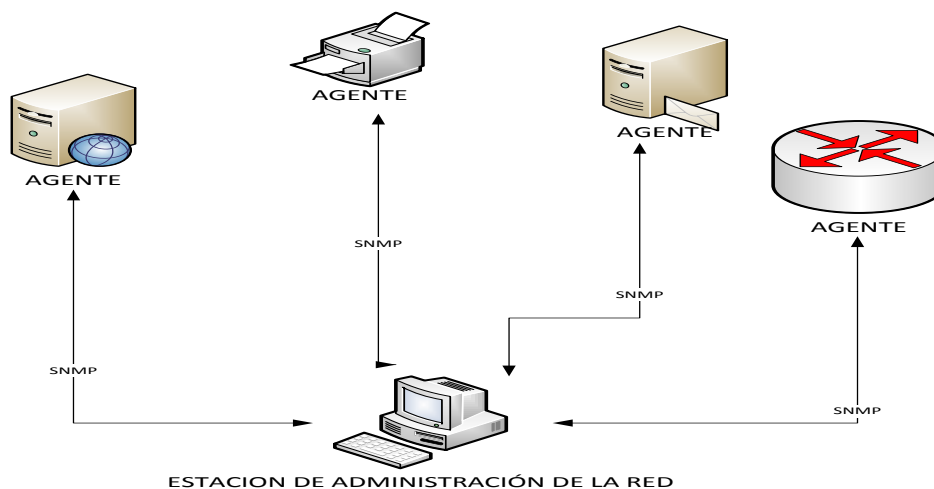
Estado	Nombre	IP	Grupo NetBIOS	Fabricante	Dirección MAC
	192.168.0.5	192.168.0.5		Hewlett Packard	88:51:F8:56:3A:FF
	uiodominio	192.168.0.6	CONTROLSANITARI		82:96:0D:A6:A8:B4
	192.168.0.10	192.168.0.10		3Com Europe Ltd	00:24:73:24:51:00
	192.168.0.14	192.168.0.14		Huawei Technologies Co., Ltd	84:DB:AC:73:46:AB
	192.168.0.18	192.168.0.18		CISCO SYSTEMS, INC.	00:04:9A:4C:F1:00
	HP-2530-24G-PoEP	192.168.0.22		Hewlett Packard	2C:59:E5:8A:C8:60
	HP-2530-24G-PoEP	192.168.0.26		Hewlett Packard	2C:59:E5:8A:A7:80
	HP V1910 Switch	192.168.0.27		Hewlett Packard	D0:7E:28:18:E4:FF
	3Com Baseline Switch	192.168.0.28		3COM EUROPE LTD	20:FD:F1:50:9B:9F
	192.168.0.34	192.168.0.34		LITE-ON Communications, Inc.	00:02:E3:4B:CD:04
	arcsa-uo	192.168.0.36	CONTROLSANITARI	Hewlett Packard	9C:B6:54:F5:77:EE

**Figura 425. Identificación de equipos conectados**

**Fuente: ARCH**

## Servidor SNMP

La forma más efectiva para documentar los activos de la agencia ARCH es configurar un servidor SNMP (Simple Network Management Protocol), donde se puede ver la información de cada dispositivo conectado en la red, como se muestra en la siguiente figura:



**Figura 436: servidor SNMP**

**Fuente: ARCH**

#### 4.8.24. Transacciones en línea.

➤ VER ANEXO

### Protocolo HTTPS

Utilizar el protocolo https para realizar transacciones seguras verificando los certificados como se muestra en la siguiente figura N°45:

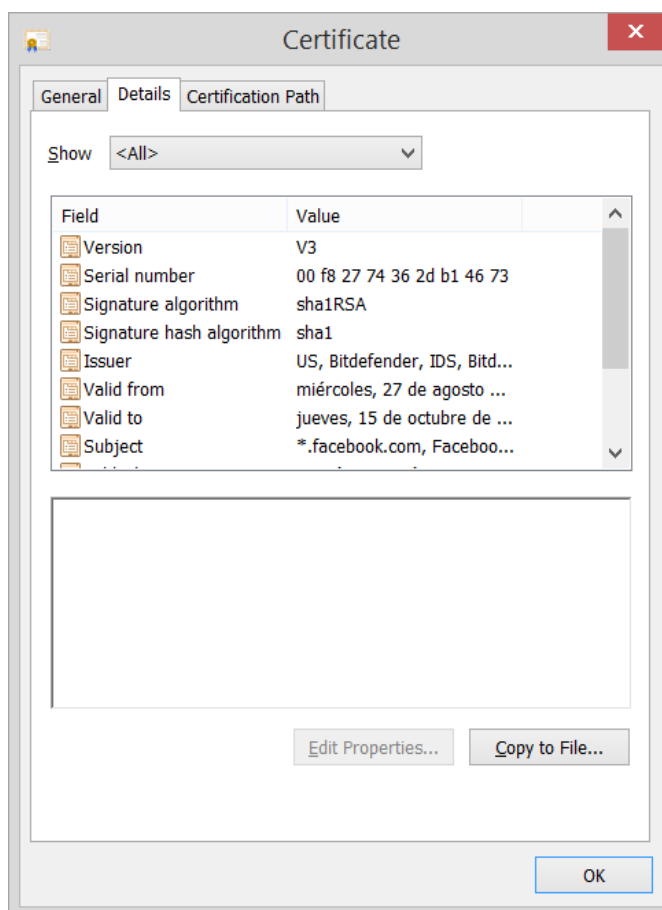


Figura 447: Protocolo Https

Fuente: ARCH

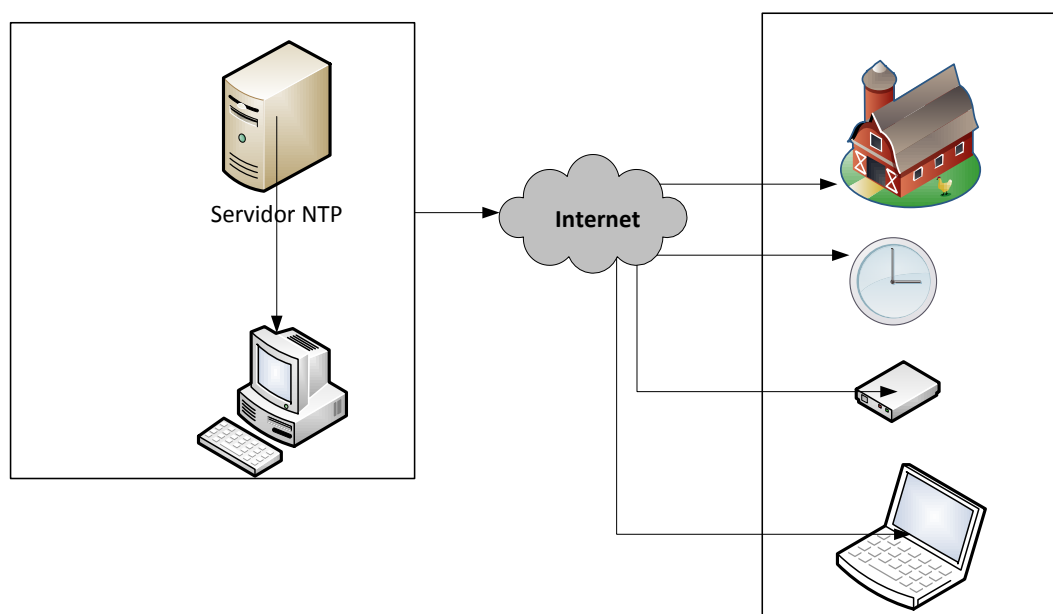
#### **4.8.31 Sincronización de relojes**

- a) Sincronizar los relojes de los sistemas de procesamiento de información pertinentes con una fuente de tiempo exacta (ejemplo el tiempo coordinado universal o el tiempo estándar local). En lo posible, se deberá sincronizar los relojes en base a un protocolo o servicio de tiempo de red para mantener todos los equipos sincronizados.
- b) Verificar y corregir cualquier variación significativa de los relojes sobretodo en sistemas de procesamiento donde el tiempo es un factor clave.
- c) Garantizar que la marca de tiempo refleja la fecha/hora real considerando especificaciones locales (por ejemplo, el horario de Galápagos o de países en donde existen representación diplomáticas del país, turistas extranjeros, entre otros).
- d) Garantizar la configuración correcta de los relojes para la exactitud de los registros de auditoría o control de transacciones y evitar repudio de las mismas debido a aspectos del tiempo.

#### **Protocolo NTP**

Lo más recomendable es configurar el protocolo NTP (Network Time Protocol), el cual permite establecer el tiempo como se muestra en la siguiente figura N°45.

## Protocolo NTP



**Figura 458: Protocolo NTP**

**Fuente: ARCH**

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



- La ARCH actualmente no cuenta con un Sistema de Gestión de Seguridad de la Información que se encuentra alineada con los objetivos institucionales.
  
- Los riesgos son elevados debido a que no se cuenta con una adecuada planificación y tratamiento del riesgo.

## CAPÍTULO V

### CONCLUSIONES Y RECOMENDACIONES

#### 5.1 Conclusiones:

1. En el desarrollo de la presente tesis se determinó que es crucial para la implementación de un SGSI las fases de levantamiento de información que permitieron el diseño de una metodología adecuada
2. Con el resultado obtenido en la investigación de las mejores prácticas de la Seguridad Informática, se generó una secuencia de dominios, dinámica y de fácil adaptabilidad a los cambios.
3. Se concluyó que el análisis de la matriz de riesgo es vital para la organización, ya que garantiza la seguridad de los activos de la información.
4. La Metodología propuesta contribuyó para que la Agencia de Regulación y Control Hidrocarburífero defina y documente de manera obligatoria e inmediata los hitos del EGSI, basándose en las normas y regulaciones del Estado.

## 5.2 Recomendaciones:

1. Se recomienda continuar con las actividades de relevamiento de la información para mejorar las actuales políticas definidas en el SGSI.
2. Es aconsejable que en futuros procesos de la organización se aplique a cabalidad la Secuencia de Dominios garantizando el cumplimiento de las mejores prácticas de Seguridad Informática.
3. Es recomendable que el personal que maneja TI valore y asigne un grado de protección según la criticidad de los riesgos para con ello mantener un adecuado resguardo de los activos.
4. Se recomienda documentar los hitos así como los procedimientos operativos indicando a detalle las actividades generados por cada una de las áreas involucradas.

## Bibliografía.-

- Bsigroup.es.* (2015). Obtenido de <http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/ISOIEC-27001>
- ISO.org.* (24 de 07 de 2015). Obtenido de - [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)
- Ministerio de Costa Rica.* (21 de 03 de 2015). Obtenido de [http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/las buenas prácticas de COBIT%20audit%20y%20ctrol%20sists%20inf.pdf](http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/las_buenas_practicas_de_COBIT%20audit%20y%20ctrol%20sists%20inf.pdf)
- SGSI.* (15 de 08 de 2015). Obtenido de <https://cert.inteco.es/Formacion/SGSI>.
- A, L. (2011). *El portal de ISO 27001*. España: Serie.
- A., C. (2009). *ISO 27001 e ISO 27004*. España: ISO.
- Brito, J. (2004). *Análisis y Aprovechamiento de los Sistema de Información para una Eficiente Auditoría y Control de Gestión*. Quito: itSMF.
- C, C. (2009). *Desarrollo de un Plan que permita la implantación de un centro de servicio al usuario para la empresa Pinto*. Quito: Crl.
- Institute, G. (2007). *COBIT*. EEUU: COBIT.
- NASAAudit. (2011). *Enterprise Risk Management*. Cali: COSO II.
- Practices.es.* (2015). Obtenido de <http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/ISOIEC-27001>
- ISO.org.* (24 de 07 de 2015). Obtenido de - [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)
- RiesgoInformatico de Costa Rica.* (21 de 03 de 2015). Obtenido de [http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/las buenas prácticas de COBIT%20audit%20y%20ctrol%20sists%20inf.pdf](http://www.hacienda.go.cr/cifh/sidovih/spaw2/uploads/images/file/las_buenas_practicas_de_COBIT%20audit%20y%20ctrol%20sists%20inf.pdf)
- SGSI.* (15 de 08 de 2015). Obtenido de <https://cert.inteco.es/Formacion/SGSI>.
- A, L. (2011). *El portal de ISO 27001*. España: Serie.
- A., C. (2009). *ISO 27001 e ISO 27004*. España: ISO.

## Tradicional

Compendio. Sistema de Gestión de la Seguridad de la Información (SGSI)

**Autor:** Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC

**Editorial:** Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC

**Edición:** Segunda, julio 2009

Tecnologías de la Información

Técnicas de seguridad: Gestión de incidentes de seguridad de la Información. / UNIT, ISO. // Montevideo: UNIT, 2004.

UNIT-ISO/IEC 27001: 2005

Documentos - Tecnologías de la Información. Técnicas de seguridad: Sistema de gestión de seguridad de la información. Requisitos. / UNIT, ISO. // Montevideo: UNIT, 2006