ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN TECNOLÓGICA
ANÁLISIS DE SISTEMAS INFORMÁTICOS

APLICACIÓN DE LA NORMA TÉCNICA ISO 27001:2005, PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA DIRECCION DE DESARROLLO INSTITUCIONAL (DDI) DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL (IESS)

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

LUIS ARMANDO CASTAÑEDA CADENA
WASHINGTON RICARDO QUEZADA SARASTI

DIRECTOR: ING. CESAR GALLARDO

Quito, Febrero 2007

DECLARACION

Nosotros, Luis Armando Castañeda Cadena y Washington Ricardo Quezada Sarasti declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual por su Reglamento y por la normatividad institucional vigente.

Luis Castañeda

Washington Quezada

CERTIFICACIÓN

Certifico que el presente proyecto fue desarrollado por Luis Armando Castañeda Cadena y Washington Ricardo Quezada Sarasti, bajo mi supervisión.

Ing. Cesar Gallardo
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Agradecemos a todos nuestros maestros y compañeros que nos apoyaron durante toda nuestra carrera, a nuestros padres, esposas e hijos que siempre nos supieron apoyar, al Coordinador de la Carrera Ing. Daniel Manangón, al Ing. César Gallardo por apoyarnos y guiarnos en el desarrollo de este proyecto, con el cual culminamos nuestra carrera universitaria.

A la Escuela de Formación Tecnológica y principalmente a la Carrera Análisis de Sistemas Informáticos por darnos la oportunidad de aprender y formarnos en esta gran Institución.

Luis Armando Castañeda

Washington Quezada Sarasti

DEDICATORIA

Dedico Esta tesis a mis padres, esposa e hija, por apoyarme para poder cumplir con esta meta.

Luis Armando Castañeda

DEDICATORIA

Esta tesis va dedicada a mis padres, los forjadores de mi vida y guías ejemplares permanentes.

A mi esposa Mary, a mis hijos Gabriela y Anthony que con todo el afán, cariño, apoyo y comprensión han hecho posible que se cumplieran mis metas.

Esta tesis es una parte de mi vida que con todo el esfuerzo la pude culminar, con ella empiezo nuevas etapas por esto y más, la dedico a Dios quien iluminó mi camino y siempre me dio fuerzas para continuar.

Washington Quezada Sarasti

ÍNDICE GENERAL

ÍNDICE GENERAL 1
ÍNDICE DE FIGURAS.....5
ÍNDICE DE TABLAS 6
ÍNDICE DE ANEXOS.....8
RESUMEN.....9
CAPÍTULO I.....1
1. INTRODUCCIÓN.....1
1.1 ASPECTOS GENERALES.....1
1.1.1 LA ORGANIZACIÓN 1
1.1.2 SITUACIÓN ACTUAL 3
1.1.3 PLANTEAMIENTO DEL PROBLEMA 4
1.2 OBJETIVOS DE LA INVESTIGACIÓN.....6
1.2.1 OBJETIVO GENERAL.....6
1.2.2 OBJETIVOS ESPECÍFICOS.....6
1.3 JUSTIFICACIÓN DEL PROYECTO.....7
1.3.1 JUSTIFICACIÓN TEÓRICA.....7
1.3.2 JUSTIFICACIÓN METODOLÓGICA.....7
1.3.3 JUSTIFICACIÓN PRÁCTICA.....8
CAPÍTULO II.....9
2. MARCO TEÓRICO.....9
2.1 SEGURIDADES INFORMÁTICAS.....9
2.2 IMPORTANCIA DE LA SEGURIDAD DE INFORMACIÓN 10
2.3 ESTABLECER LAS NECESIDADES DE SEGURIDAD 10
2.4 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD.....11
2.5 DIFERENTES TIPOS DE SEGURIDAD INFORMÁTICA.....12
2.6 NIVELES DE SEGURIDAD 13
2.7 HACKER, PHREAKER, PIRATA Y CRACKER.....14
2.8 NORMATIVA INTERNACIONAL.....16
2.9 ISM3.....18
2.10 EFECTOS DE LA CERTIFICACIÓN.....19
2.11 CONSIDERACIONES DEL ISO 27001:2005.....19
2.12 APROVECHAMIENTO DEL MODELO 20
2.13 CONTROLES.....21
2.14 BENEFICIOS AL APLICAR LA ISO 27001 25
CAPÍTULO III 27
3. ANALISIS DE LAS SEGURIDADES DEL IESS.....27
3.1 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 27
3.1.1 ORGÁNICO FUNCIONAL 28
3.1.2 ÓRGANOS DE GOBIERNO 29
3.1.3 LA DIRECCIÓN GENERAL.....29
3.1.4 LA DIRECCIÓN PROVINCIAL 30
3.1.5 DIRECCIONES ESPECIALIZADAS 30
3.1.6 ESTRUCTURA ORGANIZACIONAL DE LA DDI 30
3.1.7 ORGANIGRAMA DE LA DDI.....32
3.1.7.1 Responsabilidades. 32

3.1.7.2 Dependencias de la DDI 33
3.1.7.3 Competencia de la Subdirección de Planificación Institucional 33
3.1.7.4 Responsabilidades de la Subdirección de Planificación Institucional. 33
3.1.7.5 Dependencias de la Subdirección de Planificación 34
3.1.7.5.1 Responsabilidades de la Unidad de Planificación.- 34
3.1.7.5.2 Responsabilidades de la Unidad de Gestión de Proyectos.- 35
3.1.7.6 COMPETENCIA DE LA SUBDIRECCIÓN DE PROCESOS Y NORMATIVIDAD. 35
3.1.7.7 RESPONSABILIDADES DE LA SUBDIRECCIÓN DE PROCESOS Y NORMATIVIDAD 35
3.1.7.8 DEPENDENCIAS DE LA SUBDIRECCIÓN DE NORMATIVIDAD Y PROCESOS. 35
3.1.7.8.1 RESPONSABILIDADES DE LA UNIDAD DE NORMATIVIDAD.- 36
3.1.7.8.2 RESPONSABILIDADES DE LA UNIDAD DE PROCESOS.- 36
3.1.7.9 COMPETENCIA DE LA SUBDIRECCIÓN DE TECNOLOGÍA.- 37
3.1.7.10 RESPONSABILIDADES DE LA SUBDIRECCIÓN DE TECNOLOGÍA. 37
3.1.7.11 DEPENDENCIAS DE LA SUBDIRECCIÓN DE TECNOLOGÍA.....38
3.1.7.11.1 RESPONSABILIDADES DE LA UNIDAD DE DESARROLLO.....38
3.1.7.11.2 RESPONSABILIDADES DE LA UNIDAD DE PRODUCCIÓN. 38
3.1.7.11.3 RESPONSABILIDADES DE LA UNIDAD DE INFRAESTRUCTURA TECNOLÓGICA 39
3.1.7.12 COMPETENCIA DE LA UNIDAD DE PRESUPUESTO. 40
3.1.7.13 RESPONSABILIDADES DE LA UNIDAD DE PRESUPUESTO. 40
3.1.7.14 COMPETENCIA DE LA UNIDAD DE HISTORIA LABORAL. 41
3.1.7.15 RESPONSABILIDADES DE LA UNIDAD DE HISTORIA LABORAL..41
3.2 UNIDAD DE PRODUCCIÓN. 42
3.2.1 ÁREA DE SEGURIDADES.....43
3.2.2 ÁREA DE SERVIDORES.....44
3.2.3 DIAGRAMA DE LOS SERVIDORES.....46
3.2.4 SERVICIOS ON-LINE DEL IESS 47
3.2.5 DIAGRAMA DE ALMACENAMIENTO DE LOS SERVIDORES.....48
3.2.6 ÁREA DE REDES 49
3.2.7 DIAGRAMA DE RED DE IESS 50
3.2.8 ÁREA DE BASE DE DATOS.....50
3.2.9 ÁREA DE SOPORTE 51
3.3 CARACTERÍSTICAS DE HARDWARE DE LOS SERVIDORES 51
3.4 EVALUACIÓN Y TRATAMIENTOS DE RIESGO DEL IESS 62
3.4.1 ANÁLISIS DEL RIESGO Y LOS REQUERIMIENTOS DEL ISO 27001:2005 .63
3.4.2 PROCESO DE EVOLUCIÓN DEL RIESGO.....63
3.4.2.1 Identificación y tasación de activos.....64
3.4.2.2 Identificación de requerimientos de seguridad: 64
3.4.2.3 Identificación de amenazas y vulnerabilidades.....65
3.4.2.4 Cálculos de los riesgos de seguridad 66
3.4.2.5 Selección de opciones apropiadas de tratamiento del riesgo 66
3.4.2.6 Selección de controles para reducir los riesgos a un nivel aceptable 68
3.4.3 RIESGO RESIDUAL.....68
3.4.4 VALORACIÓN DE BIENES O ACTIVOS 69
3.4.5 CÁLCULO DEL RIESGO EN LA DDI 69

3.4.5.1 Riesgo de activos....70
3.4.5.2 Cuadro del cálculo del riesgo en la DDI....70
3.4.5.3 Cuadro del cálculo de la seguridad en la ddi....72
3.4.5.4 Análisis del cálculo de la seguridad....74
CAPÍTULO IV....75
4. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD PARA DDI....75
4.1 ANÁLISIS Y DEFINICIÓN DE POLÍTICAS INFORMÁTICA EN LA DDI....75
4.1.1 ANÁLISIS DEL TRATAMIENTO DE POLÍTICAS EN LA DDI....75
4.1.2 DEFINICIÓN DE POLÍTICAS PARA LA DDI....77
4.1.2.1 Políticas de seguridad de los activos....78
4.1.2.2 Clasificación de la información....78
4.1.2.3 Políticas de seguridad del personal....79
4.1.2.3.1 Ética....79
4.1.2.4 Políticas de passwords....79
4.1.2.5 Políticas generales de software....81
4.1.2.6 Redes....82
4.1.2.6.1 Conexión a redes:....82
4.1.2.6.2 Módems:....82
4.1.2.7 Correo electrónico....82
4.1.2.8 Internet....83
4.1.2.9 Políticas de administración del sistema....84
4.1.2.10 Seguridad física....84
4.1.2.11 Responsabilidad personal de redes....85
4.1.2.12 Directivas para el centro de cómputo....85
4.1.2.13 Control de acceso....85
4.1.2.14 Políticas de ingreso a los sistemas....86
4.1.2.15 Auditoria....87
4.1.2.16 Contabilización y auditoria....87
4.1.2.17 Políticas de respaldos y recuperación de servidor aplicaciones....88
4.1.2.18 Políticas de respaldos y recuperación de la base de datos....89
4.1.2.19 Políticas de respaldos y recuperación de servidores web....90
4.1.2.20 Administración de cambios (instalaciones o actualizaciones de software / hardware y etiquetación)....91
4.1.2.21 Políticas de las redes / sistemas distribuidos....91
4.1.2.22 Firewall para internet....94
4.1.2.23 Políticas de desarrollo de software....96
CAPÍTULO V....98
5. PLAN DE CONTINGENCIA PARA SOLUCIONES A PROBLEMAS....98
5.1 ÁREA DE REDES Y COMUNICACIONES....98
5.2 EQUIPOS Y ENLACE DE COMUNICACIONES....98
5.2.1 Fallas....98
5.2.2 Acciones a Tomar....98
5.3 ACCESO A INTERNET....100
5.3.1 Fallas....100
5.3.2 Acciones a tomar....100
5.4 SERVIDORES DE RED....101
5.4.1 FALLAS EN SERVIDOR DE DHCP....101
5.4.1.1 Acciones a Tomar....101
5.4.2 FALLAS EN EL SERVIDOR DE DNS....101

5.4.2.1 Acciones a Tomar. 102
5.5 ESTACIONES DE TRABAJO. 102
5.5.1 FALLAS EN COMUNICACIONES. 102
5.5.1.1 Acciones a tomar 102
5.6 FALLAS DE ACCESO A APLICACIONES. 103
5.6.1 ACCIONES A TOMAR. 103
5.7 EQUIPOS DE IMPRESIÓN. 103
5.7.1 FALLAS DE IMPRESIÓN 103
5.7.2 ACCIONES A TOMAR. 103
5.8 SERVIDORES DEL SISTEMA HISTORIA LABORAL. 104
5.9 SERVIDOR DE BASE DE DATOS. 104
5.9.1 ACCIONES A TOMAR 104
5.10 ÁREA DE SERVIDORES 105
5.11 FALLAS DE ACCESO A APLICACIONES HISTORIA LABORAL 105
5.11 1 FALLAS. 105
5.11.2 ACCIONES A TOMAR 106
5.12 FALLAS AL MOMENTO DE LEVANTAR LOS SERVICIOS DE HTTP CAUSADA POR SESIONES MUERTAS 107
5.12.1 FALLAS. 107
5.12.2 ACCIONES A TOMAR 107
5.13 FALLAS AL MOMENTO DE LEVANTAR LOS SERVICIOS DE HTTP CAUSADAS POR ESPACIO EN LOS DISCOS. 107
5.13.1 FALLAS. 107
5.13.2 ACCIONES A TOMAR 107
5.14 FALLAS AL MOMENTO DE LEVANTAR LOS SERVICIOS DE HTTP CAUSADAS POR LOS LOGS. 108
5.14.1 FALLAS. 108
5.14.2 ACCIONES A TOMAR 108
5.15 FALLAS DE FILE SYSTEM DE LOS SERVIDORES. 109
5.15.1 FALLAS. 109
5.15.2 ACCIONES A TOMAR 109
5.16 FALLAS DE ACCESO A WWW.IESS.GOV.EC. 109
5.16.1 FALLAS. 109
5.16.2 ACCIONES A TOMAR 109
5.17 APAGAR LOS SERVIDORES EN CASO DE FALLO EN LA CORRIENTE ELÉCTRICA. 110
5.17.1 FALLAS. 110
5.17.2 ACCIONES A TOMAR 110
CAPÍTULO VI 112
6. CONCLUSIONES Y RECOMENDACIONES 112
6.1 CONCLUSIONES 112
6.2 RECOMENDACIONES 112
BIBLIOGRAFÍA 113
GLOSARIO 114
ANEXOS 124

ÍNDICE DE FIGURAS

Figura 2.1 CONTROLES DE LA NORMA ISO\IEC 17799:2005.....21
Figura 3.1 ESTRUCTURA DE COORDINACIÓN DEL PROYECTO DE MODERNIZACIÓN.....31
Figura 3.2: ORGANIGRAMA DDI 32
Figura 3.3 ORGANIGRAMA DE PRODUCCIÓN 42
Figura 3.4 DIAGRAMA DE DISTRIBUCIÓN DE LOS SERVIDORES 46
Figura 3.5 DIAGRAMA DE ALMACENAMIENTO DE LOS SERVIDORES.....48
Figura 3.6 ESQUEMA DE LA RED 50
Figura 3.7 PROCESO DE EVALUACIÓN DEL RIESGO.....63
Figura 3.8 GRAFICO DE LA SEGURIDAD 74

ÍNDICE DE TABLAS

Tabla 3.1 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP FONDOS DE RESERVA. 52
Tabla 3.2 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL INTRANET 52
Tabla 3.3 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD MIGRACIÓN. 52
Tabla 3.4 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD PRODUCCIÓN. 53
Tabla 3.5 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL INTERNET. 53
Tabla 3.6 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD CESANTÍAS. 54
Tabla 3.7 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP CUENTAS BANCARIAS. 54
Tabla 3.8 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP FR DESARROLLO. 54
Tabla 3.9 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL DESARROLLO. 55
Tabla 3.10 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD DESARROLLO. 55
Tabla 3.11 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN CORREO. 56
Tabla 3.12 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP QAD. 56
Tabla 3.13 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL CAPACITACIÓN. 57
Tabla 3.14 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD QAD. 57
Tabla 3.15 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD QAP. 57
Tabla 3.16 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL QAP 58
Tabla 3.17 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM APP QUIROGRAFARIOS. 58
Tabla 3.18 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM BDD FONDOS RESERVA. 59
Tabla 3.19 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM DNS. 59
Tabla 3.20 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM REPORT SERVER. 59
Tabla 3.21 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM APP PENSIONES. 60
Tabla 3.22 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTRANET. 60
Tabla 3.23 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTRANET. 61
Tabla 3.24 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTERNET. 61
Tabla 3.25 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTERNET. 61
Tabla 3.26 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM PRUEBAS. 62

Tabla 3.27 ESCALA DE VULNERABILIDAD.....71
Tabla 3.28 CALCULO DEL RIESGO 72
Tabla 3.29 CÁLCULO DE SEGURIDAD 73

ÍNDICE DE ANEXOS

1. POLÍTICAS DE ADMINISTRACIÓN DE USUARIOS.....124
2. POLÍTICA PARA ADMINISTRACIÓN DE SERVIDORES 132
3. DIAGRAMA DE FLUJO EQUIPOS Y ENLACES DE COMUNICACIONES.....137
4. DIAGRAMA DE FLUJO FALLAS DE ACCESO A INTERNET 139
5. DIAGRAMA DE FLUJO FALLAS EN SERVIDOR DHCP.....140
6. DIAGRAMA DE FLUJO EN SERVIDOR DNS.....141
7. DIAGRAMA DE FLUJO FALLAS EN COMUNICACIONES 142
8. DIAGRAMA DE FLUJO FALLAS DE IMPRESIÓN 143
9. DIAGRAMA DE FLUJO FALLAS AL MOMENTO DE LEVANTAR HTTPS DEBIDO A SESIONES MUERTAS.....144
10. DIAGRAMA DE FLUJO FALLAS AL MOMENTO DE LEVANTAR HTTPS DEBIDO A ESPACIO EN DISCO 145
11. DIAGRAMA DE FLUJO FALLAS AL MOMENTO DE LEVANTAR HTTPS DEBIDO A LOGS.....146
12. DIAGRAMA DE FLUJO FALLA DE FILE SYSTEM DE LOS SERVIDORES 147
13. DIAGRAMA DE FLUJO FALLA DE ACCESO A WWW.IESS.GOV.EC.....148
14. DIAGRAMA DE FLUJO APAGAR LOS SERVIDORES EN CASO DE FALLA EN LA CORRIENTE ELECTRICA 149

RESUMEN

El IESS tiene como función primordial la de brindar servicios a afiliados y empleadores, para lo cual se crea la Dirección de Desarrollo Institucional cuya función principal es la de modernizar al IESS, se implementa el centro de cómputo con servidores SUN e IBM, el IESS al momento no cuenta con políticas para minimizar las amenazas.

Antes de implementar políticas se ha realizado un análisis para determinar los activos con lo que cuenta la Institución, se ha calculado el riesgo y la seguridad que tiene cada uno de ellos, luego de realizar los pasos anteriores se generan políticas para mitigar las amenazas.

Se realiza también un plan para resolver problemas frecuentes para poder mantener el servicio en buen estado y sobre todo saber cómo actuar ante algún problema que enfrente el centro de cómputo.

Por tal razón el presente proyecto propone realizar un estudio de la norma ISO 27001:2005, para definir políticas, abarcando todo lo concerniente a la norma dispuestos de la siguiente manera:

El capítulo 1 hace referencia al plan del proyecto, detallando la situación actual del IESS, el problema a resolver, objetivos del proyecto y la justificación del mismo.

El capítulo 2 define lo que son las Seguridades Informáticas, Importancia de la Seguridad de Información, necesidades de establecer la Seguridad, evaluación de los Riesgos de Seguridad, tipos de Seguridad Informática, niveles de Seguridad, Normativa Internacional, ISM3, Consideraciones del ISO 27001:2005, como realizar un aprovechamiento del Modelo y Beneficios al Aplicar la ISO 27001.

El capítulo 3 detalla la estructura de los diferentes departamentos de la DDI, para realizar un análisis de las seguridades, determinando los requerimientos para poder evaluar y tratar los riesgos de la seguridad de la información del IESS.

El capítulo 4 se define las diferentes políticas de seguridad que se implementarán en el Dirección de Desarrollo Institucional.

El capítulo 5 determina procedimientos de contingencia, que conjuntamente con la norma ISO 27001 se aplica al momento de presentarse alguna falla imprevista en los equipos y aplicaciones del centro de cómputo.

En el capítulo 6 se implementan políticas para procesos críticos que maneja el IESS.

En el capítulo 7 se presentan las conclusiones y recomendaciones, obtenidas luego del desarrollo de este proyecto y que pueden ayudar a la implementación de la norma ISO 27001.

CAPÍTULO I

1. INTRODUCCIÓN

1.1 ASPECTOS GENERALES

1.1.1 LA ORGANIZACIÓN

Los orígenes del sistema de Seguridad Social en el Ecuador se encuentran en las leyes dictadas en los años 1905, 1915, 1918 y 1923 para amparar a los empleados públicos, educadores, telegrafistas y dependientes del poder judicial.

El gobierno del doctor Isidro Ayora Cueva, mediante Decreto Nº 18, del 8 de marzo de 1928, creó la Caja de Jubilaciones y Montepío Civil, Retiro y Montepío Militar, Ahorro y Cooperativa, institución de crédito con personería jurídica, organizada de conformidad con la Ley que se denomina Caja de Pensiones.

En octubre de 1935 se dictó la Ley del Seguro Social Obligatorio y se crea el Instituto Nacional de Previsión, órgano superior del Seguro Social que comenzó a desarrollar sus actividades el 1º de mayo de 1936. Su finalidad fue establecer la práctica del Seguro Social Obligatorio, fomentar el Seguro Voluntario y ejercer el Patronato del Indio y del Montubio.

En la misma fecha inició su labor el Servicio Médico del Seguro Social como una sección del Instituto.

El 25 de julio de 1942 se expidió la Ley del Seguro Social Obligatorio. Los Estatutos de la Caja del Seguro se promulgaron en enero de 1944, con lo cual se afianza el sistema del Seguro Social en el país.

En diciembre de 1949, por resolución del Instituto Nacional de Previsión, se dotó de autonomía al Departamento Médico, pero manteniéndose bajo la dirección del Consejo de Administración de la Caja del Seguro, con financiamiento, contabilidad, inversiones y gastos administrativos propios.

Las reformas a la Ley del Seguro Social Obligatorio de julio de 1958 imprimieron equilibrio financiero a la Caja y la ubicaron en nivel de igualdad con la de Pensiones, en lo referente a cuantías de prestaciones y beneficios.

En 1964 se establecieron el Seguro de Riesgos del Trabajo, el Seguro Artesanal, el Seguro de Profesionales, el Seguro de Trabajadores Domésticos y, en 1966, el Seguro del Clero Secular.

En 1968, estudios realizados con la asistencia de técnicos nacionales y extranjeros, determinaron “la inexcusable necesidad de replantear los principios rectores adoptados treinta años atrás en los campos actuariales, administrativo, prestacional y de servicios”, lo que se tradujo en la expedición del Código de Seguridad Social, para convertirlo en "instrumento de desarrollo y aplicación del principio de Justicia Social, sustentado en las orientaciones filosóficas universalmente aceptadas en todo régimen de Seguridad Social: el bien común sobre la base de la Solidaridad, la Universalidad y la Obligatoriedad”. El Código de Seguridad Social tuvo corta vigencia.

En agosto de l968, con el asesoramiento de la Organización Iberoamericana de Seguridad Social, se inició un plan piloto del Seguro Social Campesino.

El Congreso Nacional, en l987, integró el Consejo Superior en forma tripartita y paritaria, con representación del Ejecutivo, empleadores y asegurados; estableció la obligación de que consten en el Presupuesto General del Estado las partidas correspondientes al pago de las obligaciones del Estado.

En l99l, el Banco Interamericano de Desarrollo, en un informe especial sobre Seguridad Social, propuso la separación de los seguros de salud y de pensiones y el manejo privado de estos fondos.

Los resultados de la Consulta Popular de l995 negaron la participación del sector privado en el Seguro Social y de cualquier otra institución en la administración de sus recursos.

La Asamblea Nacional, reunida en l998 para reformar la Constitución Política de la República, consagró la permanencia del IESS como única institución autónoma, responsable de la aplicación del Seguro General Obligatorio.

El IESS, según lo determina la vigente Ley del Seguro Social Obligatorio, se mantiene como entidad autónoma, con personería jurídica, recursos propios y distintos de los del Fisco. Bajo la autoridad de la Comisión Interventora ha reformado sus Estatutos, Reglamentos y Resoluciones para recuperar el equilibrio financiero.

El 30 de noviembre del 2001, en el Registro Oficial N° 465 se publica la LEY DE SEGURIDAD SOCIAL, que contiene 308 artículos, 23 disposiciones transitorias, una disposición especial única, una disposición general.

El IESS desde hace cuatro años decide implementar el departamento o la Dirección de Desarrollo Tecnológico, cuya finalidad es la de modernizar al IESS.

1.1.2 SITUACIÓN ACTUAL

Dado que las necesidades del IESS han crecido con el tiempo, tanto así que se han incorporado a su red nuevas ciudades, sus aplicaciones han migrado a una tecnología de tres capas para esto se adquieren nuevos equipos tanto para la parte web, para servidores de aplicaciones y base de datos.

En la actualidad se tiene una mayor responsabilidad con la administración de la información que mantiene el IESS, es por ello que se debe dar mayor importancia a los respaldos tanto de la información, como del sistema operativo, correo, servidores web, servidores de aplicaciones, etc.

Entre los equipos que adquirió el IESS está una librería (robot) para la administración y control de respaldos, se cuenta con nuevas cintas de mayor capacidad para los respaldos y sobre todo se adquiere un software que sirve para monitorear y administrar los respaldos.

Este nuevo método es el más adecuado puesto que ya no se sacan los respaldos de una manera local, si no que el robot se encuentra conectado a la red en donde están los servidores, esto facilita ya que si se daña el TABE (unidad de cinta para realizar respaldos) del equipo no importa, pues los respaldos siguen sacándose a través de la red.
La adquisición del software también fue un acierto ya que se puede realizar el monitoreo de cada una de las tareas que se crean para sacar los respaldos, al igual se puede monitorear si la cinta esta en buen estado y cuenta con espacio para la información.

El problema que se encuentra es que no se tiene definido una política de seguridad para las cintas que contienen la información, al igual que la forma de sacar los respaldos, cada que período y sobre cada que tiempo se realizaran las restauraciones para determinar si los respaldos no han sufrido ningún problema.

1.1.3 PLANTEAMIENTO DEL PROBLEMA

El IESS es una entidad Pública, tiene como función primordial la de brindar servicios a sus afiliados y empleadores, para lo cual se crea la DDI (Dirección de Desarrollo Institucional) cuya función principal es la de modernizar al IESS, se implementa el centro de computo con servidores SUN e IBM.

La información y los procesos que la apoyan, sistemas y redes son importantes activos del IESS. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, tesorería, rentabilidad, cumplimiento de la legalidad e imagen comercial. Las organizaciones y sus sistemas de información se enfrentan, cada vez mas, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas

fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que el IESS sea más vulnerable a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado. Muchos sistemas de información existentes en el IESS no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y atención al detalle.

Al momento el proceso que se realiza para tener la información segura en el IESS es el siguiente:

- Se analiza cuál es la información crítica para poder ser respaldada.
- Luego se realiza la configuración de la política con la cual se realizará el respaldo.
- El encargado de realizar la política toma su propia decisión sobre los períodos en los que se realizaran los respaldos.
- El mismo que crea la política toma la decisión de dar por caducado la información que se encuentra respaldada.
- Este proceso es el que se lleva a cabo al momento de respaldar tanto la información que se tiene en la Base de Datos al igual que la información que tiene los servidores de aplicaciones.

El problema de la seguridad de la información en el IESS se da debido a que no se implementa ninguna norma o estándar para realizar las mejores prácticas de la seguridad de la información. En consecuencia, no existe una garantía sobre la seguridad informática existente en el IESS. Este escenario conlleva a que la información de los afiliados sea fácilmente accedida por otras personas ajenas a

la Institución, específicamente a la información de los fondos de Reserva de los afiliados ya que la única práctica para la gestión de la seguridad de la información es el hecho de tener la información de los afiliados respaldada.

1.2 OBJETIVOS DE LA INVESTIGACIÓN

1.2.1 OBJETIVO GENERAL

Determinar Políticas acordes a la Norma Técnica ISO 27001:2005 para ser aplicadas a los procesos que maneja el IESS.

1.2.2 OBJETIVOS ESPECÍFICOS

- Investigar las normas ISO y en la particular la Norma técnica ISO27001-2005
- Proponer un sistema de gestión que garantice la seguridad de la información de los servicios no-line de los afiliados al IESS.
- Generar Políticas de seguridad acordes a la Norma técnica ISO27001-2005
- Determinar las Aplicaciones y los servicios vulnerables del IESS
- Generar Políticas de respaldos de los datos, del sistema operativo, correo, servidores Web, servidores de BDD, servidores de aplicaciones
- Determinar evaluaciones de riesgos de la información
- Determinar Políticas de control, ingreso, creación de usuarios y contraseñas a los servidores del área de producción
- Determinar Políticas de control del software instalado
- Determinar Políticas para el acceso a Internet de los usuarios
- Determinar Políticas de seguridad Física del personal
- Determinar Políticas de directivas para el centro de cómputo
- Determinar Políticas para administrar los cambios (instalaciones o actualizaciones software/hardware y etiquetación)
- Determinar Políticas a seguir en caso de falla de los equipos

1.3 JUSTIFICACIÓN DEL PROYECTO

1.3.1 JUSTIFICACIÓN TEÓRICA

La información es un activo que, como otros activos importantes del negocio, tiene valor para el IESS y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumple los objetivos específicos de seguridad de la organización.

1.3.2 JUSTIFICACIÓN METODOLÓGICA

El proceso para realizar la seguridad no está bajo un estándar, lo que conlleva a tener problemas al momento de tomar decisiones sobre cuáles serían las mejores prácticas a seguir en el caso de que la seguridad de la información sea accedida por personas no autorizadas.

No se lleva una documentación respecto a cómo se está administrando la seguridad de la información en el IESS, es decir, que cada uno de los ingenieros en el área de seguridad aplica su propia política de seguridad.

Actualmente, el sistema de seguridad informática existente en el IESS es muy obsoleto y no es seguro por lo que se requiere implementar un estándar internacional para gestionar la seguridad de la información.

El encargado del área de seguridad requiere aplicar su propia política al momento de aplicar las mejores prácticas y eso no garantiza que sea la correcta.

1.3.3 JUSTIFICACIÓN PRÁCTICA.

Los beneficios son tangibles al momento de implementar la NORMA ISO/IEC 27001:2005 ya que facilitará la administración de las seguridades de la información en el IESS.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 SEGURIDADES INFORMÁTICAS

La seguridad es parte vital de toda organización, constituyéndose en su principal garantía de confiabilidad. Ésta deberá protegerse de forma física y lógica. Físicamente, con una sólida infraestructura tecnológica; y lógicamente por un sistema informático que debe asegurar su inviolabilidad, todo esto manejado a través de políticas establecidas.

Mediante aplicaciones informáticas y procedimientos establecidos durante su desarrollo, por ejemplo, se tendrá un proceso uniforme para la administración de perfiles de usuario, con su respectiva contraseña, las cuales podrán ser creadas por los mismos usuarios y tendrán fechas de caducidad. Estas contraseñas permitirán el acceso a información restringida y a la administración dinámica de contenidos de acuerdo a los perfiles de usuario.

La información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Por lo tanto debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

"La seguridad de la información se caracteriza por la preservación de:

- Su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.
- Su integridad, asegurando que la información y su manera de procesarla sean exactos y completos;
- Su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran." [1]

[1] http://www.enterate.unam .mx/Articulos/2005/febrero/seguridad.htm

2.2 IMPORTANCIA DE LA SEGURIDAD DE INFORMACIÓN

La información y los procesos que la apoyan, sistemas y redes son importantes activos para toda organización. La disponibilidad, integridad y confidencialidad de la información son esenciales para mantener su competitividad, rentabilidad, cumplimiento de la legalidad o imagen comercial.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en gestiones y procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de los requisitos y en la fase de diseño.

2.3 ESTABLECER LAS NECESIDADES DE SEGURIDAD

Lo más importante es que toda organización, en este caso el IESS, tenga claro e identifique sus requisitos de seguridad.
Existen tres fuentes principales para identificar sus necesidades:

- La primera fuente procede de la valoración de los riesgos de la organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

- La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

- La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

2.4 EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad.

"Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, sólo a partes de ella o incluso a sistemas de información individuales, a componentes específicos de sistemas o a servicios donde sea factible, realista y útil, en este caso se aplicará en la parte mas importe que son los datos que maneja el ESS, ya que es allí en donde tiene información de cada uno de los afiliados, funcionarios, empleadores, y todos los prestamos que realiza el afiliado, entre otra información." [2]

La evaluación del riesgo es una consideración sistemática:

- Del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;

- De la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados.

Los resultados de ésta evaluación ayudarán a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información y la implantación de los controles seleccionados para protegerse contra dichos riesgos.

[2] http://www.abast.es/integrityit/riesgos.html

El proceso de evaluación de riesgos y selección de controles puede requerir que sea realizado varias veces para cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

- Tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización.
- Considerar nuevas amenazas y vulnerabilidades.
- Confirmar que las medidas de control siguen siendo eficaces y apropiadas.

Deberían realizarse estas revisiones con distintos niveles de detalle dependiendo de los resultados de las evaluaciones previas y de los umbrales de riesgo que la gerencia está dispuesta a aceptar. Se suelen realizar las evaluaciones de riesgo primero a alto nivel, como un medio de priorizar recursos en áreas de alto riesgo, y después en un nivel más detallado para enfocar riesgos específicos.

2.5 DIFERENTES TIPOS DE SEGURIDAD INFORMÁTICA

La seguridad, como se definió, es la calidad de algo seguro, por tanto la seguridad de un sistema informático (entendiendo como tal a un conjunto de dispositivos y programas que funcionen bajo un fin) estará fijada por todos los elementos que lo componen en software y hardware.

La seguridad a nivel informático no se limitará, por ejemplo, a la posibilidad de evitar la adulteración de la información o intromisión no autorizada a lugares restringidos de acceso, sino también a que los equipos donde se opera y almacena la información sean confiables, siendo la seguridad general establecida, tan buena como la mejor seguridad de cualquier componente.

Pero las estadísticas mundiales indican que los usuarios están preocupados más por la probabilidad que tiene un experto en filtrarse dentro de la información

existente y adulterarla, que por saber si el sistema se va a detener y no funcionar por un período de tiempo, por problemas de hardware.

Estas tendencias mundiales han llevado a que el término seguridad informática sea acotado sólo a lo concerniente a la violabilidad de claves de acceso, redes, sistemas, protecciones contra copias; en general a la seguridad del software.

2.6 NIVELES DE SEGURIDAD

Existían desde el principio de la era de las computadoras, sistemas que tenían sólo como meta establecer diferentes niveles de seguridad.

En la micro computación, con el advenimiento de las redes de área local o LAN, los sistemas operativos empezaron a implementar diferentes niveles de seguridad como: establecer fiabilidad de los datos guardados, otorgar confiabilidad del sistema frente a diferentes configuraciones de hardware, establecer restricciones de acceso ponderadas y selectivas a diferentes recursos, etc.

Así sea de la seguridad de los sistemas o de las políticas de seguridad implementadas por una oficina informática, según una reciente estadística dada a conocer, las conductas humanas naturalmente atentan contra los sistemas implementados.

Las claves de acceso en un amplio porcentaje están relacionadas a: cosas materiales, fechas de acontecimientos personales, y personas. Sobre una muestra de 10.000 individuos a los cuales se les pidió fijasen claves de acceso, el 72% de ellas fueron fácilmente descubiertas, tan sólo acotando la búsqueda a los parámetros citados, el 57% de los encuestados habían comentado o compartido sus claves, y el 62% hasta las había impreso.

Es por ello que se está intentando que cada persona no maneje claves, sino que esté definido dentro de un conjunto de características físicas únicas para que sea reconocido como clave.

Existe una rama llamada biometría que trata de cuantificar en números dichas características, no es extraño que los dispositivos biométricos se comiencen a implementar como verdaderas compuertas de acceso a sistemas, dada su eficacia, eliminando por completo los porcentajes mencionados.

Dentro de los dispositivos cuyos costos se encuentran ya dentro del rango que permite su masividad están el escáner de huellas digitales, escáner de tamaño de palma de mano, reconocedor ponderado de voz y scanner de retina.

2.7 HACKER, PHREAKER, PIRATA Y CRACKER

No existe un diccionario que defina a los términos concretamente, dado que la mayoría de ellos son derivaciones de la jerga informática y su uso ha determinado su significado.

En los años 60, se denominaba dentro del ámbito informático "hacker" a toda persona altamente capacitada, que tenía los conocimientos necesarios para violar a los sistemas existentes, mediante modificación del código que lo compone, a nuevas y más productivas instancias.

Ya entrados los 70, y debido a un descuido fortuito de una compañía telefónica y un premio de una caja de cereales, un usuario llamado John Draper alias "Capitán Crunch" logra realizar una llamada de larga distancia introduciendo un tono preciso dentro de una línea abierta de teléfono, de allí el término "phone hacker" que después deriva en "phreaker"

Los phreakers toman un nivel insospechado de popularidad, considerándoselos responsables de invaluables defraudaciones. Se llegaron hasta a fundar asociaciones que brindaban dichos servicios, como el Homebrew Computer Club, cuyos socios comercializaban cajas con la capacidad de violar sistemáticamente los sistemas de protección de llamadas telefónicas. Dos de sus miembros cuyos alias eran "Berkeley Blue" (Steve Jobs) y "Oak Toebark" (Steve Wozniak), más tarde decidieron fundar una empresa cuyo nombre marcaría un giro en la forma del manejo de las microcomputadoras: "Apple Computers Inc."

En el principio de los 80, comienza el auge de las microcomputadoras y los sistemas protegidos para las copias de los usuarios, generando un movimiento en contra de esta actitud. Desde ese momento los denominados crakers, "rompían" el código fuente de los programas eliminando las líneas que efectuaban las comprobaciones de protección.

A mediados de los 80, las redes corporativas toman características abiertas y se empieza a ver cómo individuos de muy alta capacidad empiezan a penetrarlas, no hubo desde aquel entonces empresa y/u oficinas gubernamentales que estuviesen a salvaguardo, en honor de aquellos que se los consideraba genios por entrar ("hack in") al código para mejorarlo, se les siguió dando el seudónimo de "hackers".

Se les comienza a llamar "piratas" a aquéllos que sólo les interesaba lucrar con los sistemas ya desprotegidos, para diferenciarlos de aquéllos que podían efectuar el "hackeo" o "crackeo".

Desde cualquier época hasta hoy, existen infinidad de ejemplos de cómo los sistemas considerados de máxima seguridad han sido violados, modificados, borrados, y desprotegidos.

En el caso de los sistemas informáticos que presta el IESS están expuestos al Internet por lo que es algo que atrae a muchas personas maliciosas, puesto que la información que viaja por el Internet es muy importante, por lo que se debe tener un buen respaldo de la información en el caso de que exista adulteración de la misma.

En el caso de un usuario final, generalmente introducen programas que graban todo tipo de información que el usuario escriba: nombres de usuario, números de teléfono, número de cuentas bancarias en el caso que deseen realizar algún préstamo quirografario e incluso cobrar los fondos de reserva, etc., cuando el

usuario se reconecte al lugar desde donde le fue insertado el programa, éste se encargará de enviar toda la información acumulada.

Otra operatoria similar, con generalmente resultados de catástrofe, son los denominados "virus informáticos", cuyo nombre proviene de su símil biológico por su habilidad para enfermar al "computador", e infectar todo lugar asignado posible auto reproduciéndose. La denominada "enfermedad" del computador puesta de manifiesto bajo ciertas circunstancias (fechas determinadas, cantidad de horas desde la llegada del virus, etc.) suele ir desde un aviso simple que el computador ha sido infectado con determinado virus, hasta el borrado sistemático de toda información existente.

2.8 NORMATIVA INTERNACIONAL

Este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del Information Systems Management System (ISMS) , la adopción del ISMS debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa, la dinámica que implica su aplicación, ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones.

Las políticas que se aplicarán para la obtención de respaldos, al igual que su restauración se desarrollarán de acuerdo al estudio de seguridades de la norma ISO 27001, motivo por el cual se realizará una introducción de cómo nace esta norma.

“ISO (Organización Internacional de Estándares) e IEC (Comisión Internacional de Electrotécnia) conforman un especializado sistema para los estándares mundiales. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de

interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo." [3]

"La norma ISO 27001 es una reforma a la norma 17799, ésta fue preparado inicialmente por el Instituto de Normas Británico (como BS 7799) y fue adoptado, bajo la supervisión del grupo de trabajo "Tecnologías de la Información", del Comité Técnico de esta unión entre ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales de ISO e IEC.

El estándar ISO/IEC 27001 es el nuevo estándar oficial, su título completo en realidad es: BS 7799-2:2005 (ISO/IEC 27001:2005). También fue preparado por este JTC 1 y en el subcomité SC 27, IT (Information Technology). La versión que se considerará en este texto es la primera edición, de fecha 15 de octubre de 2005, si bien en febrero de 2006 acaba de salir la versión cuatro del mismo.

La certificación ISO 27001 analiza y verifica el cumplimiento de los procesos y cumplimiento de los controles necesarios (mas adelante se detallara cada uno de los controles que utiliza la Norma) para implementar con éxito un sistema de Gestión de la información, para toda organización en nuestro caso práctico se aplicará para el IESS y específicamente en la información datos y del sistema informático de cada uno de los servidores que tiene la institución.

El conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta son:

- ISO/IEC 27000 Fundamentals and vocabulary
- ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005) - Publicado el 15 de octubre del 2005
- ISO/IEC 27002 Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
- ISO/IEC 27003 ISMS implementation guidance (bajo desarrollo)

[3] http://www.desarrolloweb.com/articulos/2435.php

- ISO/IEC 27004 Information security management measurement (bajo desarrollo)
- ISO/IEC 27005 Information security risk management (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (bajo desarrollo)

Actualmente el ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad." [4]

2.9 ISM3

"La publicación del ISM3 (Information Security Management Maturity Model) ofrece un nuevo enfoque de los sistemas de gestión de seguridad de la información (ISM). ISM3 nace de la observación del contraste existente entre el número de organizaciones certificadas ISO9000 (unas 350,000), y las certificadas BS7799-2:2002 (unos cientos en todo el mundo). ISM3 pretende cubrir la necesidad de un estándar simple y aplicable de calidad para sistemas de gestión de la seguridad de la información. ISM3 proporciona un marco para ISM que puede utilizarse tanto por pequeñas organizaciones que realizan sus primeros esfuerzos, como a un nivel alto de sofisticación por grandes organizaciones como parte de sus procesos de seguridad de la información...

Al igual que otros estándares del ISECOM, ISM3 se proporciona con una licencia de "código libre", tiene una curva de aprendizaje suave, y puede utilizarse para fortalecer sistemas ISM en organizaciones que utilicen estándares como COBIT, ITIL, CMMI y ISO17799. Está estructurado en niveles de madurez, de modo que cada organización puede elegir un nivel adecuado para su negocio, y cubrir ese objetivo en varias etapas.

En lugar de depender exclusivamente de métodos caros de análisis de riesgos, que suponen una barrera a la implantación de sistemas de ISM, ISM3 sigue un punto de vista cualitativo, empezando por analizar los requerimientos de seguridad del negocio. Permite a la empresa aprovechar la infraestructura actual,

[4] http://www.mastermagazine.info/informes/9544.php

fortaleciéndola mediante un sistema de calidad, y alcanzado niveles de madurez certificables, según el sistema de ISM evoluciona.

Utiliza un modelo de gestión para diferenciar las tareas de seguridad operativa que previenen y mitigan incidentes de tareas estratégicas y tácticas que identifican los activos a proteger, las medidas de seguridad a emplear, y los recursos que han de dedicarse a éstas. Se describe un proceso de certificación que permite a una organización autoevaluar su madurez, o bien obtener una certificación de un auditor independiente." [5]

2.10 EFECTOS DE LA CERTIFICACIÓN

A efectos de la certificación, la transición entre ambas normas queda propuesta (o establecida) por el TPS-55 de UKAS (United Kingdom Acreditación Service) "Transition Statement Regarding Arrangements for the Implementation of ISO 27001:2005". Establece que las empresas (en realidad los auditores, lo cual afecta directamente a las empresas) durante los primeros seis meses (desde que se firmó el acuerdo "MoU: Memorandum of Understanding" entre UKAS y el Departamento de Comercio e Industria de Reino Unido), pueden elegir acerca de qué estándar aplicar, a partir del 23 de julio del 2006, la única certificación que se deberá aplicar será la ISO/IEC 27001:2005. Ante cualquier no conformidad con la aplicación de la misma motivada claramente por su transición, se establece un plazo de un año para solucionarla, es decir, hasta el 23 de julio de 2007.

2.11 CONSIDERACIONES DEL ISO 27001:2005

La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la seguridad de la información", por ello propone toda una secuencia de acciones tendientes al "establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System)".

[5] http://www.kriptopolis.org/node/1414

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

- ISMS.
- Valoración de riegos (Risk Assesment)
- Controles

2.12 APROVECHAMIENTO DEL MODELO

Este estándar internacional adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el ISMS en una organización. Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un “proceso”. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

Este estándar internacional adopta también el modelo “Plan-Do-Check-Act” (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS, y significa lo siguiente:

- Plan (Establecer el ISMS): Implica, establecer la política ISMS, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, en este caso serian los datos de configuración del Sistema Operativo, los logs, etc., entregando resultados acordes a las políticas y objetivos de toda la organización.
- Do (Implementar y operar el ISMS): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

- Check (Monitorizar y revisar el ISMS): Analizar y medir dónde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- Act (Mantener y mejorar el ISMS): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la continua mejora del ISMS.

2.13 CONTROLES

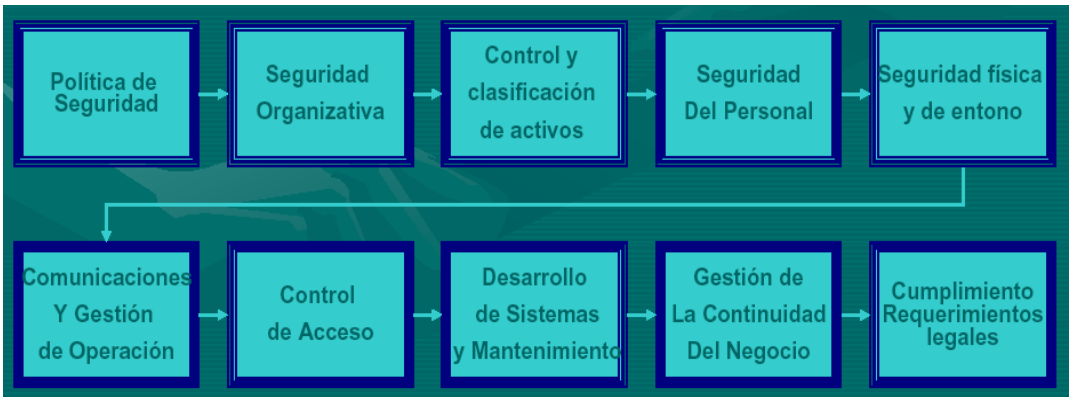


Figura 2.1 CONTROLES DE LA NORMA ISO\IEC 17799:2005

La norma ISO 27001 se basa en los controles de la norma 17799, para lo cual listaremos cada uno de los controles que utiliza dicha norma.

- **Política de seguridad:** Se necesita una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación.

- **Organización de la seguridad:** Sugiere diseñar una estructura de administración dentro de la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes. Esta sección considera las políticas generales de la organización y detalla cómo se debe administrar la seguridad de la información dentro de la compañía. Asimismo, define cómo mantener la

seguridad de las instalaciones de procesamiento de información y los activos informáticos accedidos por terceros, (proveedores, clientes, etc.).

- **Control y clasificación de los recursos de información:** Detalla los elementos de la compañía (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad, manteniendo una protección adecuada, garantizando que reciban un nivel adecuado de protección. En este sentido, los activos deben ser clasificados en: confidenciales, privados, de uso interno y de uso público. Para cada clasificación se debe implantar mecanismos adecuados de seguridad de acuerdo a su importancia.

- **Seguridad del personal:** Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan. También determina cómo incide el papel que desempeñan los empleados como corresponsales de la seguridad de la información. En esta sección se busca minimizar los riesgos ocasionados por el personal, tales como hurto y manipulación de la información, fraudes y mal uso de la plataforma tecnológica. Su propósito es crear conciencia en los usuarios sobre los riesgos que pueden amenazar a la información, para lo cual considera mecanismos y medios para informar y capacitar periódicamente a todos los usuarios (personal interno de la compañía y personal que brinde servicios) de todas las políticas, y establecer mecanismos de prevención, identificación, notificación y corrección de posibles incidentes de seguridad.

- **Seguridad física y ambiental:** Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la compañía, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se

almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.

- **Manejo de las comunicaciones y las operaciones:** Define las políticas y procedimientos para asegurar la correcta operación de las instalaciones de procesamiento (servidores y equipos de comunicación). Los objetivos de esta sección se pueden enumerar como sigue:

    - Asegurar la protección y el funcionamiento correcto de las instalaciones de procesamiento de la información.
    - Minimizar el riesgo de falla de los sistemas.
    - Proteger la integridad del software y la información.
    - Conservar la integridad y disponibilidad del procesamiento y transmisión de la información.
    - Garantizar la protección de la información en las redes y de la infraestructura de soporte.
    - Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.

- **Control de acceso:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la compañía y el personal externo que brinda servicios, en concordancia con sus responsabilidades. Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.

- **Desarrollo y mantenimiento de los sistemas:** Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en

todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información. Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la compañía (protección de archivos, programas, base de datos, políticas de cifrado, etc.), para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.

- **Manejo de la continuidad del negocio:** Considera el análisis de todos los procesos y recursos críticos del negocio, y define las acciones y procedimientos a seguir en casos de fallas o interrupción de los mismos, evitando la pérdida de información y la cancelación de los procesos productivos del negocio, lo que podría provocar un deterioro de la imagen de la compañía, una posible pérdida de clientes o incluso una dificultad severa que impida continuar operando.

- **Cumplimiento:** Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 27001, concuerda con otras leyes, reglamentos, obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorias, contrato de servicios, etc. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y a las consideraciones técnicas; asimismo, busca garantizar que las políticas de seguridad sean acordes a la infraestructura tecnológica de la compañía.

Existen además Políticas de cifrado que especifican todos los criterios que se deben considerar para determinar qué tipo de información se debe almacenar en un formato ilegible (método de cifrado) para evitar que personas no autorizadas puedan acceder a la misma y Políticas de comercio electrónico que establece todas las consideraciones que se deben adoptar si la compañía posee presencia en Internet y cuenta con prácticas de comercio electrónico.

Tomando en cuenta las áreas que cubre esta norma técnica, y considerando que el IESS no ha adoptado un programa de protección definido de la información, ISO 27001 puede servir de parámetro para que lo defina, e incluso, puede servirle de guía para configurar la política de seguridad para poder obtener una política eficiente para sacar los respaldos de datos, al igual que del sistema operativo y de los logs, etc.

En todo caso, es importante tener en cuenta que ISO 27001 es un buen esquema de seguridad que las empresas pueden adoptar.

2.14 BENEFICIOS AL APLICAR LA ISO 27001

En general, las mejores prácticas son simplemente la mejor manera de cumplir con un proceso de negocio; y a su vez representan la manera en que el IESS puede alcanzar la estabilidad con respecto a la información llegando a lograr obtener muchos beneficios.

Algunos de los beneficios perseguidos por las organizaciones al adoptar, mantener y comunicar un marco de referencia son:

- Presentan una ventaja significativa desde la perspectiva de la seguridad y control sobre aquellas que carecen de dicho marco de referencia.
- Si se utiliza un criterio estándar para la configuración y administración de los sistemas de la organización, se puede minimizar la posibilidad de que una debilidad en uno de ellos pueda comprometer los controles de acceso de los restantes (pese a que éstos cuenten con medidas de seguridad robustas) explotando sus vínculos habituales.
- Adoptando estándares y marcos de referencia común, la organización puede construir una arquitectura de seguridad que permita minimizar las brechas que se puedan registrar entre las amenazas detectadas y los controles existentes, mitigando el riesgo asociado a una eventual ocurrencia de dicha amenaza.

- Partes interesadas, como es Auditoria Interna y Administradores del Seguridad, pueden ser apoyados por la existencia de un marco de

referencia en el área de TI, facilitando su entendimiento respecto a los roles, políticas y estándares y la tarea de lograr el cumplimiento de los mismos.

- Se le facilita a la organización la simplificación, estandarización y automatización de los servicios de seguridad.

CAPÍTULO III

3. ANALISIS DE LAS SEGURIDADES DEL IESS

3.1 REQUERIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El IESS es una entidad cuya organización y funcionamiento se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia. Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del sistema nacional de Seguridad Social.

El IESS se encuentra en una etapa de transformación, el plan estratégico que se está aplicando, sustentando en la Ley de Seguridad Social vigente, convertirá a esta institución en una aseguradora moderna, técnica, con personal capacitado que atenderá con eficiencia, oportunidad y amabilidad a toda persona que solicite los servicios y prestaciones que ofrece.

El IESS tiene la misión de proteger a la población urbana y rural, con relación de dependencia laboral o sin ella, contra las contingencias de enfermedad, maternidad, riesgos del trabajo, discapacidad, cesantía, invalidez, vejez y muerte, en los términos que establece el Art. 17 de la Ley de Seguridad Social vigente.

Los orígenes remotos del sistema del Seguro Social en el Ecuador se encuentran en las leyes dictadas en los años 1905, 1915 y 1918 y 1923 para amparar a los empleados públicos, educadores, telegrafistas y dependientes del poder judicial.

El IESS tiene varias sucursales a nivel nacional a través de una red Lan y Wan.

Actualmente cuenta con una infraestructura de la plataforma SUN e IBM estos servidores se encuentra distribuidos en:

- Servidores de Base de Datos
- Servidores de Aplicaciones
- Servidores WEB

- Servidores para el área de desarrollo
- Servidores para el ares de producción
- Servidores de pruebas

Cada uno de ellos maneja información valiosa para la Institución, es por ello que nace la necesidad de aplicar normas ISO para garantizar la seguridad de la información.

Actualmente el IESS no posee políticas de seguridad que garanticen la seguridad de la información y esta información se encuentra vulnerable a cualquier ataque es por ello que se necesita implementar políticas de seguridad.

Dada esta situación es importante aplicar normas y políticas de seguridad tomando la norma ISO 27001, para con ello dar soluciones a la problemática que afronta la Institución y sobre todo considerando que la información o activo que maneja es de un alto riesgo.

3.1.1 ORGÁNICO FUNCIONAL

Mediante Resolución Nº 021, el Consejo Directivo del IESS aprobó el nuevo orgánico funcional de la Institución que cuenta con seis niveles:

- Nivel de gobierno y Dirección superior.- Responsables de la aplicación del Seguro General Obligatorio en todo el territorio nacional: Consejo Directivo, Dirección General y Dirección Provincial.
- Nivel de Dirección especializada.- Órganos especializados en el aseguramiento de las contingencias y calificación del derecho a las prestaciones que otorga el Seguro General Obligatorio: Dirección del Seguro General de Salud Individual y Familiar, Dirección del Sistema de Pensiones, Dirección del Seguro General de Riegos del Trabajo y Dirección del Seguro Social Campesino.
- Nivel de reclamación administrativa.- Responsables de la aprobación o denegación de los reclamos de prestaciones plantados por los asegurados:

Comisión Nacional de Apelaciones y Comisión Provincial de Prestaciones y Controversias. Son instancias de resolución administrativa.

- Nivel Técnico Auxiliar.- Dirección Actuarial y Comisión Técnica de Inversiones.
- Nivel de Control Interno.- La Auditoria Interna es el órgano de control independiente, de evaluación y asesoría, responsable del examen posterior, objetivo, profesional, sistemático y periódico de los procedimientos administrativos, presupuestarios y financieros del Instituto.
- Nivel de asistencia técnica y administrativa.- Dirección Económica Financiera, Dirección de Servicios Corporativos, Dirección de Desarrollo Institucional, Secretaría General y Procuraduría General.

3.1.2 ÓRGANOS DE GOBIERNO

Dentro de la estructura orgánica del Instituto, el Consejo Directivo, la Dirección General y la Dirección Provincial constituyen el nivel de gobierno y dirección superior, y son responsables de la aplicación del Seguro General Obligatorio.

El Consejo Directivo es el órgano máximo de gobierno y le corresponde dictar las políticas para la aplicación del Seguro General Obligatorio, así como las normas de organización y funcionamiento de los seguros generales y especiales aplicados por el IESS y la fiscalización de los actos de la administración. Está conformado de manera tripartita por un representante del Ejecutivo, quien lo preside, un representante de los empleadores y un representante de los trabajadores.

3.1.3 LA DIRECCIÓN GENERAL

Es el órgano responsable de la organización, dirección y supervisión de todos los asuntos relativos a la ejecución de los programas de protección provisional de la población urbana y rural, con relación de dependencia o sin ella, con sujeción a lo que determina la Ley de Seguridad Social. La autoridad responsable es el Director General.

En esta nueva estructura se crea la Subdirección General, dependencia de apoyo y asistencia a la Dirección General. La autoridad responsable es el Subdirector General, quien es designado por el Consejo Directivo. Cuando el Director General renuncia, falta o se ausenta temporalmente o por impedimento, le subroga el Subdirector General.

3.1.4 LA DIRECCIÓN PROVINCIAL

Es responsable de la aplicación de las estrategias de aseguramiento obligatorio, la recaudación oportuna de las aportaciones de los empleadores y asegurados y la calificación del derecho a prestaciones de los afiliados, comprendidos en la circunscripción geográfica de su competencia. Es el órgano responsable del manejo de las cuentas patronales e individuales de los asegurados, del ejercicio de la jurisdicción coactiva, y de la consolidación de la información presupuestaria y contable de todas las dependencias administrativas subordinadas a su autoridad.

3.1.5 DIRECCIONES ESPECIALIZADAS

Dentro del nivel de dirección especializada se encuentran las direcciones del Seguro General de Salud Individual y Familiar, el Sistema de Pensiones, el Seguro General de Riesgos del Trabajo, el Seguro Social Campesino y las direcciones provinciales, encargadas del aseguramiento de las contingencias y la calificación del derecho a las prestaciones que otorga el Seguro General Obligatorio.

3.1.6 ESTRUCTURA ORGANIZACIONAL DE LA DDI

La DDI tiene la función primordial de modernizar al IESS cuenta con la siguiente estructura.

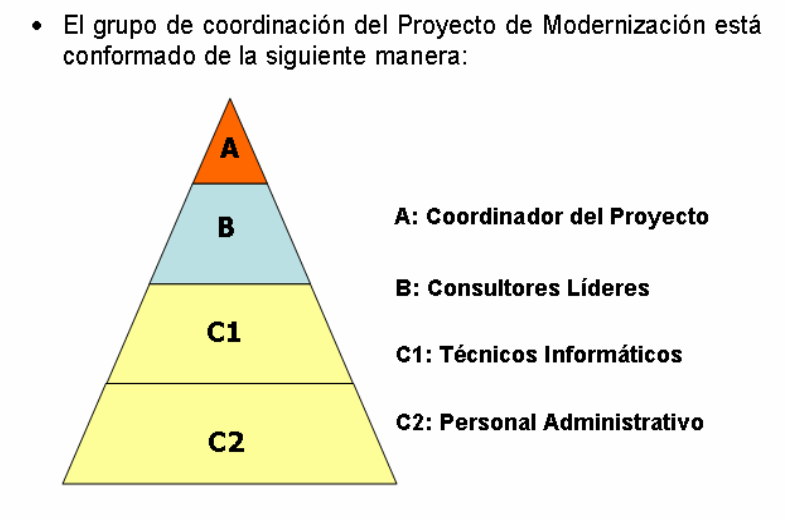


Figura 3.1 ESTRUCTURA DE COORDINACIÓN DEL PROYECTO DE MODERNIZACIÓN

En la figura 3.1 se muestra el esquema de cómo esta estructurado la coordinación del proyecto, cuenta con el Coordinador del proyecto cuya función principal es la de dotar de toda la infraestructura que necesita el proyecto como equipo, y personal capacitado para las diferentes áreas.

En segundo plano se encuentran los consultores lideres quines se encargan de el aspecto de desarrollo.

El tercer grupo son técnicos cuya función es la de administración, mantenimiento de los equipos y servidores y soporte a usuarios

El cuarto grupo maneja el aspecto administrativo, son los que se encargan del aspecto del recurso humano

Este es un esquema general de cómo esta estructurado la DDI mas adelante se detallara cada una de las ares.

3.1.7 ORGANIGRAMA DE LA DDI

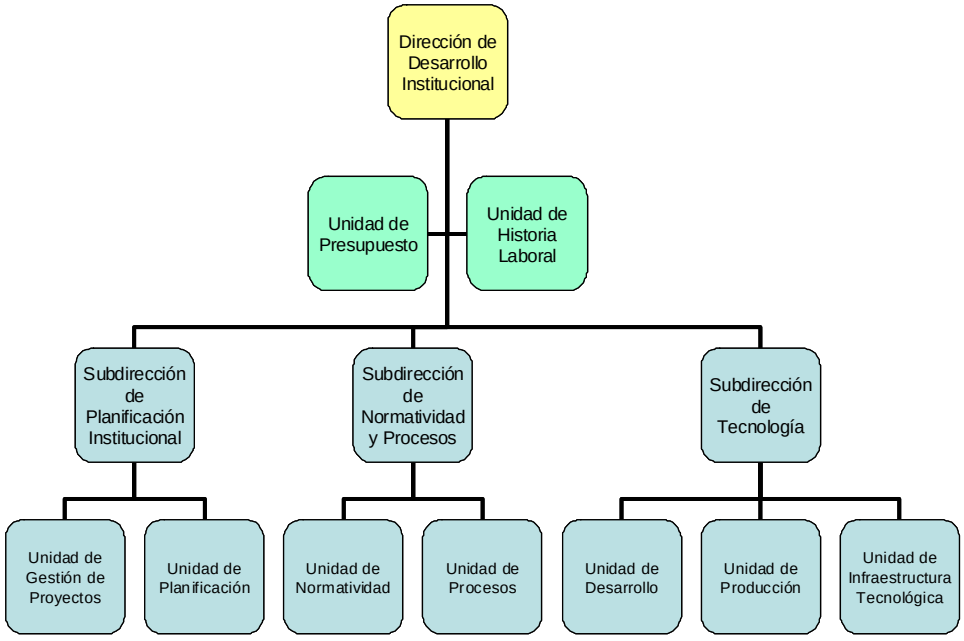


Figura 3.2: ORGANIGRAMA DDI

La DDI es la encargada de la formulación y coordinación de la ejecución de los proyectos y programas de mejoramiento y desarrollo de la Institución, en procura de la eficacia, eficiencia y economía de los procesos del IESS, de conformidad con lo establecido en el Plan Estratégico Institucional y las normas y políticas definidas por el Consejo Directivo. Así también, esta Dirección es la responsable de la administración de la infraestructura tecnológica del Instituto.

La autoridad responsable de la gestión de la Dirección de Desarrollo Institucional es su Director, nombrado por el Director General, de conformidad con las leyes y reglamentos sobre la materia.

3.1.7.1 Responsabilidades.

La DDI tiene a su cargo las siguientes responsabilidades:

- La ejecución de actividades de apoyo técnico relacionadas con el desarrollo de la Institución.

- La proposición ante la Dirección General de proyectos o programas relacionados con la sistematización de productos y procesos de la Institución; y la dirección y supervisión de los proyectos que fueren aprobados.

- La aplicación estricta de las normas legales y procedimientos vigentes, relacionados con la administración de los recursos humanos.

- El conocimiento y despacho oportuno de los asuntos de competencia del área de gestión, sometidos a consideración de la Dirección de Desarrollo Institucional, dentro de los plazos que señala la Ley.

- La presentación a la Dirección General, de los informes de rendición de cuentas, sobre el cumplimiento de sus actividades.

3.1.7.2 Dependencias de la DDI

La Dirección de Desarrollo Institucional tiene a su cargo: la Subdirección de Planificación Institucional, la Subdirección de Procesos y Normatividad, la Subdirección de Tecnología y Unidad de Presupuesto, Unidad de Historia Laboral.

3.1.7.3 Competencia de la Subdirección de Planificación Institucional

La Subdirección de Planificación Institucional es la encargada de la Planificación Estratégica Institucional, su evaluación y control, apoyada en las herramientas metodológicas y tecnológicas pertinentes; así como también la formulación y coordinación de la ejecución de los proyectos y programas de mejoramiento y desarrollo de la Institución, derivados de la planificación referida.

3.1.7.4 Responsabilidades de la Subdirección de Planificación Institucional.

El cumplimiento de actividades y gestiones atinentes a la elaboración de términos de referencia y bases de contratación de consultorías y asesorías especializadas en su ámbito de acción.

La dirección de los grupos profesionales, de consultoría y asesoría especializada, determinados por la Dirección General, para el estudio de las reformas a los programas de seguros sociales y la optimización de la organización y funcionamiento del Instituto.

La supervisión y validación del cumplimiento del Plan Estratégico Institucional y los correspondientes Planes Operativos Anuales, en coordinación con los órganos y dependencias de la Institución, y la Unidad de la Planificación.

La validación y perfeccionamiento del concepto desarrollado en los productos y procesos, para alcanzar la optimización en el otorgamiento de las prestaciones y servicios de la Institución.

Direccionamiento estratégico y operativo de las Unidades de Planificación y Gestión de Proyectos.

3.1.7.5 Dependencias de la Subdirección de Planificación

La Subdirección de Planificación Institucional tiene a su cargo: la Unidad de Planificación y la Unidad de Gestión de Proyectos.

3.1.7.5.1 Responsabilidades de la Unidad de Planificación.-

La formulación del Plan Estratégico Institucional, en coordinación con los órganos y dependencias de la Institución.

La evaluación técnico económica, sistemática y periódica, de la gestión Institucional, en cuanto al cumplimiento del Plan Estratégico Institucional y sus planes operativos; así como la elaboración del informe de evaluación sobre el cumplimiento del mismo.

La conceptualización de los productos y servicios del Instituto, para alcanzar la optimización en el otorgamiento de las prestaciones y servicios de la Institución, así como el control y evaluación de sus resultados, de conformidad con los planes y programas aprobados por el Consejo Directivo.

Análisis y diseño del sistema de control de gestión institucional.

3.1.7.5.2 Responsabilidades de la Unidad de Gestión de Proyectos.-

La evaluación, seguimiento y control del desarrollo de todos los programas y proyectos derivados de la planificación estratégica y operativa de la institución.
El registro, control y archivo de la documentación sobre el avance y resultados de los proyectos a su cargo.
Construcción, implementación y administración del sistema de control de gestión institucional.

3.1.7.6 COMPETENCIA DE LA SUBDIRECCIÓN DE PROCESOS Y NORMATIVIDAD.

La Subdirección de Procesos y Normatividad es la encargada de establecer el marco normativo en todos los ámbitos de acción institucional, así como el esquema de gestión organizacional por procesos, en concordancia con el marco Estratégico Institucional.

3.1.7.7 RESPONSABILIDADES DE LA SUBDIRECCIÓN DE PROCESOS Y NORMATIVIDAD

El cumplimiento de actividades y gestiones atinentes a la elaboración de términos de referencia y bases de contratación de consultorías y asesorías especializadas en su ámbito de acción.
La validación y perfeccionamiento de la normativa y procesos desarrollados, para alcanzar la optimización en el otorgamiento de las prestaciones y servicios de la Institución, así como en la administración y operación institucional.
Direccionamiento estratégico y operativo de la Unidad de Normatividad y la Unidad de Procesos.
Las demás que, por la naturaleza de sus procesos, le asigne el Director de Desarrollo Institucional. Normatividad

3.1.7.8 DEPENDENCIAS DE LA SUBDIRECCIÓN DE NORMATIVIDAD Y PROCESOS.

La Subdirección de Normatividad y Procesos tiene a su cargo: la Unidad de Normatividad y la Unidad de Procesos.

3.1.7.8.1 RESPONSABILIDADES DE LA UNIDAD DE NORMATIVIDAD.-

Elaborar, actualizar y/o derogar las políticas, normas, procedimientos, manuales, instructivos y formularios en general, que regulen el funcionamiento de las Dependencias y Entidades del Instituto, orientados a la estructuración de un sistema institucional de gestión de calidad.

Realizar de manera adecuada y oportuna actividades de promoción, investigación y divulgación de la normatividad y sus respectivos manuales, aprobados y autorizados por la autoridad competente, en coordinación con la Unidad de Capacitación correspondiente.

La evaluación de la aplicación de la normatividad vigente en el contexto institucional, a través de un proceso de evaluación programado, y efectuar propuestas para el mejoramiento de su gestión.

Asesorar a las unidades o departamentos, que lo solicitan en la interpretación y aplicación de procedimientos y técnicas administrativas; coordinándose con cada una de ellas e implantando nuevos y mejores sistemas de gestión y establecer conjuntamente, los proyectos de creación o modificación de alguna norma en general.

Estudio, bibliografía y documentación sobre temas de normatividad y procesos.

La preparación y presentación de los estudios técnicos para la revisión y actualización de los reglamentos, instructivos y manuales relacionados con los procesos administrativos de la Institución.

La preparación de estudios técnicos y la definición de los procedimientos para la contratación de servicios profesionales, tendientes a obtener la certificación de calidad de los distintos procesos y productos de la Institución;

3.1.7.8.2 RESPONSABILIDADES DE LA UNIDAD DE PROCESOS.-

Realización de estudios, diagnóstico y análisis de la estructura, funcionamiento y de costeo de los procesos de la organización y en especial, los de afiliación, aseguramiento y entrega de prestaciones, a fin de diseñar mejores esquemas organizacionales y de gestión orientados a un mejoramiento continúo de la Institución, permitiendo desarrollar con mayor eficiencia y productividad las actividades de los funcionarios y empleados.

Diseño de los procesos mediante los cuales se elaboran y aplican las regulaciones que norman la actividad Institucional.
Estudio, bibliografía y documentación sobre temas de normatividad y procesos.
Realizar conjuntamente con el área de tecnología el análisis de procedimientos susceptibles de automatización.

3.1.7.9 COMPETENCIA DE LA SUBDIRECCIÓN DE TECNOLOGÍA.-

La Subdirección de Tecnología es la encargada de la planificación, normatividad, programación, organización, gestión, control y evaluación de la plataforma tecnológica y de los servicios que esta brinda, derivados de la planificación estratégica institucional referida.

3.1.7.10 RESPONSABILIDADES DE LA SUBDIRECCIÓN DE TECNOLOGÍA.

La Subdirección de Tecnología tiene las siguientes responsabilidades:

La planificación, programación, organización, gestión, control y evaluación de la plataforma tecnológica y de los servicios informáticos del Instituto.

La formulación y entrega oportuna, de la pro forma presupuestaria consolidada anual de los servicios informáticos, con base en los requerimientos de cada una de las dependencias del Instituto.

Establecimiento del un sistema de administración y soporte técnico de la plataforma institucional en el ámbito nacional, a través de encargados responsables de las actividades correspondientes, y mecanismos acordes con el fin del servicio que debe prestar la plataforma tecnológica en referencia.

El establecimiento y uso de sistemas de información confiables y de sistemas apropiados de documentación y archivo de registros, informes y documentos de las actividades a cargo de esta Subdirección.

La presentación, por órgano regular, al Director General, del Informe Anual sobre el cumplimiento del Plan Estratégico Informático, aprobado por el Consejo Directivo, y sobre la efectividad y costo de los servicios proporcionados.

Las demás que, por la naturaleza de sus procesos, le asigne el Director de Desarrollo Institucional.

3.1.7.11 DEPENDENCIAS DE LA SUBDIRECCIÓN DE TECNOLOGÍA.

La Subdirección de Tecnología tiene a su cargo: la Unidad de Desarrollo, la Unidad de Producción y la Unidad de Implementación Tecnológica.

3.1.7.11.1 RESPONSABILIDADES DE LA UNIDAD DE DESARROLLO.

La asistencia técnica para el desarrollo e implantación de sistemas automatizados en los procesos institucionales.

El establecimiento de la normatividad técnica para el desarrollo de las herramientas informáticas que demande la Institución, así como la elaboración de manuales técnicos correspondientes, y su aplicación en el ámbito de gestión.

La preparación de las especificaciones técnicas, de los documentos precontractuales y la asistencia técnica a los Titulares o encargados de las Direcciones, para la adquisición y/o desarrollo de herramientas de software relativas a la razón de ser del Instituto,

El establecimiento y uso de sistemas de información confiables y de sistemas apropiados de documentación y archivo de registros, informes y documentos de las actividades a cargo de esta Unidad ;

3.1.7.11.2 RESPONSABILIDADES DE LA UNIDAD DE PRODUCCIÓN.

La coordinación de la operación y mantenimiento de los centros de cómputo, las redes de comunicación de datos y las bases de datos, a escala nacional.

El establecimiento de la normatividad técnica para la administración de la plataforma tecnológica institucional, así como la elaboración de los manuales técnicos correspondientes, y su aplicación.

La preparación de las especificaciones técnicas, de los documentos precontractuales y la asistencia técnica a los Titulares o encargados de las Direcciones, para la adquisición y/o arrendamiento de hardware, software para la administración y operación de la plataforma tecnológica, licencias, instalación, mantenimiento y soporte técnico.

La preparación de los planes para provisión de insumos, materiales de trabajo, accesorios y repuestos necesarios para el funcionamiento y mantenimiento de los equipos e instalaciones de cómputo y la supervisión de su cumplimiento.

El establecimiento y uso de sistemas de información confiables y de sistemas apropiados de documentación y archivo de registros, informes y documentos de las actividades a cargo de esta Unidad ;

3.1.7.11.3 RESPONSABILIDADES DE LA UNIDAD DE INFRAESTRUCTURA TECNOLÓGICA

La conceptualización de la infraestructura tecnológica y de los servicios informáticos de uso general en la Institución, en coordinación con la Subdirección de Planificación Institucional.

La elaboración de los proyectos de implementación de infraestructura tecnológica, de cada una de las dependencias del Instituto.

La implementación de la infraestructura tecnológica, en las dependencias de la institución.

La elaboración de especificaciones técnicas de la infraestructura tecnológica de la institución.

El análisis de las innovaciones tecnológicas, a fin de incorporar nuevas tendencias al Instituto.

El apoyo a los procesos de adquisición, en la etapa de calificación de ofertas, de equipamiento informático y/o de telecomunicaciones especializado, que se lleven adelante en las dependencias del Instituto.

Las tareas de coordinación con las demás unidades de la Subdirección de Tecnología, que permita cumplir con los objetivos del plan estratégico.

El establecimiento y uso de sistemas de información confiables y de sistemas apropiados de documentación y archivo de registros, informes y documentos de las actividades a cargo de esta Unidad.

3.1.7.12 COMPETENCIA DE LA UNIDAD DE PRESUPUESTO.

La unidad de Presupuesto es la encargada de la planificación y ejecución presupuestaria de todos los proyectos y procesos a cargo de la Dirección de Desarrollo Institucional, así como también la administración del inventario del equipamiento tecnológico institucional.

3.1.7.13 RESPONSABILIDADES DE LA UNIDAD DE PRESUPUESTO.

La elaboración de la proforma presupuestaria anual, en base a las actividades previstas en los sub-proyectos de modernización institucional, a cargo de la Dirección de Desarrollo Institucional.

La elaboración del plan anual de adquisiciones (paquetes de adquisición, en coordinación con los distintos sub-proyectos al interior del Proyecto de Modernización del IESS, a cargo de la Dirección de Desarrollo Institucional).

La solicitud de transferencia de los recursos presupuestarios del IESS al PNUD.

El registro de los recursos presupuestarios transferidos al PNUD, por sub-proyecto y por seguros / unidades de negocio.

La verificación de la emisión de los pagos por contratos y adquisiciones de bienes o servicios del Proyecto de Modernización del IESS, con cargo a las respectivas líneas presupuestarias que maneja el PNUD.

La participación en las evaluaciones del Comité de Adquisiciones del PNUD, conformadas para la compra de bienes o servicios, además del apoyo requerido para los procesos de licitación implementados.

La consolidación mensual de la ejecución presupuestaria, en base al reporte de gastos que emite el PNUD y su homologación con las partidas presupuestarias que maneja el IESS.

La emisión de reportes mensuales de gasto por sub-proyecto y por seguros / unidades de negocio.

La liquidación anual del presupuesto ejecutado por el Proyecto de Modernización del IESS, para el levantamiento de los cargos presupuestarios.

El establecimiento del sistema de inventario de hardware y software del Proyecto de Modernización / Instituto, su consolidación a escala nacional, con el detalle de las características técnicas, proveedor, forma de contratación, garantías y otra información del estado y uso de los productos;

3.1.7.14 COMPETENCIA DE LA UNIDAD DE HISTORIA LABORAL.

La Unidad de Historia Laboral es la encargada de desarrollar la conceptualización de los productos y servicios institucionales, en coordinación con las subdirecciones de planificación y Normatividad y Procesos, así como la administración de la operación de los mismos, en el ámbito nacional.

3.1.7.15 RESPONSABILIDADES DE LA UNIDAD DE HISTORIA LABORAL.

Desarrollar la conceptualización de los productos y servicios institucionales, en coordinación con la Subdirección de Planificación, aplicando criterios de eficacia, eficiencia y altos niveles de calidad.

Supervisión y apoyo al desarrollo de la normatividad y procesos que rigen el desempeño de los productos y servicios institucionales.

La verificación del cumplimiento en lo relativo a la aplicación de la normativa vigente, por parte de las herramientas tecnológicas desarrolladas e implementadas que permiten realizar la prestación de los diferentes servicios institucionales.

La difusión y capacitación en el uso de las herramientas tecnológicas institucionales, en afán de la utilización adecuada y óptima de las mismas.

Realizar la validación de la funcionalidad pertinente y conveniente de todas las herramientas tecnológicas institucionales.

Conformar el sistema de servicio al cliente interno y externo de la institución.

3.2 UNIDAD DE PRODUCCIÓN.

El área de producción es la encargada de velar que el proceso diario se encuentre en correcto funcionamiento tiene a su cargo las siguientes áreas.

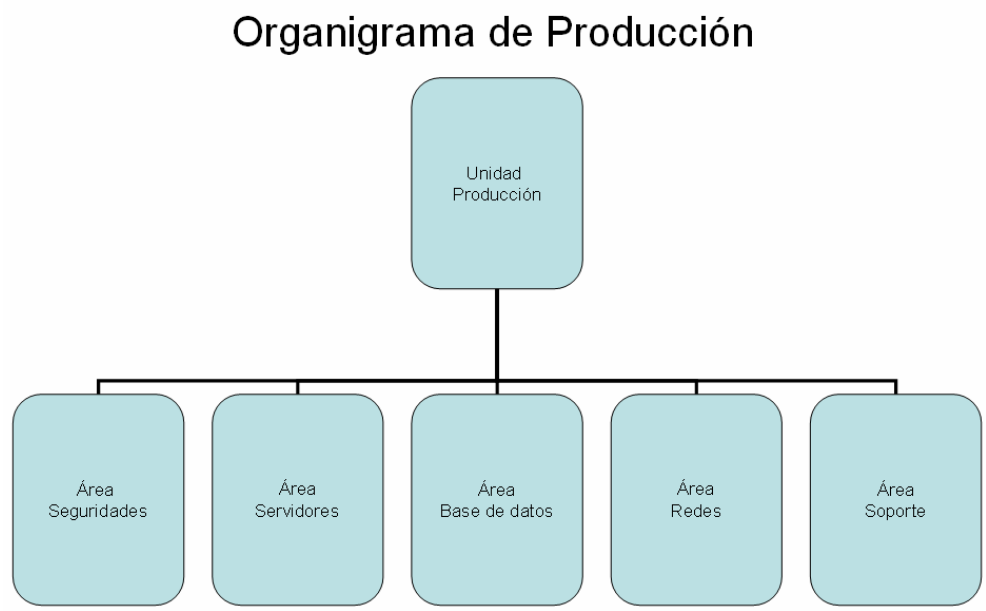


Figura 3.3 ORGANIGRAMA DE PRODUCCIÓN

3.2.1 ÁREA DE SEGURIDADES

El área de seguridades tiene las siguientes responsabilidades.

Administración de usuarios: esta actividad se refiere a la implementación de seguridades en lo que se refiere a dominios de Windows y creación de perfiles de usuario para permisos a la base de datos y a los sistemas operativos. Las tareas a cumplirse en este aspecto son:

- Configurar la seguridad para usuarios Windows
- Configurar los usuarios para Oracle y Sun

Instalación y configuración del Sistema Detector de Intrusos (IDS): consiste en la implementación del sistema que detecta intrusos de Cisco para el Internet y el IDS de ISS para la Intranet. Esto permite detectar los intentos de ataques a la red para prevenir daños a la integridad de la información y tomar acciones para evitarlas.

- Instalación y configuración Cisco IDS
- Reemplazo ISS RealSecure.
- Pruebas de funcionamiento Cisco IDS.
- Instalación y configuración ISS IDS.
- Pruebas de funcionamiento ISS IDS

Un complemento del sistema de seguridad es la configuración del Firewall

Con la finalidad de proteger la red interna de los accesos desde Internet e implementarlo para el acceso desde Internet; esto se lo logra a través de.

- Instalación y configuración del firewall
- Configuración de equipos de seguridad.
- Pruebas de funcionamiento.
- Definición políticas firewall

Instalación de nuevos ambientes de SUN Solaris: todos los servidores se cambiarán a plataforma Sun Solaris por lo que el ingreso de los nuevos servidores

a la red y el cambio de los mismos a servidores web y de aplicaciones para pruebas y producción ocasionará que se rediseñe la administración de usuarios a través de dominios, reconfiguración de los firewalls y los IDS.

- Administración de usuarios.
- Instalación Sistema Detector de Intrusos.
- Reconfiguración Firewall

Pruebas de seguridades: existen actualmente en el mercado herramientas que comprueban la existencia de huecos de seguridad y de vulnerabilidades en los servidores, por ello se analizarán las debilidades de nuestro sistema con el fin de aplicar los cambios respectivos a cada uno de ellos.

Al concluir con todas las actividades descritas anteriormente el sistema de seguridad del Centro de Cómputo del IESS estará a la vanguardia de las necesidades.

3.2.2 ÁREA DE SERVIDORES

Esta área es la que se encarga de la administración y del correcto funcionamiento de los diferentes aplicativos que presta el IESS para su empleados, funcionarios y empleadores, de los servidores, tanto en producción como en el área de desarrollo, dentro de las funciones tenemos las siguientes:

- **Adecuaciones del centro de cómputo:** debido a que se realizarán trabajos físicos en las dos salas, para proteger a los equipos se trasladarán a otro lugar todos los servidores y equipos de comunicación así como las estaciones de trabajo. Previo a este trabajo se debe adecuar el lugar donde se laborará durante la ejecución de los trabajos físicos con puntos de red y tomas de energía eléctrica.
- **Capacitación:** se elaborará un plan de capacitación en lo referente a Solaris y Oracle como requerimiento indispensable para la configuración de los nuevos servidores.
- Administración de usuarios de los servidores

- Configuración de los servidores de aplicaciones.
- Instalación del sistema operativo Windows, Linux y Solaris.
- Reestructuración de los servidores de aplicaciones.
- Migración al Application Server al 10 g
- Actualizaciones de las aplicaciones.
- Cambio en el Bios de cada uno de los servidores.
- Respaldos de backup de datos y S.O de todos los servidores de producción.
- Habilitar servidores para el departamento de desarrollo.
- Dar soporte a los funcionarios, desarrolladores y afiliados.
- Monitorear el rendimiento de los servidores.
- Eliminación de cargas enviados a los servidores de aplicaciones por parte de los usuarios del sistema.
- Tareas de Web Master.
- Configuración de file system en cada uno de los servidores
- Pruebas de rendimiento y desempeño equipos de pruebas
- Configuración de servicios DNS, Correo.
- Administración de rutas en los servidores.
- Administración de tareas de cron en todos los servidores de aplicaciones
- Aplicación de parches y manejo de versiones en los servidores de aplicaciones.

3.2.3 DIAGRAMA DE LOS SERVIDORES

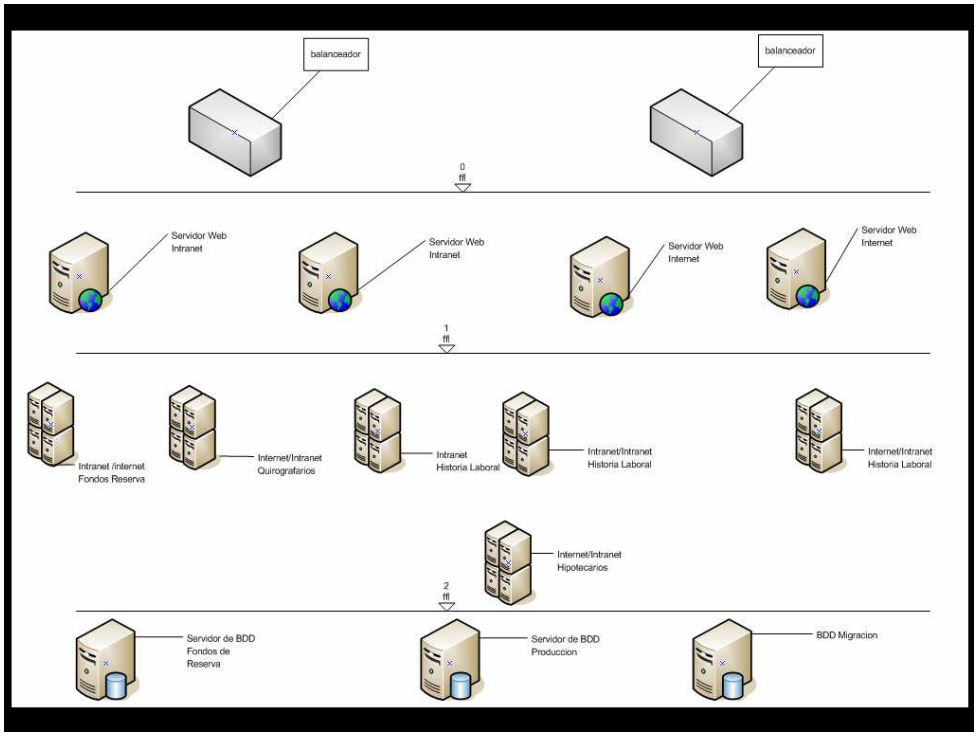


Figura 3.4 DIAGRAMA DE DISTRIBUCIÓN DE LOS SERVIDORES

Como se muestra en la figura 3.4 es el esquema de tres capas que maneja el IESS, en la primera parte contamos con dos balanceadores; el uno se encarga de balancear la carga de Intranet y el otro lo que respecta al Internet.

En segundo plano tenemos 4 servidores en la parte Web distribuidos en la siguiente:
Dos servidores atienden en la parte de intranet.
Dos en la parte de Internet

Para ingresar a estos servidores el usuario tiene que ingresar la dirección http://www.iess.gov.ec

Como tercer plano están los servidores de aplicaciones, estos servidores tienen los diferentes aplicativos que cuenta el IESS, y sirve para atender a funcionarios, afiliados y empleadores.

Como tercera y última capa se encuentran los diferentes servidores de Bases de datos.

De acuerdo a esta distribución se debe tomar muy en cuenta al momento de obtener los diferentes respaldos, puesto que el área más critica y donde se encuentra la información más importantes, está en los servidores de base de datos, luego tenemos los diferentes servidores de aplicaciones, para terminar con los servidores Web. Cabe recalcar que el orden está dado de acuerdo a la información que manejan dichos servidores.

3.2.4 SERVICIOS ON-LINE DEL IESS

El IESS tiene varios servicios en línea, el más importante y se puede decir que es la columna vertebral, es el modulo de Historia Laboral, este módulo es utilizado por funcionaros de la institución, afiliados y empleadores.

El módulo de Historia Laboral se considera el más crítico del resto de módulos ya que a través de este módulo se realizan las recaudaciones que realiza el IESS a los empleadores.

Otro de los módulos que tiene el IESS es el de Fondos de Reserva, que como es de conocimiento público este módulo es utilizado para que los afiliados puedan registrar sus retiros de fondos de reserva, también cuenta con el modulo de prestamos Quirografarios, cuentas bancarias, supervivencia, cada uno de estos módulos son accedidos por los afiliados vía Internet y sirven para brindar varios servicios que tienen la Institución.

3.2.5 DIAGRAMA DE ALMACENAMIENTO DE LOS SERVIDORES

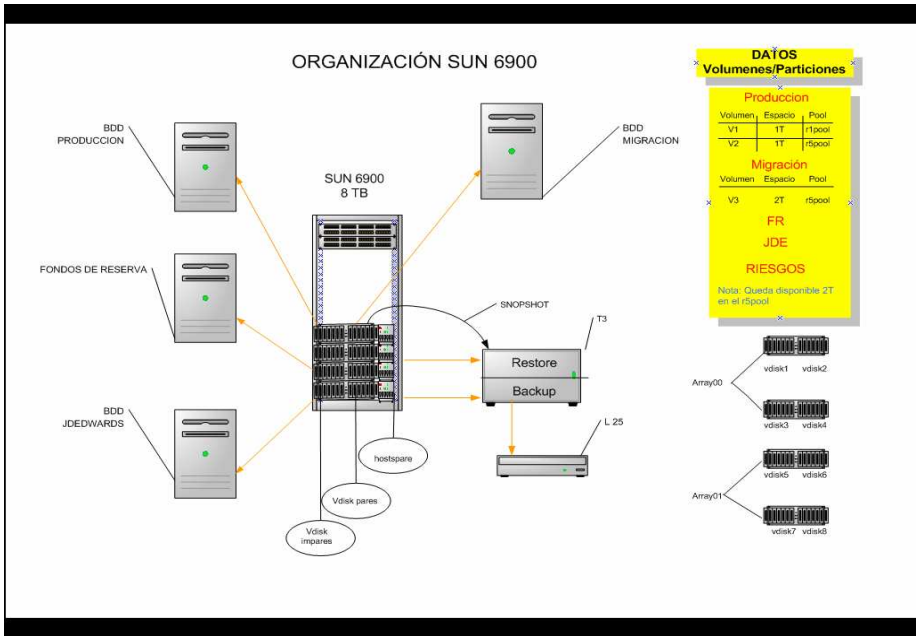


Figura 3.5 DIAGRAMA DE ALMACENAMIENTO DE LOS SERVIDORES

En la Figura 3.5 se muestra cómo se encuentran distribuidos los equipos de acuerdo al almacenamiento, como se puede observar y debido a la gran cantidad de información que maneja el IESS requiere un equipo con la capacidad de 8 Teras, distribuidos a todos los servidores que se encuentran los servidores.

Cabe recalcar y como se muestra la gráfica del equipo de almacenamiento SUN se conecta a nuestro robot, el mismo que se encargará de realizar los respaldos de datos al igual que de la información que se encuentre en cada uno de los discos del equipo SUN.

Este equipo SUN se encuentra estructurado de tal manera que sus discos se encuentran conectados a través de fibra óptica, estos nos sirve para mejorar el I/O entre los discos y el servidor de base de datos.

3.2.6 ÁREA DE REDES

- Administración de la Red LAN.
- Administración de la intranet a nivel nacional.
- Administración de la infraestructura de switchs (vlans) y cableado estructurado.
- Instalación y configuración de las redes LAN con los siguientes servicios de red: DHCP, DNS, File Servers y Controlador de Dominio.
- Administración de la red WAN.
- Monitoreo de los enlaces de comunicaciones a nivel nacional.
- Configuración y administración de equipos de comunicaciones (Inet Servers y Ruteadores).
- Implementación de redes WAN a nivel nacional.
- Generación de proyectos de infraestructura básica para diferentes dependencias del IESS
- Soporte Técnico a usuarios internos de la institución a nivel nacional.

3.2.7 DIAGRAMA DE RED DE IESS

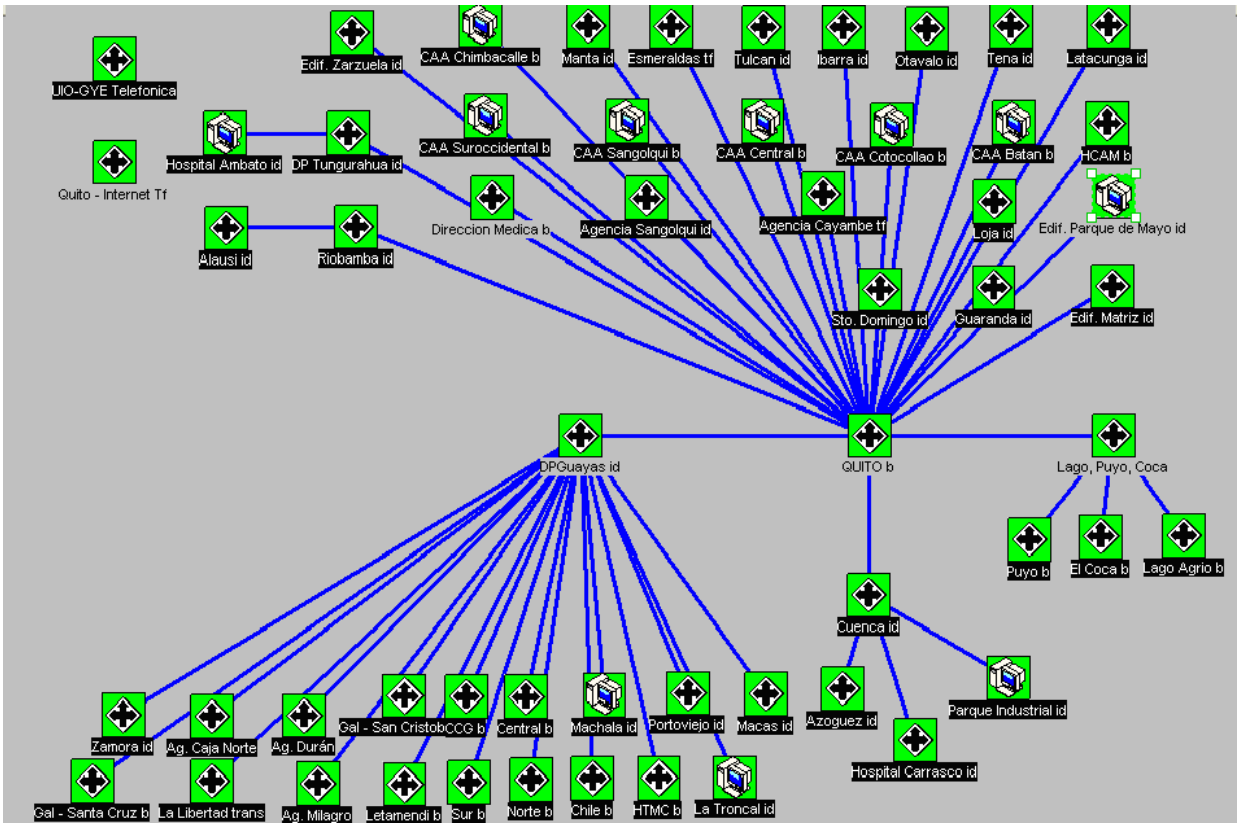


Figura 3.6 ESQUEMA DE LA RED

En la figura 3.6 se muestra cómo se realiza el monitoreo de las redes, en este se puede determinar cuándo una ciudad no se encuentra operando con normalidad, este también nos permite determinar el trafico de los paquetes, la rapidez de entregar y se puede realizar conexiones en los diferentes nodos para determinar que todo se encuentre en perfecto funcionamiento

3.2.8 ÁREA DE BASE DE DATOS

- Soporte técnico en el área de Base de Datos.
- Ejecución y monitoreo de procesos automáticos.
- Control de espacio en los servidores.
- Instalación y configuración de Base de Datos Oracle.

- Administración, Asignación de Recursos, Seguridad de las bases de datos de Producción, Migración, Capacitación, Pruebas, Repositorio y JDE.
- Automatización respaldos de RRHH en estructuras, estadísticas y dmps.
- Procesos de Respaldo y Recuperación de Base de Datos.
- Administración proceso de aplicación de parches sobre las bases de datos.
- Cambios en scripts de ejecución de parches para fondos de reserva.
- Parametrización de tabla para replicación de datos producción a migración.
- Cambios en scripts de ejecución para replicación de datos producción a migración.
- Instalación y configuración de Oracle Client 9i área fondos de reserva.
- Ejecución de scripts de anulación de comprobantes auto cancelado.
- Monitoreo de sesiones de base de datos de producción y fondos de reserva.
- Control y asignación de espacios para datafiles de bases de datos.
- Solución de errores presentados al importar base de datos de RRHH.
- Soporte en el traslado al nuevo centro de cómputo para el IESS.
- Respaldos de archivos de RRHH, producción y migración.

3.2.9 ÁREA DE SOPORTE

El área de soporte tiene las siguientes funciones:

- Instalación y configuración de estaciones de trabajo
- Soporte técnico a usuarios del Proyecto de Modernización del IESS.
- Soporte técnico a Funcionarios del IESS.
- Instalación y configuración de impresoras locales.
- Instalación y configuración de impresoras en red
- Creación y mantenimiento de cuentas de usuario.
- Instalación de Antivirus.
- Revisión y eliminación de Virus Informáticos.
- Soporte técnico vía telefónica a Funcionarios y Afiliados

3.3 CARACTERÍSTICAS DE HARDWARE DE LOS SERVIDORES

Los servidores que cuenta el IESS tienen las siguientes características:

Tabla 3.1 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP FONDOS DE RESERVA.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO01
Numero de procesadores:	4
Velocidad del procesador:	1200 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	16
Tamaño de la memoria:	512MB
Total Memoria:	8G
Disco:	SUN36G
Numero de Disco:	6
Capacidad:	36G

Tabla 3.2 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL INTRANET

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO02
Numero de procesadores:	8
Velocidad del procesador:	1050 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	32
Tamaño de la memoria:	512MB
Total Memoria:	16G
Disco:	SUN36G
Numero de Disco:	2
Capacidad:	36G

Tabla 3.3 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD MIGRACIÓN.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO03
Numero de procesadores:	8

Velocidad del procesador:	900 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	32
Tamaño de la memoria:	512MB
Total Memoria:	16G
Disco:	SUN72G
Numero de Disco:	6
Capacidad:	72G

Tabla 3.4 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD PRODUCCIÓN.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO04
Numero de procesadores:	8
Velocidad del procesador:	750 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	32
Tamaño de la memoria:	512MB
Total Memoria:	16G
Disco:	SUN72G
Numero de Disco:	8
Capacidad:	72G

Tabla 3.5 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL INTERNET.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO05
Numero de procesadores:	16
Velocidad del procesador:	1050 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	32
Tamaño de la memoria:	1024MB
Total Memoria:	32G

Disco:	SUN72G
Numero de Disco:	2
Capacidad:	72G

Tabla 3.6 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD CESANTÍAS.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO06
Numero de procesadores:	4
Velocidad del procesador:	1050 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	16
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN72G
Numero de Disco:	6
Capacidad:	72G

Tabla 3.7 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP CUENTAS BANCARIAS.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO07
Numero de procesadores:	2
Velocidad del procesador:	900 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	8
Tamaño de la memoria:	512MB
Total Memoria:	4G
Disco:	SUN36G
Numero de Disco:	2
Capacidad:	36G

Tabla 3.8 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP FR DESARROLLO.

DESCRIPCION	DETALLE
Nombre del equipo:	PRU01
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G
Numero de Disco:	2
Capacidad:	36G

Tabla 3.9 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL DESARROLLO.

DESCRIPCION	DETALLE
Nombre del equipo:	PRU02
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G
Numero de Disco:	1
Capacidad:	36G

Tabla 3.10 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD DESARROLLO.

DESCRIPCION	DETALLE
Nombre del equipo:	PRU03
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM

Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G
Numero de Disco:	1
Capacidad:	36G

Tabla 3.11 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN CORREO.

DESCRIPCION	**DETALLE**
Nombre del equipo:	CORREO10
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G
Numero de Disco:	4
EstorEdge	Tiene 3 discos de 36G
Capacidad:	36G

Tabla 3.12 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP QAD.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRU04
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G

Numero de Disco:	2
Capacidad:	36G

Tabla 3.13 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL CAPACITACIÓN.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRU05
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G
Numero de Disco:	2
Capacidad:	36G

Tabla 3.14 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD QAD.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO16
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	SUN36G y SUN18G
Numero de Disco:	4
Capacidad:	2 de 36G y 2 de 18 G

Tabla 3.15 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN BDD QAP.

DESCRIPCION	**DETALLE**

Nombre del equipo:	PRO17
Numero de procesadores:	1
Velocidad del procesador:	548 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	2
Tamaño de la memoria:	512MB
Total Memoria:	1G
Disco:	3 SUN36G y 2 SEAGATE
Arreglo de Discos	RAID 0
Numero de Disco:	5
EstorEdge	Tiene 3 discos de 36G
Capacidad:	4 de 36G y 1 de 140 G

Tabla 3.16 CARACTERÍSTICAS DE HARDWARE SERVIDOR SUN APP HL QAP

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO08
Numero de procesadores:	2
Velocidad del procesador:	900 MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	8
Tamaño de la memoria:	512MB
Total Memoria:	4G
Disco:	SUN36G
Numero de Disco:	2
Capacidad:	36G

Tabla 3.17 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM APP QUIROGRAFARIOS.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO09
Numero de procesadores:	8
Velocidad del procesador:	2.00GHz

Arquitectura de la memoria:	DIMM
Total Memoria:	3G
Configuración Disco:	RAID 0
Numero de Disco:	2
Capacidad:	36G

Tabla 3.18 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM BDD FONDOS RESERVA.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PROBDD09
Numero de procesadores:	8
Velocidad del procesador:	2.00GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	14G
Configuración Disco:	RAID 0
Numero de Disco:	4
Capacidad:	120G

Tabla 3.19 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM DNS.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRODNS10
Numero de procesadores:	8
Velocidad del procesador:	997.418 MHz
Arquitectura de la memoria:	DIMM
Total Memoria:	512MB
Numero de Disco:	6
Capacidad:	18G

Tabla 3.20 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM REPORT SERVER.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PROREPORT11

Numero de procesadores:	4
Velocidad del procesador:	1795MHz
Arquitectura de la memoria:	DIMM
Numero de memorias:	4
Tamaño de la memoria:	1G
Total Memoria:	4G
Disco:	SCOSI
Numero de Disco:	1
Capacidad:	36G

Tabla 3.21 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM APP PENSIONES.

DESCRIPCION	**DETALLE**
Nombre del equipo:	PRO12
Numero de procesadores:	4
Velocidad del procesador:	1.80GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	5G
Numero de Disco:	2
Capacidad:	36G

Tabla 3.22 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTRANET.

DESCRIPCION	**DETALLE**
Nombre del equipo:	WEB02
Numero de procesadores:	4
Velocidad del procesador:	1.80GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	5G
Configuración Disco:	RAID 0
Numero de Disco:	2
Capacidad:	36G

Tabla 3.23 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTRANET.

DESCRIPCION	DETALLE
Nombre del equipo:	WEB01
Numero de procesadores:	4
Velocidad del procesador:	1.80GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	5G
Configuración Disco:	RAID 0
Numero de Disco:	2
Capacidad:	36G

Tabla 3.24 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTERNET.

DESCRIPCION	DETALLE
Nombre del equipo:	WEB03
Numero de procesadores:	8
Velocidad del procesador:	2.00GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	18G
Configuración Disco:	RAID 0
Numero de Disco:	4
Capacidad:	2 de 146G y 2 de 36G

Tabla 3.25 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM WEB INTERNET.

DESCRIPCION	DETALLE
Nombre del equipo:	WEB04
Numero de procesadores:	8
Velocidad del procesador:	2.00GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	14G
Configuración Disco:	RAID 0
Numero de Disco:	2

Capacidad:	36G

Tabla 3.26 CARACTERÍSTICAS DE HARDWARE SERVIDOR IBM PRUEBAS.

DESCRIPCION	DETALLE
Nombre del equipo:	PRUEBA35
Numero de procesadores:	2
Velocidad del procesador:	2.00GHz
Arquitectura de la memoria:	DIMM
Total Memoria:	1G
Numero de Disco:	2
Capacidad:	18G

3.4 EVALUACIÓN Y TRATAMIENTOS DE RIESGO DEL IESS

El IESS debe mantener un control del riesgo, puesto que se encuentra siempre expuesto a amenazas y cada día tenemos nuevos ataques de personas maliciosas como Hacker, Phreaker, Pirata y Cracker.

Dada las necesidades de seguridad el IESS debe tener en claro cuáles son sus áreas de mayor crisis para poder tomar las decisiones necesarias para seleccionar los controles que permitan disminuir los riesgos y sobre todo tener un buen plan de contingencia.

Un sistema de gestión de seguridad de información tiene tres componentes para alcanzar confidencialidad y aseguramiento de la información:

- **Confidencialidad:** Protección de la información sensitiva de intercepciones no autorizadas.
- **Integridad:** La propiedad de salvaguardar la exactitud y integridad de los activos.

- **Disponibilidad:** La propiedad de estar disponible y utilizable cuando la requiera una entidad autorizada si se desea ser utilizado para la certificación.

3.4.1 ANÁLISIS DEL RIESGO Y LOS REQUERIMIENTOS DEL ISO 27001:2005

La ISO 27001:2005 requiere que toda organización que plantee un sistema de gestión de seguridad de información (SGSI), se debe primero definir el alcance del estándar en la empresa y en base a ese alcance se deben definir todos los activos de información.

Luego se debe realizar un análisis de riesgo para definir de todos los activos cuáles se les puede considerar de mayor riesgo, luego se debe conversar con los respectivos encargados de cada uno de los activos para definir qué controles se aplicarán para mitigar dichos riesgos, El ISO 27001:2005 es un sistema dinámico que obliga a la gerencia a estar constantemente revisando y definiendo controles, sus amenazas vulnerabilidad e iniciar acciones preventivas y correctivas cuando sea necesario.

3.4.2 PROCESO DE EVOLUCIÓN DEL RIESGO

En la figura 9 se muestra como es el proceso de evaluación del riesgo toda organización tiene que pasar cada una de las fases para poder evaluar y determinar los riesgos, mas adelante se detallara cada unos de los niveles.

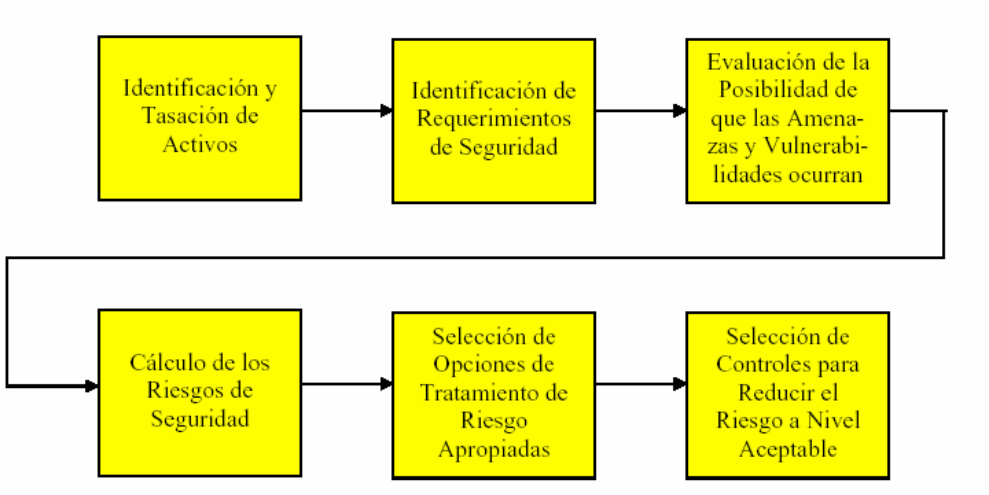


Figura 3.7 PROCESO DE EVALUACIÓN DEL RIESGO

3.4.2.1 Identificación y tasación de activos

Primero definamos lo que es un activo; para el IESS un activo es algo que tiene valor o utilidad, cada activo necesita ser protegido ya que ellos nos garantizan la continuidad de la organización.

Cada uno de los activos deben estar identificados apropiadamente y valorado; la ISO clasifica a los activos de la siguiente manera:

- **Activos de Información:** Son las base de datos y archivos de datos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimiento de operativos de apoyo, planes de continuidad.
- **Documentos Impresos:** Documentos impresos, contratos, lineamientos, documentos de la institución, documentos que contiene resultados importantes de negocios.
- **Activos de Software:** Software de aplicación, software de sistemas, herramientas de desarrollo.
- **Activos Físicos:** Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos.
- **Personas:** Personal, clientes, suscriptores.
- Imagen y Reputación de la Compañía.
- **Servicios:** Servicios de computación y comunicaciones, otros servicios técnicos.

La tasación de activos, basada en las necesidades del negocio de toda organización es un factor importante en la evaluación del riesgo. Para poder encontrar la protección apropiada para los activos es necesario evaluar su valor en términos e importancia para la institución “Para poder tasar los valores de los activos y poder relacionarlos apropiadamente, una escala de valores para activos debe ser aplicada.” (Alberts, Dorofee, 2003).

3.4.2.2 Identificación de requerimientos de seguridad:

Los requerimientos de seguridad se derivan de tres fuentes esenciales:

- El conjunto único de amenazas y vulnerabilidad que pudieran ocasionar pérdidas significativas en la institución si ocurrieran.
- Los requerimientos contractuales que deben satisfacerse por el IESS.
- El conjunto único de objetivos, principios y requerimiento para el procesamiento de la información que el IESS debe desarrollar para apoyar las operaciones de negocios y sus procesos.

Una vez que se identifiquen cada uno de estos requerimientos en necesario y recomendable formularlos en términos de requerimientos de confidencialidad, integridad y disponibilidad para el IESS.

Con ello se lograra determinar cada una de las necesidades que requiere el IESS para poder prevenir y controlar los posibles ataques que se puedan dar, y sobre todo al tener claro las necesidades y requerimientos se podrá aplicar los controles que satisfagan dichos requerimientos.

3.4.2.3 Identificación de amenazas y vulnerabilidades

Como se explicó en temas anteriores lo mas importante para toda organización son sus activos, y es por ello que se encuentran siempre sujetos a amenazas. Una amenaza es capaz de causar daño a toda organización, pues ocasiona incidentes no deseados, el cual puede ocasionar daño al sistema y sobre todo a los activos. El daño se puede dar por varias vías ya sea directamente, es decir dañar los datos, o indirectamente pude darse daños a la infraestructura.

Las amenazas pueden originarse de fuentes accidentales o de manera deliberada, para que una amenaza pueda dañar un activo debería explotar la vulnerabilidad del sistema, aplicativo o servicio.

Las vulnerabilidades son debilidades asociadas con los activos organizacionales. Las debilidades pueden ser explotadas por las amenazas, causando incidentes no deseados que ocasionarían pérdidas, daño o deterioro a los activos. La vulnerabilidad como tal, no causa daño, es simplemente una condición o

conjuntos de condiciones que pueden permitir que una amenaza afecte a un activo.

Una evaluación de la posibilidad de ocurrencia de la vulnerabilidad y las amenazas, deben ser efectuadas en esta fase.

3.4.2.4 Cálculos de los riesgos de seguridad

El objetivo de la evaluación del riesgo es la de identificar y evaluar el riesgo para poder determinar soluciones. Los riegos son calculados de una combinación de valores de activos y niveles de requerimiento de seguridad.

La evaluación de riesgos embuelve la sistemática considerando los siguientes aspectos:

- **Consecuencia:** El daño de la empresa o institución como resultado de un incumplimiento de seguridad de información considerando las potenciales consecuencias de pérdida o fallos de confidencialidad, integridad y disponibilidad de información.
- **Probabilidad:** La real posibilidad de que tal incumplimiento ocurra a la luz del reinado de amenazas, vulnerabilidad y controles.

Es importante considerar que no existe una manera buena o mala de calcular los riesgos, es por ello que cada institución tiene su propia forma de evaluación de los riesgos considerando cada uno de sus activos, por lo tanto no se puede regir a una norma o ley para poder calcular los riesgos, puesto que no todas las organizaciones cuentas con los mismos activos.

3.4.2.5 Selección de opciones apropiadas de tratamiento del riesgo

Cuando los riesgos han sido identificados y evaluados, lo próximo que se debe hacer es determinar la acción que se debe seguir para poder determinar como serán tratados cada uno de los riesgos. La decisión debe ser tomada basada en los activos involucrados y su impacto en la Institución.

Otro aspecto importante a considerar es el nivel del riesgo aceptado que ha sido identificado, siguiendo la selección de la metodología apropiada de evaluación.

El estándar ISO 27001:2005 requiere que el tratamiento del riesgo siga cuatro posibles acciones:

- Aplicación de controles apropiados para reducir los riesgos. Los controles tienen que ser identificados. Si los controles no pueden ser hallados, la firma puede crearlos y documentarlos.
- Aceptar objetivamente los riesgos partiendo del supuesto que satisfacen las políticas de la institución y sus criterios para la aceptación del riesgo.
- Evitar los riesgos.
- Transferir los riesgos asociados a otra parte.

Por cada uno de los riesgos se debe evaluar estas opciones para identificar la más adecuada.

Los resultados de esta actividad deben de ser documentados y luego la institución debe documentar su “plan de tratamiento del riesgo”.

Hay dos pociones en la identificación y evaluación del riesgo que requieren mayor explicación. Las alternativas son:

- Evitar el riesgo.
- Transferir el riesgo.

Evitar el Riesgo: Describe cualquier opción donde los activos son transferidos de las áreas riesgosas. Cuando se evalúan la posibilidad de evitar el riesgo, esto debe sopesarse entre las necesidades de la institución y las monetarias.

Transferir el Riesgo: Esta opción puede ser la mejor si no se puede reducir los niveles el riesgo. Existen muchas alternativas a considerar en relación a la estrategia de transferencia del riesgo. La transferencia del riesgo podría

alcanzarse tomándose una póliza de seguridad. Otra posibilidad podría ser la utilización e servicios de “outsourcing” para que se manejen activos y procesos críticos. La responsabilidad por los servicios tercerizados siempre recae en la Institución.

3.4.2.6 Selección de controles para reducir los riesgos a un nivel aceptable

“Para reducir el riesgo evaluado, dentro del alcance del Sistema de Gestión de Seguridad Informática, (SGSI) considerados los controles de seguridad apropiados y justificados, deben ser identificados y seleccionados. Estos controles deben ser seleccionados de ISO 27001:2005. La institución también puede utilizar el ISO 17799:2005 como guía para la implementación de los controles, pero deben ser escogidos del ISO 27001:2005.” [6]

La selección de los controles debe ser sustentada por los resultados de la evaluación del riesgo. Las vulnerabilidad con las amenazas asociadas indican dónde la protección pudiera ser requerida y que forma debe tener. Especialmente para propósitos de certificación, las relaciones con la evaluación del riesgo deben ser documentadas para justificar la selección de los controles.

Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados, incluyendo:

- Uso de controles.
- Transferencia de usuarios.
- Ayuda otorgada a los usuarios para desempeñar su función.
- Relativa fuerza de los controles.
- Tipos de funciones desempeñadas.

En términos generales, un control podrá satisfacer más de una de estas funciones y lo más que pueda satisfacer mejor.

3.4.3 RIESGO RESIDUAL

[6] http://www.unimexico.org/modules.php?name=News&file=article&sid=1586

Después de identificar los controles adecuados para reducir un riesgo específico al nivel considerado aceptable, debe evaluarse cuándo los controles, si se implementan, reducirán los riesgos; es el denominado “riesgo residual”.

El riesgo residual usualmente es difícil evaluarlo. Por los menos una estimación de cuándo los controles reducen el nivel de los requerimientos de los valores asociados de seguridad debería ser identificada, para asegurar que la suficiente protección es alcanzada.

Si el riesgo residual es inaceptable, una decisión comercial debe ser tomada sobre cómo se irá a manejar la situación. Una opción es la selección más controlada para finalmente reducir los riesgos a un nivel aceptable. Es una buena práctica no tolerar riesgos inaceptables, pero muchas veces no es posible o financieramente factible reducir todos los riesgos al nivel aceptable.

Después de implantar los controles seleccionados, es importante estar claros que siempre habrán riesgos existentes. Esto sucede por que los sistemas de información en una organización nunca podrán estar absolutamente seguros. Esta es la razón por la cual es necesario revisar la implementación, los resultados de los controles, para finalmente evaluar qué tan bien los controles implementados están operando.

3.4.4 VALORACIÓN DE BIENES O ACTIVOS

El valor de un bien se puede determinar a partir de:

- El costo inicial y operativo asumido al comprar, licenciar, desarrollar o soportar un activo
- El valor del activo para las labores de producción, investigación y desarrollo.
- El valor del activo establecido por el mercado externo.
- El valor estimado de la propiedad intelectual

3.4.5 CÁLCULO DEL RIESGO EN LA DDI

El cálculo del riesgo es importante para toda organización puesto que esto nos permite determinar como esta nuestros activos de acuerdo a las diferentes amenazas que se encuentren, también contando con el riego se puede determinar el tipo de seguridad que tendrá cada activo.

3.4.5.1 Riesgo de activos

El cálculo del riesgo es fundamental puesto que este nos permitirá calcular la seguridad que tiene cada uno de los activos en la Dirección de Desarrollo Institucional.

El riesgo, como se lo conoce está dado por el cálculo del factor de exposición (porcentaje de pérdida del activo en la organización) por la vulnerabilidad (probabilidad que ocurra un desastre)

3.4.5.2 Cuadro del cálculo del riesgo en la DDI

El cálculo del riesgo es fundamental, puesto que este nos permitirá calcular la seguridad que tiene cada uno de los activos en la Dirección de Desarrollo Institucional.

El riesgo como se lo conoce, está dado por el cálculo del factor de exposición (porcentaje de pérdida del activo en la organización) por la vulnerabilidad (probabilidad que ocurra un desastre), aplicando la siguiente relación:

R= vulnerabilidad x factor de exposición

Antes de realizar el cálculo del riesgo se debe determinar el tipo de vulnerabilidad que tiene cada uno de los activos, cabe recalcar que cada organización debe clasificar la vulnerabilidad de acuerdo a su empresa y considerando cada uno de sus activos.

El siguiente cuadro nos explica cómo está clasificada la vulnerabilidad.

Grado de vulnerabilidad	Tipo de vulnerabilidad
0.1	Vulnerabilidad baja
0.2	Vulnerabilidad baja
0.3	Vulnerabilidad baja media
0.4	Vulnerabilidad baja media
0.5	Vulnerabilidad media
0.6	Vulnerabilidad media
0.7	Vulnerabilidad media alta
0.8	Vulnerabilidad alta
0.9	Vulnerabilidad alta critica
1	Vulnerabilidad crítica

Tabla 3.27 ESCALA DE VULNERABILIDAD

Para realizar la clasificación de los activos, se ha considerado aquellos que son de mayor importancia para la Dirección de Desarrollo Institucional en este momento, pero no se descarta que a medida que se modifique las políticas de seguridad se siga aumentando mas activos.

Activo	Vulnerabilidad	Exposición (%)	Riesgo
Servidor de Aplicación de Desarrollo SUN	0,5	0,3	0,15
Clave de usuario	0,9	0,9	0,81
Servidor de Base de datos de Desarrollo SUN	0,5	0,1	0,05
Servidor de aplicación de desarrollo IBM	0,7	0,3	0,21
Servidor de base de datos de desarrollo IBM	0,8	0,5	0,40
Impresora	0,5	0,5	0,25

Manuales	0,6	0,6	0,36
Procedimientos de Operación	0,5	0,4	0,20
Documentos Impresos	0,4	0,6	0,24
Software Aplicación	0,7	0,3	0,21
Herramientas de Desarrollo	0,6	0,2	0,12
Router Central	0,6	0,2	0,12
Router Agencias	0,8	0,7	0,56
Servidor QAP SUN	0,8	0,7	0,56
Servidor QAD SUN	0,8	0,7	0,56
Switch capa 2	0,6	0,5	0,30
Switch capa 3	0,6	0,2	0,12
Cinta de Respaldo	0,5	0,8	0,40
Servidor de Base Datos SUN	0,7	1	0,70
Servidor de Aplicación SUN	0,8	1	0,80
Servidor de Aplicación IBM	0,7	1	0,70
Servidor de Correo SUN	0,7	1	0,70
Servidor Web	0,5	1	0,50

Tabla 3.28 CALCULO DEL RIESGO

3.4.5.3 Cuadro del cálculo de la seguridad en la ddi

Luego de haber calculado el riesgo se procede a determinar los valores de la seguridad de cada uno de los activos, esto nos servirá para poder definir las diferentes políticas que nos ayudara a minimizar los riesgos frente a las amenazas.

La seguridad está dada por la siguiente formula:

Seguridad = 1 - Riesgo

Activo	Valor Unitario	Riesgo	Seguridad
Servidor de Aplicación de Desarrollo SUN	1	0,15	0,85
Clave de usuario	1	0,81	0,19
Servidor de Base de datos de Desarrollo SUN	1	0,05	0,95
Servidor de aplicación de desarrollo IBM	1	0,21	0,79
Servidor de base de datos de desarrollo IBM	1	0,40	0,60
Impresora	1	0,25	0,75
Manuales	1	0,36	0,64
Procedimientos de Operación	1	0,20	0,80
Documentos Impresos	1	0,24	0,76
Software Aplicación	1	0,21	0,79
Herramientas de Desarrollo	1	0,12	0,88
Router Central	1	0,12	0,88
Router Agencias	1	0,56	0,44
Servidor QAP SUN	1	0,56	0,44
Servidor QAD SUN	1	0,56	0,44
Switch capa 2	1	0,30	0,70
Switch capa 3	1	0,12	0,88
Cinta de Respaldo	1	0,40	0,60
Servidor de Base Datos SUN	1	0,70	0,30
Servidor de Aplicación SUN	1	0,80	0,20
Servidor de Aplicación IBM	1	0,70	0,30
Servidor de Correo SUN	1	0,70	0,30
Servidor Web	1	0,50	0,50

Tabla 3.29 CÁLCULO DE SEGURIDAD

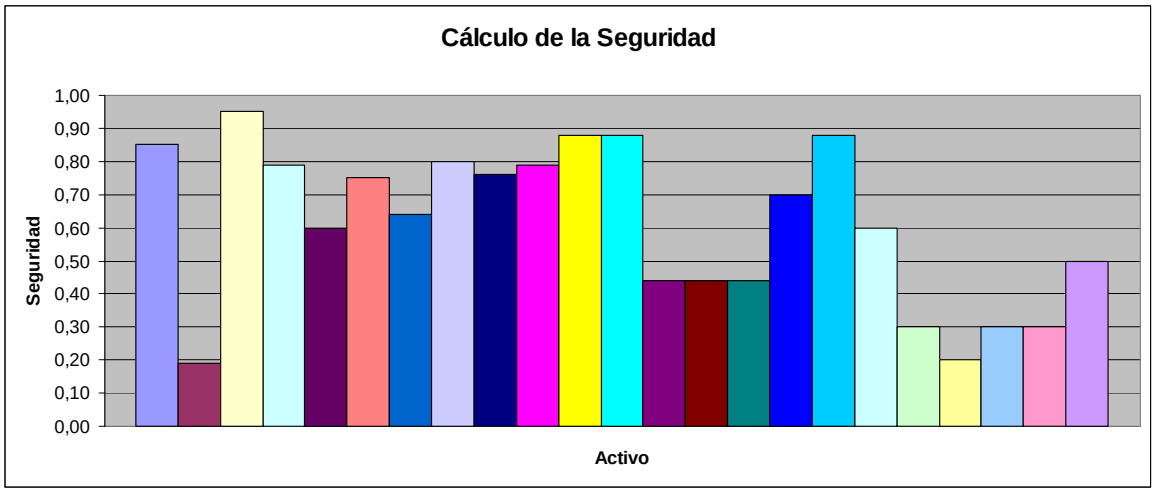


Figura 3.8 GRAFICO DE LA SEGURIDAD

3.4.5.4 Análisis del cálculo de la seguridad

De los cálculos anteriores se puede deducir que los servidores de base de datos, servidor de aplicación de producción y de desarrollo tienen un menor grado de seguridad, es por ello que al momento de generar las políticas se debe de tener mucho cuidado con estos activos.

El mismo trato se debe de tener con el Software Aplicación, claves de usuarios y las herramientas de desarrollo, para evitar futuros desmanes con estos activos.

Con respecto a los demás activos también se debe realizar políticas de seguridad de acuerdo a los rangos obtenidos en los cálculos anteriores.

CAPÍTULO IV

4. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD PARA DDI

4.1 ANÁLISIS Y DEFINICIÓN DE POLÍTICAS INFORMÁTICA EN LA DDI.

Según capítulos anteriores, la DDI tiene como finalidad principal modernizar al IESS, motivo por el cual tiene a su cargo toda la infraestructura tecnológica que sirve para lograr dicho objetivo. Este departamento es el más crítico, respecto a los demás departamentos que tiene a su cargo el IESS, por esta razón se aplicarán políticas de seguridad a esta Dirección. Mediante el mismo esquema, se pueden aplicar las mismas políticas a las otras Direcciones que maneja el IESS,

Se debe considerar que dentro de la Dirección de Desarrollo tenemos el departamento o unidad de producción, en la cual se encuentra el área de base de datos, y el área de servidores, estas áreas son las encargadas de realizar los respaldos, tanto a nivel de datos como a nivel de configuraciones y de sistema operativo. Es por ello que se tendrá un análisis especial para el tratamiento de las políticas que manejarán para poder cumplir sus objetivos.

4.1.1 ANÁLISIS DEL TRATAMIENTO DE POLÍTICAS EN LA DDI

Antes de definir los controles que se aplicarán para poder determinar las políticas necesarias, primero se realizará un análisis para determinar cuáles son las áreas de mayor vulnerabilidad.

Dentro del organigrama de la Unidad de Producción se encuentra el área de soporte, una de las funciones de esta área es dotar de recursos informáticos, tanto a funcionarios como a consultores del IESS, dentro de estos recursos se encuentran los computadores, los mismos que son entregados a sus respectivos usuarios con el software que requieren para poder realizar su trabajo. Esto se lo

realiza de esta manera, puesto que cada usuario tiene su clave dentro de un dominio.

De la investigación que se realizó a esta área se notó que al momento de asignar la clave del usuario en el dominio se lo realiza de una manera fácil de descifrar por otro usuario, esto ocasiona que otra persona ingrese a otro computador que no sea el suyo, es por ello que se tomará atención a este inconveniente al momento de definir las políticas.

El área de seguridades también es una de las más críticas, puesto que tiene la función primordial de impedir que intrusos puedan ingresar a la red del IESS, es por ello que se debe tener mucho cuidado al definir políticas en el firewall,

Dentro de otras responsabilidades que cuenta el área de seguridades, es la de encargarse de conceder permisos de acceso a los usuarios a los servidores que se encuentran en producción, es por ello que se debe tener mucho cuidado al momento se asignar los permisos y sobre todo definir bien la necesidad que tiene el usuario para acceder a los servidores.

Para concluir tenemos el área de servidores, la misma que tiene la función principal de mantener los servicios que presta la Institución a sus afiliados en perfecto funcionamiento, para ello tienen que cubrir ciertos aspectos como:

- Tener el espacio disponible para las diferentes aplicaciones.
- Tener los respaldos al día de los correos.
- Tener los respaldos de datos en perfecto estado y sobre todo confiables.
- Contar con los respaldos de Sistema Operativo de cada uno de los servidores tanto de producción como de desarrollo.
- Disponer de los respaldos de configuración de cada unos de los aplicativos en caso de una emergencia.

El área de servidores cuenta con más funciones, pero se detallan aquellas que son de mayor riesgo e importancia para la institución.

De lo que se ha podido observar, esta área no cuenta con políticas de backups y la manera que se ha estado procediendo puede ser no muy indicada, puesto que cada persona que realiza los respaldos tiene su propio criterio al momento de obtener los respaldos. Es por ello y debido a la importancia de los respaldos, se tomará un mayor interés en definir políticas de backups, como de restauración.

4.1.2 DEFINICIÓN DE POLÍTICAS PARA LA DDI

Una vez que los requisitos de seguridad han sido identificados, se elegirán e implantarán los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Hay muchas formas distintas de gestionar los riesgos y este documento proporciona ejemplos de enfoques habituales. Sin embargo hay que reconocer que ciertos controles no son aplicables para todos los sistemas o entornos de información y pueden no ser de aplicación en todas las organizaciones.

Los controles deberían elegirse por su costo de implantación en relación con los riesgos a reducir y con las posibles pérdidas si se materializa la ruptura de seguridad. También es conveniente tener en cuenta factores no económicos como la pérdida de reputación.

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.
Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

- La protección de los datos de carácter personal y la intimidad de las personas.
- La salvaguarda de los registros de la organización.
- Los derechos de la propiedad intelectual.

- Los controles que se consideran comunes para la mejor práctica habitual para conseguir la seguridad de la información comprenden:
- La documentación de la política de seguridad de la información.
- La asignación de responsabilidades de seguridad.
- La formación y capacitación para la seguridad de la información.
- El registro de las incidencias de seguridad.
- La gestión de la continuidad del negocio.

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos.

Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier otro control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

4.1.2.1 Políticas de seguridad de los activos

- Todos los activos de información del IESS tienen un propietario.
- Cada propietario clasificará la información dentro de uno de los niveles sensitivos (que se mencionan abajo) que dependen de obligaciones legales, costos, políticas institucionales y necesidades del negocio. El propietario es responsable por la protección de esta información.
- El propietario definirá cuáles usuarios pueden acceder a sus datos.
- El propietario es responsable de sus datos.
- La seguridad de los mismos tiene que estar de acuerdo al nivel de sensitividad.

4.1.2.2 Clasificación de la información

El sistema de clasificación de la información considera clasificarla en cuatro niveles:

- Información Pública.
- Información Interna.

- Información Confidencial.
- Información Secreta.

El más bajo (Pública) es el menos sensitivo y el más alto (Secreta) es para los procesos o datos más importantes. Cada nivel es un súper conjunto del nivel previo.

Por ejemplo, si un sistema está clasificado como clase Confidencial, entonces el sistema debe seguir las directivas de las clases Pública, Interna y Confidencial.

Si un sistema contiene datos de más de una clase sensitiva, debe ser clasificado de acuerdo a la necesidad de los datos más confidenciales en el sistema.

4.1.2.3 Políticas de seguridad del personal

4.1.2.3.1 Ética

No está permitido a los usuarios:

- Compartir cuentas o passwords con amigos o familiares,
- Ejecutar programas de chequeo de passwords en el archivo de passwords del sistema,
- Ejecutar programas husmeadores (sniffers) de red,
- Romper seguridades y accesar otras cuentas,
- Interrumpir el servicio,
- Abusar de los recursos del sistema,
- Hacer mal uso del correo electrónico,
- Examinar los archivos de otros usuarios a no ser que le sea permitido por parte del propietario del archivo,
- Descargar archivos binarios desde el PC,
- Copiar software no licenciado o permitir a otros usuarios copiar software no licenciado.

4.1.2.4 Políticas de passwords

La identidad de los usuarios sobre el sistema está dada por la combinación del nombre de usuario y del password.

Los passwords deben cumplir los siguientes requerimientos:

- Tener una longitud de 8 caracteres.
- Tener al menos un carácter numérico, un carácter alfabético y un carácter especial.
- Puede ser una combinación de caracteres numéricos, alfabéticos y caracteres especiales como:"_&*.".
- No debe ser fácil de recordar. Por ejemplo, no debe ser igual al nombre del usuario.
- Debe ser fácil de digitar rápidamente, para que sea difícil de mirar por un observador.
- Deben ser validados por una rutina de verificación. La rutina de verificación debe validar que el password cumpla con los requerimientos mencionados.

En la definición de los passwords evitar el uso de:

- Nombres como: esposa, padre, canción, amigo, mes, día, pueblo, mascota
- Palabras del diccionario común.
- Una serie de letras o números idénticos.
- Alguno de los casos anteriores en inverso o con un número antes o después.
- Secuencia de palabras obvias, como: “unodos”.
- Los dos últimos passwords contenidos en el historial.

Para la definición de passwords se sugiere:

- Escoger una línea de una canción, poema o cualquier párrafo y usar solo las primeras letras de un grupo de palabras.
- Juntar pequeñas palabras con un carácter de subrayado (“_”).
- Inventarse un acrónimo (siglas).

Para asegurar la privacidad de los passwords, tomar en cuenta lo siguiente:

- No escribirlo en un lugar visible, o revelarlo por e-mail.
- No de su password a otra persona.

- No compartir el password del administrador.
- Informarle a los usuarios en detalle del éxito o el peligro de que su password sea revelado. Un usuario bien educado es la mejor manera de asegurar buenas opciones de passwords.
- El password, de acuerdo a su nivel de sensitividad está clasificado como información secreta.
- Los passwords deben ser almacenados en una forma encriptada. La encriptación debe ser sólida, que resista el forcejeo de la desencripción. Usar un algoritmo de encripción como DES3.
- El password encriptado no debe estar embebido dentro del software tanto cuanto sea posible.
- El sistema debe chequear el contenido del password de acuerdo a las reglas definidas previamente, antes de aceptar el password.
- Solamente el usuario puede cambiar su password.
- Proveer una generación automática de un password por defecto cuando el usuario ingresa por primera vez y asegurar que sea entregado a su propietario.
- Proveer un proceso para que el usuario pueda cambiar su password en intervalos regulares. Este proceso debe considerar un nivel adicional de autenticación del usuario.
- Proveer un proceso que permita generar un nuevo password al usuario en caso de olvidos de su password, de modo similar a cuando ingresa por primera vez.

En el tiempo de vida de los passwords considerar:

- El tiempo máximo de vigencia para los passwords es de 1 año. El usuario debe tener un período de gracia de 5 días de tal forma que en este lapso de tiempo el usuario pueda cambiar su password. Si no lo hace, entonces su cuenta expirará.

4.1.2.5 Políticas generales de software

- El software de dominio público se evitará en los sistemas de información clasificada como confidencial. Sin embargo, cuando sea necesario, sólo

será permitido luego de que el software este en uso por al menos un año en sistemas comparables en otras (bien conocidas y confiables) compañías y el software ha sido rigurosamente probado en un ambiente protegido.

- El software de dominio público puede usarse en los sistemas de información clasificada como pública o interna, si el administrador del sistema responsable por la instalación está convencido de la integridad del autor o de las fuentes.
- El software no licenciado no debe ser usado.
- Los programas de juegos no son permitidos en las estaciones de trabajo de los usuarios.

4.1.2.6 Redes

Información confidencial:

- Los datos confidenciales transmitidos sobre redes públicas deben ser encriptados.

4.1.2.6.1 Conexión a redes:

- Un usuario no puede conectar una máquina a cualquier red excepto la LAN local.
- El acceso a redes externas (públicas y privadas) debe hacerse a través de un firewall. Todos los firewalls deberán ser instalados y mantenidos por el área de seguridad institucional.

4.1.2.6.2 Módems:

- Los usuarios no deben tener módems en sus máquinas.
- El acceso Dial-in a la LAN institucional es permitido sólo para ciertos usuarios. Todos los accesos Dial-in deberán hacerse vía servidores seguros con mecanismos de password de una vez.

4.1.2.7 Correo electrónico

- Los usuarios deben estar al tanto de que los sistemas de correo electrónico convencionales a menudo no garantizan privacidad. En muchos sistemas el administrador del sistema puede leer todos los correos electrónicos.

- La información clasificada como interna puede enviarse dentro de la compañía sin encriptación. La información clasificada como confidencial debe ser encriptada. La información clasificada como secreta no puede ser transmitida vía correo electrónico.
- Sólo la información pública y la información específicamente orientada para proyectos con entidades externas puede ser enviada por correo electrónico, fuera de la institución.
- Los usuarios deben estar al tanto de los riesgos de abrir documentos con macros, archivos postscript, y programas de instalación recibidos vía correo electrónico.
- Debe considerarse un esquema que permita la autenticación del emisor/receptor de información clasificada como confidencial. Por ejemplo, uso de firmas digitales.

4.1.2.8 Internet

La conexión al Internet es casi inevitable en el ambiente comercial de hoy, especialmente para los departamentos de investigación. Debido a su carencia de estructura y controles, el Internet debe evitar los siguientes riesgos:

- Revelación de información confidencial.
- La red institucional puede ser penetrada por hackers de Internet.
- La información puede ser cambiada o borrada.
- El acceso a los sistemas podría ser negado debido a una sobrecarga del sistema.

Si los usuarios van a tener acceso al Internet, ellos deben estar al tanto de los riesgos involucrados y la política institucional en cuanto a consideraciones de uso de Internet.

- Todos los accesos hacia el Internet deben hacerse sobre gateways de la institución los cuales han sido certificados.
- Tienen acceso al Internet personal administrativo, gerentes, técnicos y profesionales.

- Los usuarios internos de las aplicaciones de la institución están permitidos el acceso del correo electrónico por Internet.
- No se permite el acceso a Internet desde servidores de datos que contienen información clasificada como confidencial.
- El software cliente de Internet permitido puede ser el Internet Explorer y el Netscape.
- No usar el acceso a Internet para visualizar o descargar material pornográfico, descargar software peligroso o no licenciado, uso privado excesivo, etc.

4.1.2.9 Políticas de administración del sistema

El administrador tiene que asegurar que los sistemas estén disponibles cuando sea necesario, que la información confidencial esté sólo disponible para aquellos accesos autorizados y que la información no esté sujeta a cambios no autorizados, también debe considerar los siguientes aspectos:

- El Grupo Estratégico de Informática de la institución debe actualizar las políticas de administración del Sistema.
- El Administrador de la Red está autorizado para otorgar accesos y aprobar su uso.
- Sólo el Administrador de la Aplicación puede tener privilegios de administrador.
- No se permite a los usuarios acceso como administrador con privilegios a sus estaciones de trabajo.
- El directorio actual nunca debe estar en la ruta de búsqueda de directorios para usuarios administrativos (prevención de caballos de Troya).

4.1.2.10 Seguridad física

Una política de seguridad física debe existir para detallar las medidas a tomar para proteger los edificios de desastres como: inundaciones, incendios, explosiones, terremotos, apagones, robos. Considerar el control del acceso, seguridades del centro de cómputo y los gabinetes del cableado.

Deben definirse las siguientes zonas:

- Zona 1: Área abierta al público.
- Zona 2: Área no abierta al público, abierta solo para el personal de la institución.
- Zona 3: Áreas protegidas. Solamente accesibles con una identificación, acceso estrictamente restringido.

4.1.2.11 Responsabilidad personal de redes

- El personal administrativo de la red es responsable por la destrucción de cintas y discos defectuosos o viejos.

4.1.2.12 Directivas para el centro de cómputo

Se deben cumplir las siguientes directivas para el centro de cómputo.

- Todos los dispositivos del centro de cómputo deben estar limpios y etiquetados.
- El cableado debe estar limpio, bien arreglado y etiquetado, tal que las conexiones no puedan ser accidentalmente desconectadas o rotas.
- Debe haber un diagrama con la ubicación de los equipos y dispositivos instalados en el centro de cómputo.
- El transporte de los medios electrónicos (cintas, respaldos, discos) debe hacerse considerando medidas que eviten dañarlos.

4.1.2.13 Control de acceso

- Todos los usuarios deben ser autentificados.
- Los usuarios deben ser capaces de modificar los datos que les pertenecen a ellos y sólo podrán consultar los datos que pertenecen a otros usuarios siempre y cuando estos datos estén clasificados como información pública o interna.
- Se permite el acceso al sistema como administrador privilegiado solo vía consola o desde las estaciones que él defina.
- Se debe controlar el acceso de los usuarios a todos los objetos en el sistema (archivos, impresoras, dispositivos, bases de datos, comandos, aplicaciones, etc.).

- No se permite a los usuarios conocer el acceso otorgado a otros usuarios.
- Identificar la información de acuerdo a la clasificación de sensitividad previamente definida.
- El sistema debe proveer un control de acceso obligatorio.
- La asignación de privilegios debe ser hecha por tipo de usuario, para ello debemos valernos de la definición de roles. Si hay usuarios con acceso a varias aplicaciones se puede agrupar los privilegios en roles uno por cada tipo de aplicación.
- Sólo el administrador debe tener la capacidad de conectarse a los recursos del sistema en modo privilegiado para realizar tareas administrativas.

4.1.2.14 Políticas de ingreso a los sistemas

El principio básico a cumplir es dar al usuario final el mínimo de privilegios y el mínimo tiempo necesario para realizar su trabajo.

- Las cuentas de usuario deben existir sólo para el personal autorizado.
- Cada usuario debe ser identificado por un nombre y pertenecer a un grupo dentro del sistema operativo o a un rol dentro de la base de datos.
- Los usuarios y grupos deben ser administrados por el administrador de la base o su delegado, pero no por los usuarios en si.
- Cada usuario debe tener solamente una cuenta sobre el sistema operativo.
- Las cuentas como usuario huésped no son permitidas.
- No se debe permitir cuentas a las cuales se acceda de un grupo de usuarios.
- Cuando un usuario interno es transferido o termina su empleo, su cuenta debe ser eliminada inmediatamente. Los procedimientos administrativos deben contemplar esta situación para que el personal administrativo informe al administrador del sistema sobre este particular.
- Una pantalla inactiva por un período de 15 minutos debe ser reactivada con un password de protección.
- Los usuarios deberían ser informados de acciones que violan la seguridad. Similarmente ellos deben informar a su administrador de seguridades si ellos sospechan de una violación de la seguridad.

Cuando un usuario se conecte al sistema debe desplegarse:

- Información sobre implicaciones legales del abuso del sistema por parte del usuario.
- El tiempo del último ingreso exitoso o no (El usuario debería chequear que esta información esté correcta).

Ingreso de los Usuarios

- Los ingresos al sistema para usuarios internos deben ser habilitados sólo entre las 8:00 h y las 18:00 h.
- Si un usuario ingresa un nombre de usuario o password, el mensaje de error debería ser el mismo para ambos casos. Un posible intruso no debería ser informado si una cuenta de usuario es válida o no.
- Especificar como máximo una sesión simultánea por usuario.
- Debe proveerse un mecanismo que usando la dirección origen permita restringir el acceso de los usuarios a los sistemas.
- Cuando un usuario excede 3 intentos de conexión en un intervalo menor o igual a treinta minutos, y no logra ingresar al sistema, su cuenta debe automáticamente ser bloqueada por un lapso de 2 horas.

4.1.2.15 Auditoria

- Una Auditoria de seguridad debe ser corrida regularmente sobre el sistema una vez cada tres meses.
- Los nuevos servidores deben ser instalados y preparados por el administrador del sistema. Ellos deberían ser auditados y certificados a un nivel de sensitividad por el equipo de seguridad. Si todas las directivas no pueden ser implementadas por un sistema en particular aquellas excepciones deben ser claramente documentadas en la certificación.

4.1.2.16 Contabilización y auditoria

- El registro de las pistas de auditoria, programas y utilitarios deben ser protegidos, ellos deben ser accesibles sólo por el personal de seguridad.
- Los registros de auditoria no deben contener passwords.

- Las actividades del administrador del sistema deberían ser archivadas en los registros de auditoria.
- Los intentos de ingreso fallidos hacia el sistema deberían ser anotadas en un registro de auditoria y ser notificados al administrador.
- Se debe especificar una auditoria por usuarios o por recursos del sistema.
- Cada entrada dentro del registro de auditoria debe contener al menos: nombre de usuario, fecha y hora, identificador del equipo, nivel de error (para éxito o falla) y descripción del evento.
- Los registros de auditoria deben ser mantenidos sobre un dispositivo de almacenamiento que sea solamente de lectura.
- Los registros de auditoria deben ser archivados en una máquina segura, no almacenar los registros sobre sistemas de archivos compartidos.
- Todas las máquinas deben tener sus relojes sincronizados para garantizar la validez de la auditoria en el momento de estampar la hora en los registros.
- El tamaño del registro (log) de las pistas de Auditoria no debe causar una interrupción o degradación del servicio que presta el sistema. Este tamaño debe fijarlo el administrador del sistema así como su frecuencia de reutilización.

4.1.2.17 Políticas de respaldos y recuperación de servidor aplicaciones

- Definir el responsable que realizará los respaldos y la restauración.
- Solo los administradores y operadores del sistema pueden realizar las tareas de respaldar y recuperar información.
- Los respaldos deben hacerse regularmente y algunos de estos respaldos deben almacenarse en otra instalación.
- Los respaldos de información confidencial deben almacenarse en lugares con acceso restringido. Todos los respaldos deben ser contabilizados. Las cintas viejas deben ser destruidas.
- Se debe realizar un respaldo total de la configuración del IAS.
- Se debe realizar un respaldo de cada uno de los logs de las aplicaciones.
- Se debe realizar un respaldo de los usuarios y conexiones a la base de datos

Por cada sistema o grupo de sistemas, se debe:

- Hacer respaldos incrementales y respaldos totales al menos cada semana.
- Realizar con una frecuencia diaria para el incremental y al menos cada semana para el total. El responsable por chequear su correcta operación será el Operador del Sistema.
- Detallar y documentar los utilitarios se usarán para restaurar los datos para todas las aplicaciones.
- Realizar un respaldo mensual de todos los logs de las aplicaciones (Ejemplo: sistema operativo, mecanismos de restauración).
- Describir y documentar los procedimientos para restaurar el sistema operativo después de fallas serias en los discos u otros componentes de hardware.
- Documentar el tiempo de restauración esperado para varios escenarios de desastre.
- Probar las políticas de restauración cada mes.
- Determinar la vida útil de los medios físicos usados para el respaldo.

4.1.2.18 Políticas de respaldos y recuperación de la base de datos

- Definir el responsable que realizará los respaldos y la restauración.
- Sólo los DBA pueden realizar las tareas de respaldar y recuperar información.
- Los respaldos deben hacerse regularmente y algunos de estos respaldos deben almacenarse en otra instalación.
- Los respaldos de información confidencial deben almacenarse en lugares con acceso restringido. Todos los respaldos deben ser contabilizados. Las cintas viejas deben ser destruidas.
- Se debe realizar un respaldo diario los datos
- Se debe realizar un respaldo diario de los datafile.
- Realizar un respaldo semanal de los rodologs

Frecuencia de respaldos

- Hacer respaldos incrementales y respaldos totales, al menos cada semana.
- Realizar con una frecuencia diaria para el incremental y al menos cada semana para el total. El responsable por chequear su correcta operación será el DBA.
- Detallar y documentar los utilitarios se usarán para restaurar los datos para todas las aplicaciones.
- Describir y documentar los procedimientos para restaurar el sistema operativo después de fallas serias en los discos u otros componentes de hardware.
- Documentar el tiempo de restauración esperado para varios escenarios de desastre.
- Probar las políticas de restauración cada mes.
- Determinar la vida útil de los medios físicos usados para el respaldo.

4.1.2.19 Políticas de respaldos y recuperación de servidores web

- Definir el responsable que realizará los respaldos y la restauración.
- Solo los webmaster pueden realizar las tareas de respaldar y recuperar información.
- Los respaldos deben hacerse regularmente y algunos de estos respaldos deben almacenarse en otra instalación.
- Los respaldos de información confidencial deben almacenarse en lugares con acceso restringido. Todos los respaldos deben ser contabilizados. Las cintas viejas deben ser destruidas.
- Realizar un respaldo semanal de todo el equipo (Sistema Operativo y Configuraciones)

Frecuencia de respaldos

- Hacer respaldos totales al menos cada semana.
- Detallar y documentar los utilitarios se usarán para restaurar los datos para todas las aplicaciones.
- Probar las políticas de restauración cada mes.
- Determinar la vida útil de los medios físicos usados para el respaldo.

4.1.2.20 Administración de cambios (instalaciones o actualizaciones de software / hardware y etiquetación)

- Sólo los administradores del sistema deben instalar o actualizar el software en los servidores.
- Los usuarios no pueden instalar software en las estaciones de trabajo.
- Los sistemas deben ser instalados de modo limpio de acuerdo a las instrucciones de los proveedores.
- Mantener en cada servidor un archivo de cambios, que registre todos los cambios que realice el sistema.
- Se sugiere que como mínimo, un archivo de texto simple sea creado que contenga: fecha, nombre del administrador, archivos cambiados y razón ó comentario.
- Las instalaciones del sistema operativo deben incluir la instalación de todos los parches de software recomendados.
- Identificar todas las máquinas que se instalen mediante etiquetas que se adhieran en forma externa a cada uno de los equipos.
- Las etiquetas deben incluir por ejemplo: nombre del equipo, fabricante ó modelo de la máquina, dirección IP, dirección MAC, identificador del nodo en el cableado (si la topología de la red lo permite), fecha de vencimiento de la garantía y número de teléfono de la línea de ayuda o seguridad, nombre del servidor al que se conecta el equipo.
- Aplicar sólo los parches del proveedor original de software.
- Los parches descargados desde redes públicas (Por ejemplo, Internet) deben ser chequeados por integridad usando un mecanismo de hashing (Por ejemplo MD5). Los parches se usarán en cuanto estén disponibles y deberán ser pre-probados en un ambiente de pruebas (por al menos unas pocas semanas si es posible) antes de ser aplicados a los sistemas de producción.

4.1.2.21 Políticas de las redes / sistemas distribuidos

- Documentación de configuraciones de la red.
- Identificar y autenticar cualquier sujeto en la red institucional.

- Si es posible, debe haber un solo mecanismo de ingreso para los usuarios de múltiples aplicaciones y sistemas, evitando múltiples nombres de usuarios y passwords.

Contabilización y auditoria:

- Auditar las acciones de los usuarios. Los usuarios deben cumplir con las políticas de la red.
- Llevar registros de auditoria de la actividad de los nodos de la red más importantes. Estos registros deben ser regularmente analizados para detectar brechas de seguridad.

Control de Acceso

- Configuración de los nodos de la red sensitivos.
- Sólo se permiten habilitar los siguientes servicios de red: SMTP, POP3, HTTP, SSH, SFTP, HTTPS. Configurar los servicios de red de modo restrictivo e instalar todos los parches de software relacionados.
- Etiquetar en forma externa las redes disponibles como de acceso abierto, acceso restringido o acceso altamente restringido, de modo que los usuarios o propietarios de los datos estén al tanto de la protección ofrecida.

- Por ejemplo si una LAN está etiquetada como de acceso abierto y se necesita transmitir información confidencial sobre esta LAN, entonces serán necesarias medidas adicionales como encriptación a nivel de aplicaciones para corregir la deficiencia de la seguridad de la red.
- En las redes de acceso restringido, el cableado no debe pasar a través de redes públicas, su conducción debe ser protegida y los puntos de conexión deben estar disponibles sólo a las personas autorizadas. Si el cableado es proporcionado por terceros, debe ser inspeccionado y certificado.

Integridad:

- Debe chequearse regularmente la exactitud e integridad de los datos de los nodos de la red más importantes.
- Intercambio de datos:
- La información confidencial debe ser sólo transmitida a través de mecanismos de transporte certificados.

- Por ejemplo, los sistemas de correo electrónico usados para datos confidenciales deben ser certificados por la administración de seguridad.
- La información de las sesiones de ingreso (Por ejemplo, nombre de usuario y password) no deben enviarse sobre la red en forma clara (clear form).
- Los servicios de red entre hosts deben autenticarse uno a otro.
- Proteger las redes contra programas husmeadores (sniffers), tales como: snoop, etherfind, tcpdump, iptrace etc. Estos programas no deben estar disponibles a los usuarios.
- Dividir las redes en subredes, usar puentes activos y hubs y deshabilitar los puntos de conexión de red no usados.
- Encriptar los datos clasificados como confidenciales antes de su transmisión tanto en las redes internas como en las públicas.
- Cuando la información está siendo transmitida (enviada o recibida), la identidad de quien envía o recibe debe ser atachada a la información y chequeada por los varios componentes responsables por la transmisión.
- No enviar datos clasificados como confidenciales a usuarios no autorizados o a sistemas con una clasificación de sensitividad más baja.
- En ciertas aplicaciones (Por ejemplo, correo electrónico), deben existir mecanismos para probar que el emisor/receptor hicieron realmente la transmisión/recepción de los datos (Prueba de origen/recepción).

Confiabilidad del Servicio / Disponibilidad

- La red se requiere disponible las 24 horas del día, 5 días a la semana. El horario de mantenimiento será el día viernes de 18:00 a 22:00 horas.
- Monitorear los errores y problemas de desempeño de la red. Tomar acciones preventivas antes de que ocurran interrupciones serias de la red.
- Administración de cambios: Las actualizaciones y los cambios de configuración deben ser registrados y llevados a cabo de acuerdo a procesos de calidad.
- Una etiqueta que contenga la siguiente información debe ser pegada en todas las máquinas durante la instalación: nombre del equipo, fabricante modelo de la máquina, dirección IP, dirección MAC, identificador del nodo

en el cableado (si la topología de la red lo permite), fecha de vencimiento de la garantía y número de teléfono de la línea de ayuda o seguridad.

- La red institucional no debe interconectarse con otras redes (X.25, Dial-up, Internet, redes de proveedores, redes telefónicas, redes de clientes, etc.) si esto crea una brecha de seguridad. El acceso desde redes externas debe hacerse a través un firewall.
- El firewall debe cumplir con políticas de seguridad y debe ser regularmente monitoreado y auditado.

4.1.2.22 Firewall para internet

El Internet es una importante herramienta para compartir y buscar información. Todos los accesos al Internet desde la red de la institución deben hacerse a través de un Firewall.

- La política del firewall y su configuración deben ser documentadas correctamente.
- Los equipos de firewall deben estar sujetos a un monitoreo regular y a una auditoria anual.

Identificación y Autenticación

- Las conexiones de los usuarios que accedan desde el Internet deben usar un sistema de autenticación robusto: passwords de una sola vez, desaf o-respuesta, etc.
- Las cuentas del administrador deben usar además sesiones de login encriptadas.
- Instalar los equipos de firewall de modo seguro. Todos los servicios del sistema operativo no necesarios deben detenerse.

- Mantener registros de auditoria del firewall (si es posible en un servidor dedicado y sobre medios write-once).
- Mantener registros históricos de todas las auditorias de seguridad.
- Usar un software de auditoria que generen alarmas para los errores críticos.

- Examinar los registros de auditoria una vez cada semana.
- Deben haber y estar disponibles estadísticas de uso.

Control de acceso:

- Todos los accesos al Internet desde la red de la institución deben hacerse sobre proxys localizadas en un firewall.
- Los servicios de configuración por defecto están prohibidos.
- Todos los usuarios están permitidos a intercambiar correo electrónico interno.
- Los usuarios de soporte técnico informático están permitidos a usar WWW y FTP (sobre proxies). El resto de usuarios requieren autorización.
- Los departamentos que requieren acceso completo al Internet para probar nuevos servicios no deben instalar estos servicios en la red institucional, sino en una red separada, fuera del firewall.
- Ningún usuario debe ser capaz de ingresar directamente a los equipos de firewall.
- Se prohíbe el acceso por Internet a material ilícito.

Integridad

- Debe chequearse regularmente (cada mes) la exactitud e integridad de los archivos localizados en los equipos de firewall.

Intercambio de datos:

- Todas las sesiones de usuario al equipo de firewall deben hacerse usando un acceso encriptado o passwords de una sola vez.

Confiabilidad del servicio

- El firewall debe estar disponible 7x24h, máximo tiempo fuera de servicio 2 horas (horas fuera de oficina), máxima frecuencia una vez por mes, horario de mantenimiento: Sábado o Domingo después de las 18:00 horas.

- Administración de cambios: Las actualizaciones y cambios de configuración deben ser registradas y llevadas a cabo de acuerdo a procesos de calidad.
- Deben disparase alertas si los procesos o servicios importantes hacen crash.
- Los servicios importantes (tales como WWW y proxy) debe ser configurados para alta disponibilidad.
- Deben hacerse respaldos regulares de datos necesarios (Por ejemplo, archivos de configuración).

Interfaces a otras redes:

- Debe existir un documento de políticas para cada interfase, el cual detalle que información va a ser transferida, cómo se hará la transferencia, y cómo se conforma a las políticas de seguridad de la institución.
- Proteger las interfaces con otras redes por un firewall y sujetarlas a un monitoreo y auditoria regulares.
- Establecer acuerdos de niveles de servicio para comunicación con las redes externas.
- Firmar un acuerdo de privacidad con el cliente/proveedor externo, el cual asegure que ninguno de los detalles de la interfase, ni los datos accesibles por la interfase, pueden ser revelados a terceras partes.

- Proveer esquemas que permitan la autenticación del cliente/proveedor externo (usuarios especiales). Por ejemplo, uso de certificados digitales.

4.1.2.23 Políticas de desarrollo de software

- Separar los ambientes y datos de desarrollo y producción.
- Obligar a que la seguridad sea una parte integral del desarrollo de aplicaciones.
- Los datos de prueba no deben contener información confidencial.
- Usar un lenguaje seguro (Por ejemplo, Java en lugar de C).
- Usar metodologías de desarrollo bajo estándares ISO9000.

- Todos los nuevos sistemas deben ser aprobados por el área de seguridad de la información.

Guías de producción:

- Se debe entregar con la aplicación la siguiente documentación: Manuales de Operación, Instalación, Administración, Seguridad, Usuario.
- Para que una aplicación entre a producción debe pasar exitosamente un plan de pruebas.

Exigencia:

- Los usuarios que no se adhieran a estas políticas deben ser advertidos de sus consecuencias y debe ser informada la línea de administración correspondiente. Un usuario que aun siendo advertido continua ignorando estas políticas puede ser removido de su función.

CAPÍTULO V

5. PLAN DE CONTINGENCIA PARA SOLUCIONES A PROBLEMAS

Se enfoca las contingencias relacionadas con fallas menores que se suscitan en el normal funcionamiento de la Red de Información, al igual que los servidores, tanto de producción como para el área de desarrollo.

5.1 ÁREA DE REDES Y COMUNICACIONES

La ocurrencia de fallos en la red, puede darse en alguno de los componentes de la misma, a saber:

- Equipos y enlaces de Comunicaciones
- Acceso a Internet.
- Servidores de red.
- Estaciones de trabajo.
- Equipos de Impresión

El fallo de un componente es factible ser focalizado de manera precisa, dado que a cada uno de ellos le corresponde brindar un servicio, el mismo que en caso de ocurrencia de errores, deniega el servicio para el cual fue implementado.

5.2 EQUIPOS Y ENLACE DE COMUNICACIONES.

5.2.1 Fallas.

- Equipos remotos no pueden acceder a aplicaciones de los servidores.
- Los equipos de monitoreo no detectan a los equipos remotos.

5.2.2 Acciones a Tomar.

- Asegúrese que los equipos de comunicaciones están encendidos (Router, FRAD).

- Ejecute el comando ping en el Promt del sistema, a fin de verificar comunicación con la interfase LAN:

- En Primer lugar verificamos que el puerto LAN del firewall de Intranet se encuentre activo y la comunicación con este esté en buen estado, para lo cual ejecutamos el comando:

    ping puerto LAN del Firewall.

- En caso de no tener respuesta afirmativa verificar cables de comunicación y/o comunicarse con el área de seguridades a fin de verificar estado del firewall. Si la respuesta es afirmativa, se debe comprobar que la comunicación con el router esté activa, esto se hace con los siguientes comandos:

    ping para el caso del router de Quito.
    ping para el caso del router de Ambato.
    ping para el caso del router de Latacunga.
    ping para el caso del router de Ibarra.
    ping para el caso del router de Manta.
    ping para el caso del router de Otavalo.
    ping para el caso del router de Loja.

- En caso de no tener resultados positivos verifique cable de conexión del router al Firewall.

- Ejecute el comando ping en el Promt del sistema, a fin de verificar comunicación con la interfase WAN del router de Intranet.

    ping para el caso de Quito.
    ping para el caso del Hospital de Ambato.
    ping para el caso de Latacunga.
    ping para el caso de Otavalo.

ping para el caso de Ibarra.
ping para el caso de Manta.
ping para el caso de Loja.

- Si existe resultados positivos tanto en la interfase LAN como en la WAN del router local, realizar el mismo procedimiento para el router remoto, utilizando los comandos siguientes:

ping router de Regional Ambato.
ping router del Hospital de Ambato.
ping router de Latacunga.
ping router de Otavalo.
ping router de Ibarra.
ping router de Manta.
ping router de Loja.

- Si no existe resultados positivos al verificar la interfase WAN del router, se debe a fallas en el canal de comunicaciones, para lo cual hay que comunicarse con el proveedor del servicio a fin de tomar los correctivos del caso.

5.3 ACCESO A INTERNET

5.3.1 Fallas.

- Los usuarios no tienen acceso a Internet.
- El monitor de Internet reporta fallos.

5.3.2 Acciones a tomar.

- Asegúrese que los equipos de comunicaciones para Internet están encendidos, esto es: router de Internet, radio de Comunicaciones.
- Verificar que el cable de conexión de la antena al equipo de radio se encuentre conectado.

- Verificar estado de los Led´s del equipo de radio, principalmente el de RADIO FAILE que indica errores en el equipo. Debe estar encendido únicamente el indicador INPUT1.
- Desde el prompt del computador PRO04, ejecute telnet al router, con la finalidad de verificar estado de los puertos de comunicación y del enlace. Para esto utilice el siguiente comando: telnet servido de Internet
- Passwords para ingreso como administrador de los diferentes routes, solicitar al área de seguridades.
- De no existir resultados positivos verificar el cable de conexión del router al
- Switch.
- Si la conectividad con el router y el estado del Radio de comunicaciones es el correcto, se debe contactar con el proveedor del servicio a fin de realizar pruebas y tomar los correctivos del caso.

5.4 SERVIDORES DE RED.

Los servicios de red que son proveídos por servidores locales son: DHCP y DNS

5.4.1 FALLAS EN SERVIDOR DE DHCP.

- No existe comunicación entre las diferentes máquinas de la red LAN.
- Ninguna de las estaciones de trabajo tiene asignado una dirección IP.

5.4.1.1 Acciones a Tomar.

- Verifique que el equipo servidor esté encendido.
- Verifique que el equipo servidor esté conectado a la red
- Verifique que la configuración de acceso a redes, del equipo, se encuentre bien.
- Verifique que el servicio de DHCP server se encuentre iniciado.
- En caso de no tener respuesta positiva con todas estas acciones es necesario verificar configuración ó definitivamente reconfigurar el servicio.

5.4.2 FALLAS EN EL SERVIDOR DE DNS.

- Al intentar comunicación con otros equipos, utilizando el nombre de alto nivel del equipo destino, obtenemos el mensaje de Host no reconocido.

5.4.2.1 Acciones a Tomar.

- Verificar si el equipo servidor de DNS se encuentra encendido.
- Verificar que el equipo servidor se encuentre conectado a la red.
- Verificar que la configuración de acceso a redes, del equipo, se encuentre bien.
- Verificar que el servicio de DNS server se encuentre iniciado.
- En caso de no tener respuesta positiva con todas estas acciones es necesario verificar configuración ó definitivamente reconfigurar el servicio.

5.5 ESTACIONES DE TRABAJO.

Dado que las estaciones de trabajo son usuarias de todos los servicios de red, así como de las aplicaciones que se hallan en producción, existe mayor cantidad de parámetros por verificar, tanto en la parte de comunicaciones como de acceso a aplicaciones.

5.5.1 FALLAS EN COMUNICACIONES.

- No se visualiza ningún computador perteneciente al grupo de trabajo de la estación.
- No se tiene asignada una dirección IP.
- No se tiene respuesta utilizando nombres de alto nivel.

5.5.1.1 Acciones a tomar

- Verificar que patch cord se encuentre conectado a tarjeta de red y al punto de datos del cableado estructurado.
- Ejecutar el comando ipconfig en el Promt del sistema, a fin de obtener información de dirección IP, default gateways, etc.
- Si no se tiene respuesta positiva al requerimiento anterior, se debe habilitar en cada uno de los clientes de los servicios la configuración automática, a fin de obtener estos parámetros de los respectivos servidores.
- Habilitar, en la parte de servicios, el DHCP client y el DNS client.

5.6 FALLAS DE ACCESO A APLICACIONES.

- El browser del Internet Explorer no despliega la aplicación Historia Laboral.

5.6.1 ACCIONES A TOMAR.

- Verificar estado de las comunicaciones tanto de acceso a la red local como del enlace de comunicaciones
- Verificar configuración del Internet Explorer, haciendo clic derecho en el icono del IE, utilizar la opción Propiedades de Internet, en la viñeta conexión verificar que la casilla de configurar una conexión a Internet, no contenga ninguna cuenta, debe estar habilitado únicamente la opción de configuración de la Red de Area Local, en esta hay que activar la casilla de configuración automática.

5.7 EQUIPOS DE IMPRESIÓN.

5.7.1 FALLAS DE IMPRESIÓN

- Al realizar el envío de impresión, a una impresora de red, esta no es detectada por la máquina origen.
- No se encuentra ninguna impresora instalada en un computador personal.
- Es detectada la impresora de red pero no se produce la impresión.

5.7.2 ACCIONES A TOMAR.

- Verificar que la impresora de red se encuentre encendida.
- Ejecute el comando ping en el Promt del sistema, a fin de verificar comunicación con la impresora de red: C:\> ping <DIR IP-IMPRESORA>
- De no tener resultados positivos verificar el cable de comunicación de la impresora.
- Verificar que la impresora tenga disponibilidad de papel.
- Ejecutar en la impresora una impresión de prueba y de seteo de la impresora, si la impresora ha cambiado sus parámetros de configuración, volver a realizar la configuración utilizando como procedimiento el mencionado en el respectivo manual.
- Verificar que el software de impresión de la impresora local, no haya cambiado sus parámetros de configuración.

5.8 SERVIDORES DEL SISTEMA HISTORIA LABORAL.

El sistema Historia Laboral está implementado en dos ambientes, Pruebas y Producción. En cada uno de estos ambientes existen servidores de Base de Datos, servidores de Aplicaciones y servidores de Web.

5.9 SERVIDOR DE BASE DE DATOS.

- La ocurrencia de fallos en estos servidores puede darse a nivel de conexiones de red, motor de base de datos y/o sistema operativo.

5.9.1 ACCIONES A TOMAR

- Verificar que el equipo se encuentre encendido.
- Verificar que se encuentre conectado el cable de red.
- Desde una estación de trabajo ejecutar el comando ping a la dirección del servidor que se trate:
- Si no se obtiene resultados positivos, verificar condiciones del cable de red y/o configuración del sistema operativo para trabajo en red.

Para el caso de sistema operativo. Windows 2000 Server realizar:

- Clic derecho en: Entorno de red / Propiedades / Conexión de Área Local /Propiedades/Protocolo de Internet (TCP/IP)
- Dirección IP 192.168.10.41
- Máscara 255.255.255.0
- Default Gateway (No se necesita definir Default Gateway)
- Servidor DNS 192.168.10.42

Para el caso de Sistema Operativo Solaris:

- En un terminal ejecutar el comando ifconfig -a, se despliega información de la configuración de las interfaces de red. La interfaz de red que se encuentra habilitada es la eri0. Con los siguientes valores:
- Dirección IP 192.168.10.1

- Netmask
- Para realizar la configuración de la interface, en un terminal se ejecuta el siguiente comando: ifconfig eri0 inet 192.168.10.1 netmask 255.255.255.0

Adicionalmente es necesario verificar archivos de configuración que se encuentran en el directorio /etc, estos son: defaultrouter y defaultname.

Mediante la ejecución del comando more defaultrouter, desplegamos información del default gateway del equipo, para este caso la dirección de defaoult gateway es 192.168.10.3.

Mediante la ejecución del comando more defaultname, desplegamos información del dominio del equipo, para este caso el dominio es iess.gov.ec.

En caso de requerirse que se edite estos archivos, lo podemos realizar utilizando el editor de texto vi, mediante el siguiente comando:

vi defaultname y/o vi defaultrouter.

Si la verificación de las interfaces no tiene ningún problema y la comunicación está funcionando bien, pero no se logra conexión a la Base de Datos, es necesario verificar parámetros de configuración del motor de base de datos conjuntamente con el Administrador de Base de Datos.

5.10 ÁREA DE SERVIDORES

Como se dijo en capítulos anteriores el área servidores es la que tiene como función primordial el mantener las diferentes aplicaciones que presta el IESS en perfecto funcionamiento, para lo cual hay que tomar las siguientes directrices en caso de un comportamiento poco normal o fuera del funcionamiento diario.

5.11 FALLAS DE ACCESO A APLICACIONES HISTORIA LABORAL

5.11 1 FALLAS.

- Los usuarios nos comunican que no pueden ingresar al aplicativo de Historia laboral.

5.11.2 ACCIONES A TOMAR

- Se debe conectar desde una estación hacia al servidor de historia laboral vía telnet.
- Si no tenemos respuesta del equipo debemos verificar físicamente que el servidor se encuentra prendido.
- Luego de verificar que el servidor se encuentra prendido ingresamos vía consola; se debe realizar un ping a la interfaz local del equipo para verificar que se encuentra levantada, luego realizar un ping a un servidor que se encuentre en la misma red.
- Si al momento de realizar el ping a otro servidor no tengo respuesta se debe comunicar al responsable del área de redes que verifique por que no se encuentra el servidor en la red.
- Luego de haber solucionado los pasos anteriores ingresamos al respectivo servidor con el usuario adecuado del IAS (Internet Aplication Server).
- Verificar si el servicio de http esta levantado para lo cual se debe realizar la ejecución del siguiente comando:

  dcmctl getstate -v -d
- Si el servicio de http se encuentra abajo se debe ejecutar el siguiente comando para levantar el servicio.

  dcmctl start -v -d

- Ingresar al Internet explorar a la dirección http://hl.iess.gov.ec (dirección de intranet) o http://hl2.iess.gov.ec (dirección de Internet) de a cuerdo de donde se nos reporto el daño y verificar si muestra la pagina de inicio de la sección.
- Si ya se muestra la página se debe comunicar a los usuarios que prueben para ver si ya no existe problemas.

5.12 FALLAS AL MOMENTO DE LEVANTAR LOS SERVICIOS DE HTTP CAUSADA POR SESIONES MUERTAS

5.12.1 FALLAS.

- Al momento de levantar los servicios del servidor no se levanta el servicio de http

5.12.2 ACCIONES A TOMAR

- Se sobre entiende que ya se encuentra dentro del servidor, para lo cual debe comenzar a matar las sesiones de java y http con los siguientes comandos.
- pkill -9 java
- pkill -9 httpd
- Luego de haber matado todas las sesiones verificar si ya no tenemos conexiones activas e inactivas a la base de datos con el siguiente comando.
- netstat -na|grep IP_BDD |wc -l
- Si ya no existen sesiones en la base de datos se debe realizar el siguiente comando para levantar las sesiones.
- dcmctl start -v -d
- Ingresar al Internet explorar a la dirección http://hl.iess.gov.ec (dirección de intranet) o http://hl2.iess.gov.ec (dirección de Internet) de a cuerdo de donde se nos reporto el daño y verificar si muestra la pagina de inicio de la sección.

5.13 FALLAS AL MOMENTO DE LEVANTAR LOS SERVICIOS DE HTTP CAUSADAS POR ESPACIO EN LOS DISCOS.

5.13.1 FALLAS.

- Al momento de levantar los servicios de http se presenta el problema de que no cuenta con el espacio suficiente el servidor de aplicaciones.

5.13.2 ACCIONES A TOMAR

- Desde el servidor de aplicaciones se debe verificar el espacio que cuenta el equipo para lo cual se ejecuta el comando.
- df -h

- La raíz debe contar con el 30% de espacio disponible para que la aplicación puede funcionar correctamente.
- Se debe revisar directorios que no deben estar y proceder a eliminarlos, pero se debe tener mucho cuidado con los directorios o archivos del sistema operativo, los cuales no se deben tocar, estos son los que se encuentran en /var, /usr, /proc tomar muy en cuenta con el archivo del core ya que este sí se puede eliminar, el comando que nos permite la eliminación es:
- rm -rf nombre del archivo
- Luego de eliminar archivo y directorios innecesarios se procede a ejecutar el comando df -h para verificar el espacio en el disco para luego levantar las sesiones.

5.14 FALLAS AL MOMENTO DE LEVANTAR LOS SERVICIOS DE HTTP CAUSADAS POR LOS LOGS.

5.14.1 FALLAS.

- Al momento de levantar los servicios de http se presenta el problema de que los log de la aplicación esta lleno.

5.14.2 ACCIONES A TOMAR

- Desde el servidor de aplicaciones dirigirse al path donde se encuentra instalado la aplicación APP/Apache/Apache/log con el siguiente comando.
- cd /App/ Apache/Apache/log

- Mover el log que genera la aplicación en este caso el access_log con el siguiente comando.
- mv access_log /path en donde se pondrá el log

- Cabe recalcar que al momento de mover el log es recomendable cambiar el nombre o aumentar con la fecha. Ejemplo access20060717_log.

5.15 FALLAS DE FILE SYSTEM DE LOS SERVIDORES.

5.15.1 FALLAS.

- El servidor no reconoce algún arreglo al momento de iniciar, cuando tuvo un apagón brusco.

5.15.2 ACCIONES A TOMAR

- Cuando un servidor no reconoce un arreglo al momento de reiniciar, se queda intentando montar el arreglo hasta que le pide el login de root
- Luego de haber ingresado el login de root, ingresamos el siguiente comando.
- fsck -y
- Si no se reparo se debe ingresar el mismo comando pero en lugar de la (y) ingresamos la unidad lógica, esta se la puede tomar del archivo vfstab que el que utiliza el servidor para montar los diferentes arreglos.
- fsck nombre lógico de la unidad
- Luego de haber reparado el file system escribimos el comando para verificar que todos los arreglos están levantando df -h.
- Ingresamos el comando exit y el equipo se reinicia sin ningún problema.

5.16 FALLAS DE ACCESO A WWW.IESS.GOV.EC.

5.16.1 FALLAS.

- Los usuarios nos informan que no pueden ingresar a la dirección www.iess.gov.ec.

5.16.2 ACCIONES A TOMAR

- Ingresamos al servidor de intranet o Internet de a cuerdo desde donde se nos comunicó el problema.

- Comprobamos que los servicios de http estén corriendo con el siguiente comando.
- service httpd status
- Si al comprobar que los servicios están abajo, se debe ejecutar el siguiente comando para levantarlos.
- service httpd start
- Ingresamos desde el Internet Explorer a la dirección www.iess.gov.ec para ver si nos muestra la página de inicio de sesión.
- Si luego de realizar el paso anterior no se muestra la página puede ser que el balanceador de carga no se encuentra balanceando.
- Realizamos una sesión de telnet a la IP del balanceador.
- Ingresamos la clave de usuario de telnet.
- digitamos usuario y luego ponemos la clave del balanceador.
- Ingresamos el comando wr term para mirar si está incluido los dos equipos web dentro del balanceador, debe aparecer lo siguiente.
- real IP_SERVIDOR_WEB1:0:0:tcp is
- real IP_SERVIDOR_WEB2:0:0:tcp is

- Si nos aparece en lugar de (is) esta (os) se debe incluir el equipo que no se encuentra registrado, con el siguiente comando.
- In_service real IP_SERVIDOR_WEB is
- Para finalizar grabamos con el comando wr mem y listo, probamos desde el Internet Explorer.

5.17 APAGAR LOS SERVIDORES EN CASO DE FALLO EN LA CORRIENTE ELÉCTRICA.

5.17.1 FALLAS.

- Suspensión brusca del servicio de corriente eléctrica.

5.17.2 ACCIONES A TOMAR

- Para que la base de datos pueda bajar de una manera rápida, se debe matar todas las sesiones de los diferentes aplicativos.

- Bajamos los servicios de todos los servidores de aplicaciones, con el comando dcmctl stop.
- Matamos todas las sesiones de java y http con el comando pkill -9 java y pkill -9 httpd en todos los servidores de aplicaciones.
- Se le informa al DBA que ya no tenemos sesiones para que proceda a bajar las diferentes bases de datos.
- Apagamos por completo todos los equipos en las diferentes capas (web, aplicaciones y base de datos).

CAPÍTULO VI

6. CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Al término del proyecto se cumplió con todos los objetivos propuestos, ayudando así a mejorar la seguridad de la información en el IESS.
- Al aplicar la norma ISO 27001, en procesos críticos que se manejan en el IESS se garantizó la seguridad y disponibilidad los servicios que presta la Institución.
- La políticas permitirán tener un mayor control sobre todos los activos que maneja el IESS.
- La información es el principal activo que tiene el IESS, es por ello que se debe tener mucho cuidado al momento de almacenar y trasladar los dispositivos de respaldos.
- El análisis del riesgo determina la probabilidad, ocurrencia de las amenazas y determinar el impacto potencial en la Institución.
- El riesgo informático es todo factor que pueda generar una disminución en la confidencialidad, integridad y disponibilidad en la Institución.

6.2 RECOMENDACIONES

- Se recomienda que la cúpula de Directivos consideren como prioridad principal la aplicación y cumplimiento de la norma .
- El personal involucrado en la aplicación, ejecución y control de las políticas deben sujetarse a lo sugiere la norma.
- Se recomienda realizar una evaluación de las políticas semestralmente, para que sigan manteniéndose acorde a las necesidades de la empresa.
- Se recomienda realizar un control del acceso de las personas que ingresan al centro de cómputo a través de dispositivos de seguridad electrónicos, para impedir futuros desmanes en el mismo.
- Se recomienda realizar equipos de almacenamiento en Guayaquil y Cuenca para almacenamiento de los respaldos.

BIBLIOGRAFÍA

- Información del IESS
- Seguridad de la Información para la Empresa (Álvarez, Pedro Pablo Pérez)
- Seguridad Practica en Unix e Internet (Simson Garfinkel y Gene Spafford)
- http://www.solocursos.net/introduccion_a_la_seguridad_informatica_en_redes_corporativas-slccurso2231596.htm
- http://barrapunto.com/article.pl?sid=04/06/01/1119205&mode=thread
- http://sgsi-iso27001.blogspot.com/
- http://documentos.shellsec.net/otros/analisis_iso-27001_shellsec.net.pdf.
- http://www.kriptopolis.org/node/1414
- http://www.unixmexico.org/modules.php?name=News&file=article&sid=1586
- http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/impariesgo.pdf
- http://www.enterate.unam.mx/Articulos/2005/febrero/seguridad.htm
- http://www.abast.es/integrityit/riesgos.html
- http://www.ibermatica.com/ibermatica/seguridad/ofertaanalisis
- http://sgsi-iso27001.blogspot.com/
- http://www.desarrolloweb.com/articulos/2435.php
- http://www.desarrolloweb.com/articulos/2446.php
- http://www.mastermagazine.info/informes/9544.php
- http://seguridadit.blogspot.com/2006/01/norma-iso-17799-vs-iso-27001.html
- http://www.rzw.com.ar/modules.php?name=News&file=article&sid=3681

GLOSARIO

A

Aceptación del Riesgo

(Inglés: Risk acceptance). Según [ISO/IEC Guía 73:2002]: Decisión de aceptar un riesgo.

Activo

(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Alcance

(Inglés: Scope). Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Amenaza

(Inglés: Threat). Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos

(Inglés: Risk analysis). Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor

(Inglés: Auditor). Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría

(Inglés: Audit). Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación

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

B

Bios

Sistema de configuración principal de las computadoras.

BDD

Base de Datos.

COBIT

Control Objectives for Information and related Technology

C

Cron

Servicio para tareas programadas.

CMMI

Capability Maturity Model Integration.

CIA

Acrónimo inglés de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

CID

Acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

CobiT

Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Compromiso de la Dirección

(Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

Confidencialidad

(Inglés: Confidenciality). Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por

la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

D

DDI

Dirección de Desarrollo Institucional

DBA

Data Base Administrator.

DES3

Algoritmo de Encriptación.

Dial-in

Conexión a Internet que se establece a través de un modem y una línea.

DHCP

Protocolo de configuración dinámica.

Datafiles

Archivo de datos.

DNS

Domain Name Service.

Desastre

(Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad

(Inglés: Availability). Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

E

Encriptada

Información Codificada.

Evaluación de riesgos

(Inglés: Risk evaluation). Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento

(Inglés: information security event). Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

F

FRAD

Conmutadores de protocolos multiples.

Firewall

Sistema de protección de agentes externos.

G

Gestión de riesgos

(Inglés: Risk management). Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Gateways

Puertos de Enlace.

H

Hadware

Sistema Físico de computación.

http

HyperText Transfer Protocol.

HTTPS

Security HyperText Transfer Protocol.

Hosts

Sistema AS400 que manejaba el IESS.

HUBS

Dispositivo para comunicar equipos.

I

IP

Protocolo de Internet.

IAS

Internet Aplication Server.

IDS

Sistema Detector de Intrusos.

ISS

Internet Security System.

IESS

Instituto Ecuatoriano de Seguridad Social.

ISMS

Information Security Management System.

IT

Information Technology.

ITIL

IT Infrastructure Library.

ISM3

Information Security Management Maturity Model.

ISECOM

Institute for Security and Open Methodologies.

IEC

International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Impacto

(Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Integridad

(Inglés: Integrity). Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos

(Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISMS

Information Systems Management System. Véase: SGSI.

ISO

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

ISO 27001

Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005

ISO/IEC TR 13335-3

“Information technology . Guidelines for the management of IT Security .Techniques for the management of IT Security.” Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

J

JTC1

Joint Technical Committee. Comité técnico conjunto de ISO e IEC específico para las TI.

JDE

Software financiero del IEES.

L

LED

Indicador Luminoso.

LAN

Local Area Network.

Logs

Archivo donde se almacena en detalle el proceso de las aplicaciones.

M

MAC

Número único asignado a cada tarjeta de red.

MoU

Memorandum of Understanding.

O

Outsoucing

Externalización de Servicios.

Objetivo

(Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

P

Política de seguridad

(Inglés: Security policy). Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. según [ISO/IEC 17799:2005]: intención y dirección general expresada formalmente por la Dirección.

PDCA

Plan-Do-Check-Act.

PROXY

Ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

POP3

Protocolo de Transferencia.

PING

Comando de monitoreo de conectividad.

PNUD

Proyecto de las Naciones Unidas.

R

Riesgo

(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Router

Dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres.

S

SCSI

Sistema de gestión de seguridad de información .

Software

Sistema lógico de computación.

Sniffers

Husmeadores.

Switchs

Dispositivo para comunicar equipos.

SMTP

Simple Mail Transfer Protocol.

SSH

Security Shell.

SFTP

Security File Transfer Protocol.

Sun

Sistema Operativo Solares.

Seguridad de la información

Según [ISO/IEC 17799:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Selección de controles

Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI

(Inglés: ISMS). Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

T

Tratamiento de riesgos

(Inglés: Risk treatment). Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

TELNET

Programa que permite acceder a ordenadores distantes en Internet.

TABE

Unidad de cinta para realizar respaldos.

U

UKAS

United Kingdom Acreditación Service.

V

Vlans

Red Virtual.

Valoración de riesgos

(Inglés: Risk assessment). Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Vulnerabilidad

(Inglés: Vulnerability). Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

W

Wan

World Area Network.

Webmaster

Adminitrador de la WEB.

WWW

World Wide Web**.**

ANEXOS

IMPLEMENTACIÓN DE POLÍTICAS PARA CASOS CRÍTICOS

1. POLÍTICAS DE ADMINISTRACIÓN DE USUARIOS

PROPÓSITOS

Normar la administración de usuarios y acceso a los servidores del IESS.

ALCANCE

Esta política es aplicable para todas las dependencias del IESS

DEFINICIONES

Red de datos: Red física compuesta por diferente tipo de cables y equipos de comunicación, que permite el envío y recepción de información de un equipo a otro.

Servidor: Equipo que controla las seguridades y presta diferentes servicios en una red de datos.

Solaris 9: Sistema operativo de red creado por Sun Micro Systems.

Red Hat Enterprise: Sistema operativo de red creado por Red Hat.

Nombre de usuario: Nombre con el que se le conocerá a un usuario en la red.

Contraseña de usuario: Clave secreta que solamente el usuario dueño de una cuenta podrá saberla.

NORMAS

- Las cuentas de usuario de acceso a los servidores del IESS controlado por los equipos Sun FIRE 4900 deben ser solicitadas al Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional, por el jefe superior del departamento en donde trabaja el nuevo usuario, indicando los servicios a los que debe tener acceso, tales como: servicio de correo electrónico, espacio en algún servidor, conexión a una determinada aplicación de la Empresa, etc.
- Cada usuario que trabaje en la red de datos controlada por los servidores Sun FIRE 4900 del IESS deberá poseer su cuenta de usuario para el ingreso a la misma. Esto hace que cada usuario sea

responsable de lo que se realice en la red con esa cuenta, por tal motivo las claves de ingreso deben ser secretas.

- Las cuentas de usuario en los servidores Sun FIRE 4900 deben tener una caducidad de 3 meses en cuanto a claves de usuarios. Esto quiere decir que los usuarios deberán cambiar su clave obligatoriamente cada 3 meses, de lo contrario no podrán ingresar a los servidores.
- Las cuentas de usuario se bloquean automáticamente luego del tercer intento fallido de ingreso a la Red. Para el desbloqueo de la cuenta, el usuario deberá comunicarse con el departamento de redes de la Dirección de Desarrollo Institucional.
- Solamente el responsable de la cuenta o el Jefe superior del usuario pueden solicitar la intervención de una cuenta específica, de lo contrario éstas no pueden ser cambiadas.
- El Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional está facultado para realizar auditorias de las cuentas de usuario creadas en los servidores. Estas auditorias servirán para detectar si existen personas que quieren ingresar indebidamente a la red. Las auditorias se realizarán indistintamente. Los Vicepresidentes y Gerentes de área también pueden solicitar al Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional la auditoria de las cuentas por un tiempo determinado.
- De detectar que un usuario está haciendo mal uso de su cuenta, el Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional solicitará la sanción correspondiente a Recursos Humanos y procederá al bloqueo temporal de la misma, hasta que reciba las correspondientes disposiciones.
- Es obligación de los Responsables de Área comunicar cuándo un empleado sale de la empresa al Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional para actualizar la lista de usuarios de la red.
- La red de datos del IESS es para exclusiva utilización de trabajos relacionados con la Empresa. En caso que se detecte una mala

utilización de los recursos de la red se solicitará la sanción correspondiente a cada responsable de área.

- Cualquier adición de un Servidor con su respectivo Software para su funcionamiento en la Intranet deberá ser administrado por el departamento de Servidores.

PROCEDIMIENTOS

SOLICITUD CREACIÓN DE CUENTAS DE USUARIO

Para la solicitud de creación de cuentas de usuario en los servidores del IESS se deberá seguir el siguiente procedimiento:

- El Jefe superior del usuario que requiere la nueva cuenta deberá solicitar al Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional la creación de la misma con los diferentes servicios que necesita la persona, los principales son:

  Acceso a un servidor de la Red.
  Acceso a una Aplicación específica creada para la Intranet.

- El jefe del departamento de Servidores de la Dirección de Desarrollo Institucional asignará un Ingeniero de Soporte para la creación de la cuenta y de los diferentes servicios que se solicite, así como también la configuración del equipo del nuevo usuario.
- El jefe del departamento de Servidores bloqueará temporalmente una cuenta cuyo usuario haya salido de la empresa o se despidiera de la misma hasta recibir las instrucciones por parte de recursos humanos.
- El Ingeniero de Soporte reportará al jefe del departamento de Servidores de la Dirección de Desarrollo Institucional el cumplimiento del trabajo.

CREACIÓN DE CUENTAS DE USUARIO EN SERVIDORES SOLARIS

Para la creación de cuentas en servidores Solaris se deberá seguir el siguiente procedimiento:

- En la consola del servidor ingresar a: programas-Herramientas administrativas-Administrador de usuario de dominio.
- Escoger el Server en donde se va a crear la cuenta.
- Escoger en el menú principal Usuario-usuario nuevo, entonces se desplegará la ventana
- En la pantalla se ingresará el nombre de usuario. Para esto se llevará el siguiente estándar:

  La inicial del primer nombre y a continuación el primer apellido. Por ejemplo, si el usuario se llama Ricardo Adalberto Rodríguez Tuarez, el nombre de usuario será: rrodriguez

  Si existen algún otro usuario ya creado con el mismo nombre de usuario, luego la inicial del primer nombre se incrementará la inicial del segundo nombre. Si todavía se repite el nombre de usuario, al final del apellido se incrementará la inicial del segundo apellido. En caso de volver a repetirse al final del nombre se añadirá un número secuencial para los casos que existan.

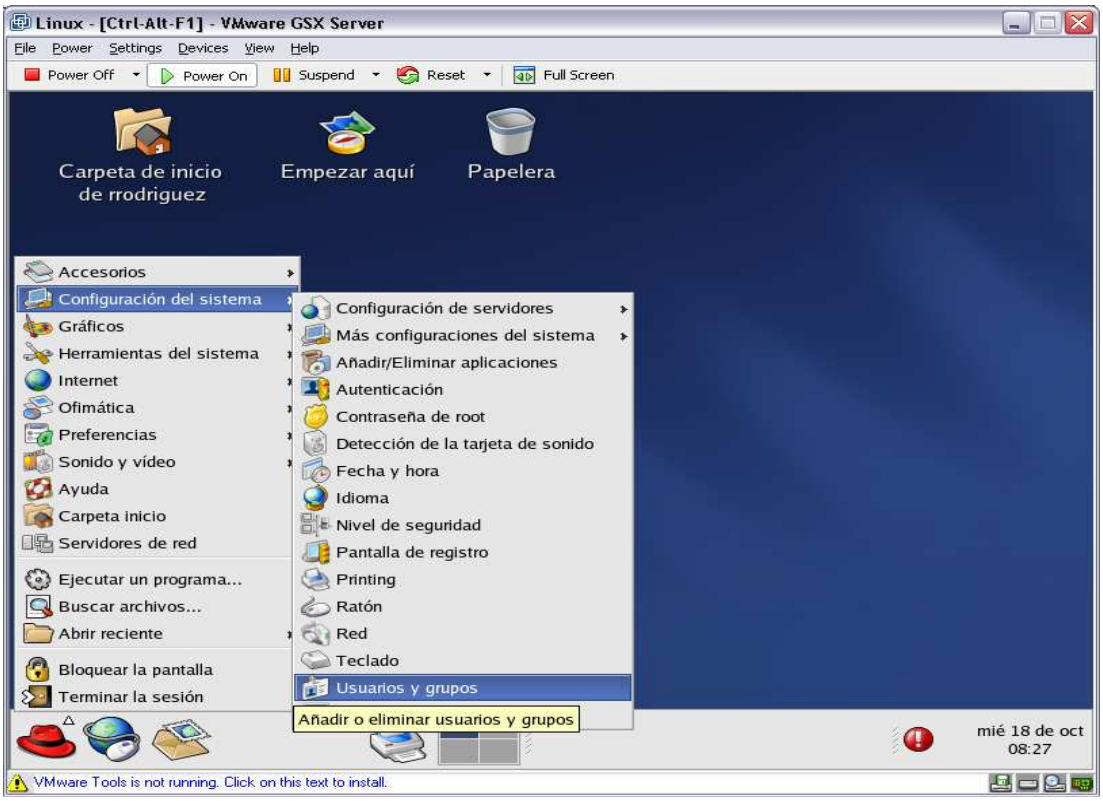
- Posteriormente se ingresará en el campo “Nombre Completo” el nombre completo de la persona.
- En el campo Descripción se ingresará la ciudad en donde trabaja y el departamento.
- En el campo Contraseña se ingresará el mismo nombre de usuario.
- Se dejara el visto en la opción: “El usuario debe cambiar la contraseña en el siguiente inicio de sesión”. Esto permitirá al usuario cambiar su contraseña al entrar por primera vez a la red, y luego periódicamente según instrucciones emitidas vía Correo para el efecto.
- En caso que el usuario pertenezca a un grupo de trabajo especial se le añadirá a este presionando en el botón de Grupos.
- Luego de realizar estos pasos, se deberá presionar el botón de Agregar.
- Con esto el usuario será agregado al dominio.

CREACIÓN DE CUENTAS DE USUARIO EN SERVIDORES RED HAT

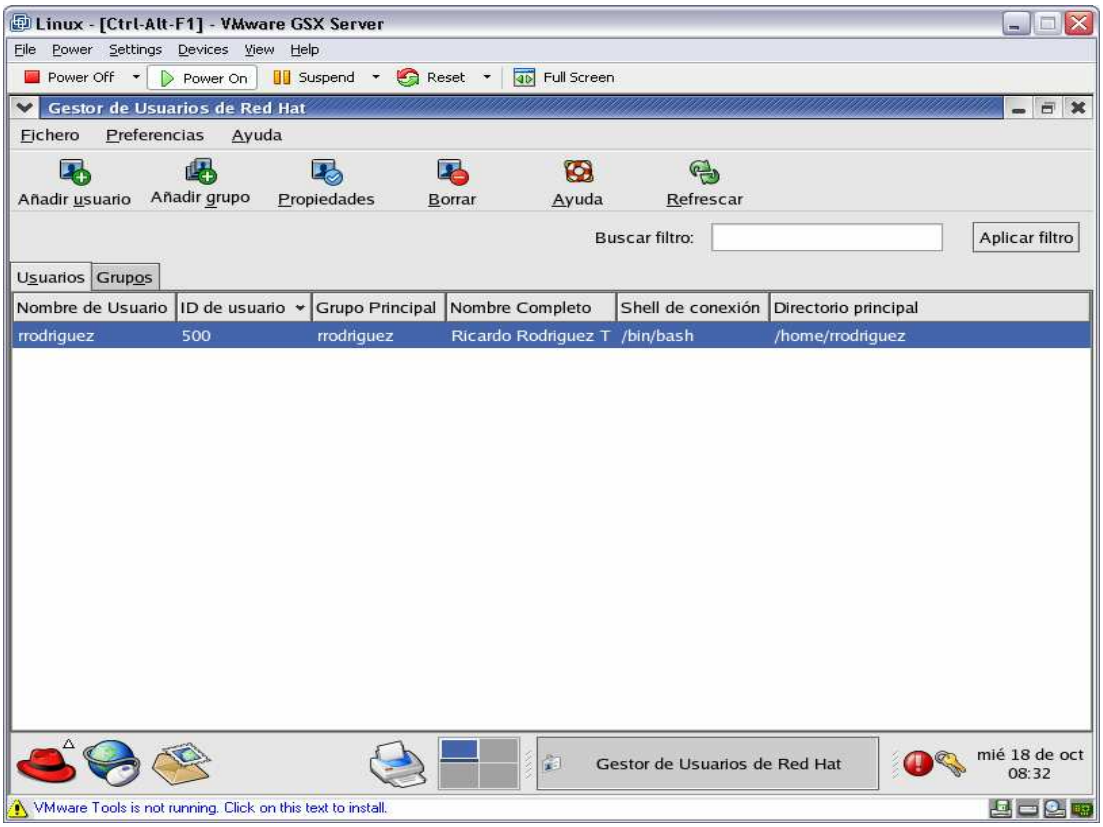
Para la creación de cuentas en servidores RED HAT se deberá seguir el siguiente procedimiento:

EN MODO GRÁFICO:

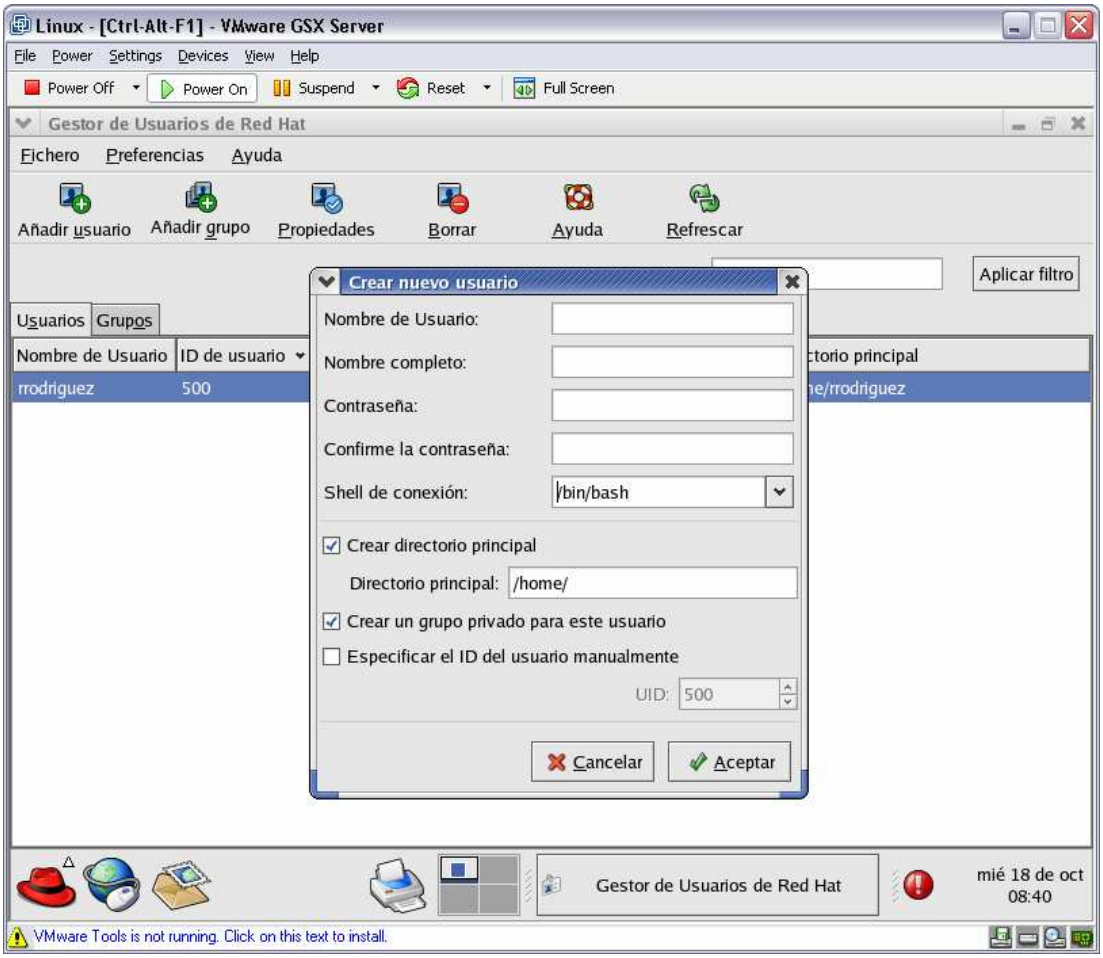
- En primera instancia debemos haber realizado Login en el servidor con el usuario root.
- Nos dirigimos al botón del menú principal, escogemos la opción configuración del sistema y en el submenú damos un clic en usuarios y grupos.



- A continuación se nos abrirá el gestor de usuarios de RED HAT



- Damos un clic en el botón que indica añadir usuario, y se nos desplegara una nueva ventana en la cual llenaremos la información personal del usuario, crearemos el directorio de trabajo del usuario, asignaremos una contraseña, y caso de que requiera grupo de trabajo se le creará o asignará el grupo solicitado.



SOLICITUD DE INTERVENCIÓN DE UNA CUENTA

La intervención de una cuenta se da por diferentes motivos, la más común es por el olvido de la contraseña. Para realizar este trabajo se seguirá el siguiente procedimiento.

- El responsable de la cuenta o el jefe del mismo solicitará al Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional el cambio de clave de la cuenta.
- El responsable del área de Servidores de la Dirección de Desarrollo Institucional asignará un Ingeniero de Soporte para realizar este trabajo.
- El Ingeniero de Soporte cambiará la contraseña con el nombre de usuario del responsable de la cuenta y habilitará la opción: “El usuario

debe cambiar la contraseña en el siguiente inicio de sesión", para que luego el usuario o el Jefe superior ingrese su contraseña secreta.

- Una vez terminado el trabajo, el Ingeniero de Soporte notificará el trabajo cumplido al usuario que solicitó y al responsable del área de Servidores de la Dirección de Desarrollo Institucional.

AUDITORIA A CUENTAS DE USUARIO

Para realizar la auditoria de las cuentas de usuario de los servidores Solaris se deberá seguir el siguiente procedimiento

- Los Vicepresidentes y Gerentes de área solicitarán al responsable del área de Servidores de la Dirección de Desarrollo Institucional la auditoria de las cuentas de usuario indicando el motivo de la misma.
- Dependiendo del motivo se levantarán las auditorias en el servidor.
- Una vez pasado el período de auditoria solicitado, al responsable del área de Servidores de la Dirección de Desarrollo Institucional enviará el informe respectivo a la persona que lo solicitó.

SOLICITUD DE ELIMINACIÓN DE CUENTAS DE USUARIO

Para la solicitud de eliminación de cuentas de usuario se deberá seguir el siguiente procedimiento:

- Cada responsable de área enviará una solicitud al Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional indicando la cuenta que debe ser eliminada.
- El Jefe del departamento de Servidores de la Dirección de Desarrollo Institucional bloqueará esta cuenta por una semana, para luego ser borrada definitivamente. Al borrar la cuenta, se borrará el acceso a todos los servicios de la red.

- El Jefe del departamento de Servidores notificará al Responsable del área solicitante cuando la cuenta haya sido borrada.

2. POLÍTICA PARA ADMINISTRACIÓN DE SERVIDORES

PROPÓSITOS

Normar la adquisición de Servidores por parte de IESS.

Normar la utilización de Servidores.

ALCANCE

Esta política es aplicable para todas las dependencias del IESS.

DEFINICIONES

- **Red de datos:** Red física compuesta por diferente tipo de cables y equipos de comunicación, que permite el envío y recepción de información de un equipo a otro.
- **Servidor:** Equipo que controla las seguridades y presta diferentes servicios en una red de datos.
- **Solaris 9:** Sistema operativo de red creado por Sun Micro Systems.
- **Red Hat Enterprise:** Sistema operativo de red creado por Red Hat.
- **Nombre de usuario:** Nombre con el que se le conocerá a un usuario en la red.
- **Contraseña de usuario:** Clave secreta que solamente el usuario dueño de una cuenta podrá saberla.

NORMAS

- De acuerdo a las necesidades de los usuarios del IESS, los equipos Servidores pueden ser reubicados por el personal de Administración Tecnológica.
- La autorización para la reubicación de equipos Servidores la emitirá el Gerente de Administración Tecnológica.
- La movilización o cambio de ubicación de cualquier equipo de computación deberá ser coordinada por el Gerente de Administración Tecnológica. con el fin de que se registre el cambio que se va a realizar. El cambio de responsable también se notificará por escrito al departamento de Inventarios.

- Si no se notifica la movilización del equipo, el responsable del equipo seguirá siendo el anterior usuario y tendrá que responder por todos los equipos y sus accesorios que tiene registrado en el departamento de Administración Tecnológica y en el departamento de Inventarios del IESS.
- Cualquier solicitud de compra de un equipo Servidor será evaluada por el departamento de Administración Tecnológica en representación del primero, quien emitirá un informe autorizando o negando la compra del equipo.
- Todo equipo Servidor que adquiere, el proveedor debe entregarlo con la configuración correspondiente. Previo el registro en bodegas, el proveedor debe entregar el equipo en el departamento de Administración Tecnológica para la verificación de sus características, registro de partes y licencias.
- Un técnico del departamento de Administración Tecnológica se encargará de verificar la entrega del equipo de acuerdo a las especificaciones solicitadas al proveedor por parte del IESS.
- Sólo los técnicos del departamento de Administración Tecnológica están autorizados a dar el visto bueno para la recepción del equipo por parte del IESS una vez que se haya verificado que el equipo tiene todos los dispositivos. Sólo este visto bueno autoriza realizar los trámites de pago al proveedor.
- Toda la documentación y software que llegue con el equipo será retirado por el técnico del departamento de Administración Tecnológica para su inventario y resguardo.
- El departamento de Administración Tecnológica no se responsabilizará de equipos Servidores que no pertenezcan al IESS.
- El departamento de Administración Tecnológica no se responsabilizará de equipos Servidores que hayan sido recibidos por algún personal del IESS sin la supervisión de uno de sus técnicos.
- Cuando los equipos Servidores son para provincias, se realizará la coordinación con la Gerencia de la Sucursal del IESS para el envío del mismo al destinatario.

- El usuario que firma el acta de entrega-recepción del equipo Servidor, es el único responsable del mismo. Si el usuario no firma esta acta, no se le entregará el equipo.
- Si la compra de un equipo Servidor nuevo es para sustituir uno antiguo, cuando llegue el equipo nuevo, el Ingeniero de Soporte del departamento de Administración Tecnológica retirará el equipo antiguo con el debido descargo, para que luego este equipo sea reasignado o dado de baja y su consiguiente notificación al Departamento de Inventarios para su respectivo registro.
- Toda entrega y retiro de equipos Servidores debe ir acompañada de una acta de entrega – recepción con la firma del responsable del Servidor.
- El departamento de Administración Tecnológica está facultada de escoger al funcionario que se le entregará un nuevo equipo que adquiera el IESS. La entrega del Servidor dependerá del cargo que tenga la persona y de las funciones que realice.

PROCEDIMIENTOS

ADQUISICIÓN DE UN NUEVO EQUIPO SERVIDOR

Para la adquisición de un nuevo equipo Servidor, se seguirá el siguiente procedimiento:

- El jefe del departamento donde se necesita el equipo Servidor deberá enviar un comunicado (vía oficio o correo electrónico) al Gerente del departamento de Administración Tecnológica indicando las razones por las que se necesita adquirir un nuevo equipo Servidor.
- Una vez recibido el comunicado, El Gerente del departamento de Administración Tecnológica asignará personal para que realice una inspección del lugar verificando la necesidad del equipo.
- El Gerente del departamento de Administración Tecnológica emitirá el informe respectivo al jefe del departamento que solicitó el equipo Servidor, aprobando o negando su compra. Si aprueba, en el informe deberá constar las características técnicas del mismo.

INSTALACIÓN DE UN NUEVO EQUIPO SERVIDOR EN QUITO

Para la instalación de un nuevo equipo Servidor en el perímetro urbano de Quito se seguirá el siguiente proceso:

- Una vez que el IESS adquiera el equipo Servidor, éste será entregado al departamento de Administración Tecnológica, una vez que haya hecho los trámites respectivos en bodega. El equipo deberá ser abierto con el fin de que se constate las especificaciones solicitadas, junto con sus implementos y manuales.
- Si el equipo Servidor está con todas las características especificadas, el técnico del departamento de Administración Tecnológica dará el visto bueno para la recepción del equipo por parte del IESS, caso contrario se devolverá al proveedor a fin de que entregue el equipo cumpliendo con las especificaciones solicitadas por el IESS.
- El técnico del departamento de Administración Tecnológica procederá a copiar el número de serie del equipo y traerá la información junto con el software y la documentación que llegó con el equipo. Toda esta información será ingresada en el Sistema de control de equipos del departamento de Administración Tecnológica.
- El técnico del departamento de Administración Tecnológica configurará el equipo Servidor de acuerdo al ambiente de trabajo del IESS.
- El técnico del departamento de Administración Tecnológica firmará el acta entrega – recepción con el responsable del equipo y notificará este particular al Departamento de Inventarios.

INSTALACIÓN DE NUEVO EQUIPO SERVIDOR FUERA DE QUITO

Para la instalación de un nuevo equipo Servidor fuera del perímetro urbano de Quito se seguirá el siguiente proceso:

- Una vez que se adquiera el equipo de computación, éste será entregado al departamento de Administración Tecnológica, una vez que haya hecho los trámites respectivos en bodega. El equipo

deberá ser abierto con el fin de que se constate que el Servidor haya llegado con todas especificaciones solicitadas, junto con sus implementos y manuales.

- Si el equipo Servidor está con todas las características especificadas, el técnico del departamento de Administración Tecnológica dará el visto bueno para la recepción del equipo por parte del IESS, caso contrario se devolverá al proveedor a fin de que entregue el equipo cumpliendo con las especificaciones solicitadas por el IESS.
- El técnico del departamento de Administración Tecnológica procederá a copiar los números de serie del equipo y traerá la información junto con el software y documentación que llegó con el equipo.
- El técnico del departamento de Administración Tecnológica configurará el equipo de acuerdo al ambiente de trabajo del IESS.
- La Gerencia de la Sucursal del IESS firmará el acta entrega – recepción con el responsable del equipo Servidor y notificará este particular al Departamento de Inventarios.

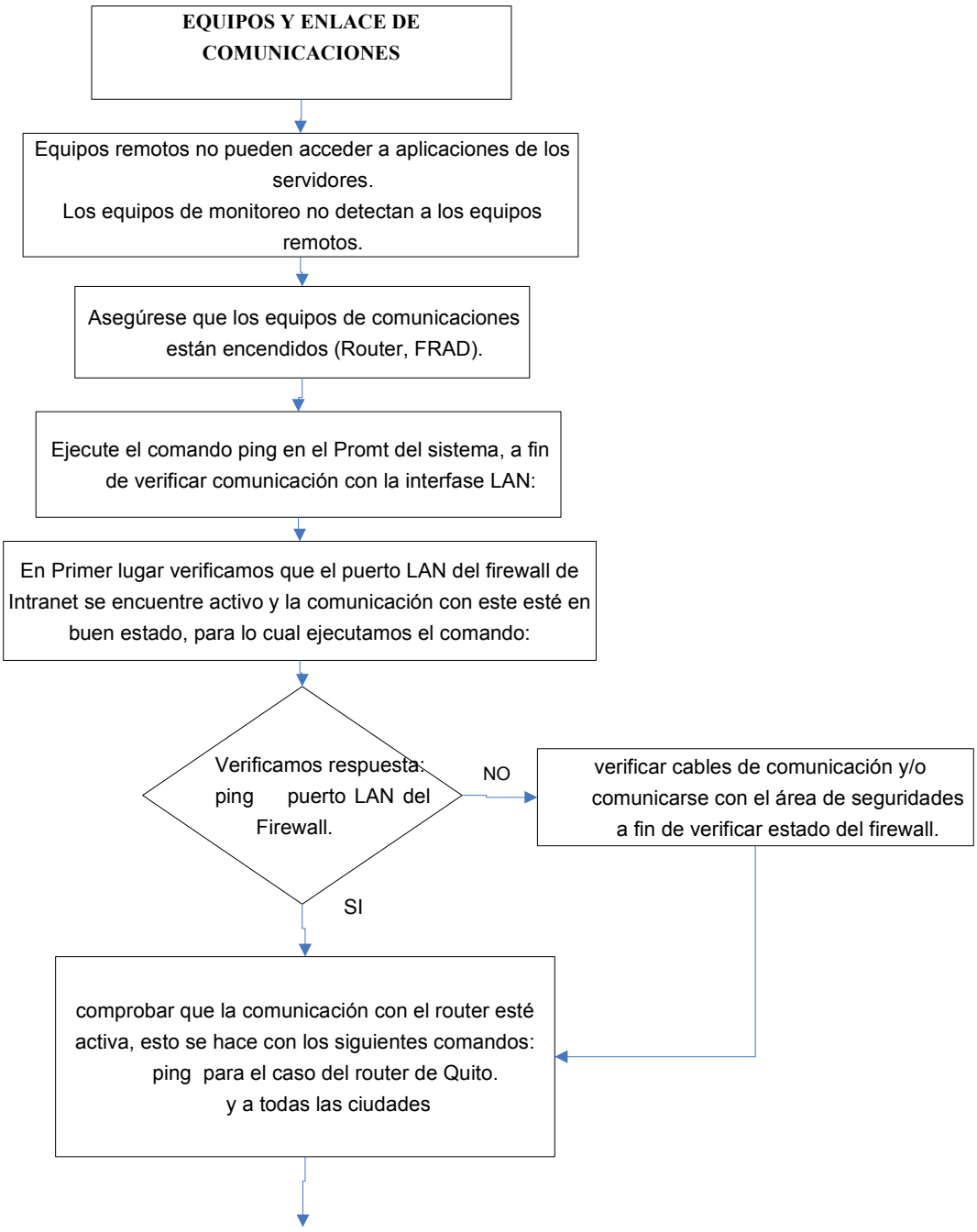
REUBICACIÓN DE UN EQUIPO SERVIDOR

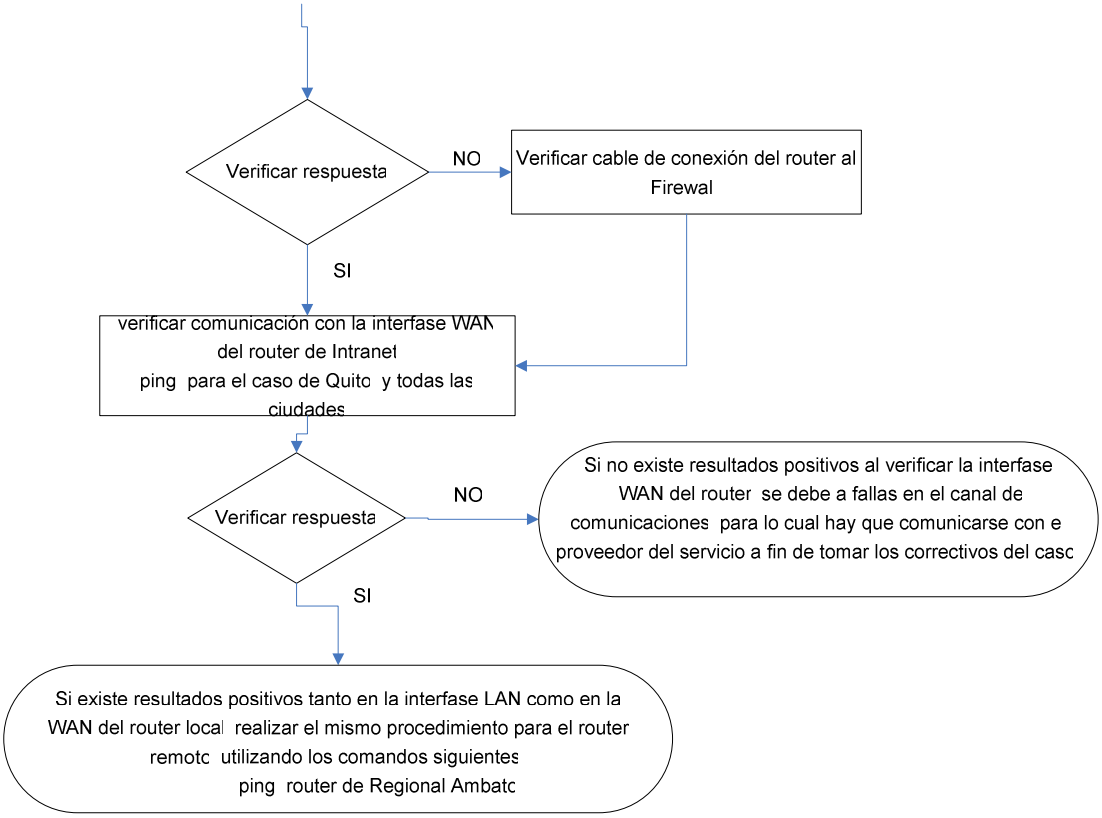
Para reubicar un equipo Servidor se debe seguir el siguiente procedimiento.

- El Jefe del departamento donde se quiere reubicar un equipo Servidor enviará un comunicado al departamento de Administración Tecnológica indicando este particular.
- El departamento de Administración Tecnológica asignará un técnico para recibir el equipo, firmando un acta de entrega recepción provisional. Posteriormente irá al lugar en donde se va a reubicar el equipo para configurarlo.

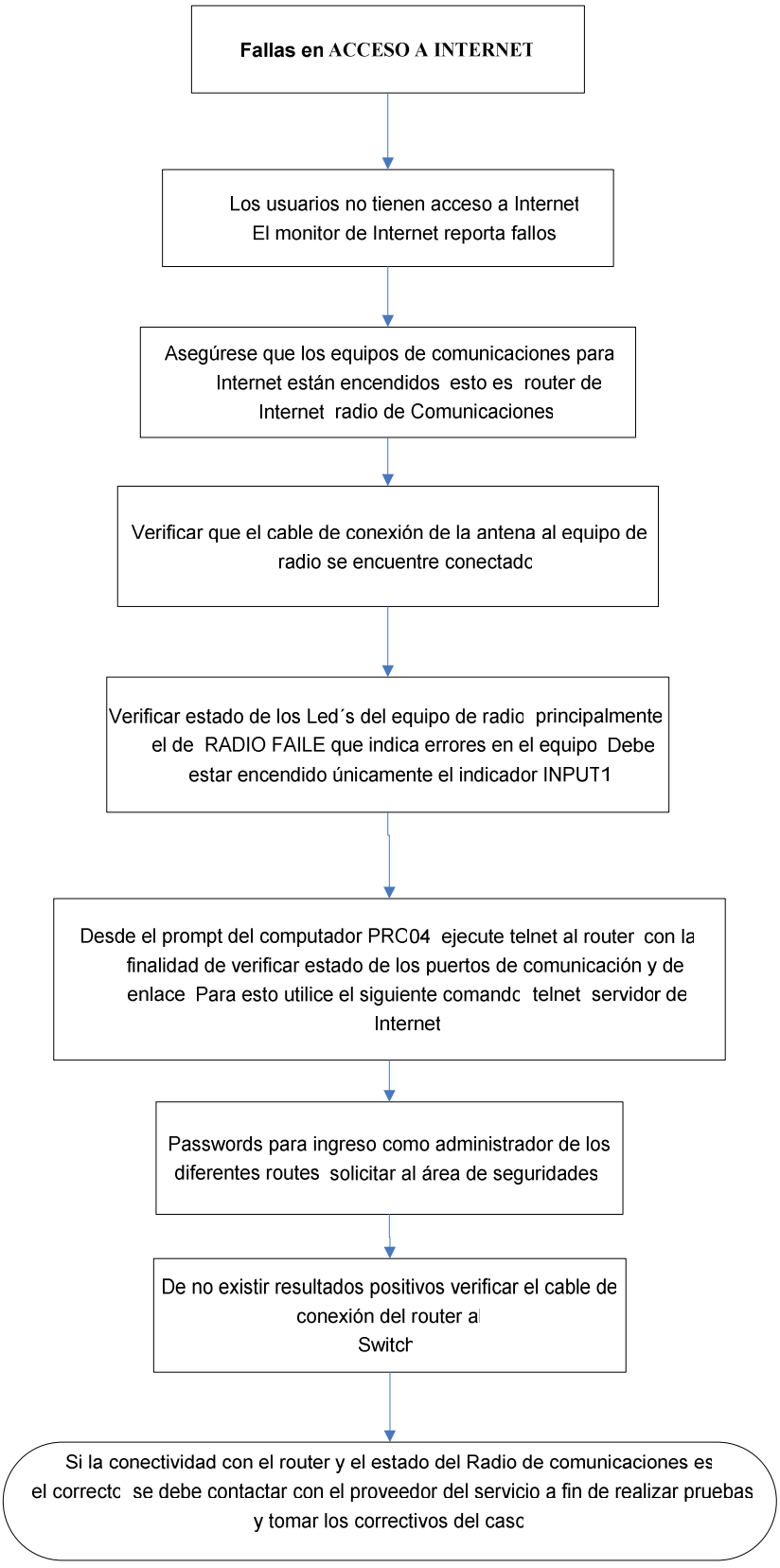
El departamento de Administración Tecnológica se encargará de hacer firmar el acta de entrega - recepción al nuevo usuario y recopilará los datos necesarios para actualizar el sistema de control de equipos y luego la notificación escrita al Departamento de Inventarios.

3. DIAGRAMA DE FLUJO EQUIPOS Y ENLACES DE COMUNICACIONES

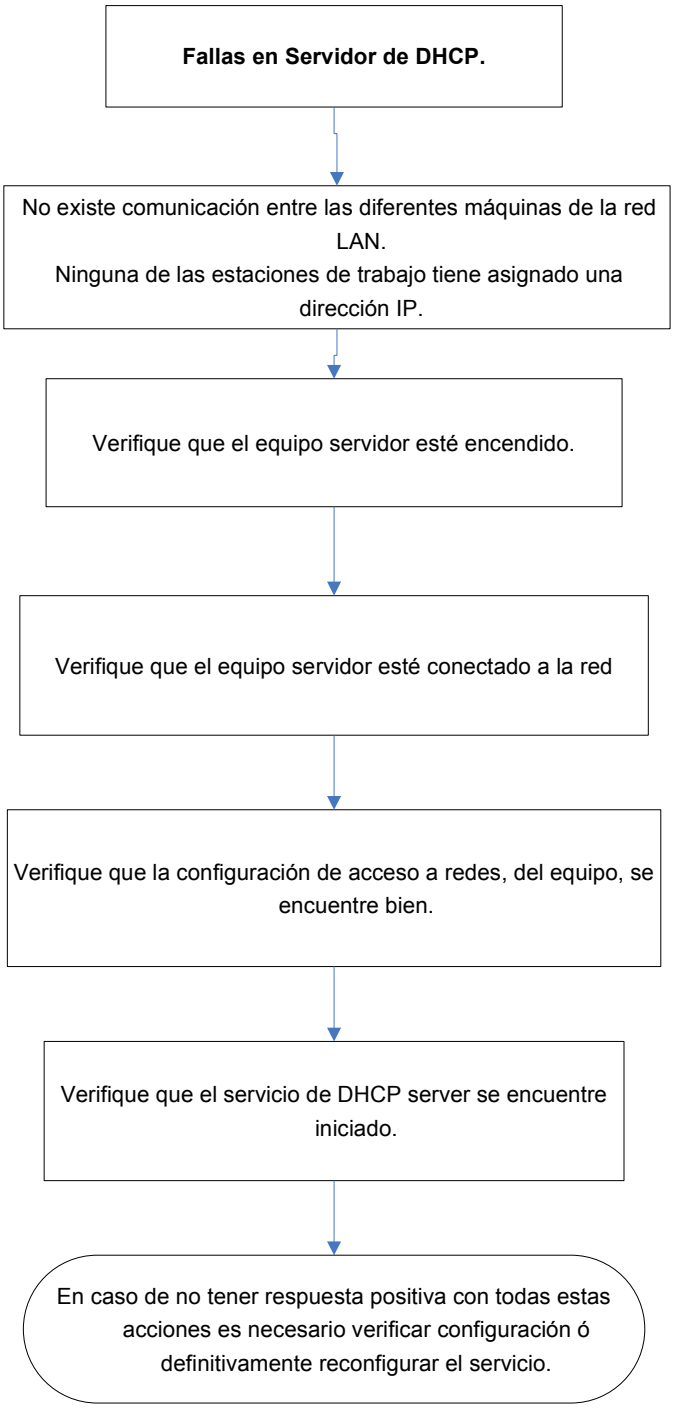



Verificar respuesta
NO
Verificar cable de conexión del router al Firewal
SI
verificar comunicación con la interfase WAN del router de Intranet ping para el caso de Quito y todas las ciudades
Verificar respuesta
NO
Si no existe resultados positivos al verificar la interfase WAN del router se debe a fallas en el canal de comunicaciones para lo cual hay que comunicarse con e proveedor del servicio a fin de tomar los correctivos del casc
SI
Si existe resultados positivos tanto en la interfase LAN como en la WAN del router local realizar el mismo procedimiento para el router remotc utilizando los comandos siguientes ping router de Regional Ambatc

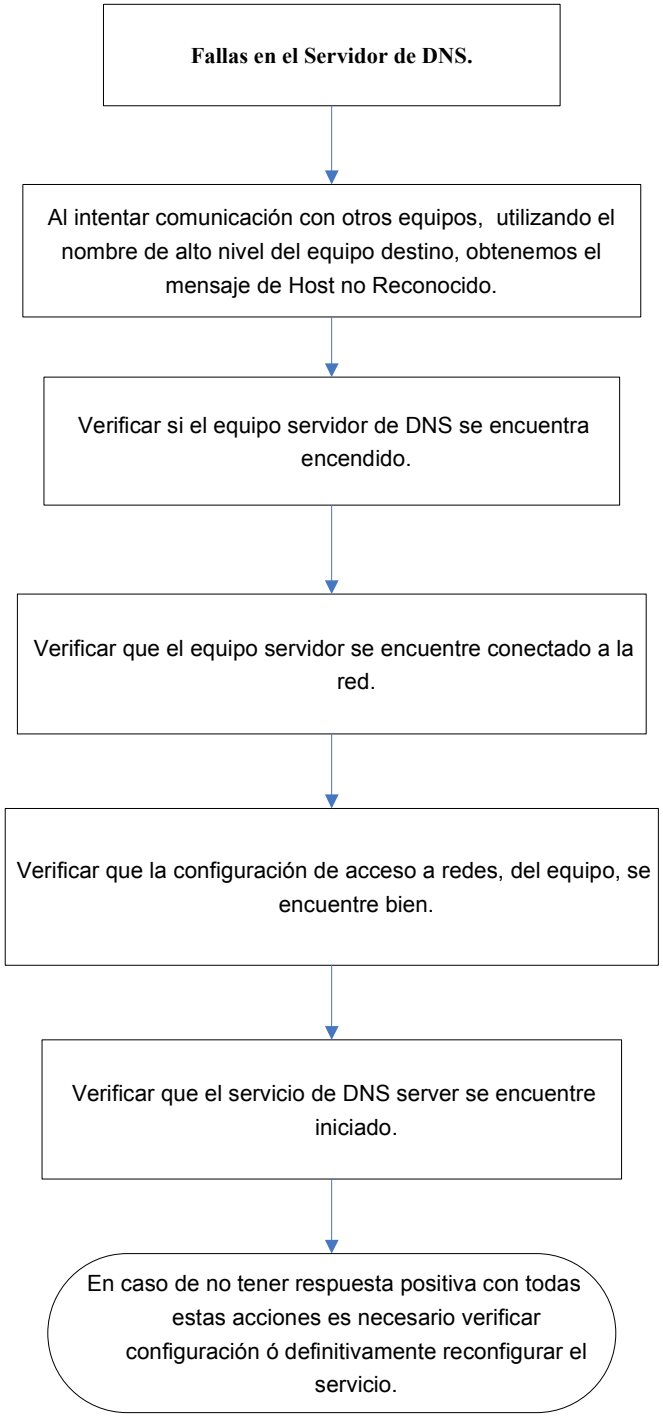
4. DIAGRAMA DE FLUJO FALLAS DE ACCESO A INTERNET



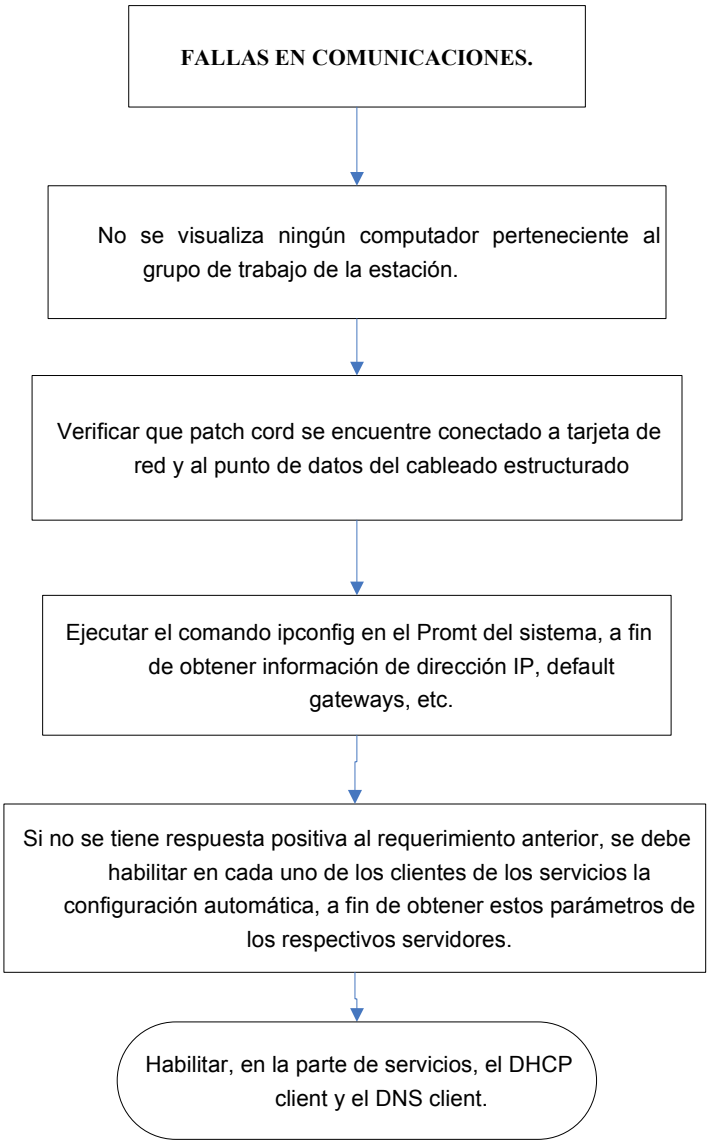
5. DIAGRAMA DE FLUJO FALLAS EN SERVIDOR DHCP



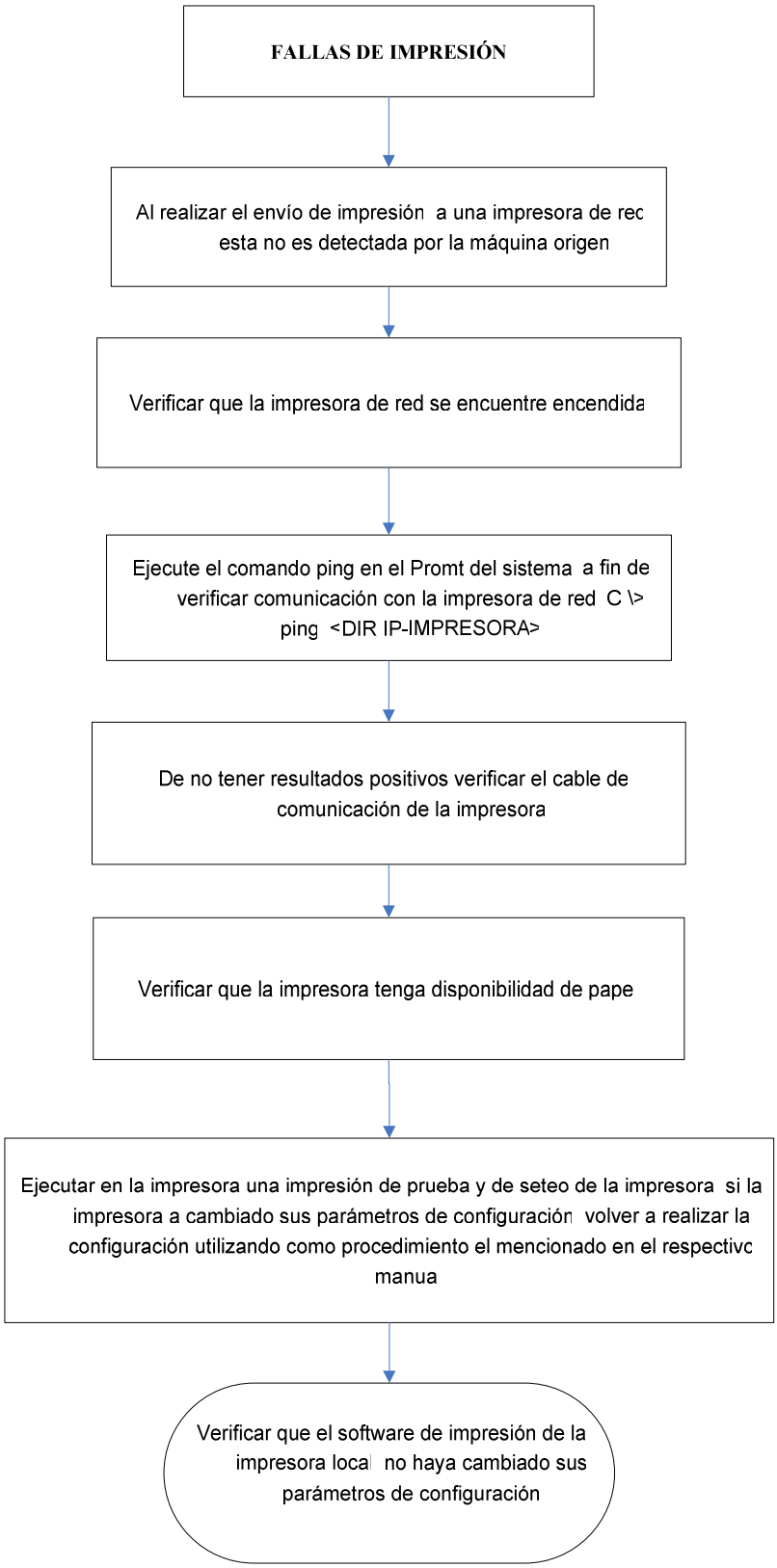
6. DIAGRAMA DE FLUJO EN SERVIDOR DNS



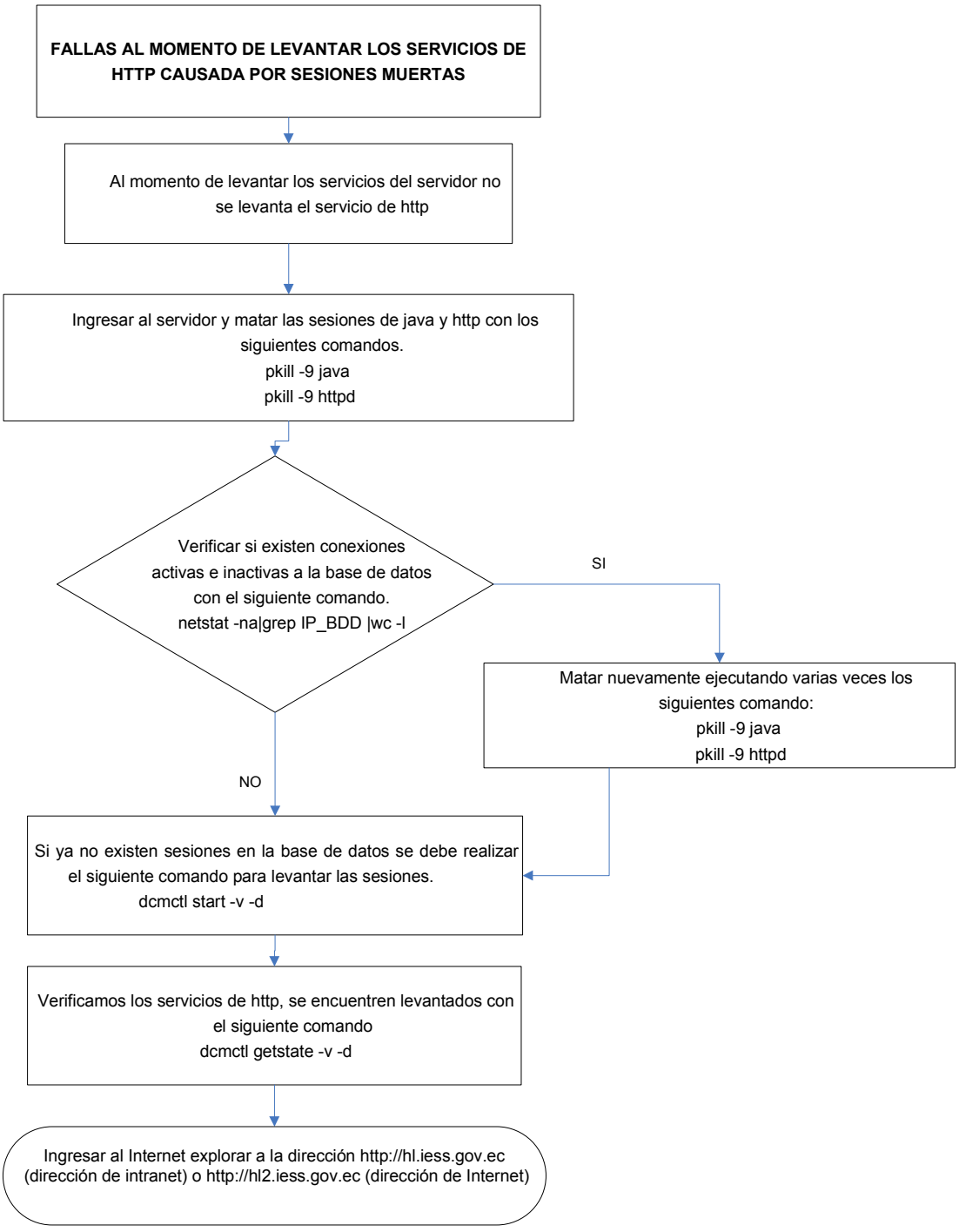
7. DIAGRAMA DE FLUJO FALLAS EN COMUNICACIONES



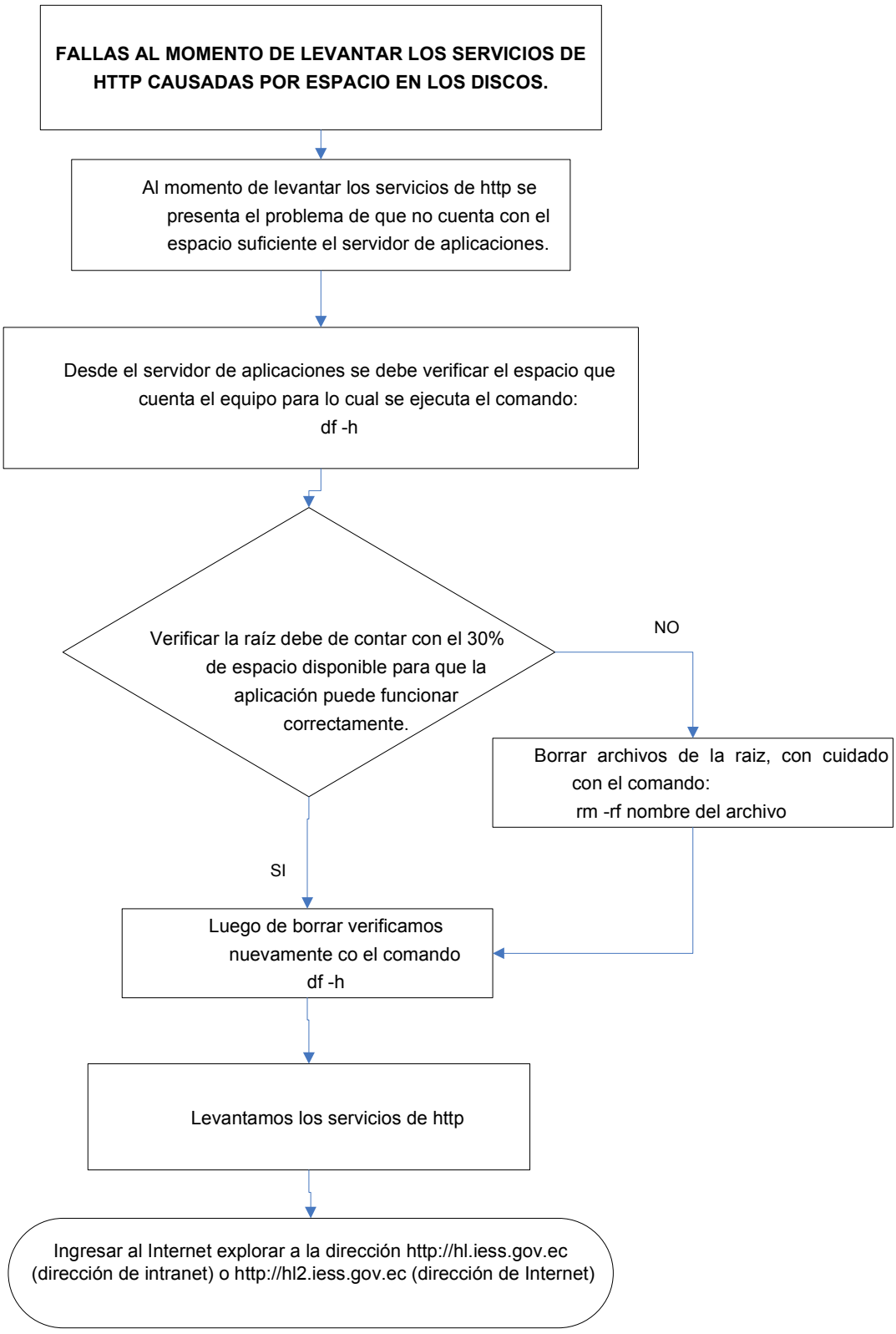
8. DIAGRAMA DE FLUJO FALLAS DE IMPRESIÓN



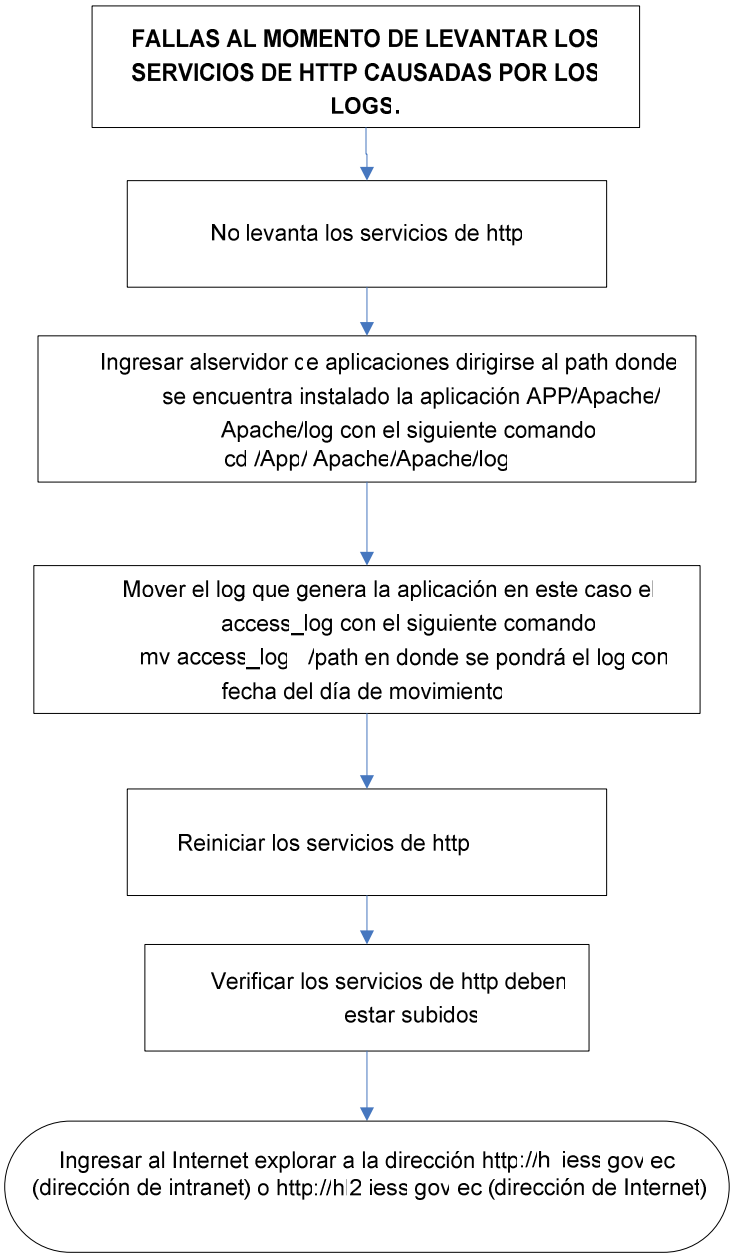
9. DIAGRAMA DE FLUJO FALLAS AL MOMENTO DE LEVANTAR HTTPS DEBIDO A SESIONES MUERTAS



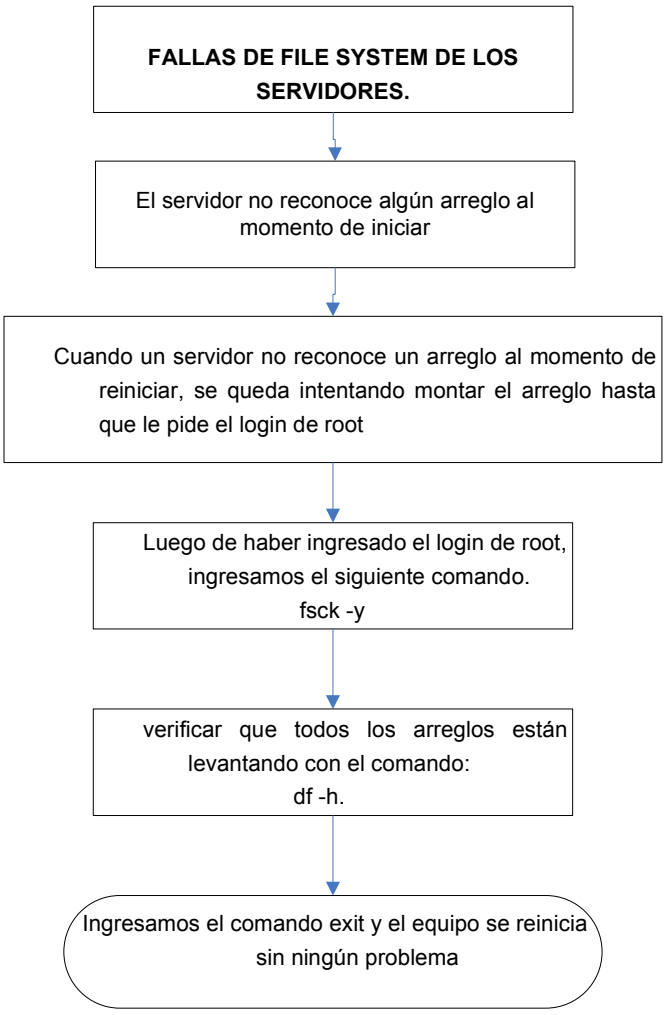
10. DIAGRAMA DE FLUJO FALLAS AL MOMENTO DE LEVANTAR HTTPS DEBIDO A ESPACIO EN DISCO



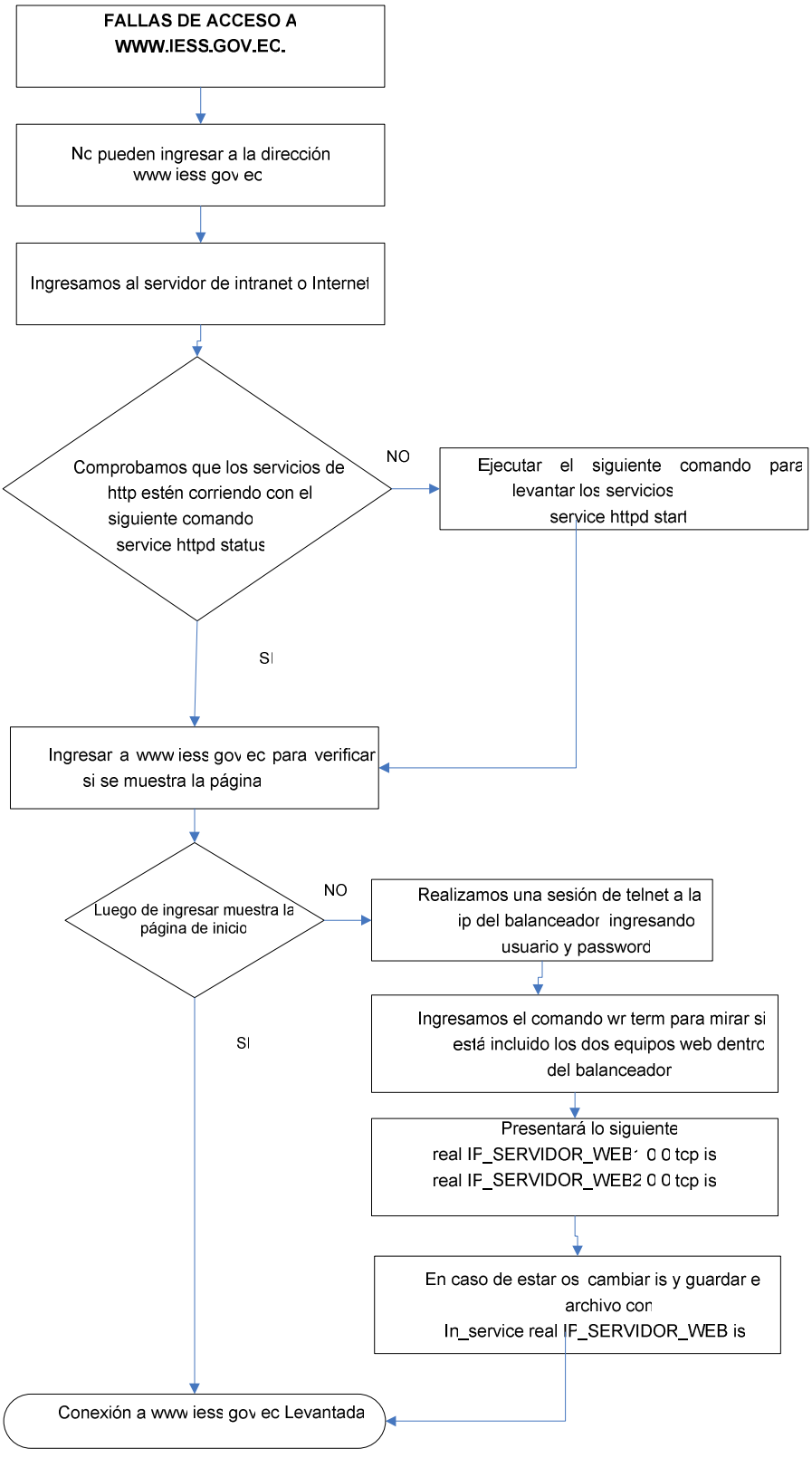
11. DIAGRAMA DE FLUJO FALLAS AL MOMENTO DE LEVANTAR HTTPS DEBIDO A LOGS



12. DIAGRAMA DE FLUJO FALLA DE FILE SYSTEM DE LOS SERVIDORES



13. DIAGRAMA DE FLUJO FALLA DE ACCESO A WWW.IESS.GOV.EC



14. DIAGRAMA DE FLUJO APAGAR LOS SERVIDORES EN CASO DE FALLA EN LA CORRIENTE ELECTRICA