UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERÍA
Especialización en Sistemas de Información

Trabajo Especial de Grado

DISEÑO DE UN SISTEMA DE SEGURIDAD PARA REDES DE DATOS DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN

Presentado por:
Jaspe Díaz, Harry José;
Para optar por el título de
Especialista en Sistemas de Información

Asesor
Dr. Bonillo, Pedro

Caracas, Julio de 2011

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE INGENIERÍA
Especialización en Sistemas de Información

Trabajo Especial de Grado

DISEÑO DE UN SISTEMA DE SEGURIDAD PARA REDES DE DATOS DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN

Presentado por:
Jaspe Díaz, Harry José;
Para optar por el título de
Especialista en Sistemas de Información

Asesor
Dr. Bonillo, Pedro

Caracas, Julio de 2011

Caracas, 05 de Julio de 2011

Universidad Católica Andrés Bello
Dirección General de los Estudios de Postgrado
Postgrado Sistemas de Información
Ciudad.-

Por medio de la presente me permito comunicar que he sido el asesor del Trabajo Especial de Grado titulado "Diseño de un Sistema de Seguridad para Redes de Datos del Ministerio del Poder Popular para la Educación", elaborado por el Ingeniero Jaspe Díaz, Harry José, C.I. 6.869.193, para optar al título de Especialista en Sistemas de Información.

Sin otro particular al cual hacer referencia, se despide.

Atentamente,

Dr. Pedro Bonillo
C.I. 10.868.538

DEDICATORIA

A Dios… porque es bueno y su amor es eterno…!

A Isabel Díaz, mi madre, gracias por tu amor incondicional y tu apoyo.

A Ulices Maldonado, mi amigo y maestro, por enseñarme el arte de vencer las dificultades mediante la constancia y la tenacidad.

RECONOCIMIENTOS

El presente reconocimiento al Dr. Pedro Bonillo, tutor de la presente investigación, a la Prof. María Esther Remedios y al Prof. Alberto Rodríguez, por el apoyo prestado.

Agradezco a mis compañeros de trabajo, Wilfer Osorio, Carlos Botia, Yomar Vera, Jaqueline Ulgiati y Neida Rivas. En especial a Norelis Monteverde y Raquel González, por la colaboración prestada para el desarrollo de la presente investigación.

También agradezco a mi compañero de estudios, el Lic. Felipe Hernández, por el apoyo prestado.

Especial reconocimiento al personal docente del Post-Grado en Sistemas de Información de la Universidad Católica Andrés Bello (UCAB), cuya dedicación y profesionalismo superaron todas mis expectativas.

A todos mi sentido de agradecimiento, por su colaboración y amistad, por brindarme su comprensión, tiempo y dedicación.

¡A todos gracias!

TABLA DE CONTENIDO

TABLA DE CONTENIDO VI

LISTA DE TABLAS XI

LISTA DE FIGURAS XIII

RESUMEN XV

INTRODUCCIÓN 16

CAPITULO I 21

PLANTEAMIENTO DEL PROBLEMA 21

PROBLEMA DE INVESTIGACIÓN 21
FORMULACIÓN DEL PROBLEMA 25
OBJETIVOS DE LA INVESTIGACIÓN 26
Objetivo general *26*
Objetivos específicos *26*
JUSTIFICACIÓN DE LA INVESTIGACIÓN 27
ALCANCE Y LIMITACIONES 28

CAPITULO II 30

MARCO TEÓRICO 30

ANTECEDENTES DE LA INVESTIGACIÓN 30
BASES TEÓRICAS 37
Seguridad de la Información *37*
Sistemas de información 38
Definición de seguridad de información 39
Necesidad de la seguridad de la información 40
Vulnerabilidad, amenazas y ataques 41
Clasificación de los ataques de red 45
Ataques internos, externos, pasivos y activos 46
Denegación de servicio 46
Suplantación de identidad 46
Ataques Sybil 47
Principios de Seguridad 47
Confidencialidad 47
Integridad 48
Disponibilidad 49
Identificación 49
Autentificación 49
Autorización 50
Auditabilidad 50
Funcionalidad Vs. Seguridad 50
Privacidad 51
No Repudio 51
Cifrado 51
Redes *52*
Definición 52
Tipo de redes 53

Redes LAN 53
Redes MAN 53
Redes WAN 53
Metro Ethernet 54
Redes inalámbrica 54
Frame relay 54
Medios de transporte o transmisión de datos 55
Par trenzado 55
Fibra óptica 56
Dispositivos activos de red 56
Repetidor o concentrador 56
Puentes 57
Encaminadores o routers 57
Pasarelas 57
Seguridad en redes de datos. *57*
Antecedentes e importancia de la seguridad de redes 58
Calidad de servicio 59
Seguridad del enrutamiento 59
Software malicioso 60
Cortafuegos o firewall 61
Gestión de red 62
Proxy 62
Normas internacionales de seguridad *62*
CobiT 4.1 62
Grupos Objetivos de CobiT 63
ITIL V3 65
Normas ISO, Serie 27000 66
MARCO ORGANIZACIONAL 67
Ministerio del Poder Popular para la Educación *67*
BASES ÉTICAS Y LEGALES 69

CAPITULO III 71

MARCO METODOLÓGICO 71

NIVEL DE INVESTIGACIÓN 71
DISEÑO DE INVESTIGACIÓN 72
TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS 73
Población y muestra *75*
Instrumentos de recolección de datos *76*
Medición, validez y confiabilidad *77*
Las variables, sus dimensiones e indicadores *79*
Definición operacional 80
Definición operacional de la presente investigación 81
Operacionalización de las variables de la presente investigación 82
TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS 88

CAPÍTULO IV 91

RESULTADOS OBTENIDOS, ANÁLISIS E INTERPRETACIÓN 91

INVESTIGACIÓN DE CAMPO 91
Resultados de la Investigación de Campo *91*
Marco Organizacional para la seguridad de la información y de las redes de datos en del MPP Educación 91
Estructura organizacional 91
Políticas y normas de seguridad 92

Planes de seguridad 93
Amenazas 93
Procedimientos para enfrentar amenazas 93
Vulnerabilidades 94
Control de vulnerabilidades 94
Seguimiento de reportes de vulnerabilidades 94
Gestión de usuarios 95
Registro de usuarios. 95
Otorgamiento de roles y privilegios 95
Normativas sobre el uso de contraseñas 96
Registros y auditorías 96
Auditoría de sistemas 96
Logs de los sistemas 98
Sincronización de relojes 101
Código malicioso o virus 101
Control de propagación de código malicioso 101
Continuidad 102
Desempeño futuro 102
Umbrales de servicio 102
Planes de continuidad 103
Contingencia y recuperación 104
Identificación de amenazas y de recursos críticos 104
Planes y programas 104
Soporte de terceras partes en los procesos de contingencia y recuperación 105
Seguridad en las redes de datos 105
Planes y programas para el desarrollo de las redes de datos 105
Separación de redes 107
Políticas y normas 108
Seguridad física 109
Acceso físico 109
Control de Errores 110
Adiestramiento 110
Síntesis de resultados 111
Análisis de los resultados obtenidos en la investigación de campo *111*
Marco Organizacional para la seguridad de la información y de las redes de datos en del MPP Educación 111
Amenazas 112
Vulnerabilidades 112
Gestión de usuarios 112
Registros y auditorías 112
Código malicioso o virus 113
Continuidad 113
Contingencia y recuperación 113
Seguridad en las redes de datos 113
Seguridad física 114
Control de errores 114
Percepción general de seguridad 114
Análisis de las Debilidades, Oportunidades, Fortalezas y Amenazas (DOFA) *114*
INVESTIGACIÓN DOCUMENTAL 116
Resultados de la investigación Documental *116*
Alineación CobiT, ITIL, ISO 270002 116
Esquema de implementación CobiT, ITIL e ISO/IEC 27002 117
Elaboración 118
Priorización 119
Planificación 120
Evitar Obstáculos 122

Alinear las mejores prácticas 123
Gerencia de la Seguridad 123
Análisis de los resultados obtenidos en la investigación documental 125
Características del sistema de redes del MPP Educación 128
Características del Diseño *130*
DISEÑO DEL SISTEMA DE SEGURIDAD PARA LAS REDES DE DATOS DEL MPP EDUCACIÓN 133
CAPÍTULO V **151**
CONCLUSIONES Y RECOMENDACIONES **151**
CONCLUSIONES 151
RECOMENDACIONES 155
CAPÍTULO VI **157**
LA PROPUESTA **157**
CONSIDERACIONES GENERALES 157
OBJETIVO DE LA PROPUESTA 157
JUSTIFICACIÓN DE LA PROPUESTA 157
BENEFICIOS DE LA PROPUESTA 157
LOCALIZACIÓN FÍSICA Y COBERTURA ESPACIAL 158
EVALUACIÓN 158
ESTUDIO DE FACTIBILIDAD O VIABILIDAD. 159
DESCRIPCIÓN DE LA PROPUESTA 160
REFERENCIAS BIBLIOGRÁFICAS **179**
ANEXO A **183**
CUESTIONARIO **183**
ANEXO B **190**
CONSTANCIA DE VALIDACIÓN **190**
ANEXO C **194**
COBIT 4.1, ESTRUCTURA Y DOMINIOS **194**
ESTRUCTURA DE COBIT 195
COBIT: DOMINIOS Y PROCESOS 195
DESCRIPCIÓN DE LOS DOMINIOS 199
Planificación y Organización (PO) *199*
Adquisición e Implementación (AI) *200*
Entrega y Soporte (DS) *202*
Monitoreo y Evaluación (ME) *204*
COBIT Y LOS RECURSOS DE TI 204
CRITERIOS DE CALIDAD 206
COBIT COMO MARCO DE GOBIERNO DE TI 208
CobiT como Marco de Control *208*
Área de negocios *208*
Proceso de Orientación *209*
Aceptabilidad General *209*
Requisitos regulatorios *210*
Lenguaje Común *210*
PRINCIPIOS DE GOBIERNO DE TI 211

Dirección y control 211
Responsabilidad 211
Rendición de cuentas 211
ACTIVIDADES DE TI 212
Áreas de enfoque de Gobierno de TI 212

ANEXO D 214

ITIL V 3.0 214

DEFINICIÓN DE SERVICIO DE GESTIÓN 215
SERVICIO DE GESTIÓN DE LA TECNOLOGÍA 215
CICLO DE VIDA DE LOS SERVICIOS EN ITIL V3 217
CONTENIDO DE ITIL V3 222
Introducción a las funciones y procesos 222

ANEXO E 226

SERIE ISO/IEC 27000 226

LA SERIE 27000 227
ISO/IEC 27000 227
ISO/IEC 27001 227
ISO/IEC 27002 227
ISO/IEC 27003 229
ISO/IEC 27004 229
ISO/IEC 27005 229
ISO 27006 230
ISO/IEC 27011 230
ISO/IEC 27033 230
ISO/IEC 27799 231

ANEXO F 232

ALINEACIÓN COBIT 4.1, ITIL V3 E ISO/IEC 27002 232

TABLA 52. ALINEACIÓN COBIT 4.1, ITIL V3 E ISO/IEC 27002 233

LISTA DE TABLAS

TABLA 1. SEGURIDAD DEL ENRUTAMIENTO 59
TABLA 2. DEFINICIÓN OPERACIONAL 81
TABLA 3. OPERACIONALIZACIÓN DE LAS VARIABLES 82
TABLA 4. RESPUESTA AL ÍTEM 1 91
TABLA 5. RESPUESTA AL ÍTEM 2 92
TABLA 6. RESPUESTA AL ÍTEM 3 92
TABLA 7. RESPUESTA AL ÍTEM 4 93
TABLA 8. RESPUESTA AL ÍTEM 5 93
TABLA 9. RESPUESTA AL ÍTEM 6 94
TABLA 10. RESPUESTA AL ÍTEM 7 94
TABLA 11. RESPUESTA AL ÍTEM 8 95
TABLA 12. RESPUESTA AL ÍTEM 9 95
TABLA 13. RESPUESTA AL ÍTEM 10 96
TABLA 14. RESPUESTA AL ÍTEM 11 96
TABLA 15. RESPUESTA AL ÍTEM 12 97
TABLA 16. RESPUESTA AL ÍTEM 13 97
TABLA 17. RESPUESTA AL ÍTEM 14 98
TABLA 18. RESPUESTA AL ÍTEM 15 98
TABLA 19. RESPUESTA AL ÍTEM 16 99
TABLA 20. RESPUESTA AL ÍTEM 17 99
TABLA 21. RESPUESTA AL ÍTEM 18 100
TABLA 22. RESPUESTA AL ÍTEM 19 100
TABLA 23. RESPUESTA AL ÍTEM 20 101
TABLA 24. RESPUESTA AL ÍTEM 21 101
TABLA 25. RESPUESTA AL ÍTEM 22 102
TABLA 26. RESPUESTA AL ÍTEM 23 102
TABLA 27. RESPUESTA AL ÍTEM 24 103
TABLA 28. RESPUESTA AL ÍTEM 25 103
TABLA 29. RESPUESTA AL ÍTEM 26 104
TABLA 30. RESPUESTA AL ÍTEM 27 104
TABLA 31. RESPUESTA AL ÍTEM 28 105
TABLA 32. RESPUESTA AL ÍTEM 29 105
TABLA 33. RESPUESTA AL ÍTEM 30 106
TABLA 34. RESPUESTA AL ÍTEM 31 106
TABLA 35. RESPUESTA AL ÍTEM 32 107
TABLA 36. RESPUESTA AL ÍTEM 33 107
TABLA 37. RESPUESTA AL ÍTEM 34 108
TABLA 38. RESPUESTA AL ÍTEM 35 108
TABLA 39. RESPUESTA AL ÍTEM 36 109
TABLA 40. RESPUESTA AL ÍTEM 37 109
TABLA 41. RESPUESTA AL ÍTEM 38 110
TABLA 42. RESPUESTA AL ÍTEM 39 110
TABLA 43. SÍNTESIS DE RESULTADOS 111

TABLA 44. ANÁLISIS DE LA DEBILIDADES, OPORTUNIDADES, FORTALEZAS Y AMENAZAS (DOFA) 115
TABLA 45. BASE DE NORMAS INTERNACIONALES UTILIZADAS PARA EL DISEÑO DEL SISTEMA DE SEGURIDAD PARA LAS REDES DE DATOS DEL MPP EDUCACIÓN. 132
TABLA 46. DISEÑO DEL SISTEMA DE SEGURIDAD PARA LAS REDES DE DATOS DEL MPP EDUCACIÓN. 134
TABLA 47. RECOMENDACIONES AL MPP EDUCACIÓN. 148
TABLA 48. ANÁLISIS DOFA DE LA PROPUESTA PRESENTADA. 159
TABLA 49. DISEÑO DEL SISTEMA DE SEGURIDAD PARA LAS REDES DE DATOS DEL MPP EDUCACIÓN. 162
TABLA 50. RECOMENDACIONES AL MPP EDUCACIÓN. 176
TABLA 51. ASPECTOS DE LA FORMULACIÓN DEL PROBLEMA 198
TABLA 52. ALINEACIÓN COBIT 4.1, ITIL V3 E ISO/IEC 27002 233

LISTA DE FIGURAS

FIGURA 1. MODELO DE GESTIÓN DE SEGURIDAD 32
FIGURA 2. MAPA MENTAL DE LAS BASES TEÓRICAS 38
FIGURA 3. TRIÁNGULO DE LA SEGURIDAD DE LA INFORMACIÓN 48
FIGURA 4. PAR TRENZADO 55
FIGURA 5. DISPOSITIVOS DE RED. 56
FIGURA 6. DESARROLLO DE LAS DIFERENTES VERSIONES DE COBIT 64
FIGURA 7. ORGANIGRAMA SIMPLIFICADO DEL MPP EDUCACIÓN 68
FIGURA 8. ORGANIGRAMA SIMPLIFICADO DE LA DIRECCIÓN DE INFORMÁTICA 69
FIGURA 9. TIPOS DE VARIABLES SEGÚN SUS RELACIONES 79
FIGURA 10. RESPUESTA AL ÍTEM 1 91
FIGURA 11. RESPUESTA AL ÍTEM 2 92
FIGURA 12. RESPUESTA AL ÍTEM 3 92
FIGURA 13. RESPUESTA AL ÍTEM 4 93
FIGURA 14. RESPUESTA AL ÍTEM 5 93
FIGURA 15. RESPUESTA AL ÍTEM 6 94
FIGURA 16. RESPUESTA AL ÍTEM 7 94
FIGURA 17. RESPUESTA AL ÍTEM 8 95
FIGURA 18. RESPUESTA AL ÍTEM 9 95
FIGURA 19. RESPUESTA AL ÍTEM 10 96
FIGURA 20. RESPUESTA AL ÍTEM 11 96
FIGURA 21. RESPUESTA AL ÍTEM 12 97
FIGURA 22. RESPUESTA AL ÍTEM 13 97
FIGURA 23. RESPUESTA AL ÍTEM 14 98
FIGURA 24. RESPUESTA AL ÍTEM 15 98
FIGURA 25. RESPUESTA AL ÍTEM 16 99
FIGURA 26. RESPUESTA AL ÍTEM 17 99
FIGURA 27. RESPUESTA AL ÍTEM 18 100
FIGURA 28. RESPUESTA AL ÍTEM 19 100
FIGURA 29. RESPUESTA AL ÍTEM 20 101
FIGURA 30. RESPUESTA AL ÍTEM 21 101
FIGURA 31. RESPUESTA AL ÍTEM 22 102
FIGURA 32. RESPUESTA AL ÍTEM 23 102
FIGURA 33. RESPUESTA AL ÍTEM 24 103
FIGURA 34. RESPUESTA AL ÍTEM 25 103
FIGURA 35. RESPUESTA AL ÍTEM 26 104
FIGURA 36. RESPUESTA AL ÍTEM 27 104
FIGURA 37. RESPUESTA AL ÍTEM 28 105
FIGURA 38. RESPUESTA AL ÍTEM 29 105
FIGURA 39. RESPUESTA AL ÍTEM 30 106
FIGURA 40. RESPUESTA AL ÍTEM 31 106
FIGURA 41. RESPUESTA AL ÍTEM 32 107
FIGURA 42. RESPUESTA AL ÍTEM 33 107
FIGURA 43. RESPUESTA AL ÍTEM 34 108
FIGURA 44. RESPUESTA AL ÍTEM 35 108
FIGURA 45. RESPUESTA AL ÍTEM 36 109

Figura 46. Respuesta al Ítem 37 109
Figura 47. Respuesta al Ítem 38 110
Figura 48. Respuesta al Ítem 39 110
Figura 49. Síntesis de resultados 111
Figura 51. Sistema del Sistema de Seguridad para las Redes de Datos del MPP Educación. 128
Figura 50. Diagrama de Red Simplificado del MPP Educación 130
Figura 52. Organigrama Simplificado del MPP Educación 158
Figura 53. Sistema del Sistema de Seguridad para las Redes de Datos del MPP Educación 161
Figura 54. Representación del Cubo CobiT 195
Figura 55. Ciclo de Gestión 196
Figura 56. CobiT Proyectado Sobre el Ciclo de Gestión 197
Figura 57. Estructura del Dominio de Planificación y Organización 200
Figura 58. Estructura del Dominio de Adquisición e Implementación 201
Figura 59. Estructura del Dominio de Entrega y Soporte 203
Figura 60. Estructura del Dominio de Monitoreo y Evaluación 205
Figura 61. Transición de los Requerimientos a Criterios de Calidad 207
Figura 62. Áreas de Enfoque de CobiT 4.1 212
Figura 63. Ciclo de Vida de los Servicios 221

UNIVERSIDAD CATÓLICA ANDRES BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
AREA DE INGENIERÍA
Postgrado en Sistemas de Información

DISEÑO DE UN SISTEMA DE SEGURIDAD PARA REDES DE DATOS DEL MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN

Autor: Harry Jaspe
Tutor: Dr. Pedro Bonillo
Fecha: Julio, 2011

RESUMEN

La seguridad en las redes de datos se ha convertido en una constante en todas las organizaciones, no es una tarea que se pueda dejar a futuro, mucho menos solapar, tal es el caso del Ministerio del Poder Popular de Educación, que en los últimos años ha recibido ataques a su red de computadoras. Es por ello que se hace necesaria la creación de un sistema de seguridad para las redes de datos, mediante la instauración de mejores prácticas, técnicas y metodologías de trabajo que permitan la prevención de dichos ataques informáticos. Para ello la investigación se fundamentará en estándares de seguridad, tal como CobiT 4.1, ITIL V3 e ISO 27002, los cuales permitirá establecer el marco de trabajo necesario para alinear las estrategias de negocios con la tecnología y la seguridad en las redes de datos, permitiendo así facilitar el alcance de los objetivos de la presente investigación.

Descriptores: Sistemas de información, seguridad, redes, estándares, ataques de red, principios de seguridad, activos de red, mitigación de ataques de red, gestión de seguridad, marco de trabajo, continuidad, contingencia, recuperación, control, documentación administración pública.

INTRODUCCIÓN

El Ministerio del Poder Popular para la Educación (MPP Educación), es el organismo público que administra todos recursos destinados a proveer educación pública, gratuita y obligatoria en los niveles de inicial, básica y diversificada en la República Bolivariana de Venezuela. Su misión, según el Ministerio del Poder Popular para la Educación (2010); es la de disponer de hombres y mujeres con una formación acorde a las necesidades de la sociedad, con pertinencia social, emprendedores, solidarios, activos, éticos y comprometidos con el desarrollo socio-político y económico del país.

Dentro de su estructura administrativa se encuentra la Dirección de Informática, integrada a su vez por las Direcciones de Sistemas, Redes y Telefonía, Apoyo al Usuario y Operaciones y Base de Datos. Esta última dirección es la responsable de la administración de los equipos de servidores que prestan servicios a la red informática del MPP Educación en todo el país. En dichos servidores se encuentran alojados sistemas como la nómina del personal (consideradas unas de las de mayor magnitud en Latino América), así como aplicaciones y bases de datos relacionas con Misión Robinson, seguro médico del personal adscrito, prestaciones sociales, pensionados y jubilados, control de estudios, entre otros.

La intercomunicación entre el Ministerio de Educación y las diversas zonas educativas (representación de este ente público ante cada estado o territorio nacional), se realiza mediante enlaces dedicados tipo F*rame Relay*, sin embargo, para algunos otros servicios como la página Web oficial del ministerio, así como servicios de archivos FTP, se prestan a través de un enlace con tecnología Metro Ethernet, la cual es provista por la empresa telefónica nacional CANTV, esta es una red avanzada de fibra óptica de alta velocidad y banda ancha. Además de estos enlaces, también

existen otras formas de acceder a Internet, como lo son conexiones telefónicas de banda ancha (ABA).

Pese a las medidas de seguridad existentes en las redes de datos del MPP Educación, en los últimos años se han recibido ataques a la red informática, algunos por ejemplo se originaron por la intromisión accidental de técnicos y usuarios. Dichos accidentes provocaron la interrupción del servicio de la red. También se han recibido ataques desde Internet que han afectado el servicio de la página Web ministerial, haciendo peligrar el contenido de las bases de datos

Son usuales los ataques directos a los equipos que se encuentran prestando servicios a Internet, en general son atacados por sus diversos puertos de comunicaciones, inclusive han logrado infiltrarse en dichos equipos, colocando programas y códigos maliciosos que le permiten a los atacantes entrar a los sistemas, causando daño para luego retirarse, no sin antes borrar todos los *logs* o registros del ataque causado. Esta problemática aunado a la proliferación de correos basura (*spam*) y de virus informáticos hacen necesario el diseño y la implantación de un sistemas de seguridad para las redes de datos.

Para lograr un sistema de seguridad para las redes de datos del MPP Educación, se hace imprescindible establecer un marco de trabajo que sirva como guía, por tal motivo es necesaria la adaptación de normas internacionales o estándares a la realidad existente, tales como CobiT 4.1, Norma ISO/IEC 27002, e ITIL V3, estas normas establecen un conjunto de directrices y principios generales que permite iniciar, implementar, mejorar y mantener la gestión de la seguridad de la información en una organización.

Según la indagación previa realizada, ya existen trabajos que han tratado esta problemática, como el realizado por Méndez (2006), donde se establecieron un conjunto de mejores prácticas para garantizar la seguridad en redes inalámbricas. Otro trabajo con similar característica es el de Bolívar (2007), el cual se basó en los riesgos existentes en la banca universal venezolana en lo relativo a la seguridad de datos, entre una de las conclusiones más importantes de dicho trabajo se encuentra

que la seguridad es de carácter integral, abarcando múltiples áreas dentro de la organización. También existen otros trabajos como los de Navarro (2007) y Palacios (2008) que coinciden con los trabajos anteriores, en cuanto a la multidimensionalidad que representa la seguridad de la información, así como la necesidad de integrar todos los esfuerzos de la organización para lograr este objetivo. Finalmente se tiene el trabajo de Caicedo (2009), el cual trata el tema de la migración de redes dedicadas tipo *Frame Relay*, a redes de alta velocidad de fibra óptica o Metro Ethernet, aunque explícitamente no trata los problemas de seguridad, esta investigación llega entre una de sus conclusiones, que la Metro Ethernet posee ventajas comparativas en relación a otro tipos de enlaces, en especial características relacionadas a la seguridad de datos.

En cuanto a los aspectos metodológicos de la presente investigación, se puede clasificar como de tipo proyecto factible, según UPEL (2006), denominado también investigación proyectiva por Hurtado (2010-a), esto debido a que el resultado del estudio es la satisfacción de una necesidad que es cubierta mediante la adaptación de conocimientos anteriores. En cuanto al diseño de la investigación; la cual está ligada a los aspectos operativos relacionados con la recolección de datos, según Hernández (2010), se tiene que esta investigación es de tipo mixto, ya que requiere levantar información para diagnosticar el problema (investigación de campo), y también realizar una investigación de carácter documental para recopilar las mejores prácticas que sirvan de marco de trabajo para el establecimiento de un sistema de seguridad en las redes de datos.

El presente trabajo se ha estructurado en seis capítulos, en el primer capítulo se tiene el planteamiento y la formulación del problema, así mismo se detallan el objetivo general y los objetivos específicos de la investigación. Finalmente en este capítulo se tienen la justificación, el alcance y las limitaciones encontradas.

El segundo capítulo contiene cinco antecedentes de la investigación, posteriormente se exponen las bases teóricas que han sido divididas en:

- Seguridad de la información: Se tratan los temas de seguridad, vulnerabilidad, la clasificación de los ataques de red, principios de seguridad y cifrado.

- Redes: Definición de redes, características de los enlaces físicos, medios de transporte y dispositivos activos de red.
- Seguridad en redes de datos: Se tratan los temas relativos a calidad de servicio, seguridad de enrutamiento, software malicioso donde se da una breve descripción de ellos, tipos de ataques, mitigación de ataques, tipos de atacantes, sistemas de detección de intrusos, cortafuegos, gestión de red, entre otros.
- Normas internacionales de seguridad: En este apartado se describen las normas: CobiT 4.1, ISO/IEC 27002 e ITIL V3.
- Marco organizacional: Describe el contexto organizacional donde se realizará la investigación.
- Bases éticas y legales: Se exponen las bases legales que le sirven de marco a la presente investigación.

El tercer capítulo contiene el marco metodológico, se exponen el tipo de investigación, diseño, las técnicas e instrumentos de recolección de información, se señala la muestra y población, la medición y validez de los instrumentos, se definen la variables operacionales, se operacionalizan la variables y finalmente se exponen las técnicas de procesamiento y análisis a utilizar en la investigación. Finalmente se da cuenta de los recursos materiales, así como del tiempo necesario para la realización de la investigación.

El en cuarto capítulo se exponen los resultados de la investigación, mediante tablas y gráficos, haciendo un análisis de los resultados obtenidos. Asimismo se revela el resultado de la investigación documental realizada, principalmente se exponen las principales características de los marco de trabajo de seguridad tales como CobiT 4.1, ITIL V3 e ISO/IEC 27002, así como el esquema de implementación de los tres estándares anteriores, los resultados de este estudio documental son analizados al final de éste capítulo, así mismo se esboza el contenido del Diseño para la Seguridad de las Redes de Datos del Ministerio del Poder Popular para la Educación.

El quinto capítulo da a conocer las conclusiones y recomendaciones a las que ha llegado el presente trabajo investigativo.

El sexto capítulo expone la propuesta del sistema de seguridad de forma ampliada, dándose a conocer sus objetivos, justificación, beneficios, localización física y cobertura y evaluación mediante matriz DOFA, así como un breve estudio de factibilidad.

La propuesta del sistema de seguridad, está basada en las tres normativas internacionales antes mencionadas, pero enmarcada dentro del sistema administrativo clásico, compuesto por: (1) Planeación, (2) Organización, (3) Dirección y (4) Control. Dicha propuesta se divide en cuatro partes principales:

- Seguridad de los sistemas
    - Seguridad de los sistemas de información
    - Seguridad de las redes de datos
    - Seguridad relacionada con los usuarios
- Desempeño y capacidad
- Continuidad del servicio
- Educar y entrenar a los usuarios

CAPITULO I

Planteamiento del Problema

Problema de Investigación

Las redes de datos se han convertido en una herramienta fundamental que facilita los procesos de toda organización, al permitir el intercambio continuo de información. Este fenómeno se ha dado gracias a la globalización, producto del desarrollo tecnológico en las áreas de la computación y de las telecomunicaciones. Las redes de datos, según Olifer (2009), se puede definir como el conjunto de sistemas de cómputo distribuido, en los cuales varias computadoras trabajan de manera coordinada, para realizar tareas interrelacionadas mediante el intercambio de datos de manera automática, donde la información puede viajar unas decenas de metros de un equipo a otro, o inclusive recorrer grandes distancias de miles de kilómetros.

Muchas de las tareas y procesos automatizados de la organización se fundamentan en el uso de las redes de datos, tales como: Sistemas contables, nómina, inventarios, archivos, entre otros; colocando a disposición de los interesados la información de forma casi instantánea. Además las organizaciones pueden tener presencia en Internet, ofreciendo productos, servicios e información vital para clientes, proveedores y trabajadores.

En un ambiente ideal no existirían fallas, amenazas, accidentes o vulnerabilidades que afectarían negativamente el desempeño de las redes de datos, pero el mundo, el entorno de toda organización está lejos de ser ideal. Las vulnerabilidades, según Aceituno (2007), es la probabilidad de sufrir un determinado

ataque, donde los ataques son protagonizados por actores internos o externos a la organización y que intentan hacer daño a los sistemas. Las amenazas por su parte, son cualquier circunstancia que potencialmente pueda entorpecer los procesos de la organización, así mismo los accidentes son generado por el desgaste físico de los equipos o por el efecto de catástrofes naturales. Las fallas o los errores por lo general ocurren sin que exista una motivación, pero pueden enmascarar en muchos casos un ataque. Más allá de toda resignación, se debe evitar y hasta reducir la incidencia de errores y ataques con los medios disponibles.

Según Alexander (2007), más del 80% de los valores intelectuales de una organización son de carácter electrónico, los escenarios de amenazas pueden presentarse en cualquier momento, colapsando los procesos automatizados de la organización. Por tal razón se debe contar con estrategias de continuidad claramente definidas para cada escenario de amenaza previamente identificado, además de planes que permitan la reanudación y continuidad de las operaciones.

El Ministerio del Poder Popular para la Educación (MPP Educación), posee una amplia red de datos que permiten la prestación de variados servicios, desde la página Web oficial, donde además de información se ofrecen servicios a los trabajadores, tales como recibos de pago, notificación de pago de prestaciones sociales y jubilaciones entre otros. Además cuenta con servicios de red interna o Intranet, la cual permite la conexión de múltiples usuarios a los servidores de datos con la finalidad de facilitar todos los procesos de índole administrativo. Dicha Intranet no sólo está disponible para el personal que labora en el edificio sede del MPP Educación, ubicado en Caracas, sino que también para las veinticuatro zonas educativas ubicadas en los distintos estados del interior del país.

Dichos enlaces de comunicaciones están activos las veinticuatro horas de todos los días del año, por medio de tecnología *Frame Relay*, la cual es “una red de datos de conmutación de paquetes” (Sackett, 2002, p.68), dicha red utiliza una línea telefónica dedicada que interconectan dos puntos. Para los otros servicios que se

ofrecen, se utiliza tecnología Metro Ethernet o de fibra óptica y conexiones de banda ancha o ABA.

Sin embargo, antes de la entrada en funcionamiento de la Metro Ethernet, la cual contribuyó a mejorar el servicio de Internet dentro de la organización, muchos departamentos adquirieron servicio de banda ancha (ABA) por su cuenta, lo que ocasionó la proliferación de redes paralelas a las establecidas, sin ningún tipo de control o de sistemas de seguridad, ofreciendo así nuevos puntos vulnerables susceptibles de ser blancos de ataques externos.

Los ataques desde Internet se han caracterizado por afectar principalmente el servicio Web, por lo general dichos ataques se realizaban mediante la inyección de código SQL o *Structured Query Language*, el cual "es una herramienta para organizar, gestionar y recuperar datos almacenados en una base de datos informática" (Groff y Weinberg, 1998, p. 3). Dicho script o código usualmente era colocado en la barra de navegación Web de los exploradores, provocando intrusiones a las bases de datos, originando problemas como la eliminación de tablas, modificación de datos o redireccionamiento de páginas hacia otros sitios de la Web.

En la actualidad es usual la intromisión directa a los equipos que prestan servicios Web, generalmente son atacados por sus diversos puertos, un puerto se puede definir como una "designación lógica de un grupo de direcciones E/S (entrada y salida) que le 'dice' a un ordenador que 'se enchufe' para enviar comunicaciones" (Clayton, 2002, p. 335). Inclusive han logrado infiltrarse a equipos y colocado programas o códigos maliciosos, que permiten saltar hacia otros equipos de la red para causar daño, borrando inclusive todos los *logs* o registros del sistema para no dejar rastro de la intromisión.

Se han tomado medidas como por ejemplo la implementación de *firewalls* internos (entre la red ministerial y las zonas educativas), y *firewalls* externos (entre la red ministerial e Internet). Los *firewalls* son "sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es" (Borghello, 2010).

También se han implementado sistemas proxy, es decir sistemas que según Borghello (2010), actúan de intermediarios entre el cliente y el servidor real de la aplicación, siendo este proceso totalmente transparente para los usuarios, la función del proxy es la de analizar el tráfico de la red y buscar contenido que viole la seguridad de la misma. Sin embargo, todavía existen riesgos potenciales como por ejemplo la conexión de redes inalámbricas realizadas arbitrariamente por algunos usuarios.

Otro de los problemas frecuentes que incrementa el tráfico de la red y la hace congestionar, es la proliferación de correos basura o *spam*, este tipo de correos es definido por Borghello (2010) como mensajes no solicitados, de tipo publicitario y que son enviados de forma masiva. Paralelamente a este problema, existe el riesgo de correos enviados masivamente a grupos de usuarios, con el objeto de desprestigiar y someter al escarnio público a uno o varios funcionarios.

El correo electrónico, dentro del MPP Educación, es una herramienta esencial para el trabajo y las operaciones diarias, sin embargo hasta ahora no ha logrado sustituir los tradicionales memos impresos con sello húmedo, por lo que sería interesante la implementación de la firma digital. La firma digital según Stallings (2004), son los datos criptográficos añadidos al correo electrónico y que permiten verificar la fuente y la integridad de los datos, protegiéndola así de la falsificación por parte del receptor. Han sido implementado exitosamente en muchas organizaciones y han reemplazado los oficios y memos (con sello húmedo) escritos en tinta y papel.

Los virus informáticos son otro de los males que afectan negativamente el rendimiento de la red de datos, se pueden definir como un “programa que se transmite de un sistema a otro, necesitando cierta intervención del usuario, que normalmente consiste en ejecutar un programa para difundirse” (Aceituno, 2007, p. 34). Muchos de tales virus se especializan en propagarse por las redes de datos.

De continuar esta situación los problemas de seguridad en la red informática se agravarían en el futuro, la información contenida en los repositorios de datos relativa a los trabajadores, nóminas de personal fijo, contratado y jubilado, nóminas

de las misiones, becas, calificaciones y certificaciones de los alumnos; serían vulnerables, ante la posibilidad de ser eliminada, modificada o alterada. Además se desmejoraría notablemente el servicio a todos los usuarios de los sistemas informáticos del MPP Educación.

Los hechos anteriormente descritos han llevado a que exista un problema de seguridad crítico en el MPP Educación, que abarca desde los continuos ataques externos a todos los servicios y sistemas de información del ministerio, así como de ataques internos, voluntarios o involuntarios, realizados por los propios miembros de la organización, propagación de correos no autorizados, correos *spam* o basura, virus, congestionamiento del tráfico de red y ataques mediante el uso del correo electrónico institucional, entre otros.

Formulación del Problema

La problemática que se presenta en relación a la seguridad de las redes de datos del MPP Educación, es la inexistencia de un adecuado sistema de seguridad que establezca las políticas, normas, procedimientos y estructura organizacional; mediante la implementación de métodos y mejores prácticas existentes en tecnología de la información y telecomunicaciones; que permita minimizar y en algunos casos erradicar los diversos problemas de seguridad originados por las amenazas, vulnerabilidades y ataques a las redes de datos de esta institución, que resulta de gran importancia para la administración y control de todas las actividades educativas desde educación inicial hasta básica y diversificada a nivel nacional. Siendo la responsable de dictar las normativas, asignación de cargos, presupuestos, entre otra su sus múltiples funciones, para todas las escuelas y liceos del país.

En consecuencia, de lo anteriormente expuesto, se desprende la siguiente interrogante:

- ¿Cuáles elementos debe contener una propuesta de sistema de seguridad para las redes de datos del MPP Educación, que permita minimizar o erradicar las amenazas, vulnerabilidades y ataques de la cual es objeto?

Para resolver esta pregunta, se necesita a su vez, responder otras de carácter particular, que ayudarán a definir los objetivos de la investigación y que servirán de guía para su realización, tales como:

1. ¿Cuál es la situación actual de seguridad en las redes de datos en el MPP Educación?
2. ¿Cuáles normas, mejores prácticas y estándares internacionales de seguridad de datos pueden servir de guía para la elaboración de la propuesta?
3. ¿Cuáles de las medidas de seguridad adoptadas en la actualidad por el MPP Educación deben permanecer o ser mejoradas?
4. ¿Qué medidas deben ser implementadas para mejorar la seguridad en las redes de datos?
5. ¿Cómo organizar este conjunto de medidas de seguridad en una propuesta de fácil implementación?

Objetivos de la Investigación

Objetivo general.

Diseñar una propuesta de seguridad para las redes de datos del Ministerio de Poder Popular para la Educación fundamentada en las mejores prácticas y estándares internacionales.

Objetivos específicos.

1. Conocer la situación de seguridad de las redes de datos en el MPP Educación.
2. Determinar cuáles de las mejores prácticas y estándares, relativos a la seguridad de datos y redes, pueden ser aplicados al problema de estudio.
3. Identificar cuáles de las medidas de seguridad tomadas en la actualidad debe pasar a formar parte de la presente propuesta.
4. Precisar cuáles medidas de seguridad, provenientes de los estándares y mejores prácticas existentes previamente seleccionadas, deben formar parte de la propuesta.

5. Formular la propuesta de seguridad de tipo preventiva, correctiva, de contingencia y recuperación para las redes de datos del MPP Educación, de manera organizada y sistematizada.

Justificación de la Investigación

Según Hernández (2010) la justificación de la investigación comprende la exposición de las razones, es decir, el por qué y para qué del estudio, demostrando así la importancia y la necesidad de la investigación. En este sentido se tiene que la necesidad de dicho sistema de seguridad para las redes de datos se fundamenta en la importancia de la información que transita por ellas tales como:

- Los datos del sistema de nómina, con más de cuatrocientos cincuenta mil registros perteneciente al personal docente, administrativo y obrero.
- Datos relacionados con becas escolares.
- Registros de pagos realizados al personal contratado y perteneciente a las misiones especiales de alfabetización y alimentación escolar.
- Datos correspondientes al sistema de control de estudios, los cuales son la base para la emisión de títulos de bachiller; notas certificadas de toda la población estudiantil del país, entre otros.

La finalidad de la presente investigación es el diseño de un sistema de seguridad preventivo, correctivo y de manejo de contingencias para las redes de datos para el MPP Educación, que permita salvaguardar la información que por ellas transita, así como evitar ataques que atenten contra la integridad de los datos almacenados en sus sistemas informáticos.

Como valor agregado tenemos que este sistema de seguridad, permitiría crear conciencia dentro de las instituciones públicas de las graves amenazas que continuamente acechan sus redes informáticas. Si bien dicho sistema está diseñado para ser aplicado en el MPP Educación, el mismo puede hacerse extensivo a otros entes públicos con las respectivas adaptaciones a que haya lugar.

Dentro de las diversas áreas temáticas de sistema de información, la presente investigación se sitúa dentro de las tecnologías de información, específicamente en el ámbito de redes de computadoras, pero enfocado en aspectos relacionados con la seguridad.

Así mismo, el presente estudio puede servir de punto de partida para otros investigadores que deseen profundizar sobre el tema de la seguridad en las redes de datos, como por ejemplo la propuesta de un modelo o metodologías de seguridad aplicado a las redes de datos de los organismos e instituciones públicas.

Alcance y Limitaciones

La presente investigación se circunscribe al diseño de un sistema de seguridad, basado en las mejores prácticas y estándares internacionales relacionados con el aseguramiento de las redes de datos.

La investigación sólo comprende las redes de datos que se encuentran edificio sedes del MPP Educación, ubicado en la Parroquia Altagracia de Caracas, así como las veinticuatro zonas educativas adscritas a este ente y que se encuentran físicamente ubicadas en la capital de cada estado o territorio nacional.

Entre las limitaciones encontradas tenemos:

- Algunos de los estándares de seguridad y normas internacionales no son de libre acceso, debido a que se deben adquirir previo pago en moneda extranjera.
- Las propuestas de mejores prácticas se limitan a la bibliografía existente.
- La disponibilidad de la información dependió de la disposición de tiempo del personal de la Dirección de Operaciones y Base de Datos del MPP Educación.
- La información de carácter confidencial no fue divulgada.
- El diseño del sistema de seguridad para redes de datos estuvo basado fundamentalmente en herramientas de software libre, en consonancia con el decreto N° 3.390 que dicta los lineamientos de las tecnologías de software a utilizar por el Estado Venezolano.

- Se realizó una investigación documental en escritos técnicos referidos a normas de seguridad y herramientas de software libre, así como en los manuales de procedimiento y configuración de la red del MPP Educación.

CAPITULO II

Marco Teórico

Antecedentes de la Investigación

La presente investigación tuvo como antecedente cinco estudios previos relacionados con redes, seguridad y sistemas de información.

En primer lugar se tiene la investigación de Méndez (2006), el cual en su trabajo de grado de especialización en Gerencia y Tecnología de las Telecomunicaciones de la Universidad Metropolitana, titulado "Estudios de Metodologías para la Implantación de la Seguridad en Redes de Inalámbricas de Área Local", plantea como problema; considerar los elementos que, según las mejores prácticas existentes en materia de seguridad, se puedan implantar en redes inalámbricas para alcanzar el más alto nivel de productividad.

El diseño de investigación utilizado por este autor fue netamente documental, basándose en normas internacionales como CobiT, UNE 71502 e ISO 17799.

Entre las conclusiones más importantes a las que llegó en su investigación tenemos:

- Las vulnerabilidades de seguridad en las redes inalámbricas son consecuencia del desconocimiento sobre esta tecnología, así como de los estándares y metodologías de seguridad.
- Las metodologías y los estándares internacionales proporcionan un marco de referencia basado en las mejores prácticas, los cuales se complementan uno a otro, con lo que se obtiene un marco de referencia adaptado a las necesidades reales existentes.

- En las organizaciones competitivas es fundamental como estrategia de negocio la disponibilidad de la información, como herramienta fundamental para la toma de decisiones asertivas.
- Las unidades de tecnología de la información y comunicación adquieren cada vez mayor importancia dentro de la línea estratégica de las organizaciones, lo cual implica una mayor responsabilidad y por lo tanto la optimización de los procedimientos existentes con la finalidad de garantizar la continuidad del negocio.
- La seguridad debe ser considerada como una de las principales misiones de los directivos de la organización, debido a los elevados costos que representa la paralización de la cadena de valor debido a incidentes originados por imprevistos en la seguridad.

El principal aporte de esta investigación, debido a su diseño documental, fue la bibliografía consultada para su elaboración, las normas y estándares utilizados, así como todos los procesos relativos al establecimiento de la seguridad en redes inalámbricas. Sin embargo, cabe destacar que la norma utilizada por Méndez (2006) es la ISO 17799, debido a procesos de actualización dio origen a la norma ISO 27002, que es la norma utilizada en el presente trabajo. No obstante, los cambios realizados en la norma ISO 17799 son superficiales, por lo que el aporte del trabajo del Méndez (op. cit.) a la presente investigación sigue siendo válido.

En este trabajo de investigación, Méndez (2006) considera a la seguridad como un proceso (ver Figura 1), que se inicia con la planificación del modelo de gestión, realizando un análisis de riesgos para así seleccionar los respectivos controles; continua con el hacer, donde se pone en funcionamiento los controles propuestos, estableciendo las pautas para la verificación de los controles implantados; posteriormente le sigue la verificación del comportamiento en función de los objetivos previamente establecidos, haciendo énfasis en la detección de nuevos riesgos y amenazas que puedan suscitarse; finalmente se encuentra el actuar, es decir, la revisión continua y sistemática mediante auditorías periódicas y permanentes para

así aplicar medidas correctivas sobre las debilidades detectadas, iniciando nuevamente el ciclo con la planificación.

Figura 1. Modelo de Gestión de Seguridad

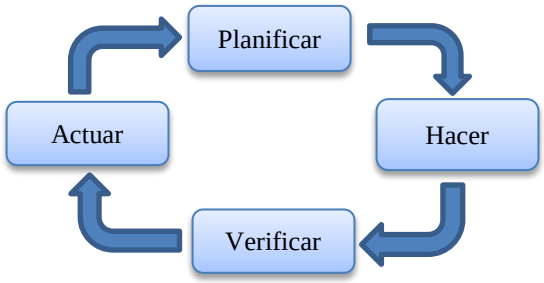

Figura 1. Representa el modelo simplificado de la gestión de la seguridad, compuesto por cuatro procesos básicos: Planificar, hacer, verificar y actuar. Adaptado de la tesis "Estudios de Metodologías para la Implantación de la Seguridad en Redes Inalámbricas de Área Local", por Méndez, 2006, (p. 71)

La segunda tesis utilizada como antecedente en la presente investigación fue la de Mariana Bolívar, titulada "Seguridad de la Información Dentro de la Banca Universal Venezolana", trabajo de grado de maestría en administración, gerencia de empresas, de la Universidad Metropolitana, elaborado en el año 2007.

El problema planteado por Bolívar (2007) en dicho estudio, fue el establecimiento del esquema básico de seguridad en la banca universal venezolana para reducir los riesgos existentes. El diseño utilizado fue de tipo mixto, donde se combinaron la investigación de campo y la documental.

El trabajo de Bolívar (2007) versó sobre la evaluación de los riesgos existentes en la banca universal venezolana, en lo relativo a las prácticas de seguridad existentes, haciendo énfasis en las amenazas internas y externas que tiene por objetivo el ataque a los sistemas de información, esta investigación demostró la necesidad de desarrollar una solución efectiva e integral para el establecimiento de las mejores prácticas de seguridad.

Entre las conclusiones a las que llegó Bolívar (2007) tenemos:

- El plan de seguridad a implantar debe ser integral, ya que según observó, muchos de los planes existentes se enfoca en amenazas particulares y no en su posible combinación, perdiendo así su efectividad.
- La seguridad debe abarcar todos los niveles de la organización.
- Los elementos de seguridad en la banca universal se centran en el uso de mecanismos como corta fuegos, antivirus y mecanismos de encriptación de datos, monitoreo de red, filtrado de paquetes y la implementación de redes virtuales privadas (VPN), así como de sistemas de detección de intrusos, es decir, se centran en la seguridad lógica, abandonando la seguridad física como por ejemplo las tarjetas inteligentes y sistemas biométricos que permitan identificar con exactitud a las personas que entran en contacto con los equipos informáticos.
- También descubrió la falta de personal calificado en materia de seguridad dentro de la banca universal, así como de aplicaciones y tecnología que faciliten la gestión de la seguridad.
- La gestión de seguridad parece no estar integrada con las demás áreas de la organización, de esta manera no se le otorga la debida importancia a dicha integración.
- La mayor debilidad en cuanto a la seguridad se refiere a las redes de datos, en especial las inalámbricas, servicios Web, redes VPN.
- El establecimiento de un esquema de seguridad está en relación directa al nivel de madurez que posee la institución.
- La seguridad debe ser integral, abarcando todos los niveles de la organización, así como actualizable, de manera que se permita descubrir nuevas amenazas y vulnerabilidades.
- Se debe crear una unidad técnica responsable de la seguridad de la información dentro de la organización, alineada con los objetivos del negocio.

Los aportes de la investigación de Bolívar (2007), además sus abundantes fuentes bibliográficas, es el diseño de campo utilizado para levantar la información,

así como el análisis de la información recabada. Además coincide con la investigación de Méndez (2006), en cuanto al enfoque integral de la seguridad dentro de la organización. Resalta también que el punto álgido de la seguridad en la banca universal está relacionado con las redes de datos, sobre la cual se centrará la presente investigación.

La tercera investigación utilizada como antecedente fue la de Amilcar Navarro, titulada "Metodología para la Gestión de Seguridad de Información en Venezuela", publicada en el año 2007, como trabajo de grado de especialización en gerencia y tecnología de las telecomunicaciones, de la Universidad Metropolitana.

El problema planteado por Navarro (2007) fue la comparación de metodologías existentes y relativas a la seguridad de información, tales como CobiT, ISO/IEC 27000, GMITS y CC; para de esta manera proponer un modelo propio de gestión de seguridad en la gestión de riesgos. El diseño de investigación utilizado por Navarro (2007) es completamente documental.

Entre las conclusiones a las que llegó Navarro (2007) tenemos:

- La seguridad debe abarcar todos los aspectos de la organización y debe ser asumida globalmente.
- Existen cuatro aspectos fundamentales de la seguridad, ellos son:
    - La cultura, donde esté involucrada directamente la gerencia de la organización, de forma que lidere todas las iniciativas relativas a la seguridad.
    - Políticas y planes de seguridad: Se hace necesaria una planificación continua para implementar una adecuada gestión de seguridad, mitigando así las amenazas que se ciernen sobre los sistemas de información.
    - Estructura organizacional: Es la implementación de una unidad administrativa, responsable de la seguridad dentro de la organización.

- Educación: El entrenamiento y la concientización en materia de seguridad como herramienta efectiva para el desarrollo de la cultura de seguridad dentro de la organización.

- Los marcos de referenciales de seguridad (CobiT, ISO/IEC 27000, GMITS y CC), no son fácilmente integrables entre sí, más bien proporcionan diversos puntos de vista sobre una misma problemática como lo es la seguridad de datos, por lo que pueden ser utilizados independientemente para problemas específicos.

En este trabajo existe coincidencia con Bolívar (2007), en cuanto a que la seguridad es un aspecto que debe ser asumida integralmente por toda la organización. El principal aporte es la alineación de cinco estándares internacionales en un modelo de gestión de seguridad, en especial lo concerniente al análisis de riesgos, la propuesta de Navarro (2007) es sólida, además de multidimensional, debido a los diversos puntos de vistas que en materia de seguridad aportan los cinco estándares estudiados en dicha investigación.

El cuarto trabajo de investigación utilizado como antecedente, fue el elaborado por Juan Carlos Palacios, titulado "Evaluación del Desarrollo de los Fundamentos Teóricos de Seguridad de la Información en la Banca Comercial y Universal de Venezuela", publicado en el año 2008, como trabajo de grado de maestría en gerencia de sistemas de información de la Universidad Católica Andrés Bello.

El problema planteado por Palacios estuvo referido a los fundamentos teóricos de la seguridad de la información en la organización, el desarrollo de las mejores prácticas gerenciales de seguridad, la planificación de la seguridad de la información, así como la continuidad del negocio y recuperación ante desastres, así como del marco legal existente en Venezuela relacionado con la seguridad.

El diseño de investigación utilizado por Palacios (2008) fue mixto, combinando investigación documental e investigación de campo, centrándose en la

descripción que en materia de seguridad poseen instituciones bancarias comerciales y universales.

Entre las principales conclusiones a las que llegó Palacios (2008) tenemos:

- Planteamiento de las mejores prácticas de seguridad basado en los estándares internacionales.
- Establecimiento de los planes de continuidad del negocio.
- Exposición del marco legal existente en Venezuela en materia de seguridad de la información.
- Clasificación de las diversas instituciones bancarias, según la certificación ISO.

La investigación de Palacios (2008) fue básicamente descriptiva, dando a conocer los diversos mecanismos que en materia de seguridad son implementados por la banca comercial y universal en Venezuela, el principal aporte de dicha investigación al presente trabajo radica en la abundante investigación documental realizada y desde el punto de vista metodológico, en la investigación de campo realizada, sobre todo en lo relativo a los instrumentos de recolección de información utilizados.

Finalmente como quinto y último trabajo de investigación que se utilizó como antecedente, fue el elaborado por Héctor Caicedo, titulado "Metro Ethernet: aplicación en el sector financiero venezolano", publicado en el año 2009, como trabajo de grado de especialización en gerencia de tecnología y telecomunicaciones de la Universidad Metropolitana.

El problema planteado por Caicedo (2009) fue determinar las ventajas que ofrece el componente tecnológico Metro Ethernet en su aplicación para el sector financiero. El diseño de la investigación es documental.

El trabajo de Caicedo (2009) se centró en la evolución de antiguas conexión *Frame Relay* (conexiones privadas a baja/media velocidad) a conexiones de alta

velocidad a través de fibra óptica como lo es la Metro Ethernet, siendo una tecnología flexible y escalable.

Entre las principales conclusiones del trabajo de Caicedo (2009) tenemos la resistencia al cambio existente en las instituciones bancarias para pasar de tecnologías *Frame Relay* a Metro Ethernet, pese a las ventajas comparativas existentes, además de la velocidad, ofrecen mayor seguridad en el transporte de datos,

En cuanto al aporte de dicho trabajo a la presente investigación, se tiene que aunque explícitamente no trata de seguridad en los sistemas de información, aporta valiosos datos relativos a las ventajas de la Metro Ethernet sobre el *Frame Relay*, entre dichas ventajas señala sus características de seguridad. Además, existe cierto paralelismo entre el problema planteado por Caicedo (2009) y el caso del MPP para la Educación, en donde existen ambas tecnologías (*Frame Relay* y Metro Ethernet), sin embargo aún muchos de los enlaces no han sido migrados a Metro Ethernet.

Bases Teóricas

Las bases teóricas según Palella (2006), brinda el soporte principal al estudio, puesto que permite integrar la teoría con la investigación, estableciendo sus interrelaciones. En cuanto a su contenido, señala también que está compuesto por un sistema coordinado y coherente de conceptos que permiten abordar la investigación. La estructura de las bases teóricas del presente estudio puede ser observado en la Figura 2.

Seguridad de la Información.

Para Alexander (2007), el 80% de los valores intelectuales de las organizaciones se encuentran en medios electrónicos, por lo que se requieren esfuerzos que permitan minimizar los riesgos de fuga y alteración de información, o simplemente que no esté disponible cuando se necesite. Todos estos escenarios de amenazas en cualquier momento pueden ponerse de manifiesto, haciendo colapsar a cualquier organización, por tal motivo se hace imprescindible la formulación de

estrategia de continuidad que permita neutralizar o al menos minimizar tales amenazas.

Figura 2. Mapa Mental de las Bases Teóricas

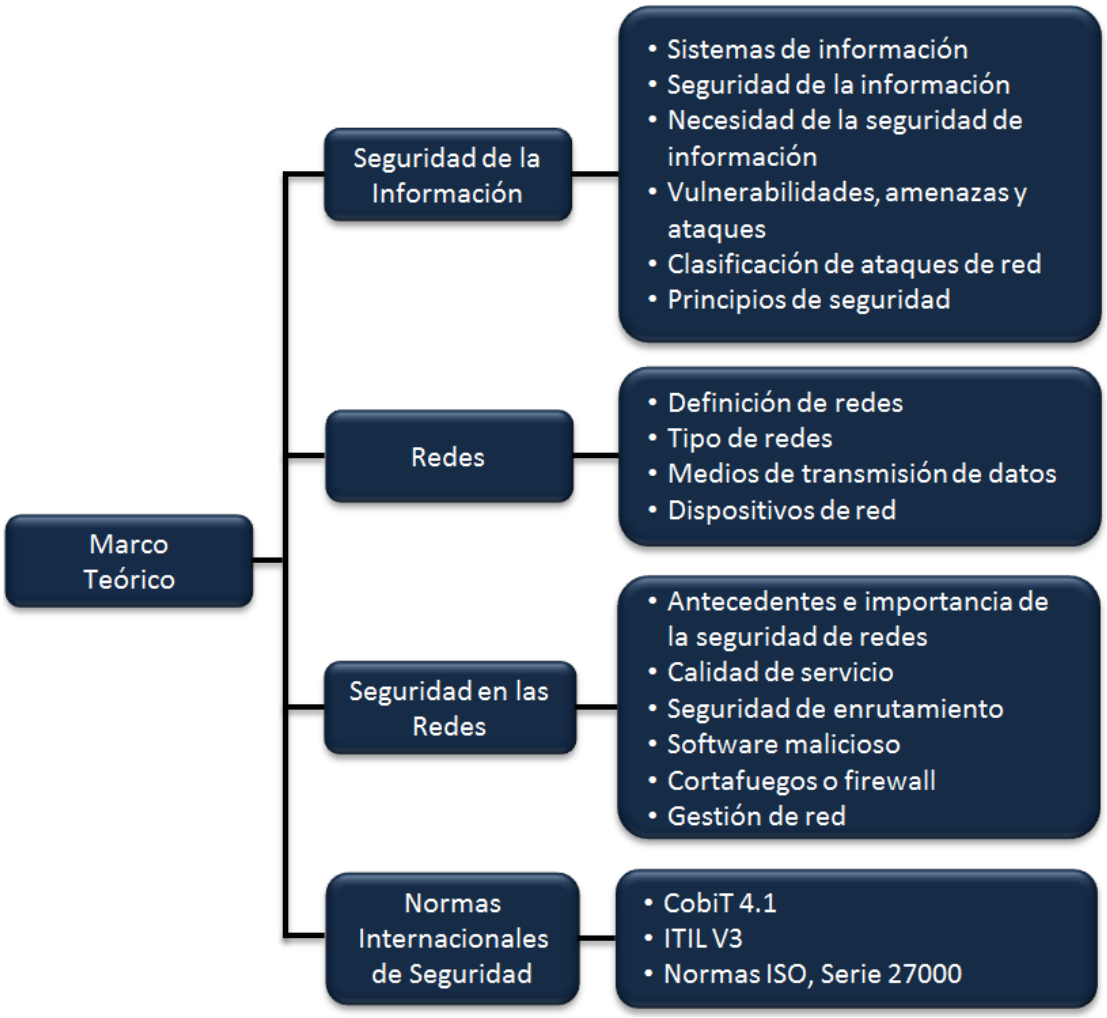

Figura 2. Mapa mental de los tópicos tratados en el marco teórico de la presente investigación. Elaborado por el autor.

Sistemas de información.

Según Laudon (2008), define sistemas de información como un conjunto interrelacionados de elementos que recaban, procesan, almacenan y distribuyen información, con la finalidad de apoyar el proceso de toma de decisiones y de proveer

de control a las organizaciones. Pero también los sistemas de información sirven de soporte para que gerentes y trabajadores analicen problemas, visualicen asuntos complejos y creen nuevos productos, entendiéndose por información los datos, la secuencia de hechos en bruto que representan eventos que ocurren en las organizaciones, que se han resumido y moldeado de forma significativa y útil para los seres humanos.

Según la definición anterior, los sistemas de información son todas aquellas aplicaciones que permiten desde el punto de vista operativo y gerencial, resolver problemas y tomar decisiones asertivas, sin embargo, la información requiere de un proceso, para lo cual se sirve de múltiples tecnologías, desde el transporte de datos, hasta sistemas de bases de datos que permiten centralizar y procesar los datos recabados para obtener como como producto final la información.

Definición de seguridad de información.

Según la norma ISO 27002 (2005), la seguridad de la información es la protección de la información contra todo tipo de amenazas, y tiene la finalidad de asegurar la continuidad del negocio, con el objeto de maximizar el retorno de la inversión y las oportunidades de negocio. Todas las obras humanas son falibles, por lo que es frecuente conseguir puntos de falla en toda la tecnología relacionada con la información, sin embargo, aunque es inevitable la ocurrencia de fallas, ello no implica que se asuman conductas de resignación, de esa actitud surge el concepto de seguridad de la información, como la vía para hacer frente, para prever y evitar errores o ataques.

Aunque la seguridad absoluta no es factible, se hace necesario lograr la mayor posible con los medios tecnológicos disponibles, pero dicha solución no debe ser parcial, sino al contrario, soluciones totalmente integrales que sean capaces de afrontar los retos que en materia de seguridad surgen con el devenir de los tiempos y con el desarrollo de nuevas tecnologías.

La seguridad según Kendall (2005), abarca tres aspectos fundamentales, tales como:

- Seguridad física: La seguridad física consiste en proteger el sitio donde se encuentra el computador, equipo electrónico y software instalado, este tipo de seguridad incluye acceso controlado a las salas de cómputo. Pero además del acceso a los equipos instalados, se debe garantizar las condiciones medioambientales para su correcto funcionamiento, ello incluye control de temperatura, humedad y flujo eléctrico, de manera que se proporcione un suministro ininterrumpido de energía eléctrica. Además se deben extremar las medidas para evitar catástrofes producto de incendios, inundaciones, terremotos, entre otros.
- Seguridad lógica: Se refiere a los controles lógicos de software y de transporte de datos por las redes de computadoras. Están compuestos de contraseñas, códigos de autorización, sistemas de reconocimiento biométrico y otros procedimientos que permitan identificar y autenticar al usuario que intenta acceder a los sistemas. También incluye software de encriptación para proteger el contenido de los datos almacenados o transportados por las redes de computadoras.
- Seguridad conductual: Los controles físicos y lógicos son importantes, pero no suficientes para proporcionar la seguridad adecuada, se requieren cambios conductuales. Es por ello que se debe hacer énfasis en el adiestramiento y la concientización del recurso humano de la organización sobre el tema de la seguridad. Se hace necesario entonces, supervisar regularmente el comportamiento de los usuarios, para corregir preventivamente cualquier desviación que contribuya a los fallos en la seguridad.

Necesidad de la seguridad de la información.

Los sistemas de información ofrecen ciertas ventajas en el cometimiento de actos delictivos y vandálicos, debido al carácter impersonal que puede asumir el atacante, es decir, no requiere de la presencia o contacto físico con la persona o

institución señalada como el objetivo del atacante, basta con sortear algunos impedimentos de carácter técnico para tener acceso a la información, por ello es que las redes de datos constituyen la principal vía de estos ataques. Las organizaciones y sus sistemas de redes de datos enfrentan múltiples amenazas de seguridad, procedentes de una extensa variedad de fuentes, esta puede incluir: fraudes asistidos por computador, espionaje, saboteo, vandalismo, incendios, inundaciones. Las causas de daño tales como códigos maliciosos y ataques de piratería por computador y denegación de servicio son los más comunes, volviéndose cada vez más sofisticados.

Según la norma ISO 27002 (2005), la seguridad de la información es importante tanto para los negocios privados como públicos, así como para proteger la infraestructura crítica, en ambos sectores, la seguridad de la información actúa como un elemento facilitador para lograr, por ejemplo, el gobierno en línea, los negocios electrónicos, evitando o reduciendo los riesgos inherentes, es decir, la seguridad de la información está orientada a garantizar la continuidad del negocio, por lo que debe ser considerada como materia de carácter estratégico dentro de toda organización.

Vulnerabilidad, amenazas y ataques.

Según Aceituno (2007), el riesgo es una medida cuantitativa de la importancia de un incidente que es mayor cuanto mayor es su impacto y probabilidad de ocurrencia. Así mismo integra al concepto los temas de vulnerabilidad, debilidad y oportunidad, entendiéndose por vulnerabilidad como la probabilidad de sufrir un determinado ataque en un plazo de tiempo dado, sin embargo, debido a que se basa en hechos probabilísticos y no determinísticos, se hace difícil predecir con certeza la ocurrencia de tal evento, más aún cuando la tecnología en su continuo avance abre nuevas brechas en materia de seguridad.

Continúa Aceituno (2007) planteando la definición de amenazas, señalando que son cualquier circunstancia que potencialmente pueda afectar a los procesos y las expectativas de la organización, sugiriendo que para proteger estas expectativas, se debe identificar, evaluar y prever cuáles amenazas pueden afectar negativamente a la organización, para lo cual se deben medir, desde el punto de vista cualitativo y

cuantitativo, en función de establecer la posibilidad y probabilidad de la ocurrencia de dichas amenazas.

Aceituno (2007) clasifica en tres grandes grupos a las amenazas:

- Amenazas terciarias: También denominadas directas, son las que afectan directamente el cumplimiento de las expectativas de la organización, coloca como ejemplo catástrofes como incendios, inundaciones. Dentro de las amenazas terciarias establece una división entre accidentes, ataques y errores, donde los accidentes son de tipo natural, como terremotos, fallos electrónicos ocasionados por el uso, entre otros. Los ataques son ocasionados por un actor con determinada motivación, medios y la capacidad para ejecutarlos. Los errores pueden ser naturales, pero también son susceptibles de ser manipulados, convirtiéndose en ataques.
- Amenazas secundarias: Son las que aminoran el grado de éxito de las medidas propuestas para mitigar las amenazas primarias, como por ejemplo fallas en el cortafuego o *firewall*.
- Amenazas primarias: Son aquellas que evitan que se establezcan o se mantengan las medidas que mitigan las amenazas terciarias o secundarias, ejemplo de ello sería una organización de seguridad ineficaz.

Los ataques son incidentes provocados por actores internos o externos, entre los ataques más comunes tenemos:

- El espionaje: Acceso ilegítimo a la información desde el punto de vista físico o lógico, utilizando para ello las escuchas de mensajes por canales no protegidos; la lectura o copia de información mediante el acceso a dispositivos de almacenamiento masivo; la lectura de mensajes o información cifrada; la suplantación, intermediario y reproducción, cuando alguien simula ser otra persona o ambas partes de la comunicación, en caso de la reproducción tiene la finalidad de evitar la autentificación de la fuente en tiempo real; el análisis de tráfico para determinar la ruta de los mensajes transmitidos.

- El sabotaje: Es un ataque destructivo con la finalidad de producir el máximo daño posible; interrupción y borrado, la modificación y generación malintencionada de datos o información; la denegación de servicio o negación de recursos impidiendo a los sistemas de información cumplir con sus funciones; el terrorismo, el cual persigue la destrucción no sólo de equipos e instalaciones, sino de vidas humanas.
- Compromiso de medios de autentificación: Cada medio de autentificación (contraseña, medidas biométricas, llaves o tarjetas de identificación) tiene sus puntos débiles, que pueden ser aprovechado para vulnerar la seguridad y realizar un ataque.
- Compromiso de claves: Implica además de la suplantación de identidad, la imposibilidad de demostrar que la persona debidamente autorizada no fue quien realizó en ataque, comprometiendo la integridad y la confiabilidad de dicha persona.
- Infracción de derechos de autor: Consiste en el uso de una copia, como por ejemplo el software, sin pagar los derechos correspondientes. En el peor de los casos se trata de plagio, cuando otra persona se adjudica la autoría de una obra que no le pertenece.
- Repudio: Es lo contrario del ítem anterior, es decir, es la negación de la autoría propia, ocurre cuando una persona niega la autoría de un hecho o acción.
- Código malicioso: Está compuesto por piezas de código que tienen por finalidad ocasionar daños a equipos y sistemas de información, existe una gran variedad tales como: virus, gusanos, *exploit*, troyanos entre otros.
- Ingeniería social: Explota una característica de la naturaleza humana como lo es confiar y seguir instrucciones de las demás personas, lo cual es utilizada por los atacantes para usurpar contraseñas o información valiosa que le sirva para planificar y ejecutar nuevos ataques.
- Hurtos y robos: Hurto es la sustracción de un activo sin violencia, mientras el robo implica el uso de la violencia.

- Acceso físico no autorizado: Consiste en el acceso a una zona reservada, por lo general mediante usurpación de identidad, o debido a barreras de acceso físico.
- Pérdida de sincronía: Está relacionado con la pérdida de sincronía en lo relativo a la fecha y hora de los sistemas, que pueden afectar el normal funcionamiento de los sistemas.
- Fraudes: Es el aprovechamiento de los recursos de la organización de forma no legítima, como por ejemplo la adquisición de materiales con sobreprecios.

Los accidentes, continúa Aceituno (2007), se deben a causas naturales o al desgaste por el uso de los elementos físicos, se dividen en:

- Catástrofes: Son incidentes no provocados, como terremotos, inundaciones, tornados, rayos, huracanes, entre otros. La protección contra las catástrofes consiste en la redundancia de información, detectores de incendios y sistemas de alarmas.
- Fallos de comunicación y almacenamiento: Son ocasionados por ruido, generado principalmente por conductores eléctricos, se mitiga con protocolos de verificación y corrección de errores.
- Fallos en el hardware o en el software: Ambos elementos son susceptibles de fallos, sean aleatorios o por fabricación, se mitigan mediante el control de calidad y el mantenimiento continuo dispensado a tales equipos.

Finalmente Aceituno (2007) describe los errores, los cuales pueden suceder sin intención alguna, en otras ocasiones sólo sirven para enmascarar un ataque, incluye estos aspectos:

- Permanencia incontrolada de la información o servicios: Es lo contrario a la pérdida de información, es un error frecuente de diseño en los sistemas de información que evita deshacerse de la información que ya no es valiosa.
- *Hoax,* cartas encadenadas y *spam*: Los *hoax* son cartas encadenadas con información falsa y obsoleta que, recurriendo a la superstición, invitan al

destinatario en convertirse en agente multiplicador de dicho mensaje incrementando el tráfico en la red.

- Interfaces pobres: Las interfaces pobres hacen que los usuarios realicen acciones como borrar información, confirmar acciones u otros fallos, con consecuencias potencialmente graves. Se puede pensar en adjudicarle el error al usuario, pero el responsable directo es el diseñador de la aplicación.
- Error humano: Es ocasionado generalmente por falta de diligencia o incompetencia.
- Cesión de medios de autentificación: Consiste de préstamos entre usuarios de contraseñas o medios de identificación, de esta forma alguien no autorizado obtiene acceso a los sistemas.
- Derechos excesivos: Es la asignación de derechos excesivos originados por errores cometidos por los administradores de los sistemas.
- Incumplimiento de normativas: Como su nombre lo indica, es el fallo en el cumplimiento de leyes, normas y regulaciones establecidas.
- Baja de personal: Consiste en no revocar los permisos concedidos a un trabajador, luego de que este deja de prestar sus servicios en la organización.
- Falta de suministros o de distribución: Es la falta de materias primas para el normal desenvolvimiento de las actividades y procesos de la organización.
- Violación de la seguridad: Las organizaciones almacenan información de sus clientes y proveedores, la cual sería inconveniente si se publicara libremente.

Todos los aspectos anteriormente señalados, sirven de preámbulo a la presente investigación, muchos de ellos serán abordados en profundidad, sobre todo aquellos que atañen a la seguridad de las redes de datos.

Clasificación de los ataques de red.

Existen diversas formas de ejecutar ataques a las redes de datos, a continuación se exponen brevemente algunos de los ataques de red más conocidos.

Ataques internos, externos, pasivos y activos.

Otra clasificación más profunda de los ataques pero focalizada al área de redes de datos, es la dada por Mishra (2008), en dos grupos: activos y pasivos. Esto debido a que el atacante en primer lugar se centra en alterar los mecanismos básicos de la red, en segundo lugar, el atacante intenta causar daño en los mecanismos de seguridad empleados, tales como claves, cifrado, entre otros.

Un ataque pasivo implica escuchar los datos que transitan por la red, los ataques activos son acciones específicas realizadas por el atacante, como por ejemplo la modificación o la supresión de datos. En los ataques activos, el atacante, intentan cambiar el comportamiento de los mecanismos operativos, mientras en los pasivos, intenta pasar desapercibido. Cabe destacar que la información recabada en los ataques pasivos, puede servir de base para la realización de ataques activos.

Los ataques, continúa Mishra (2008), pueden ser externos o internos. Los ataques externos, son ataques activos que tienen por objetivo causar congestión en la red, propagar información de enrutamiento incorrecta, impedir que los servicios de red funcionen correctamente o en casos extremos, paralizar por completo los servicios de red. Los ataques internos usualmente son más graves, ya que los nodos desde donde se realiza el ataque pertenecen a la red interna de la organización.

Denegación de servicio.

La denegación de servicio o ataque DoS (de las siglas en inglés *Denial of Service*), es producido según Mishra (2008), por una falla no intencional en el sistema o por una acción maliciosa. Una de las formas clásicas de crear un ataque DoS es sobrecargar las redes de datos de modo que ya no funcionen correctamente y se bloqueen.

Suplantación de identidad.

La suplantación de identidad, según Mishra (2008), se origina cuando un nodo no autorizado es capaz de unirse a la red, enviando información falsa de enrutamiento y pasando de un nodo de confianza a otro.

Ataques Sybil.

Este tipo de ataques recibe el nombre de Sybil, originado de la película del mismo nombre, donde Sally Field interpreta a una joven con trastornos disociativos de identidad o personalidades múltiples. Según Mishra (2008), los ataques de suplantación representan un grave riesgo de seguridad, donde un nodo malicioso actúa como si se tratara de un gran número de nodos, en lugar de uno, o simplemente se hace pasar por otros nodos. Las identidades adicionales que adquiere el atacante, se denominan nodos Sybil.

Los ataques descritos anteriormente son una muestra de la diversas formas que existen de crear el caos en una red de datos, pero dicha clasificación de ataques no es estática, continuamente se producen nuevas formas, nuevas herramientas y técnicas que facilitan dichos ataques.

Principios de Seguridad.

Algunos de los autores consultados como Palacios (2008), Chirilo (2005) y otros, centran los principios de la seguridad en tres aspectos como lo son la confidencialidad, la disponibilidad y la integridad, conformando el llamado triángulo de la seguridad de la información (ver Figura 3). Sin embargo existen otros elementos que vienen a enriquecer esta perspectiva, a continuación se expondrán dichos elementos como principios de seguridad, también llamado en ocasiones elementos de la seguridad.

Confidencialidad.

Según Chirilo (2005), en el contexto de seguridad de la información, la confidencialidad significa que la información confidencial sólo debe estar disponible para las personas debidamente autorizadas para acceder a ella. Para Daswani (2007), el objetivo de confidencialidad es mantener el contenido de una comunicación transitoria o de datos en los medios de almacenamiento en secreto, inclusive en caso que el atacante tenga acceso a dicha información, éste no debe ser capaz de

entenderla. Al respecto Vyncke (2008) dice que la confidencialidad es el principio más evidente y consiste en la capacidad de garantizar el secreto, sólo los destinatarios deben ser capaces de ver la información. Finalmente Harris (2003) asocia confidencialidad a garantizar el secreto.

Figura 3. Triángulo de la Seguridad de la Información

Figura 3. Principios de la Seguridad Informática, conformado por la disponibilidad, la confidencialidad e integridad, elaborado por el autor.

Desde tiempos remotos la humanidad está consiente que la información es poder, por lo que en la era de la información el acceso a la misma es más importante que nunca. El acceso no autorizado a información confidencial puede tener consecuencias devastadoras, no sólo en aplicaciones de seguridad nacional, sino también en el comercio y la industria, los principales mecanismos de protección a la confidencialidad en los sistemas de información son la criptografía y los controles de acceso.

Integridad.

La integridad es la fiabilidad, la legitimidad y exactitud de la información según lo expresa Chirilo (2005), continúa señalando, de lo que se trata es de prevenir que la información haya sido modificada sin autorización durante su tránsito, o peor aún, durante su previo almacenamiento. Vyncke (2008), también establece que la integridad se trata de evitar la alteración de los datos sin que sea detectado, es decir,

no se puede modificar la información excepto con las credenciales apropiadas, en este caso se refiere a la legitimidad de modificar la información, por lo que debe haber un registro o log que permita auditar tales cambios. Este último concepto nos introduce la idea de auditabilidad, el cual será descrito a su debido momento.

Disponibilidad.

Con respecto a la disponibilidad, Vyncke (2008) dice que uno de los aspectos más importantes de la seguridad, es la disponibilidad de datos y servicios, tener datos secretos y legítimos es totalmente inútil si no están disponibles para el uso de las personas a quienes está destinado. De allí la importancia de contar con sistemas redundantes, de alta disponibilidad. Señala que los ataques contra la disponibilidad se denominan interrupciones, pero en el caso específico de las redes de datos, el ataque de disponibilidad a las redes se denomina denegación de servicio, aspecto anteriormente descrito en esta investigación. Para Daswani (2007), el concepto de disponibilidad incluye otros factores como el tiempo razonable de respuesta a un usuario que ha realizado una petición, es decir, además de un objetivo de seguridad, lo considera un objetivo de rendimiento.

Identificación.

Además de los tres aspectos anteriormente señalados, denominados como triangulo de la seguridad, Chirilo (2005), añade la identificación, como el primer paso del proceso de identidad – autentificación, el cual se da cada día en innumerables ocasiones entre seres humanos y sistemas de información. La singularidad de la identificación se refiere a que todo usuario debe poseer un identificador o *login* inequívoco, es decir, que no permita confundirlo con ningún otro.

Autentificación.

La autentificación, señala Chirilo (2005), es el proceso mediante el cual se verifica la autenticidad de la identidad declarada en la fase de identificación. Ocurre justo después de la identificación y antes de la autorización, es decir, es la fase donde el usuario demuestra ser la persona que es o el sistema dice ser. Los tres métodos de

autentificación son: Saber (contraseñas), lo que tienes (llave, tarjeta de identificación) o lo que eres (identificación biométrica).

Autorización.

Una vez declarada la identidad, continúa Chirilo (2005), a los usuarios se les asigna un conjunto de derechos, privilegios o permisos que determinan que pueden y no pueden hacer en el sistema. Estos permisos por lo general son asignados por el administrador del sistema y están basados en políticas previamente establecidas. Como se puede observar la autentificación y autorización dependen de la identificación, siendo el objetivo final de todo proceso hacer cumplir con el control de acceso establecido para poder rendir cuentas, el cual es el proceso que se describe a continuación.

Auditabilidad.

La rendición de cuentas para Chirilo (2005), es otro principio importante de la seguridad de la información, se refiere a la posibilidad de rastrear las acciones y eventos que en determinada fecha y hora realizaron los usuarios, sistemas o procesos, con la finalidad de establecer la responsabilidad por las acciones u omisiones. Estos registros se denominan *logs*, a los cuales evidentemente se hace necesario garantizarles su integridad, para evitar sean modificados para ocultar las trazas de las posibles violaciones realizadas a los sistemas, además de estar correctamente sincronizados con el tiempo real para determinar la fecha y hora de la ocurrencia de tales eventos.

Funcionalidad Vs. Seguridad.

Este aspecto se refiere, dice Chirilo (2005), a la capacidad que tiene un sistema de seguridad de funcionar de acuerdo a lo que dice hacer. Un sistema de seguridad en particular puede pretender aplicar una docena de características de seguridad, pero esto es muy diferente a la capacidad de hacerlo con un alto grado de confianza, es decir, con la capacidad de implementar correctamente el sistema de seguridad para el cual fue diseñado, sin que se comporte de manera inesperada.

Privacidad.

Para este autor, Chirilo (2005), la privacidad está orientada a respetar los derechos individuales de las personas, en especial lo relativo a la información personal, tal como nombre, dirección, sueldo, cuentas bancarias, entre otras. Por esta razón las organizaciones deben tomar las precauciones y las medidas necesarias para proteger la confidencialidad de la información personal recopilada en sus bases de datos, así como el tratamiento que se le va a dar a la misma.

No Repudio.

No repudio en el contexto de la seguridad de la información hace referencia a una de las propiedades criptográficas de la firma digital, que ofrece la posibilidad de probar si un mensaje en particular ha sido firmado por el titular de una determinada firma digital, según Chirilo (2005). Básicamente consiste en prever que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido), en el primer caso el repudio se denomina en origen y en el segundo en destino, según lo clasifica la Guía de Seguridad de las TIC (2009).

Cifrado.

El cifrado o criptografía, según Aceituno (2007), es una operación reversible mediante la cual se convierte el mensaje en un conjunto de datos cuasi aleatorios, o mensaje cifrado. Entendiéndose por mensaje a un conjunto de datos ordenados que se transmiten o almacenan. Como entrada a esta operación se tiene el mensaje y la clave, está última sirve para permitir que el número de posibles cifrados distintos a partir del mismo mensaje sea un número muy grande, dificultando así la obtención del mensaje original a partir del mensaje cifrado, cuando no se posee la clave. La calidad del cifrado es proporcional a lo aleatorio que sea el mensaje cifrado y al mayor número de claves posibles. La criptografía no se basa en el secreto del algoritmo de cifrado, sino en la dificultad computacional del descifrado cuando no se tiene la clave

El cifrado según Vyncke (2008), está basado en funciones matemáticas, aplicadas como algoritmos computacionales a los datos contenidos en los mensajes. El objetivo primordial de la criptografía es la confidencialidad. Otro uso de la criptografía es validar la fuente de datos, tal como lo hace la firma digital. Los sistemas basados en criptografía se denominan criptosistemas.

Redes.

Las redes de datos son una de las tecnologías de comunicaciones vitales para la ejecución de una gran parte de los procesos de cualquier organización, permiten a sus miembros colaborar entre sí, además de hacer uso compartido de los recursos informáticos disponibles, bien sea por el uso de aplicaciones, compartir archivos en línea, servicio de impresión, entre otros.

Definición.

La red se puede definir, según Jimeno (2008), como un conjunto de computadores interconectados entre sí, que permiten a sus usuarios compartir información, recursos, tales como archivos, impresoras, servicios, entre otros. Las tecnologías de red son muy diversas, entre las más utilizadas se encuentran la Ethernet, *Token Ring*, SNA, DECNET, entre otras.

Las redes de computadoras son también conocidas como redes de comunicación de datos o de transmisión de datos, según Olifer (2009), representan el resultado lógico de la evolución de dos ramas de la ciencia y de la tecnología más importante de la civilización moderna, como lo son las computadoras y las telecomunicaciones. En las redes de datos, un grupo de computadores trabajan de manera coordinada, distribuyéndose entre sí la carga de trabajo realizando una serie de tareas interrelacionadas, mediante el intercambio de datos de forma automática. Las redes de computadoras también pueden considerarse como un medio de transmitir información a larga distancia.

Tipo de redes.

Según Forouzan (2002), existen tres tipos importantes de redes: las redes de área local, las redes de área metropolitana y las redes de área amplia. A qué clase pertenece una red viene determinado por su magnitud, su propietario, la distancia que cubre y su arquitectura.

Redes LAN.

En su libro, Forouzan (2002) nos señala que las redes de área local o LAN (*Local Area Network*), generalmente son de propiedad privada, conectan enlaces de una oficina, edificio o una casa. Son tan pequeñas como dos computadoras y una impresora conectadas, la cual se puede extender por toda una empresa. No se limitan sólo a la transmisión de datos, también pueden incluir sonido, voz y video. Actualmente las LAN están limitadas a unos pocos kilómetros.

Redes MAN.

Para Forouzan (2002), las redes de área metropolitana o MAN (*Metropolitan Area Network*), han sido diseñadas para extenderse a lo largo de una ciudad entera. Pueden ser redes únicas o como medio de conectar varias redes LAN a una red mayor, para de esta manera compartir recursos de redes LAN a LAN, ejemplo de ello tenemos a una organización que desee compartir sus recursos a través de todas sus oficinas o sucursales distribuidas en una amplia área geográfica.

Redes WAN.

Paradójicamente, según Olifer (2009), las redes de área amplia o WAN (*Wide Area Network*), pese a su complejidad, fueron las primeras en ser desarrolladas, conectaban computadoras distribuidas en una amplia área geográfica, ubicadas en diferentes ciudades y países. Forouzan (2002), nos señala que las redes WAN no sólo transmiten datos, también pueden transportar voz, imágenes, videos, entre otros. En contraste con las redes LAN, que depende de su propio hardware para transmisión, las redes WAN pueden utilizar diversos dispositivos de comunicación públicos, alquilados o privados, habitualmente en combinaciones. También puede existir una

variedad de WAN, la cual puede ser propiedad de una organización o empresa específica, a ésta se le denomina como red de empresa.

Metro Ethernet.

Según Johnson (2009), la tecnología Metro Ethernet, es una conexión de telecomunicaciones hacia Internet, típicamente utilizada para interconectar Web corporativa. Es una red que proporciona servicios de convergencia de voz, datos, servicios de video a velocidades Ethernet.

Cioara (2008) señala que las tecnología Metro Ethernet es de reciente aparición, surgió a principios del nuevo milenio como una alternativa viable a las conexiones WAN, como consecuencia del desplome económico de las compañías punto com, las cuales durante su breve existencia, dejaron tras de sí, numerosas redes de fibra óptica de alta velocidad no administrado bajo las calles de las ciudades, estas redes fueron adquiridas rápidamente por el servicio local de proveedores y fueron ofrecidas a los clientes locales.

Redes inalámbrica.

Para Tanenbaum (1997), las redes inalámbricas surgen ante la necesidad de conectar dispositivos como laptop, asistentes personales o PDA (*Personal Digital Assistants*) a redes LAN o WAN, puesto que la conexión por cables se dificulta para este tipo de dispositivos.

Frame relay.

Este tipo de red, según Tanenbaum (2003), está orientada a conexión, es decir, los paquetes se entregan en orden, esto significa que no se requiere control de errores ni de flujo, por lo que *Frame Relay* es lo más parecido a una LAN de área amplia. Por lo general, la conexión tipo *Frame Relay* se da mediante la conexión de una línea telefónica dedicada, donde existe uno o varios circuitos que interconectan diversos equipos informáticos y de comunicaciones, situados a gran distancia uno de otros, por lo general a cientos de kilómetros.

Medios de transporte o transmisión de datos.

Según Forouzan (2002), las computadoras y los dispositivos de comunicación, utilizan señales para representar los datos, estas señales son transmitidas de un dispositivo a otro en forma de energía electromagnética, las cuales viajan a través de un medio, sea este en el vacío, el aire u otros medios de transmisión.

De allí la importancia de los medios guiados, los cuales son aquellos que proporcionan un conductor, o medio de transmisión, para conectar un dispositivo con otro, entre ellos tenemos: Cables de pares trenzados, cables de fibra óptica y cables coaxiales, estos últimos debido a su obsolescencia han caído en desuso.

Par trenzado.

El cable de par trenzado existe con blindaje o STP (*Shielded Twisted Pair*) y sin blindaje o UTP (*Unshielded Twisted Pair*). El cable de par trenzado sin blindaje (UTP), es el más frecuentemente usado como medio de transmisión (ver Figura 4), debido a su bajo costo y facilidad de instalación. Está formado por dos conductores de cobre (par trenzado), cada uno en su aislamiento plástico, son trenzados debido a que si fuesen paralelos, las interferencias electromagnéticas originadas por conductores de electricidad producirían ruido en la transmisión. Por lo general los cables de redes contienen cuatro pares trenzados, es decir, ocho conductores. Existe de varias categorías, dependiendo de la capacidad o velocidad de transmisión.

Figura 4. Par Trenzado

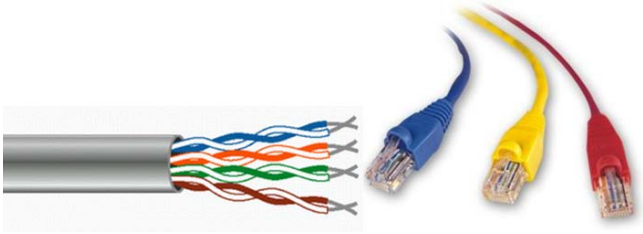

Figura 4. Cables de par trenzado UTP de 4 pares y su forma final una vez unidos a los conectores o RJ-45. Imagen tomada de http://concavoyconverso.blogia.com/2010/julio.php, consulta: 2010, Diciembre, 28.

El cable de par trenzado blindado o STP, posee una funda de metal o un recubrimiento de malla que rodea a los conductores, esto con la finalidad de aislar el ruido o la interferencia electromagnética, dicho blindaje es conectado a tierra.

Fibra óptica.

La fibra óptica, continúa Forouzan (2002), transmite las señales en forma de luz, están hechas de plástico o de cristal, medio por el cual se propaga la luz.

Dispositivos activos de red.

Según Forouzan (2002), los dispositivos que interconectan las redes son: repetidores, puentes, encaminadores o ruteadores y pasarelas, ver Figura 5.

Figura 5. Dispositivos de Red.

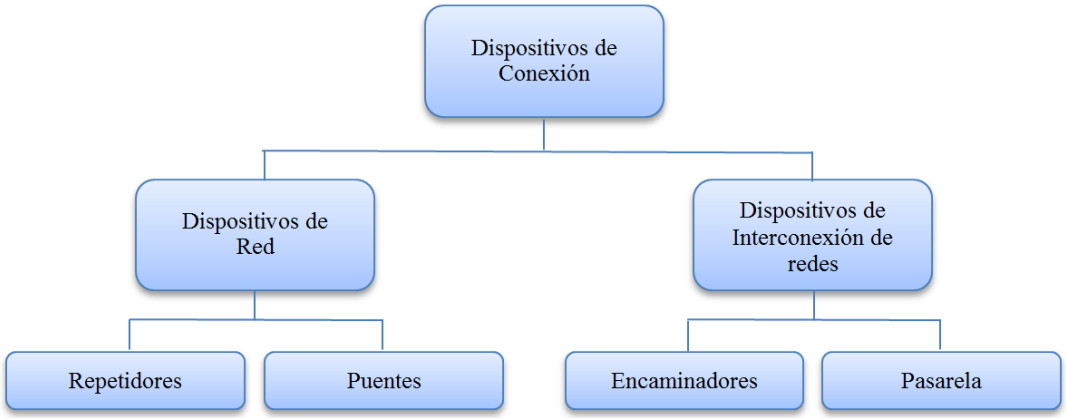

Figura 5. Representa los diversos dispositivos activos de red existentes. Adaptado de "Transmisión de datos y Redes de Comunicaciones", por Forouzan, 2002, (p. 594)

Repetidor o concentrador.

Un repetidor o regenerador es un dispositivo, debido a que las señales que viajan por la red recorren grandes distancias a través del medio de transporte, y sabiendo que las señales viajan en forma de energía eléctrica o lumínica, la señal tiende a atenuarse o disminuir de intensidad, por tal motivo el repetidor se hace necesario para evitar dichas pérdidas. Los repetidores son colocados a cierta distancia

uno del otro, permitiendo así extender la longitud física de la red más allá de sus limitaciones por atenuación de señal. El repetidor regenera la señal, mas no la amplifica

Puentes.

Tienen por misión dividir una red grande en segmentos más pequeños. También pueden retransmitir tramas entre dos LAN originalmente separadas, al contrario de los repetidores, los puentes poseen la lógica necesaria para separar el tráfico de cada segmento, de esta forma filtran el tráfico, siendo útiles para controlar la congestión y aislar enlaces con problemas, así mismo proporcionan seguridad mediante la división del tráfico.

Encaminadores o routers.

Los repetidores y puentes son sencillos dispositivos de hardware, Forouzan (2002) señala, que los encaminadores son más sofisticados que los dispositivos anteriormente descritos, tienen acceso a las direcciones del nivel de red y contienen software que facilitan determinar cuál de los diversos caminos existentes es el mejor para una transmisión determinada.

Pasarelas.

Una pasarela es un convertidor de protocolos, un encaminador transfiere, acepta o retransmite paquetes sólo entre redes que utilizan protocolos similares, en contraposición, una pasarela puede aceptar un paquete formateado para un protocolo y convertirlo a un formato distinto antes de encaminarlo.

Una pasarela está constituido generalmente por software instalado dentro de un encaminador, la pasarela está compuesta por los protocolos utilizados por cada red enlazada al encaminador, por tal motivo es capaz de traducir los mismo.

Seguridad en redes de datos.

Para Stalling (2004), vivimos en una era donde la conectividad electrónica es universal, sin embargo, existen peligros representados por virus, hackers y fraudes

electrónicos; por lo que no hay momento en el que no importe la seguridad. A continuación se exponen algunos de los tópicos más importantes relativos a la seguridad en las redes de datos.

Antecedentes e importancia de la seguridad de redes.

La seguridad es ahora parte fundamental de las redes de datos, según señala Cisco Networking Academy (2010), ella envuelve un conjunto de protocolos, tecnología, dispositivos, herramientas y técnicas para asegurar y mitigar los posibles ataques a las redes de datos. Esta iniciativa por la seguridad se inició en los albores de la década de 1960, pero no es sino hasta principios del siglo XXI cuando se hace más patente, convirtiéndose en un conjunto de soluciones para las redes modernas.

La seguridad en redes es en gran medida un esfuerzo por estar un paso delante de los atacantes o hackers, así como la medicina intenta prevenir enfermedades, los profesionales de la seguridad intentan prevenir los ataques y reducir al mínimo sus efectos, todo ello en pro de la continuidad del negocio de cada organización.

Muchas organizaciones han sido creadas específicamente para promover la seguridad en redes de datos, estas organizaciones establecen normas, fomentan la colaboración y proporcionan oportunidades de desarrollo laboral para los profesionales de la seguridad. Pero no es un trabajo sencillo, la seguridad en redes de datos se hace difícil, sobre todo por el amplio ámbito que le caracteriza, debido a ello se subdivide en dominios o áreas que faciliten su estudio e investigación.

Las políticas de seguridad de redes de datos es otro de sus aspectos, son creadas por empresas y organizaciones gubernamentales para proporcionar un marco de trabajo que guie a la acción. De esta forma, todas las prácticas de seguridad de redes de datos se relacionan y son guiados por las políticas de seguridad.

Así como la seguridad de red se divide en dominios, los ataques se clasifican por sus características distintivas. Los virus, gusanos y troyanos son tipos específicos de ataques de red. De manera general se clasifican como ataques de reconocimiento,

de acceso y denegación de servicios. Aspectos antes señalados y explicados en esta investigación.

Calidad de servicio.

Respecto a la calidad de servicio o QoS (*Quality of Service*), Mishra (2008), señala que las vulnerabilidades y los ataques a las redes de datos, afectan negativamente la calidad de servicio, pues degradan la calidad del mismo; las redes de datos, como Internet, sólo hacen su mejor esfuerzo para transportar los paquetes de datos desde su origen hasta su destino; pero sin ningún tipo de garantía. Por este motivo la calidad de servicio es uno de los desafíos imperantes para las redes de datos.

Seguridad del enrutamiento.

Las propiedades deseables, continua Mishra (2008), de una ruta segura son: La puntualidad, el orden, la autenticación, la autorización, la integridad de datos, la confidencialidad y el no repudio. Cada una de estas características tiene técnicas propias que permiten su aplicabilidad en las redes de datos, como se puede observar en la Tabla 1.

Tabla 1. Seguridad del Enrutamiento

Propiedad	Técnica
Puntualidad.	Marca de tiempo o timestamps.
Orden.	Número secuenciador.
Autenticidad.	Contraseñas, certificados.
Autorización.	Credencial.
Integridad.	Firma digital.
Confidencialidad	Encriptación.
No repudio.	Encadenamiento de la firma digital.

Nota: Adaptado de “Security and Quality of Service in Ad Hoc Wireless Networks” de Mishra (2008), p.130.

Software malicioso.

Al respecto Jimeno (2008), señala que son programas que se ejecutan en un computador con la finalidad de alterar su correcto funcionamiento. Un virus tiene por objeto expandirse por la red o redes a la cual el computador infectado esté conectado, protegiéndose y ocultándose para no ser destruido. El modo de actuar del virus depende de su naturaleza, por lo que no todos tienen la misma misión. La concepción o el diseño de un virus toma en cuenta tres fases fundamentales, que determinan su forma de actuar, estas son:

- Fase de reproducción: Esta fase es fundamental, pues garantiza la supervivencia del virus, ya sea en el equipo infectado o propagándose por la red.
- Fase de ataque: También conocido como *PayLoad*, y dependerá de las intenciones del virus, si el virus busca causar daño directo y no congestión (de las redes o del espacio de los medios de almacenamiento masivos), esta fase será vital para su correcto funcionamiento y su misión destructiva.
- Fase de defensa: Esta fase permite la detección de programas antivirus, alargando la vida del virus en el sistema infectado, burlando los mecanismos de prevención y detección.

Según Aycock (2006), existen cuatro amenazas claves a considerar: el *spam*, los *bugs* o errores en el software, la denegación de servicio y los programas maliciosos. Como se puede observar tres de estas cuatro amenazas son patentes en las redes de datos. El termino *spam* es utilizado para describir la abundancia de basura no solicitada en los correos electrónicos, según este autor, más del 70% del tráfico de correo electrónico está clasificado en esta categoría.

No existe una clasificación o taxonomía científicamente elaborada para clasificar los virus, tampoco una definición universalmente aceptada de términos como “virus” o “gusano”, sino más bien se describen las características comunes de

estas amenazas. El malware puede ser dividido en tipos, de acuerdo al método en que operan, esta clasificación según Aycock (2006), es la siguiente:

- Auto replicación: El virus intenta propagarse mediante la creación de nuevas copias o instancias; aunque el malware puede propagarse en forma pasiva, como por ejemplo al ser copiado accidentalmente por un usuario, esto no se trata de auto replicación.
- Crecimiento de la población: Es el índice de crecimiento por auto replicación del malware, si no se auto replica entonces tiene crecimiento nulo.
- Malware parasitario: Requiere de un código ejecutable para poder existir, ya sea el sector de arranque del disco duro, un código binario, una aplicación, entre otras.

Cortafuegos o firewall.

Para Stallings (2004), los cortafuegos son un medio de protección eficaz para los sistemas basados en redes de datos, mientras simultáneamente proporcionan acceso al exterior de dichas redes. Los cortafuegos, *firewall* o pasarelas, son definidos por Sackett (2002), como herramientas que proporcionan seguridad a las redes contra los atacantes.

Las principales características de un *firewall* según Bellovin (1994 c.p. Stallings, 2004), son:

- Todo trafico entrante y saliente debe pasar a través del cortafuegos, esto se consigue bloqueando todos los accesos restantes a la red local, excepto al cortafuegos.
- Sólo se permitirá el tráfico autorizado, previamente definido por la política de seguridad.
- El propio cortafuego debe ser inmune a la penetración.

Gestión de red.

Para Stallings (2004), un sistema de gestión de red es un conjunto de herramientas utilizadas para la supervisión y control de la red y está integrado por:

- Una sola interfaz de operador con un grupo de comandos para realizar la mayor parte, o todas las tareas de gestión de red.
- El hardware y software necesario para su funcionamiento debe estar dispuesto en una estación de trabajo, que permita su administración.

Proxy.

Según Stallings (2004), el servicio proxy permite la administración de la red, es parte de un conjunto de herramientas para su supervisión y control. Los sistemas de gestión de red se componen de hardware y software que mediante comandos sencillos permiten la administración de la red, como por ejemplo bloquear páginas de Internet con contenido violento o de adultos (pornografía).

Normas internacionales de seguridad.

Los estándares y mejores prácticas internacionales que sirven de base a la presente investigación son CobiT 4.1, ITIL V3 e ISO/IEC 27002, a continuación se describen los resultados de cada uno de ellos:

CobiT 4.1.

Según Brand y Boonen (2007), CobiT (*Control Objectives Control Objectives for Information and related Technology*), u Objetivos de Control para la Información y la Tecnología Relacionada, es un modelo diseñado para gobernar las funciones de la Tecnología de Información (TI). Este modelo fue desarrollado en principio por la ISACF (*Information Systems Audit and Control Foundation*) e ISACA (*Information Systems Audit and Control Association*). En 1999 las labores realizadas por ISACF fueron transferidas a ITGI (*IT Governance Institute*), el cuál actúa como órgano independiente de ISACA.

CobiT comenzó a desarrollarse, según Brand y Boonen (op. cit.), en 1994 con una primera versión publicada en 1996 (basado en auditoría), con subsiguientes versiones posteriores en 1998 (haciendo énfasis en control), en el año 2000 (desarrollando en concepto de administración) y el año 2005 (añadiendo gobierno de TI) ver Figura 6. La versión actual de CobiT se enfoca en el marco de gobierno de las Tecnologías de la Información (TI).

De esta forma CobiT apoya la gobernabilidad de TI, al proporcionar una descripción completa de los objetivos de control de todos los procesos de TI, ofreciendo la posibilidad de examinar minuciosamente cada uno de estos procesos. Esto ayuda a comprender, evaluar y gestionar los riesgos relativos a TI, proporcionando los instrumentos necesarios para tal fin.

Dicho instrumento permite a los gerentes reducir la brecha con respecto a los requisitos de control, sistemas de información y las tecnologías de la información junto con los problemas y riesgos del negocio, con la finalidad de comunicar tal nivel de control a los interesados, permitiendo así de desarrollo de políticas claras y buenas prácticas para el control de las TI dentro de la organización.

Grupos Objetivos de CobiT.

Continúa Brand y Boonen (2007), que de acuerdo a ISACA, CobiT está orientado principalmente a la gestión, los usuarios empresariales de TI y los auditores, entre los principales involucrados tenemos:

- Gerentes: Son aquellos que tienen la responsabilidad ejecutiva de guiar los destinos de las organizaciones, necesitan información para el control de las operaciones internas y para dirigir los procesos de negocio, siendo las TI una parte integral de dichas operaciones. CobiT puede ayudar a las empresas y a los gerentes de TI a equilibrar el riesgo de la inversión y a controlar el entorno de las TI, la cual es con gran frecuencia, impredecible.

Figura 6. Desarrollo de las Diferentes Versiones de CobiT

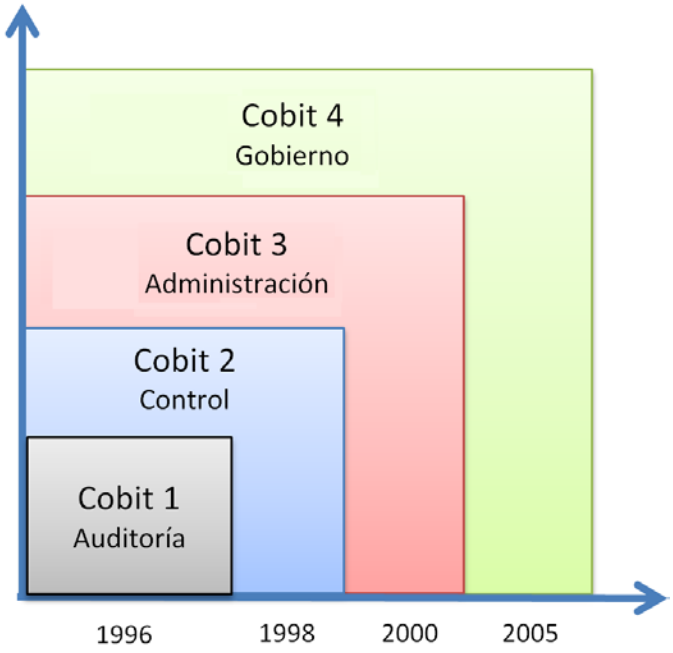

Figura 6. Muestra el desarrollo de CobiT a través del tiempo y los énfasis en funciones de auditoria, control, administración y gobierno en cada uno de ellos. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 21)

- Usuarios finales: La mayoría de las organizaciones se dan cuenta que tener el derecho de los servicios de TI es la responsabilidad del propietario de procesos de negocio. Este siempre es el caso cuando la prestación de servicios de TI se delega a los proveedores de servicios internos o externos. CobiT ofrece un marco para obtener garantías sobre la seguridad y control de los servicios de TI que aporten las partes internas o externas.
- Auditores: Con el fin de proporcionar una garantía independiente de la calidad y la aplicabilidad de los controles, las organizaciones utilizan los auditores. Con frecuencia, un comité de auditoría en el consejo o la alta dirección es quien dirige los procesos de auditoría. CobiT ayuda a los auditores a estructurar y fundamentar sus opiniones, así como a ofrecer asesoramiento a la dirección sobre cómo mejorar los controles internos.

- Negocios y Consultores de TI: Los nuevos marcos y métodos en el gobierno de TI con frecuencia se originan fuera de la organización. Consultores de negocio y TI pueden aportar este conocimiento en la organización y así proporcionar asesoramiento a las organizaciones y a la administración de TI en la mejora de la gobernabilidad de TI.
- Profesionales de TI en gestión de servicios: En la comunidad de gestión de servicios, ITIL (*Information Technology Infrastructure Library)* resulta ser el marco de trabajo dominante. CobiT refuerza el mejoramiento de la gestión de servicios de TI, al proporcionar un marco que cubre el ciclo de vida completo de los sistemas de servicios.

En el Anexo C del presente estudio se profundiza sobre el contenido de CobiT 4.1, su estructura y las interrelaciones de sus elementos.

ITIL V3.

Según De Jong et al. (2008), la Biblioteca de Infraestructura de Tecnologías de Información (*Information Technology Infrastructure Library* ITIL), ofrece una aproximación sistemática para la entrega de servicios TI de calidad. ITIL fue desarrollado en los años 1980 y 1990 por la Central de Informática y Telecomunicaciones de la Agencia (*Computer and Telecommunications Agency* CCTA), denominada ahora la Oficina de Gobierno y Comercio (*Office of Government Commerce*, OGC), bajo contrato con el Gobierno del Reino Unido.

Desde entonces, ITIL ha proporcionado no sólo un mejor marco de trabajo para la práctica basada en la gestión de TI, sino también un enfoque y una filosofía compartida por las personas que trabajan con ella. ITIL ha sido actualizada en dos ocasiones, la primera vez en el período 2000-2002 Versión 2 (V2), y la segunda vez en 2007 (V3). ITIL es apoyado por el *IT Service Management Forum* (itSMF), una organización internacional sin fines de lucro dedicada a apoyar el desarrollo de la gestión de servicios. Se compone de un número cada vez mayor de los capítulos

nacionales, en la actualidad más de cincuenta, con itSMF como órgano de control internacional.

En el Anexo D de la presente investigación se describe en profundidad el contenido de la librería ITIL 3.0.

Normas ISO, Serie 27000.

Desde 1901 la BSI (*British Standards Institution*) como primer ente normalizador a nivel mundial, es la responsable de publicar normas, según ISO2700.es (2011). La norma BS 7799 aparece por primera vez en 1995 con la finalidad de proporcionar un conjunto de buenas prácticas para la gestión de la seguridad de la información de las empresas. La primera parte de la norma (BS 7799-1) fue desarrollada como una guía de buenas prácticas, para la cual no había certificación, pero es en la segunda parte (BS 7799-2) publicada en 1998 la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Posteriormente ambas partes de la norma BS 7799 se revisaron en 1999, la primera parte se adoptó como ISO (*International Organization for Standardization*), bajo en número ISO 17799 en el año 2000.

En el año 2002 se revisó el BS 7799-2 con la finalidad de adecuarla a la filosofía de normas ISO de sistemas de gestión. En 2005 con más de 1700 empresas certificadas en BS 7799-2, se publicó el estándar ISO 27001 al mismo tiempo que se revisó y actualizó el estándar ISO 17799, está última tomó el nombre de ISO 27002:2005. Sin embargo, ISO continúa desarrollando dicha norma, para así dar soporte a las organizaciones en la interpretación y aplicación de la ISO/IEC 27001, la cual es la norma principal y única certificable dentro de la serie.

Fundamentalmente, continúa ISO2700.es (2011), ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC (*International Electrotechnical Commission*) que establecen un marco de trabajo para la seguridad de la información

y que puede ser adaptada por cualquier organización sin importar su naturaleza o su magnitud.

En el Anexo E de la presente investigación se presenta las características de la Serie ISO 27000.

Marco Organizacional

A continuación se expone el marco organizacional que sirvió de contexto a la presente investigación, debido al inconveniente que resultaría señalar todos y cada uno de las diversas oficinas ministeriales, direcciones, departamentos y divisiones que la componen, sólo se han tomado en cuenta las más importantes respecto a la investigación a realizar.

Ministerio del Poder Popular para la Educación.

La investigación se realizó en la Dirección de Informática del Ministerio del Poder Popular para la Educación (ver Figura 7), específicamente involucró a la Dirección de Operaciones y Base de Datos.

La Dirección de Informática es el ente encargado dentro del MPP Educación de coordinar y ejecutar todas aquellas labores referida al uso de las tecnologías de información, como por ejemplo la creación de nuevas aplicaciones, labor que es llevada a cabo por la Dirección de Sistemas, también se le presta servicio de soporte técnico a los usuarios que presenten problemas con el software o hardware instalado en sus computadores, dicha servicio es prestado por la Dirección de Apoyo a Usuarios.

En lo relativo al tendido y mantenimiento de las redes de datos y telefonía, así como de la administración de los dispositivos activos de red del edificio sede del MPP Educación, se encuentra la Dirección de Redes y Telefonía. Finalmente la Dirección de Operaciones y Bases de Datos es la unidad responsable por la administración de los equipos servidores, en dichos equipos se concentran todas las

aplicaciones compartidas, tal como el sistema de nómina, control de estudios, repositorios de archivos, portales, entre otros.

Figura 7. Organigrama Simplificado del MPP Educación

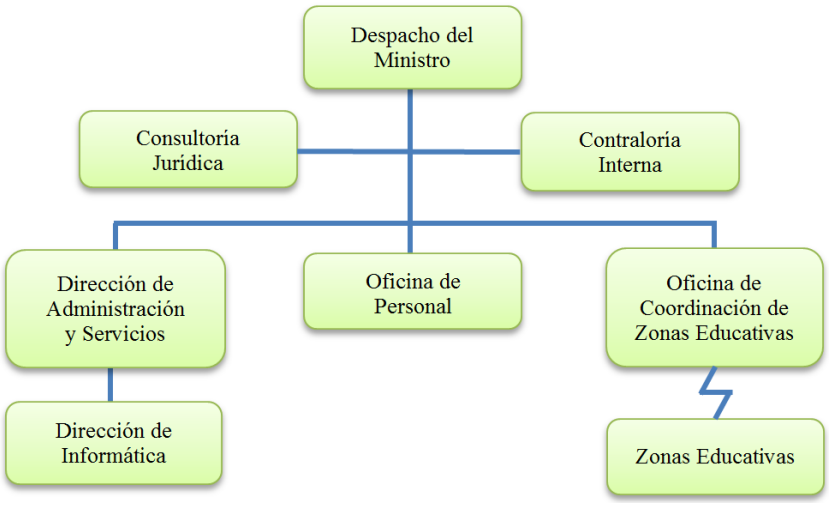

Figura 7. Organigrama simplificado del MPP Educación, donde se muestran las zonas educativas como entes desconcentrados, elaborado por el autor.

Además de esta función, la Dirección de Operaciones y Bases de Datos administra todos los enlaces de redes de datos, tanto internos, que comunican el edificio sede del MPP Educación con las diversas zonas educativas del país, como externos, al administrar la salida de los portales institucionales a la Web, así como también ofrecer a los usuarios el servicio de Internet (ver Figura 8).

La información relativa a las redes de datos se encuentra plasmada en algunos manuales operativos y de normas y procedimientos, así como en gráficos que esquematizan la estructura de la red existente, la información contenida en dichos manuales servirá como referencia para el diseño del sistema de seguridad de redes de datos, objetivo fundamental de la presente investigación.

Figura 8. Organigrama Simplificado de la Dirección de Informática

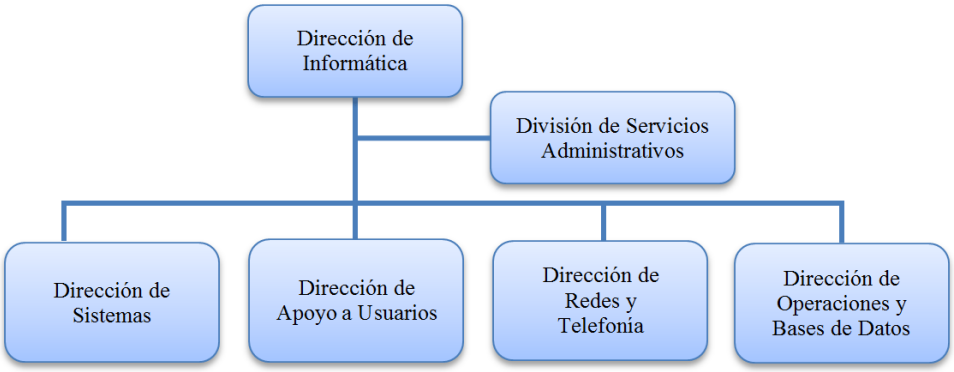

Figura 8. Organigrama simplificado de la Dirección de Informática, elaborado por el autor.

Bases Éticas y Legales

Entre las bases éticas y legales que sirvieron de marco a la presente investigación tenemos:

La Constitución Nacional de la República Bolivariana de Venezuela, República Bolivariana de Venezuela (1999), de los Derechos Humanos y Garantías y de los Deberes, Capítulo VI, de los derechos culturales y educativos. Artículo 110:

Establece que el Estado reconocerá el interés público de la ciencia, de la tecnología, el conocimiento, la innovación y sus aplicaciones y de los servicios de información, así como también garantizará el cumplimiento de los principios éticos y legales que se deberán regir las actividades en cuanto a la investigación científica, humanística y tecnológica, por ser estos, instrumentos fundamentales para el desarrollo económico, social y político de la nación, así como también para la seguridad y soberanía nacional. En tal sentido, el Estado destinará los recursos suficientes y creará el sistema nacional de ciencia y tecnología. Para el sector privado le corresponderá aportar los recursos para las mismas.

Decreto N°. 3.390. República Bolivariana de Venezuela (2004):

Mediante este decreto se dispone que la administración pública nacional emplee prioritariamente software libre desarrollado con estándares abiertos, en sus sistemas, proyectos y servicios informáticos. Este está compuesto por 14 artículos, en los cuales se detalla cuáles son los lineamientos del estado venezolano en cuanto a la búsqueda de la soberanía tecnológica y sobre todo al apoyo que proporcionará a los distintos organismos responsables para la prosecución de estos lineamientos. De igual forma deja claro la responsabilidad del ejecutivo nacional, de promover y desarrollar mecanismos orientados a capacitar e instruir a los usuarios en el uso del software libre. Finalmente deja claro que todos los organismos del Estado, deben llevar a cabo el diseño de sus planes de implantación progresiva del software libre, en un plazo no mayor de 24 meses, dependiendo de las características de los sistemas informáticos.

Ley Especial Contra Los Delitos Informáticos. República Bolivariana de Venezuela (2001).

Esta Ley tiene por objeto, la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los cometidos mediante el uso de dichas tecnologías. Dispone de 33 artículos que van desde varios conceptos básicos tecnológicos y de informática, así como sanciones, responsabilidad de las personas jurídicas, contra los sistemas que utilizan tecnologías de información, acceso indebido, sabotaje o daños a sistemas, espionaje informático, hurto, fraude, entre otros.

CAPITULO III

MARCO METODOLÓGICO

Nivel de Investigación

Según Palella (2006), la investigación proyectiva tiene por objeto el diseño o la creación dirigida a cubrir una necesidad basada en conocimientos anteriores. Que en el caso de la presente investigación consistió en diseñar un sistema de seguridad para redes de datos (necesidad), basada en las mejores prácticas (conocimientos anteriores).

A lo anterior se debe agregar lo expresado por UPEL (2006), donde se describe como modalidad de investigación, la de proyectos factibles, la cual define como una investigación, elaboración y desarrollo de una propuesta de modelo operativo que sirva para dar solución a una problemática existente, requerimiento o necesidad de una organización o grupos sociales. También señala que puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. Esta definición es similar a la dada por Ballestrini (2002), a lo que este autor añade que; este tipo de investigación se caracteriza por el diagnóstico de una situación existente y la determinación del hecho estudiado, con la finalidad de formular un modelo operativo en función de las exigencias de la realidad abordada.

Profundizando la concepción de proyecto factible, Hurtado (2010-a), cambia la denominación a investigación proyectiva y establece que este tipo de estudio propone soluciones a una situación determinada a partir de procesos de investigación compuesto a su vez por la exploración, descripción, explicación y finalmente la propuesta de alternativas de cambio, pero deja en claro que no necesariamente

conlleva la ejecución de la propuesta. Esta autora propone como ejemplos de este tipo de investigación lo estudios de arquitectura, los proyectos de tipo económico, social, educativo y tecnológicos.

En conclusión y según lo anteriormente expuesto, se tiene que la presente investigación es de tipo proyecto factible o investigación proyectiva, que tal como lo señala Hurtado (2010-b), debido a que potencia el desarrollo tecnológico.

Diseño de Investigación

El diseño de la investigación, según Hurtado (2010-b), establece que depende de los aspectos operativos relacionados con la recolección de los datos. Hernández (2010), define diseño de investigación como el plan o la estrategia que se desarrolla para obtener la información requerida en una investigación.

En relación al diseño de la investigación UPEL (2006) señala que los proyectos factibles pueden tener el apoyo de una investigación de tipo documental, de campo o un diseño mixto que incluya ambas categorías.

Partiendo de la definición de diseño de investigación, es decir, la forma en la que se recopilarán los datos, se hace necesario en primer lugar describir las características de la investigación proyectiva, para luego establecer las fuentes y tipos de datos a recopilar.

A este respecto Hurtado (2010-b), señala que la investigación proyectiva tiene por característica partir de la identificación de un evento a modificar, es decir, de una problemática existente a la cual se le dará solución, por lo que amerita de la realización de un diagnóstico de la situación, lo que además permite corroborar que la propuesta es necesaria.

Según lo planteado anteriormente y en base a los objetivos de la presente investigación, se debe diagnosticar una problemática existente, por lo que es necesario desarrollar una investigación de campo, es decir, tomar los datos en el lugar donde ocurren los hechos. Pero además, se debe diseñar una solución que incluye la propuesta de un escenario donde los problemas encontrados sean resueltos

satisfactoriamente, a partir de la investigación y la adaptación de un conjunto de conocimientos disponibles, los cuales se encuentran en los documentos y bibliografía existente, esto implica el desarrollo de una investigación de tipo documental. Este razonamiento confirma lo establecido por UPEL (2006), donde se enmarca el diseño de la investigación de proyecto factible, como de tipo mixto, combinando la investigación de campo, para diagnosticar y establecer la problemática relacionada con la seguridad en las redes de datos, y la documental, basada en las mejores prácticas existentes para la seguridad de la redes de datos, originando así una propuesta que permita solucionar el problema existente. Por lo que en conclusión, la presente investigación se fundamentó en el diseño mixto.

Técnicas e Instrumentos de Recolección de Datos

Las técnicas de recolección de información, según Palella (2006), son las distintas formas o maneras de obtener la información, para la recolección de datos se utilizan técnicas como la observación, entrevista, encuesta y pruebas entre otras. Es en definitiva cualquier recurso del cual pueda valerse el investigador para acercarse a los fenómenos y extraer de ellos información. El instrumento sintetiza toda la labor anterior a su aplicación, resume los aportes del marco teórico al permitir la selección de datos que corresponden a los indicadores, y en consecuencia, a las variables o conceptos utilizados. Expresan el contenido empírico de la investigación. De esta forma mediante la adecuada construcción de los instrumentos de recolección de información, es como se puede evidenciar la correspondencia entre la teoría y la práctica

Según Hernández (2010), señala que una vez elegido el diseño de la investigación y la muestra adecuada (probabilística y no probabilística), la siguiente etapa consiste en recolectar los datos relativos a los atributos, conceptos o variables de la unidades de análisis. Recolectar datos para este autor implica elaborar un plan detallado de procedimientos que permitan reunir dichos datos con un propósito específico, dicho plan debe contemplar lo siguiente:

- Las fuentes de donde se obtendrán los datos, los datos pueden ser proporcionados por personas, mediante observación o pueden encontrarse en documentos, archivos, bases de datos, entre otros.
- Ubicación de las fuentes de datos.
- Medios utilizados para recolectar la información.
- Una vez recolectado los datos, se debe preparar de antemano el procedimiento mediante el cual serán analizados y condensados para dar respuesta al planteamiento del problema.

Continúa Hernández (2010), dicho plan se nutre de diversos elementos, tales como:

- Las variables, que son los conceptos o atributos a medir, las cuales están contenidas en el planteamiento del problema.
- Las definiciones operacionales, es decir, la manera como se han operacionalizado las variables, este aspecto resulta vital para determinar el método a utilizar para medirlas, es fundamental para realizar las inferencias de los datos.
- La muestra.
- Los recursos disponibles, tal como tiempo, apoyo institucional, económico, entre otros.

Profundizando en el tema, Hurtado (2010-b), denomina a esta parte de la investigación como el abordaje, definida como la forma en que el investigador se acerca a sus eventos de estudio, señala que el abordaje puede tener diferentes maneras, según el grado de estructuración previa del estudio, este acercamiento puede ser flexible, inestructurado y abierto. El otro tipo de abordaje, denominado cosmológico, se caracteriza por ser estructurado, cerrado y focalizado. Según la perspectiva de investigación, continúa Hurtado (op. cit.), se clasifica en, etic o emic, ambos se refieren al punto de vista del investigador en relación al fenómeno estudiado. En el caso de etic, el observador es ajeno o externo al fenómeno

observado. Por el contrario, el abordaje emic, implica que el investigador forma parte del objeto estudiado. También señala que de acuerdo el grado de participación de los investigados, puede ser endógena; donde la investigación surge como inquietud de la colectividad afectada por la problemática y en donde los miembros de dicha colectividad participan activamente en la toma de decisiones correspondientes a cada una de las fases del estudio. Por el contrario, el abordaje exógeno, es aquel que parte del interés del investigador por conocer algún evento o fenómeno determinado, los investigados se limitan a proporcionar la información que el investigador solicita.

De acuerdo a la anterior clasificación, el abordaje de esta investigación se puede clasificar como estructurada, tipo emic, ya que el investigador forma parte del objeto estudiado y exógena, debido a que el investigador dirigirá cada una de las fases de la investigación.

Población y muestra.

Todo estudio implica la determinación del tamaño poblacional y muestral necesario para su ejecución, para Palella (2006), la población de una investigación es el conjunto de unidades de las que se desea obtener la información y sobre las que se va a generar conclusiones, donde las unidades pueden ser personas, familias, grupos sociales, entre otros. Existen dos alternativas para el estudio de la población; el primero consiste en tomar la totalidad de la misma, el segundo en tomar una parte representativa del conjunto de características de dicha población, esta última se denomina muestra.

El tipo de muestreo utilizado en este estudio es, según Palella (2006), muestreo de tipo no probabilístico intencional, debido a que el investigador establece previamente los criterios para seleccionar las unidades de análisis. La presente investigación se realizó en el Departamento de Operaciones y Bases de Datos del MPP Educación (que actuó como fuente de datos), compuesto por un jefe de unidad y cinco administradores de sistemas, esto debido a que es la totalidad del personal responsable de las labores relacionadas con la administración de las redes de datos y del cual el autor forma parte.

En cuanto a la investigación documental, la misma se basó en la aplicación de tres normas internacionales, como lo son: CobiT 4.1, ITIL V3 e ISO/IEC 27002, las cuales constituyeron la segunda fuente de datos.

Instrumentos de recolección de datos.

Dentro de los instrumentos más utilizados para la recolección de datos, tenemos según Palella (2006), la observación, la cual es el empleo sistemático de los sentidos orientados a la captación de la realidad que se estudia. Aunque pudiese ser un instrumento valioso, la complejidad de la presente investigación obliga al uso de herramientas que permitan conocer profundamente el fenómeno estudiado, como lo es la seguridad en la redes de datos.

La entrevista es otra de las técnicas citadas por Palella (2006), en donde mediante un diálogo que se realiza entre dos o más personas, el investigador obtiene información sobre el problema planteado. Tiene por desventaja que la persona entrevistada dará su opinión subjetiva de aquello que se le pregunte. Por tal motivo es recomendable estructurar previamente la entrevista. Esta técnica en recomendable para poblaciones pequeñas.

La encuesta es otra técnica destinada a obtener datos, consiste en un listado de preguntas escritas que se le entregan las personas, fuentes de información, quien de forma anónima las responden, es recomendada para sectores amplios de la población.

Finalmente se encuentra el fichaje, el cual consiste en registrar por escrito los datos obtenidos en la investigación bibliográfica. A lo que Ballestrini (2002), añade además del fichaje:

- La observación documental: Lectura general del texto.
- La presentación resumida: Es la síntesis de las obras consultadas.
- El resumen analítico: Descubre la estructura del texto consultado, delimitando su contenido básico.
- El análisis crítico: Contiene las dos técnicas anteriores, pero introduce su evaluación interna.

Debido a que el diseño de la presente investigación fue de tipo mixto, es decir envuelve la investigación de campo y documental, además de contar con una población reducida, se seleccionó como instrumento de recolección de información:

- La entrevista estructurada para cubrir la investigación de campo.
- El fichaje por medio electrónico y el análisis crítico, que permitió la aplicación de las normas CobiT 4.1, ITIL V3 e ISO/IEC 27002 a la realidad existente, constituyó la investigación documental.

Medición, validez y confiabilidad.

Para Hernández (2010), la medición es un proceso en el cual se vinculan conceptos abstractos con indicadores empíricos, por lo que implica organizar, clasificar y en ocasiones cuantificar la información. Para ello se emplean instrumentos de medición, como los mencionados en el apartado anterior.

La confiabilidad para Hernández (2010), es el grado en que un instrumento produce resultados coherentes y consistentes, es decir, en caso de ser aplicados consecutivamente sobre la misma muestra y en un espacio corto de tiempo, el resultado debería ser el mismo. Para Palella (2006), la confiabilidad es la ausencia de error aleatorio en el instrumento de recolección de datos, es decir, si está libre de las desviaciones producidas por errores causales, también recomienda, que posterior a la validación del instrumento, este se aplique sobre un pequeño grupo de la población, a manera de prueba piloto, con el objeto de verificar si produce los resultados deseados.

En cuanto a la validez, continua Hernández (2010), es el grado en que un instrumento realmente mide la variable que pretende medir, que en verdad haga lo que dice hacer. De esta forma la validez es un concepto del cual puede tenerse diferentes tipos de evidencia, tales como:

- Evidencia relacionada con el contenido, la validez de contenido: Se refiere al grado en que un instrumento refleja un dominio específico de contenido de lo que se pretende medir.

- Evidencia relacionada con el criterio, la validez de criterio: En cuando se establece la validez de un instrumento propio de medición, al comparar sus resultados con los de algún criterio externo que pretende medir la misma variable.
- Evidencia relacionada con el constructo, la validez de constructo: Se refiere a que tan exitosamente un instrumento representa y mide un concepto teórico, es decir, determina qué está midiendo y cómo opera para medirlo.

Pero existe otra forma de medir la validez, continúa Hernández (2010), denominada validez por expertos, el cual se refiere al grado en que un instrumento de recolección de datos mide la variable en cuestión, de acuerdo al juicio o criterio de personas calificadas, con amplios conocimientos y experiencia al respecto. Por lo que esta última forma de medir la validez se constituye en otro tipo de evidencia. A lo anterior Palella (2006) agrega, que el número de expertos puede variar entre tres, cinco o siete, pero que en todo caso dicho número siempre debe ser impar.

La presente investigación utilizó como pruebas de validez el juicio de tres expertos, los cuales validaron el instrumento de recolección de información, dicho instrumento fue incluido en el Anexo A, las constancias de validación se encuentran en el Anexo B. Cabe destacar la realización de tres pruebas pilotos, con el objeto de probar la pertinencia y eficacia de las preguntas a plantear, esto según recomendación de Hernández (2010), con el objeto de medir la confiabilidad y la validez inicial del instrumento. Una de las pruebas fue realizada a un miembro integrante de la Dirección de Operaciones y Bases de Datos, la persona que fue seleccionada es la encargada de la administración de la plataforma de telecomunicaciones, las otras dos fueron realizadas en el Departamento de Redes, la cual es una dirección afín a Operaciones y Bases de datos. Dichas pruebas pilotos arrojaron como resultados la modificación de algunas de las preguntas del cuestionario, las cuales debieron ser clarificadas mediante la descripción del concepto al cual hacían referencia. Por ejemplo en la pregunta 14 “¿Usualmente se activan para su funcionamiento los avisos o logs de los sistemas?”, se le debió añadir el concepto de “log”, de la siguiente

manera: “Entendiéndose por log, los archivos o registros que automáticamente son generados por el sistema para reportar fallos o ataques”, esto hizo más entendible el instrumento de recolección de información.

Las variables, sus dimensiones e indicadores.

En este punto de la investigación se hace necesario definir las variables de investigación, establecer sus dimensiones, indicadores, así como su operacionalización.

Una variable, según Sabino (2006), es cualquier característica o cualidad de la realidad que puede asumir diferentes valores, por lo que pueden ser cualitativas o cuantitativas, tomar valores continuos (infinitos valores) o discretos (valores enteros). Según este autor, existen al menos tres tipos de variables, dependiendo de sus relaciones. Las variables independientes, las cuales no se encuentran condicionadas por ninguna otra variable, las variables dependientes, condicionadas por las variables independientes y las variables intervinientes que actúa entre las anteriormente mencionadas (ver Figura 9).

Figura 9. Tipos de Variables Según sus Relaciones

Figura 9. Las variables de investigación y sus relaciones, elaborado por el autor.

Las variables, continúa Sabino (2007), poseen sub-cualidades que la integran, éstas se denominan dimensiones, las cuales son los componentes significativos de una variable. Arias (2006) complementa el concepto de dimensión al plantear que éstas integran a las variables complejas y son el resultado de su análisis y descomposición, entendiéndose por variable compleja aquellas que se pueden descomponer en dos

dimensiones como mínimo. A su vez, las dimensiones se descomponen en indicadores, definidas por Hurtado (2010-b), como aspectos específicos y perceptibles de un evento que dan cuenta de la presencia o intensidad del mismo, a modo de indicios. Palella (2006) añade que los indicadores son elementos, factores, rasgos o componentes más representativos, característicos o típicos de una variable.

Definición operacional.

La definición operacional consiste según Palella (2006), en identificar las variables a estudiar y establecer el significado que el investigador les atribuye dentro de la investigación. Esta definición conceptual o nominal se limita a explicar el significado de la variable, utilizando para ello un lenguaje sencillo. De esta manera se identifican los elementos y datos empíricos que expresan y especifican el fenómeno estudiado, indican qué hacer para que el investigador pueda realizar sus observaciones. Así la definición operacional asigna significado a la variable, describiéndola en términos observables y comprobables para poder identificarla, a través de la caracterización o tipificación proporcionados por sus indicadores.

Definición operacional de la presente investigación.

Tabla 2. Definición Operacional

Objetivos Específicos	Variables	Definición
1. Conocer la situación de seguridad de las redes de datos en el MPP Educación.	Problemática de la seguridad en las redes de datos que se presenta en el MPP Educación.	Permite determinar los problemas de seguridad en redes de datos que en la actualidad están presentes. Conocer las fortalezas y oportunidades que pueden ser aprovechadas para la propuesta, así como también las debilidades y amenazas que deben ser subsanadas.
2. Determinar cuáles de las mejores prácticas y estándares, relativos a la seguridad de datos y redes, pueden ser aplicados al problema de estudio.	Normativas, estándares y mejores prácticas relacionadas a la seguridad de datos y redes.	Establecer la idoneidad de los estándares, entre el conjunto de diversas normas vigentes, que servirán de base para el desarrollo de la propuesta.
3. Identificar cuáles de las medidas de seguridad tomadas en la actualidad debe pasar a formar parte de la presente propuesta.	Medidas efectivas de seguridad en redes de datos que en la actualidad son utilizadas.	Identificación de las medidas de seguridad en redes de datos que en la actualidad son utilizadas y que merecen formar parte de la propuesta.
4. Precisar cuáles medidas de seguridad, provenientes de los estándares y mejores prácticas existentes previamente seleccionadas, deben formar parte de la propuesta.	Medidas de seguridad en redes de datos basadas en los estándares y mejores prácticas.	Identificación de las medidas de seguridad en redes de datos provenientes de los estándares y mejores prácticas que pueden ser adaptados a la realidad del MPP Educación.
5. Formular la propuesta de seguridad de tipo preventiva, correctiva, de contingencia y recuperación para las redes de datos del MPP Educación, de manera organizada y sistematizada.	Sistematización y organización de la propuesta de seguridad de redes de datos.	Es la organización y sistematización de la propuesta de seguridad para redes de datos, de manera que sea efectiva, eficiente y factible en cuanto a su aplicación.

Nota: Definición operacional de las variables de la presente investigación, elaborado por el autor.

Operacionalización de las variables de la presente investigación.

Tabla 3. Operacionalización de las Variables

Variables	Dimensión	Indicadores	Ítems	Fuente	Instrumento Recolección de Información
1. Conocer la situación de seguridad de las redes de datos en el MPP Educación.	Marco Organizacional para la Seguridad de la información y de las redes de datos en del MPPE	Estructura organizacional	¿Existe la estructura organizacional que sirva de apoyo a la seguridad de los sistemas y las redes de datos? ¿Existe la estructura organizacional que realice las funciones de auditoría de sistemas?	Entrevista a los administradores de sistemas.	Entrevistas.
		Políticas y normas de seguridad	¿Existen políticas, normas y procedimientos, claramente establecidas, destinada a fortalecer la seguridad de los sistemas y las redes de datos?		
		Planes de seguridad	¿Se diseñan planes y programas de seguridad, manteniéndolos actualizados?		
	Amenazas	Procedimientos para enfrentar amenazas	¿Existen planes, programas y procedimientos que permitan el manejo de catástrofes tales como: Incendios, inundaciones, fallas eléctricas y ataques a los sistemas de TI?		
	Vulnerabilidades	Control de vulnerabilidades	¿Se realizan planes que permitan controlar las vulnerabilidades? Entendiéndose por vulnerabilidad la probabilidad de sufrir un ataque en el corto plazo.		
		Seguimiento de reportes de vulnerabilidades	¿Se siguen las publicaciones referidas a las vulnerabilidades de los sistemas?		

Variables	Dimensión	Indicadores	Ítems	Fuente	Instrumento Recolección de Información
1. Conocer la situación de seguridad de las redes de datos en el MPP Educación. (cont.)	Gestión de usuarios	Registro de usuarios	¿Se tiene un registro detallado que incluya datos personales, roles así como de las transacciones realizadas por los usuarios del sistema? Entendiéndose por roles los privilegios que posee el usuario dentro del sistema.	Entrevista a los administradores de sistemas.	Entrevistas.
		Otorgamiento de roles y privilegios	¿Se tienen procedimientos detallados y escritos que regulen en otorgamiento de privilegios o roles?		
		Normativas sobre el uso de contraseñas	¿Existen políticas o normas escritas y referidas al uso, cambio y responsabilidades asociadas con las contraseñas del sistema?		
	Registros y auditorías	Auditoría de sistemas	¿Existen políticas y planes relativos a los procesos de auditoría y control en materia de seguridad de TI? ¿Se realizan auditoría de los sistemas de información? ¿Se utiliza la figura de auditores externos?		
		Logs de los sistemas	¿Usualmente se activan para su funcionamiento los avisos o logs de los sistemas? Entendiéndose por log, los archivos o registros que automáticamente son generados por el sistema para reportar fallos o ataques. ¿Se protegen los logs contra modificaciones maliciosas? ¿Se analizan los registros o logs de los sistemas en búsqueda de posibles intrusiones? ¿Se registran por medios manuales o automatizados, los eventos e incidentes que afectan la seguridad de las redes de datos y los sistemas? ¿Se utilizan analizadores de tráfico de red para determinar el tipo de protocolos que circulan por ésta?		
			¿Se utilizan sistemas de control de intrusos o IDS?		

Variables	Dimensión	Indicadores	Ítems	Fuente	Instrumento Recolección de Información
1. Conocer la situación de seguridad de las redes de datos en el MPP Educación. (cont.)	Registros y auditorías (cont.)	Sincronización de relojes	¿Se tiene un proceso automatizado que permita la sincronización de los relojes de los sistemas?	Entrevista a los administradores de sistemas.	Entrevistas.
	Código malicioso o virus	Control de propagación de código malicioso	¿Se realizan periódicamente controles para impedir la propagación de códigos maliciosos o virus?		
	Continuidad	Desempeño futuro	¿Se realizan mediciones periódicas que permitan prever el desempeño futuro, la capacidad o calidad del servicio de los sistemas o de la red de datos?		
		Umbrales de servicio	¿Se conoce en detalle los umbrales del servicio de red que permitan establecer cuáles son los valores normales de tráfico? Entendiéndose por umbrales, los niveles aceptables de tráfico previamente definido.		
		Planes de continuidad	¿Existen planes o programas escritos y detallados que permitan garantizar la continuidad de los servicios de información y de las redes de datos? ¿Se tiene actualizado los contratos de mantenimiento de TI que permitan garantizar la continuidad del servicio?		
	Contingencia y recuperación	Identificación de amenazas y de recursos críticos	¿Se han identificado por escrito los recursos críticos de TI que en caso de incidentes puedan afectar el normal desempeño de los procesos de la organización?		
		Planes y programas	¿Se tienen planes detallados que describan los procedimientos a seguir para la recuperación y reanudación de los servicios de TI luego de la ocurrencia de un incidente?		
		Soporte de terceras partes en los procesos de contingencia y recuperación	¿Se tienen contratos con terceras partes específicamente para que sirvan de soporte en caso de requerir escalar problemas relacionados con la continuidad de las operaciones?		

Variables	Dimensión	Indicadores	Ítems	Fuente	Instrumento Recolección de Información
1. Conocer la situación de seguridad de las redes de datos en el MPP Educación. (cont.)	Seguridad en las redes de datos	Planes y programas para el desarrollo de las redes de datos	¿Se tienen planes relacionados a la instalación o ampliación de las redes de datos? ¿Se tiene documentada en detalle la arquitectura de red? ¿Se tienen identificados claramente y en detalle todos los equipos de red de la organización?	Entrevista a los administradores de sistemas.	Entrevistas.
		Separación de redes	¿Los sistemas sensitivos se encuentran identificados? En caso de responder afirmativamente la pregunta anterior, ¿Dichos sistemas se encuentran en redes separadas?		
		Políticas y normas	¿Se tienen normas claras y escritas que normen el tipo de información que puede transitar por la red de datos? ¿Se tienen por escrito las normas que regulen la disposición del cableado de red y de energía eléctrica?		
	Seguridad física	Acceso físico	¿Se tienen políticas escritas y claras que normen el acceso físico a la infraestructura e instalaciones de TI? ¿Se utilizan dispositivos de identificación que controlen el acceso físico a las instalaciones de TI, tales como tarjetas magnéticas, reconocimiento de medidas biométricas, etc.?		
	Control de Errores	Adiestramiento	¿Se realizan periódicamente detección de necesidades y adiestramientos relacionados con la seguridad de la información y de redes de datos? ¿Se realizan campañas de concientización sobre seguridad de TI a los usuarios del sistema?		

Variables	Dimensión	Indicadores	Ítems	Fuente	Instrumento Recolección de Información
2. Determinar cuáles de las mejores prácticas y estándares, relativos a la seguridad de datos y redes, pueden ser aplicados al problema de estudio.	Recopilar el conjunto de estándares relativos a la seguridad de redes de datos.	Estándares de seguridad de redes de datos aplicables al estudio.	¿Cuántos estándares de seguridad en redes de datos existen? ¿Cuántos estándares de seguridad adaptable a las redes datos existen? ¿Cuáles de los estándares de seguridad encontrados son los más destacados o reconocidos? ¿Cuáles de los estándares encontrados se adaptan mejor a la realidad existente? ¿Cuáles normas de seguridad en redes son aplicables al estudio?	Investigación documental de las mejores prácticas existentes	Investigación documental.
3. Identificar cuáles de las medidas de seguridad tomadas en la actualidad debe pasar a formar parte de la presente propuesta.	Fortalezas y oportunidades encontradas en los actuales planes de seguridad de las redes de datos que pueden formar parte de la propuesta.	Fortalezas existentes	¿Qué aspectos positivos dentro de la seguridad de las redes de datos del MPPE pueden formar parte de la propuesta?	Comparación de los resultados de la entrevista con las mejores prácticas existentes	Investigación documental.
		Oportunidades existentes	¿Cuáles oportunidades o ventajas existen en la seguridad de las redes de datos del MPPE que puedan formar parte de la propuesta?		

Variables	Dimensión	Indicadores	Ítems	Fuente	Instrumento Recolección de Información
4. Precisar cuáles medidas de seguridad, provenientes de los estándares y mejores prácticas existentes previamente seleccionadas, deben formar parte de la propuesta.	Normas y estándares de seguridad aplicables al estudio	Normas y estándares relativos a la seguridad de las redes de datos.	¿Cuáles normas y estándares de seguridad de redes de datos son aplicables al MPPE?	Investigación documental de las mejores prácticas existentes.	Investigación documental.
		Normas y estándares generales de seguridad en tecnología de la información que pueden ser adaptadas a las redes de datos.	¿Cuáles normas y estándares de seguridad para las tecnologías de la información pueden ser adaptados a las redes de datos?		
5. Formular la propuesta de seguridad de tipo preventiva, correctiva, de contingencia y recuperación para las redes de datos del MPP Educación, de manera organizada y sistematizada.	Componentes de la propuesta	Aspectos correctivo	¿Cuáles aspectos correctivos contendrá la propuesta?	Investigación documental de las mejores prácticas existentes y de los datos previamente recabados.	Investigación documental.
		Aspectos preventivo	¿Cuáles aspectos preventivos contendrá la propuesta?		
		Aspectos de contingencia y recuperación.	¿Cuáles aspectos de contingencia y recuperación contendrá la propuesta?		

Nota: Definición operacional de las variables de la presente investigación, elaborado por el autor.

Técnicas de Procesamiento y Análisis de Datos

Respecto a procesamiento y análisis de datos, Méndez (2009) precisa; que se trata del ordenamiento de la información, la cual debe ser procesada por ítem, agrupada por variables, de manera que permita su presentación en tablas. Esto requiere la realización de cálculos, gráficos, cuadros y tablas. Posterior a este ordenamiento se procesan los datos, de cuyos resultados se nutrirá el posterior análisis e interpretación.

Por otra parte Sabino (2007), profundiza en la forma de hacer dicho procesamiento y análisis. Señala que como primer paso debe separarse los datos numéricos de los cualitativos, ya que el tratamiento de la información difiere uno del otro.

Los datos que se presentan en forma no verbal pueden tener dos destinos distintos, el primero es convertirlo en datos numéricos, en segundo lugar, en caso de no poder hacer dicha conversión, se tratará como información no cuantificada o cualitativa. Una vez adoptado el criterio anterior frente a los datos, se procede a revisarlos en cuanto a su coherencia, en la búsqueda de incongruencias, omisiones o errores, corrigiéndolos si fuera posible.

Los datos numéricos se agrupan en intervalos para su tabulación; los datos verbales que se puedan presentar como datos numéricos, requieren de un proceso de codificación, para luego ser tratados como datos numéricos. Existen datos de contenido verbal que no soportan esta codificación, por lo que es necesario practicar procesos de análisis y síntesis sobre ellos, para este fin se hace necesario ordenar estos datos, preferiblemente en forma esquemática, ordenado por temas, capítulos puntos, para efectuar sobre ellos un proceso de inspección sistemática y profunda.

Para la codificación, se agrupan numéricamente los datos de tipo verbal, a partir de cúmulos de información que tengan una mínima homogeneidad, dividiendo las respuestas en subgrupos, creando de esta manera categorías para cada pregunta formulada, a cada categoría se le asigna un código particular que sirve para agrupar todas las respuestas con

características similares, de esta forma según Hurtado (2010-b), el investigador, al no tener unas respuestas preestablecidas, las categorías surgen de la misma información recolectada.

Una vez definidos los códigos entonces se hace posible la tabulación, según Sabino (2007), de esta forma los datos se muestran agrupados y contabilizados por categoría o códigos previamente establecidos. El resultado de la codificación aún no puede presentarse como resultado de la investigación, para ello se hace necesario efectuar procesos de análisis, comparación y síntesis, según sea necesario.

El análisis implica descomponer el todo en sus partes constitutivas, continúa Sabino (2007), la síntesis por el contrario consiste en estudiar las partes y a partir de ellas construir la totalidad inicial. En el análisis de toma cada uno de los datos o conjunto de datos, se hace necesario interrogarse sobre su significado, explorar y examinar con métodos conocidos, existiendo dos formas de hacerlo:

- Análisis cuantitativo: Este tipo de análisis se efectúa sobre toda la información numérica resultado de la investigación, en este tipo de análisis se correlacionan las variables numéricas, detectando las influencias que existan.
- Análisis cualitativo: Se aplica a la información de tipo verbal, una vez clasificada se comparan, sacando de ellas pequeñas conclusiones específicas o notas, las cuales posteriormente servirán para hacer inferencias sobre las mismas y de esta forma llegar a conclusiones más amplias.

En cuanto a la síntesis, Sabino (2007), señala que es una conclusión final, la cual engloba la totalidad de las apreciaciones que se han venido haciendo al o largo del trabajo. La síntesis se basa en los análisis previos donde se encuentran registrados los hallazgos parciales.

En la presente investigación y según el tipo de instrumento de recolección de datos, se aplicaron las siguientes técnicas de procesamiento de datos:

- En el caso de las entrevistas, se categorizaron los datos antes de su recolección, se codificaron para agruparlos y realizar sobre ellos análisis de tipo numérico, originando tablas y gráficos representativos de cada categoría. Esta información fue analizada para descubrir las interrelaciones existentes entre las variables, lo que permitió elaborar una síntesis o conclusión de los datos recopilados.
- En cuando a la investigación documental se basó en el análisis de los estándares CobiT 4.1, ITIL V3 e ISO/IEC 27002, siguiendo lo señalado en el manual de Alineación CobiT, ITIL V3 e ISO/IEC 27002 de IT Governance Institute (2008).

CAPÍTULO IV

RESULTADOS OBTENIDOS, ANÁLISIS E INTERPRETACIÓN

Investigación de Campo

Resultados de la Investigación de Campo.

Marco Organizacional para la seguridad de la información y de las redes de datos en del MPP Educación.

Estructura organizacional.

1. ¿Existe la estructura organizacional que sirva de apoyo a la seguridad de los sistemas y las redes de datos?

Tabla 4. Respuesta al Ítem 1

Si	No
0	6

Nota: Respuesta ítem 1. Elaborado por el autor

Figura 10. Respuesta al Ítem 1

Figura 10. Respuesta al ítem 1. Elaborado por el autor

2. ¿Existe la estructura organizacional que realice las funciones de auditoría de sistemas?

Tabla 5. Respuesta al Ítem 2

Si	No
0	6

Nota: Respuesta ítem 2. Elaborado por el autor

Figura 11. Respuesta al Ítem 2

Figura 11. Respuesta al ítem 2. Elaborado por el autor

Políticas y normas de seguridad.

3. ¿Existen políticas, normas y procedimientos, claramente establecidas, destinada a fortalecer la seguridad de los sistemas y las redes de datos?

Tabla 6. Respuesta al Ítem 3

Si	No
0	6

Nota: Respuesta ítem 3. Elaborado por el autor

Figura 12. Respuesta al Ítem 3

Figura 12. Respuesta al ítem 3. Elaborado por el autor

Planes de seguridad.

4. ¿Se diseñan planes y programas de seguridad, manteniéndolos actualizados?

Tabla 7. Respuesta al Ítem 4

Si	No
0	6

Nota: Respuesta ítem 4. Elaborado por el autor

Figura 13. Respuesta al Ítem 4

Figura 13. Respuesta al ítem 4. Elaborado por el autor

Amenazas.

Procedimientos para enfrentar amenazas.

5. ¿Existen planes, programas y procedimientos que permitan el manejo de catástrofes tales como: Incendios, inundaciones, fallas eléctricas y ataques a los sistemas de TI?

Tabla 8. Respuesta al Ítem 5

Si	No
0	6

Nota: Respuesta ítem 5. Elaborado por el autor

Figura 14. Respuesta al Ítem 5

Figura 14. Respuesta al ítem 5. Elaborado por el autor

Vulnerabilidades.

Control de vulnerabilidades.

6. ¿Se realizan planes que permitan controlar las vulnerabilidades? Entendiéndose por vulnerabilidad la probabilidad de sufrir un ataque en el corto plazo.

Tabla 9. Respuesta al Ítem 6

Si	No
1	5

Nota: Respuesta ítem 6. Elaborado por el autor

Figura 15. Respuesta al Ítem 6

Figura 15. Respuesta al ítem 6. Elaborado por el autor

Seguimiento de reportes de vulnerabilidades.

7. ¿Se siguen las publicaciones referidas a las vulnerabilidades de los sistemas?

Tabla 10. Respuesta al Ítem 7

Si	No
0	6

Nota: Respuesta ítem 7. Elaborado por el autor

Figura 16. Respuesta al Ítem 7

Figura 16. Respuesta al ítem 7. Elaborado por el autor

Gestión de usuarios.

Registro de usuarios.

8. ¿Se tiene un registro detallado que incluya datos personales, roles así como de las transacciones realizadas por los usuarios del sistema? Entendiéndose por roles los privilegios que posee el usuario dentro del sistema.

Tabla 11. Respuesta al Ítem 8

Si	No
1	5

Nota: Respuesta ítem 8. Elaborado por el autor

Figura 17. Respuesta al Ítem 8

Figura 17. Respuesta al ítem 8. Elaborado por el autor

Otorgamiento de roles y privilegios.

9. ¿Se tienen procedimientos detallados y escritos que regulen el otorgamiento de privilegios o roles?

Tabla 12. Respuesta al Ítem 9

Si	No
0	6

Nota: Respuesta ítem 9. Elaborado por el autor

Figura 18. Respuesta al Ítem 9

Figura 18. Respuesta al ítem 9. Elaborado por el autor

Normativas sobre el uso de contraseñas.

10. ¿Existen políticas o normas escritas y referidas al uso, cambio y responsabilidades asociadas con las contraseñas del sistema?

Tabla 13. Respuesta al Ítem 10

Si	No
1	5

Nota: Respuesta ítem 10. Elaborado por el autor

Figura 19. Respuesta al Ítem 10

Figura 19. Respuesta al ítem 10. Elaborado por el autor

Registros y auditorías.

Auditoría de sistemas.

11. ¿Existen políticas y planes relativos a los procesos de auditoría y control en materia de seguridad de TI?

Tabla 14. Respuesta al Ítem 11

Si	No
0	6

Nota: Respuesta ítem 11. Elaborado por el autor

Figura 20. Respuesta al Ítem 11

Figura 20. Respuesta al ítem 11. Elaborado por el autor

12. ¿Se realizan auditoría de los sistemas de información?

Tabla 15. Respuesta al Ítem 12

Si	No
0	6

Nota: Respuesta ítem 12. Elaborado por el autor

Figura 21. Respuesta al Ítem 12

Figura 21. Respuesta al ítem 12. Elaborado por el autor

13. ¿Se utiliza la figura de auditores externos?

Tabla 16. Respuesta al Ítem 13

Si	No
0	6

Nota: Respuesta ítem 13. Elaborado por el autor

Figura 22. Respuesta al Ítem 13

Figura 22. Respuesta al ítem 13. Elaborado por el autor

Logs de los sistemas.

14. ¿Usualmente se activan para su funcionamiento los avisos o logs de los sistemas? Entendiéndose por log, los archivos o registros que automáticamente son generados por el sistema para reportar fallos o ataques.

Tabla 17. Respuesta al Ítem 14

Si	No
4	2

Nota: Respuesta ítem 14. Elaborado por el autor

Figura 23. Respuesta al Ítem 14

Figura 23. Respuesta al ítem 14. Elaborado por el autor

15. ¿Se protegen los logs contra modificaciones maliciosas?

Tabla 18. Respuesta al Ítem 15

Si	No
0	6

Nota: Respuesta ítem 15. Elaborado por el autor

Figura 24. Respuesta al Ítem 15

Figura 24. Respuesta al ítem 15. Elaborado por el autor

16. ¿Se analizan los registros o logs de los sistemas en búsqueda de posibles intrusiones?

Tabla 19. Respuesta al Ítem 16

Si	No
2	4

Nota: Respuesta ítem 16. Elaborado por el autor

Figura 25. Respuesta al Ítem 16

Figura 25. Respuesta al ítem 16. Elaborado por el autor

17. ¿Se registran por medios manuales o automatizados, los eventos e incidentes que afectan la seguridad de las redes de datos y los sistemas?

Tabla 20. Respuesta al Ítem 17

Si	No
2	4

Nota: Respuesta ítem 17. Elaborado por el autor

Figura 26. Respuesta al Ítem 17

Figura 26. Respuesta al ítem 17. Elaborado por el autor

18. ¿Se utilizan analizadores de tráfico de red para determinar el tipo de protocolos que circulan por ésta?

Tabla 21. Respuesta al Ítem 18

Si	No
4	2

Nota: Respuesta ítem 18. Elaborado por el autor

Figura 27. Respuesta al Ítem 18

Figura 27. Respuesta al ítem 18. Elaborado por el autor

19. ¿Se utilizan sistemas de control de intrusos o IDS?

Tabla 22. Respuesta al Ítem 19

Si	No
0	6

Nota: Respuesta ítem 19. Elaborado por el autor

Figura 28. Respuesta al Ítem 19

Figura 28. Respuesta al ítem 19. Elaborado por el autor

Sincronización de relojes.

20. ¿Se tiene un proceso automatizado que permita la sincronización de los relojes de los sistemas?

Tabla 23. Respuesta al Ítem 20

Si	No
5	1

Nota: Respuesta ítem 20. Elaborado por el autor

Figura 29. Respuesta al Ítem 20

Figura 29. Respuesta al ítem 20. Elaborado por el autor

Código malicioso o virus.

Control de propagación de código malicioso.

21. ¿Se realizan periódicamente controles para impedir la propagación de códigos maliciosos o virus?

Tabla 24. Respuesta al Ítem 21

Si	No
0	6

Nota: Respuesta ítem 21. Elaborado por el autor

Figura 30. Respuesta al Ítem 21

Figura 30. Respuesta al ítem 21. Elaborado por el autor

Continuidad.

Desempeño futuro.

22. ¿Se realizan mediciones periódicas que permitan prever el desempeño futuro, la capacidad o calidad del servicio de los sistemas o de la red de datos?

Tabla 25. Respuesta al Ítem 22

Si	No
2	4

Nota: Respuesta ítem 22. Elaborado por el autor

Figura 31. Respuesta al Ítem 22

Figura 31. Respuesta al ítem 22. Elaborado por el autor

Umbrales de servicio.

23. ¿Se conoce en detalle los umbrales del servicio de red que permitan establecer cuáles son los valores normales de tráfico? Entendiéndose por umbrales, los niveles aceptables de tráfico previamente definido.

Tabla 26. Respuesta al Ítem 23

Si	No
1	5

Nota: Respuesta ítem 23. Elaborado por el autor

Figura 32. Respuesta al Ítem 23

Figura 32. Respuesta al ítem 23. Elaborado por el autor

Planes de continuidad.

24. ¿Existen planes o programas escritos y detallados que permitan garantizar la continuidad de los servicios de información y de las redes de datos?

Tabla 27. Respuesta al Ítem 24

Si	No
2	4

Nota: Respuesta ítem 24. Elaborado por el autor

Figura 33. Respuesta al Ítem 24

Figura 33. Respuesta al ítem 24. Elaborado por el autor

25. ¿Se tiene actualizado los contratos de mantenimiento de TI que permitan garantizar la continuidad del servicio?

Tabla 28. Respuesta al Ítem 25

Si	No
0	6

Nota: Respuesta ítem 25. Elaborado por el autor

Figura 34. Respuesta al Ítem 25

Figura 34. Respuesta al ítem 25. Elaborado por el autor

Contingencia y recuperación.

Identificación de amenazas y de recursos críticos.

26. ¿Se han identificado por escrito los recursos críticos de TI que en caso de incidentes puedan afectar el normal desempeño de los procesos de la organización?

Tabla 29. Respuesta al Ítem 26

Si	No
1	5

Nota: Respuesta ítem 26. Elaborado por el autor

Figura 35. Respuesta al Ítem 26

Figura 35. Respuesta al ítem 26. Elaborado por el autor

Planes y programas.

27. ¿Se tienen planes detallados que describan los procedimientos a seguir para la recuperación y reanudación de los servicios de TI luego de la ocurrencia de un incidente?

Tabla 30. Respuesta al Ítem 27

Si	No
1	5

Nota: Respuesta ítem 27. Elaborado por el autor

Figura 36. Respuesta al Ítem 27

Figura 36. Respuesta al ítem 27. Elaborado por el autor

Soporte de terceras partes en los procesos de contingencia y recuperación.

28. ¿Se tienen contratos con terceras partes específicamente para que sirvan de soporte en caso de requerir escalar problemas relacionados con la continuidad de las operaciones?

Tabla 31. Respuesta al Ítem 28

Si	No
0	6

Nota: Respuesta ítem 28. Elaborado por el autor

Figura 37. Respuesta al Ítem 28

Figura 37. Respuesta al ítem 28. Elaborado por el autor

Seguridad en las redes de datos.

Planes y programas para el desarrollo de las redes de datos.

29. ¿Se tienen planes relacionados a la instalación o ampliación de las redes de datos?

Tabla 32. Respuesta al Ítem 29

Si	No
2	4

Nota: Respuesta ítem 29. Elaborado por el autor

Figura 38. Respuesta al Ítem 29

Figura 38. Respuesta al ítem 29. Elaborado por el autor

30. ¿Se tiene documentada en detalle la arquitectura de red?

Tabla 33. Respuesta al Ítem 30

Si	No
1	5

Nota: Respuesta ítem 30. Elaborado por el autor

Figura 39. Respuesta al Ítem 30

Figura 39. Respuesta al ítem 30. Elaborado por el autor

31. ¿Se tienen identificados claramente y en detalle todos los equipos de red de la organización?

Tabla 34. Respuesta al Ítem 31

Si	No
4	2

Nota: Respuesta ítem 31. Elaborado por el autor

Figura 40. Respuesta al Ítem 31

Figura 40. Respuesta al ítem 31. Elaborado por el autor

Separación de redes.

32. ¿Los sistemas sensitivos se encuentran identificados?

Tabla 35. Respuesta al Ítem 32

Si	No
4	2

Nota: Respuesta ítem 32. Elaborado por el autor

Figura 41. Respuesta al Ítem 32

Figura 41. Respuesta al ítem 32. Elaborado por el autor

33. En caso de responder afirmativamente la pregunta anterior, ¿Dichos sistemas se encuentran en redes separadas?

Tabla 36. Respuesta al Ítem 33

Si	No
2	3

Nota: Respuesta ítem 33. Elaborado por el autor

Figura 42. Respuesta al Ítem 33

Figura 42. Respuesta al ítem 33. Elaborado por el autor

Políticas y normas.

34. ¿Se tienen normas claras y escritas que normen el tipo de información que puede transitar por la red de datos?

Tabla 37. Respuesta al Ítem 34

Si	No
2	4

Nota: Respuesta ítem 34. Elaborado por el autor

Figura 43. Respuesta al Ítem 34

Figura 43. Respuesta al ítem 34. Elaborado por el autor

35. ¿Se tienen por escrito las normas que regulen la disposición del cableado de red y de energía eléctrica?

Tabla 38. Respuesta al Ítem 35

Si	No
2	4

Nota: Respuesta ítem 35. Elaborado por el autor

Figura 44. Respuesta al Ítem 35

Figura 44. Respuesta al ítem 35. Elaborado por el autor

Seguridad física.

Acceso físico.

36. ¿Se tienen políticas escritas y claras que normen el acceso físico a la infraestructura e instalaciones de TI?

Tabla 39. Respuesta al Ítem 36

Si	No
1	5

Nota: Respuesta ítem 36. Elaborado por el autor

Figura 45. Respuesta al Ítem 36

Figura 45. Respuesta al ítem 36. Elaborado por el autor

37. ¿Se utilizan dispositivos de identificación que controlen el acceso físico a las instalaciones de TI, tales como tarjetas magnéticas, reconocimiento de medidas biométricas, etc.?

Tabla 40. Respuesta al Ítem 37

Si	No
5	1

Nota: Respuesta ítem 37. Elaborado por el autor

Figura 46. Respuesta al Ítem 37

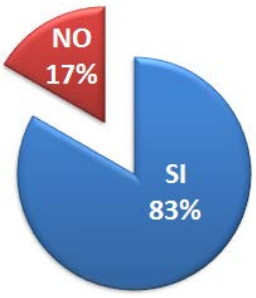

Figura 46. Respuesta al ítem 37. Elaborado por el autor

Control de Errores.

Adiestramiento.

38. ¿Se realizan periódicamente detección de necesidades y adiestramientos relacionados con la seguridad de la información y de redes de datos?

Tabla 41. Respuesta al Ítem 38

Si	No
4	2

Nota: Respuesta ítem 38. Elaborado por el autor

Figura 47. Respuesta al Ítem 38

Figura 47. Respuesta al ítem 38. Elaborado por el autor

39. ¿Se realizan campañas de concientización sobre seguridad de TI a los usuarios del sistema?

Tabla 42. Respuesta al Ítem 39

Si	No
0	6

Nota: Respuesta ítem 39. Elaborado por el autor

Figura 48. Respuesta al Ítem 39

Figura 48. Respuesta al ítem 39. Elaborado por el autor

Síntesis de resultados.

La síntesis de resultados es la sumatoria de preguntas respondidas positiva y negativamente, dando así la percepción general de la seguridad de las redes de datos dentro del MPP Educación.

Tabla 43. Síntesis de Resultados

Si	No
8	31

Nota: Síntesis de resultados. Elaborado por el autor

Figura 49. Síntesis de resultados

Figura 49. Síntesis de resultados. Elaborado por el autor

Análisis de los resultados obtenidos en la investigación de campo.

Marco Organizacional para la seguridad de la información y de las redes de datos en del MPP Educación.

Los resultados obtenidos respecto al marco organizacional requerido para dar respaldo a las actividades de seguridad, fueron todos negativos, no existe un departamento de seguridad de la información, como tampoco de auditoría de sistemas, así mismo no se cuenta con políticas, normas y procedimientos claramente definidos que regulen lo relativo a la seguridad.

Amenazas.

Con respecto a las amenazas, no se diseña ningún tipo de planificación que permita afrontar efectivamente tales incidentes.

Vulnerabilidades.

Tampoco existen planes que permitan realizar una labor preventiva respecto a la vulnerabilidades de los sistemas y de las redes de datos, lamentablemente tampoco se siguen las notificaciones y publicaciones de vulnerabilidades.

Gestión de usuarios.

La gestión de usuarios, también presenta algunas deficiencias, no existen los registros adecuados que permitan ejecutar procesos de auditorías, no se regula adecuadamente el proceso de otorgamiento de privilegios, así como tampoco existen las políticas y normas relativas a las responsabilidades de los usuarios y sus contraseñas en el sistema.

Registros y auditorías.

A este respecto tampoco existen planes y programas de ejecución de auditorías, no se cuenta con auditores externos, sin embargo se hace un esfuerzo por activar los registros o logs de los sistemas, pero dicho esfuerzo no es suficiente, ya que al no contar con un departamento de seguridad de sistemas y de auditoría de sistemas, se descuida la labor referida a la revisión de tales logs, su protección contra modificaciones, así como el registro de incidentes de seguridad.

En cuanto a la seguridad de la red, la misma presenta algunos problemas, no se supervisa el tipo de protocolos que circula por ella, también se carece de sistemas de control de intrusos. La sincronización de los relojes es una de las actividades que se realiza eficientemente, sin embargo, está motivada más por la necesidad de mantener la fecha y hora correcta para las aplicaciones del sistema que por motivos de seguridad.

Código malicioso o virus.

Con respecto a los códigos maliciosos, no existen controles que impidan su propagación.

Continuidad.

La continuidad de los servicios no está garantizada, no se realizan mediciones de la capacidad actual, por lo que no se puede predecir la demanda futura. Así mismo se carece de planes y programas de continuidad de los servicios. Los contratos de mantenimiento con terceros no existen o están desactualizados.

Contingencia y recuperación.

Los planes de contingencia y recuperación son inexistentes, tampoco se tienen identificados los recursos críticos del sistema, ni se cuenta con soporte de terceras partes que permitan prestar su apoyo en las tareas de la recuperación. De esta forma la contingencia y recuperación dependen de la experiencia y los conocimientos de los administradores y operadores del sistema.

Seguridad en las redes de datos.

La seguridad de las redes de datos no escapa de la realidad anteriormente descrita, no existen planes y programas para la ampliación de las redes de datos, la actual arquitectura de redes no está debidamente documentada, sin embargo, los equipos y puntos claves de la red se encuentran perfectamente identificados.

Los equipos que se conectan a la red están identificados, así como, los sistemas sensitivos, sin embargo, tales sistemas sensitivos no se encuentran en redes separadas como lo aconsejan las buenas prácticas.

Tampoco se cuenta con la normativa necesaria para regular el tráfico de la red, ni con las normas que regulen la disposición del cableado.

Seguridad física.

La carencia de políticas y normas de seguridad afectan la seguridad física, no existe normativa alguna que la regule, sin embargo, se hacen esfuerzos por restringir el acceso de personas no autorizadas a las instalaciones sensibles de TI, se tienen dispositivos de identificación mediante el uso tarjetas magnéticas que permiten la apertura de puertas.

Control de errores.

Lamentablemente tampoco se imparten cursos de adiestramiento al personal técnico, administradores y operadores en materia de seguridad de la información o de redes de datos. Las campañas de concientización a los usuarios son inexistentes.

Percepción general de seguridad.

La percepción negativa de seguridad es cercana al 80%, es decir, de los 39 aspectos consultados 8 fueron positivos y 31 negativos, lo que significa que la mayoría de los integrantes del Departamento de Operaciones y Bases de Datos del MPP Educación perciben que las condiciones de seguridad no son las más adecuadas.

Análisis de las Debilidades, Oportunidades, Fortalezas y Amenazas (DOFA).

En la Tabla 44 se ha colocado el análisis DOFA correspondiente a los resultados del estudio de campo.

Tabla 44. Análisis de la Debilidades, Oportunidades, Fortalezas y Amenazas (DOFA)

Fortalezas	Debilidades
Pese a los resultados mayoritariamente negativos arrojados por esta parte del estudio, se puede observar que se han realizado esfuerzos por dotar al MPP Educación de equipos y tecnología de avanzada, evidentemente este único aspecto no garantiza la seguridad de la información, pero serviría de punto de partida para iniciar los cambios requeridos. El Recurso Humano con el que cuenta este Ministerio también es una de sus fortalezas, pese a las precarias condiciones de seguridad existentes, el personal ha sabido afrontar los incidentes de seguridad y ha mantenido la plataforma operativa en todo momento.	Existen múltiples debilidades en la seguridad de información dentro del MPP Educación, debido a la falta de políticas que permitan imponer en la agenda de trabajo este tema. Sin embargo, teniendo como ejemplo, el impuso del uso de software libre en la administración pública mediante el Decreto 3.390, una similar medida de este tipo serviría como estímulo para impulsar las iniciativas requeridas en los temas relativos a la seguridad.
Oportunidades	**Amenazas**
En cuanto a las oportunidades, se tiene el conjunto de recomendaciones y estándares internacionales que pueden ser adaptados para incrementar la seguridad de la red de datos y de los sistemas de información de esta institución, el presente trabajo de investigación puede perfectamente servir de punto de partida para incentivar el desarrollo de la estructura organizativa, las políticas, normas y procedimientos requeridos para tal fin.	Las amenazas a la seguridad de las redes de datos y los sistemas de información seguirán estando presentes en el entorno de esta organización, cada nueva tecnología instalada posee sus propias y particulares vulnerabilidades

Nota: Elaborado por el autor.

Investigación Documental

Resultados de la investigación Documental.

En el marco teórico del estudio se expusieron los tres estándares más comúnmente utilizados en materia de seguridad de la información, como lo son: CobiT, ITIL e ISO/IEC 27002, sin embargo, la alineación de dichas normas estaría fuera del alcance del presente estudio, tal vez sólo sería posible llegar a una aproximación, tomando arbitrariamente algunos de los elementos que las conforman.

Profundizando en la investigación que permitiera alinear dichas normas, se encontró que ISACA en el año 2008, publicó el reporte de mejores prácticas denominado: "Alineación CobiT 4.1, ITIL V3 e ISO/IEC 27002", donde CobiT 4.1 e ISO/EC 27002 permiten señalar lo qué debe hacerse, mientras ITIL V3 indicaría el cómo realizarse. Además mediante el uso de un sencillo esquema de trabajo, marcado por cinco pasos tales como: La elaboración, priorización, planificación, evitar obstáculos y alinear las mejores prácticas, garantiza la adopción de un modelo de procesos de TI adaptada a las necesidades de cada organización

Alineación CobiT, ITIL, ISO 270002.

En el año 2008 se ISACA publica un reporte de mejores prácticas para la alineación de CobiT 4.1, ITIL V3 e ISO/IEC 27002, según IT Governance Institute (2008), CobiT e ISO/IEC 27002 permitirían definir el marco de trabajo para determinar qué debe hacerse, mientras ITIL V3 proporcionaría el cómo, para manejar los aspectos de gestión de servicios. Sin embargo, menciona que existe el peligro que el resultado de la implantación de dichas prácticas resulte costoso y desenfocado al tratarlas como guías técnicas, por lo que deben ser adaptadas al contexto de la organización, ya que el objetivos de las mejores prácticas es la conducción de los servicios de TI económicos y bien controlados.

Continúa IT Governance Institute (op cit.), señalando que las mejores prácticas posibilitan:

- Una mejor gestión de TI, lo cual es fundamental para el éxito de la estrategia de la organización.
- Un gobierno eficaz de las actividades de TI.
- Un marco de referencia eficaz para la gestión de políticas, controles internos y prácticas definidas que sirvan de guía que todos tengan conocimiento de qué hacer.
- Beneficios derivados tal como ganancia de eficiencia, menor dependencia de expertos, disminución de los errores así como mejorar la confianza de los socios del negocio.

IT Governance Institute (op cit.) hace énfasis en que la aplicación de tales normas no garantiza el éxito en materia de seguridad, por el contrario, su efectividad depende de cómo se implementen y se mantengan en el tiempo, más a modo de principios que se adapten a los procedimientos específicos existentes en la organización, esto con el objeto de evitar el enunciado de prácticas que nunca llegan a ejecutarse. La dirección y los miembros de la organización deben entender claramente lo que hay que hacer, cómo hacerlo y porqué es importante hacerlo.

Esquema de implementación CobiT, ITIL e ISO/IEC 27002.

IT Governance Institute (op cit.) expone un esquema para la implementación de CobiT, ITIL e ISO/IEC 27002 que consta de los siguientes pasos:

- Elaboración
- Priorización
- Planificación
- Evitar obstáculos
- Alinear las mejores prácticas

Dichos pasos serán explicados en detalle a continuación:

Elaboración.

CobiT e ISO/IEC 27002 pueden ayudar a definir el qué debería hacerse, mientras ITIL señalaría el cómo pero específicamente para la gestión de los servicios, la aplicación sería la siguiente:

- Para apoyar la gobernabilidad a través de:
  - Proporcionar políticas de gestión y marco de control.
  - Facilitar el proceso de asignación de propietarios, establecimiento de responsabilidades y rendición de cuentas para todas las actividades de TI.
  - Alinear los objetivos de TI con los objetivos del negocio, al definir las prioridades y al asignar recursos.
  - Asegurar el retorno de la inversión, así como la optimización de los costos.
  - Asegurar la identificación de los riesgos significativos para la organización.
  - Asignar la responsabilidad de la gestión de riesgos integrada a la estructura organizacional, para así asegurar a la dirección que se han implementado controles eficaces.
  - Asegurar la correcta y efectiva distribución de los recursos, de manera que se cuente con la infraestructura técnica, los procesos y las habilidades requeridas para ejecutar exitosamente la estrategia de TI.
  - Asegurar el monitoreo y la medición de las actividades críticas de TI, identificando correctamente los problemas así como las medidas correctivas que puedan ser adoptadas para dar solución.
- Para definir los requisitos del servicio y las definiciones del proyecto, tanto desde el punto de vista interno como de los proveedores de servicios:
  - Establecer objetivos de TI relacionados con el negocio y sus respectivas métricas.
  - Definir los servicios y proyectos en términos del usuario final.

    - Elaborar acuerdos de niveles de servicios y contratos que puedan ser monitoreados por los clientes.
    - Asegurarse que los requerimientos del cliente han sido descritos adecuadamente en los requisitos operativos y técnicos de TI.
    - Considerar los portafolios de servicios y proyectos en conjunto, para establecer las prioridades, así se garantiza la distribución equitativa de los recursos.
- Para verificar la capacidad profesional o demostrar la competencia en el mercado mediante:
    - Las evaluaciones y auditorías independientes realizadas por terceros
    - Compromisos contractuales
    - Constancias y certificaciones
- Para facilitar la mejora continua por:
    - Evaluación de madurez
    - Análisis de brechas
    - Benchmarking
    - Planificación de la mejora
    - Evitar la reinvención de buenos enfoques ya probados
- Como marco para la auditoria, evaluación y visión externa mediante:
    - Criterios objetivos y mutuamente entendidos
    - Benchmarking para justificar las debilidades y brechas de los controles
    - Incrementando la profundidad y el valor de las recomendaciones a través de enfoques generalmente aceptados

Priorización.

Esta etapa permite evitar la implementación de estándares y mejores prácticas costosas e innecesarias, por ello la organización debe priorizar dónde y cómo utilizarlos, para ello se requiere de un plan de acción que se adapte a sus necesidades particulares. De

allí que es importante en esta etapa que la alta dirección asuma el liderazgo del gobierno de TI, estableciendo la dirección que debe seguir, por esta razón la alta dirección debe:

- Asegurarse que TI se encuentre en la agenda de trabajo.
- Evaluar las actividades de gestión de TI con la finalidad de asegurarse que los posibles problemas existentes sean develados.
- Guiar a la administración para alinear las iniciativas de TI con las necesidades reales del negocio, para crear conciencia del impacto potencial de los riesgos de TI en el negocio.
- Garantizar la medición del desempeño de TI, así como su comunicación a la alta dirección.
- Establecer un comité de dirección o consejo de gobierno de TI, que se haga responsable de comunicar todos los aspectos de TI a la alta dirección y a la administración.
- Garantizar que exista un marco de trabajo para el gobierno de TI basado en enfoques comunes, tales como CobiT, ITIL e ISO/IEC 27002.

Planificación.

Su objetivo es facilitar la implementación, facilitando el establecimiento de puntos de partida y asegurar el logro de resultados positivos, estaría compuesto por:

1. Establecer un marco organizativo con objetivos y responsabilidades definidas, para garantizar la participación de todas las partes involucradas, permitiendo impulsar la implementación como una iniciativa propia.
2. Alinear la estrategia de TI con los objetivos del negocio, determinado la contribución de TI a dichos objetivos. En este sentido CobiT permite enunciar los objetivos y las métricas de TI, mientras que ITIL facilita los acuerdos de niveles de servicio en términos del usuario final.
3. Entender y definir los riesgos en función de los objetivos de negocio, se debe considerar:

- Antecedentes y patrones de desempeño.
- Los actuales factores organizacionales de TI.
- La complejidad, el tamaño y alcance de la infraestructura de TI existente o prevista.
- Las vulnerabilidades que pueden afectar la infraestructura de TI o prevista.
- La naturaleza de las iniciativas de TI que están siendo consideradas, tales como nuevos proyectos, cambios de arquitectura, entre otros.

En este sentido el proceso PO9 para la gestión del riesgo y el marco de control de CobiT permiten la identificación de dichos riesgos, igualmente la implementación de ITIL permite definir los riesgos operativos mientras ISO/IEC 27002 se enfoca es establecer los riesgos de seguridad.

4. Se debe definir las áreas objetivo y de proceso de TI críticas para la entrega de valor, permitiendo gestionar dichas áreas de riesgo. En este sentido CobiT puede ser utilizado como base en conjunto a ITIL el cual respalda la definición de procesos claves de entrega de servicio, aunado a los objetivos de seguridad de ISO/IEC 27002.
5. Analizar la capacidad existente e identificar sus puntos débiles, esta evaluación de la capacidad de madurez permite conocer aquellas áreas en las que se necesitan realizar mejoras, en este sentido CobiT aporta sus modelos de madurez, los cuales se presentan con mejor detalle en ITIL y las prácticas ISO/IEC 27002.
6. Desarrollar estrategias de mejora y decidir cuáles de tales proyectos son de mayor prioridad en la mejora de la gestión de gobierno, la decisión debe basarse en el beneficio potencial que ofrece, así como en la facilidad de implementación enfocada en los procesos más importantes de TI. Estos proyectos deben formar parte de una estrategia de mejora continua. Se pueden fundamentar en los

objetivos de control de CobiT y las prácticas de control detalladas de ITIL, así como las guías de ISO/IEC 27002.

7. Se deben medir los resultados obtenidos, mediante métricas tanto del desempeño actual como de las nuevas mejoras, se debe asegurar que:
    - La estructura organizacional apoye la implementación de las estrategias.
    - Que las responsabilidades de la gestión de riesgos esté integrada a la organización.
    - Asegurarse de la existencia de una adecuada infraestructura que permita el intercambio de información.
    - Asegurarse de la comunicación de estrategias y objetivos a todos los interesados dentro de la organización.

    En este sentido los objetivos y las métricas de CobiT, además del enfoque de mejora continua de los siete pasos de ITIL pueden servir de base para el sistema de puntuación.
8. Los pasos del 2 al 7 se deben repetir regularmente para adaptarse a los continuos cambios del entorno.

Evitar Obstáculos.

La Administración debería seguir las siguientes reglas pragmáticas tales como:

- Enfocar la iniciativa de implementación como una actividad de proyecto dividida en fases y no como un sólo esfuerzo extraordinario.
- La implementación requiere de un cambio cultural, la implementación de nuevos procesos, por lo que se necesita el cambio de conductas y actitudes que se verán reforzadas gracias a agentes motivadores.
- Se deben comprende claramente los objetivos.
- La supervisión exitosa de TI requiere tiempo y es un proceso de mejora continua, no se logra de inmediato.

- Los esfuerzos deben concentrarse en aquellas áreas donde se hace más fácil realizar los cambios y lograr mejoras, a partir de este punto es posible extenderse a otras áreas paulatinamente.
- Se debe obtener el apoyo de la alta dirección.
- Evitar las iniciativas que sean percibidas como un ejercicio burocrático.
- Evitar las listas de verificación que se encuentren fuera de foco.

Alinear las mejores prácticas.

Las mejores prácticas de TI deben ajustarse a los requisitos del negocio para ser integradas entre sí a los procedimientos internos existentes. CobiT es altamente recomendable para esta tarea, ya que ofrece un marco general de control que está basado en un modelo de procesos de TI que puede ser adaptado por cada organización. Los estándares y prácticas específicas como ITIL e ISO /IEC 27002 abarcan áreas más específicas y pueden ser integradas en el marco CobiT.

Es importante destacar que para una mejor ubicación dentro de este reporte de mejores práctica, el mismo está diseñado para ser utilizado desde cualquiera de los tres punto de vista posible, en su primera parte alinea las disposiciones CobiT 4.1 en relación a ITIL V3 e ISO/IEC 27002, la segunda parte alinea ITIL V3 en relación a CobiT 4.1 e ISO/IEC 27002 y finalmente la tercera parte alinea ISO/IEC 27002 con CobiT 4.1 e ISO/IEC 27002. De esta manera si quien realiza en análisis está más familiarizado con uno de estos estándares en particular, tomará dicho estándar como punto de referencia para compararlo con los otros dos. Debido a las facilidades ofrecidas por CobiT 4.1, dicho estándar fue tomado como referencia para su comparación con los dos restantes en la presente investigación.

Gerencia de la Seguridad.

El diseño fue planteado como un sistema que se perfecciona y actualiza a sí mismo, pero como cita Llorens (2009), la informática no es un problema técnico, sino más bien un problema de gerencia, y la seguridad de las redes de datos no escapa a esta realidad, la

gobernanza según Llorens (op cit.), establece la orientación, el marco general para decidir, los valores y principios, los ciclos de regulación y adaptación así los lineamientos tácticos y estratégicos. En este sentido CobiT 4.1, ITIL V3 e ISO/IEC 27002 aporta perfectamente dicho marco de trabajo, sin embargo, para dar viabilidad a sus propuestas es necesario a su vez enmarcarlos dentro de un proceso administrativo que proporcione la dirección estratégica, asegure el cumplimento de los objetivos y garantice que los recursos sean utilizados y asignados adecuadamente.

Según Chiavenato (2006), el modelo de administración está compuesto por cuatro procesos básicos, como lo son:

- Planeación: Se definen los objetivos así como los planes para alcanzarlos, dichos planes están compuestos de actividades que consumen recursos (tiempo, recursos financieros, técnicos y humanos) colocados sobre una línea de tiempo.
- Organización: Es una estructura que propone la división del trabajo, asignando la ejecución de tareas a sus miembros. Permite organizar, estructurar e integrar recursos así como los órganos involucrados en la ejecución, establece sus relaciones y las atribuciones de cada uno de ellos.
- Dirección: Permite dar marcha a las actividades previamente planificadas, dentro del marco organizacional, las personas son asignadas a sus cargos, entrenadas, guiadas y motivadas para alcanzar los resultados esperados.
- Control: Evita las posibles desviaciones del plan previamente trazado, garantizando el normal flujo de los procesos, debe estar basado en estándares o criterios previamente establecidos y que representen el desempeño deseado, para de esta manera hacer los ajustes o las correcciones necesarias, contribuyendo así al mejoramiento continuo de las labores realizadas. Sin embargo el control requiere la realización de mediciones constantes, tal como lo señala Office Government Commerce (2008):
    - Si no se mide, no se puede gestionar
    - Si no se mide, no se puede mejorar
    - Si no se mide, es probable que no importe

- Si no se puede influir o controlar, entonces no se mide

Análisis de los resultados obtenidos en la investigación documental.

Para el presente análisis se tomó en cuenta el contenido de CobiT 4.1, ITIL V3 e ISO/IEC 27000 incluido en el marco teórico del estudio. Dichos estándares se complementan entre sí, CobiT 4.1 está orientado fundamentalmente a control de procesos, es un modelo muy completo y con múltiples convergencias entre sus diversos procesos, es decir, se encuentra muy bien cohesionado e interrelacionado, abarcando desde procesos de auditoría, controles, administración y finalmente gobierno de TI. Sin embargo, resultaría altamente costoso e ineficaz aplicarlo en su totalidad al caso de estudio, por lo que de él se deben seleccionar aquellos aspectos más resaltantes y que contribuyan al logro del objetivo del presente estudio.

En CobiT 4.1 se tienen aspectos dentro de Entrega y Soporte (DS), específicamente DS5 relativo a Garantizar la seguridad de los sistemas, pero según la investigación realizada, se observa que este proceso no se encuentra aislado, se encuentra asociado a otros tres como lo son DS3 (Administrar desempeño y capacidad), DS4 (Garantizar la continuidad del servicio) y DS7 (Educar y entrenar a los usuarios), por lo que muchos aspectos de estos tres procesos deben ser tomados en cuenta. En este punto se encuentra una coincidencia con ITIL V3, en cuanto a garantizar la continuidad del servicio. CobiT también proporciona las métricas necesarias para medir el desempeño de sus procesos, resultando ser una herramienta útil.

Con respecto a ITIL V3, se tiene que está orientado a la gestión de servicios mediante el enunciado de buenas prácticas, para esta investigación es importante garantizar que el servicio de red del MPP Educación se encuentre operativo la mayor parte de tiempo posible, por lo que ITIL V3 está perfectamente alineado con esta necesidad, las cinco fases del ciclo de vida propuesto por ITIL V3 así lo garantizan, por lo que resulta ser una herramienta fundamental para el diseño propuesto por este estudio.

ITIL V3 es fundamentalmente una herramienta administrativa, en su ciclo de vida propuesto se puede observar el proceso administrativo de: Planificación, organización, dirección y control propuesta por las teorías clásicas administrativas pero orientada a TI, en combinación al tradicional modelo del ciclo de vida de los sistemas. La Estrategia de Servicio y el Diseño del Servicio permiten conocer las necesidades existentes, los recursos con los que se cuenta, el modelo o la arquitectura deseada de servicio que se requiere. La Transición del Servicio permite ejecutar los planes minimizando el posible impacto negativo que pudiese tener, todo esto bajo rigurosos controles y validaciones. La Operación del Servicio está destinada a lograr la eficiencia del sistema puesto en ejecución y finalmente la Mejora Continua del Servicio permite el perfeccionamiento de los servicios.

Sin embargo, la advertencia dada en el análisis de CobiT 4.1 sigue siendo válida para ITIL V3, toda la norma no puede ser aplicada en su totalidad al problema que se presenta, sino que debe ser adaptada a los requerimientos existentes.

Finalmente se tiene la serie de normas ISO 27000, en ella se encuentra específicamente la norma ISO/IEC 27002 la cual es fundamental para cualquier desarrollo de sistemas de seguridad de la información, es un compendio de buenas prácticas y recomendaciones que sirven de punto de partida para cualquier diseño de seguridad de datos y con la cual afortunadamente se cuenta para el desarrollo del presente estudio. Las otras normas ISO que resulta interesante son las ISO/IEC 27033, la cual tiene siete variantes, que abarcan un amplio espectro de todo lo relativo a la seguridad de las redes de datos, sin embargo, debido a las limitaciones existentes para su obtención, la misma no fue utilizada en la presente investigación, no obstante el marco teórico y los antecedentes de ésta investigación proporcionó una excelente fuente de datos y recomendaciones para el mejoramiento de la seguridad en las redes.

Para hacer converger las recomendaciones de los tres estándares antes citados, el reporte de ISACA denominado: Alineación CobiT 4.1, ITIL V3 e ISO/IEC 27002, resulta fundamental, ya que sirve de punto de partida para esta labor.

Según los resultados de la investigación documental, se tiene que la mejor perspectiva para la aplicación de las tres normas en el presente estudio, parte de seleccionar desde CobiT 4.1 el proceso de control denominado DS5 Garantizar la seguridad de los sistemas, sin embargo, según Brand y Boonen (2007), dicho proceso está asociado a otros tres como lo son DS3 (Administrar desempeño y capacidad), DS4 (Garantizar la continuidad del servicio) y DS7 (Educar y entrenar a los usuarios). Por lo que se deben alinear las normas ITIL V3 e ISO/IEC 27002 con los procesos de control DS5, DS3, DS4 y DS7 de CobiT. El contenido de dicha alineación se presenta en el Anexo F de la presente investigación.

Además de los procesos de CobiT 4.1 mencionados, se deben utilizar las siguientes normas ITIL V3:

- SD Diseño del servicio (*Service Design)*
- SO Operación del Servicio (S*ervice Operation*)
- CSI Mejora Continua del Servicio (*Continual Service Improvement*)

En relación a las normas ISO/IEC 27002 se deben utilizar aquellas que mejor se adapten a la realidad existente, de nuevo se toma como base lo expuesto por la Alineación CobiT 4.1, ITIL V3 e ISO/IEC 27002, se puede observar más detalladamente el Anexo F.

De esta manera, los procesos de CobiT 4.1 pasan a constituir el punto de partida que será complementado con las dos restantes normas como lo son ITIL V3 e ISO/IEC 27002, pero enfocado dentro de un sistema administrativo donde el control actúa como retroalimentación del sistema, permitiendo realizar las correcciones oportunas a que haya lugar, dicho control es la herramienta que permite al diseño mantenerse actualizado a través del tiempo.

Por lo antes expuesto se llegó al siguiente diseño del sistema de seguridad de las redes de datos del MPP Educación, para facilitar la comprensión de dicho diseño, el mismo puede ser observado en la Figura 51.

Figura 50. Sistema del Sistema de Seguridad para las Redes de Datos del MPP Educación.

Figura 51. Sistemas de Seguridad para las Redes de Datos del MPP Educación, en la cual se integran CobiT 4.1, ITIL V3 e ISO/IEC 27002, dentro del marco de los procesos administrativos. Elaborado por el autor.

Características del sistema de redes del MPP Educación.

La red del MPP Educación posee las siguientes características:

- Veinte Vlan o redes virtuales que permiten aislar una red de otra, instaladas en cada piso del edificio sede del MPP Educación.
- Dos conexiones a Internet de alta velocidad de tipo ABA.

- Una antena de radio frecuencias para salida a Internet ofrecida por el CNTI (Centro Nacional de Tecnologías de Información).
- Cinco servicios de Frame Relay con 23 circuitos para la interconexión de las zonas educativas conectado a un firewall interno.
- Un servicio de antena satelital para la conexión con la zona educativa del estado Vargas.
- Un servicios de fibra óptica o Metro Ethernet para Internet banda ancha, conectado a tres servidores proxy para su administración.
- Dos enlaces Frame Relay bidireccionales para prestar servicios Web, conectados a un firewall externo.
- Un servicio Metro Ethernet para servicios Web conectado a un firewall externo.
- Los sistemas proxy permiten el filtrado de páginas no autorizadas.
- No se permiten mensajes ICMP (*Internet Control Message Protocol*), echo, ping sobre los equipos firewall para evitar ataques externos.
- Se utilizan software anti *spam* en el servidor de correos, así como el bloqueo de archivos ejecutables adjuntos.
- Existen servidores de monitoreo que permiten:
    - Conocer el estado de los equipos, en cuanto a espacio en disco, memoria, servicios.
    - Monitorear la red interna, tráfico de red, protocolos, ancho de banda y fallos en las interfaces de red.
    - Estado de las interfaces de los *routers*.
    - Tráfico entre los enlaces de tipo *Frame Relay*, específicamente las conexiones a las zonas educativas.

El esquema general simplificado de la red se observa en la Figura 50.

Figura 51. Diagrama de Red Simplificado del MPP Educación

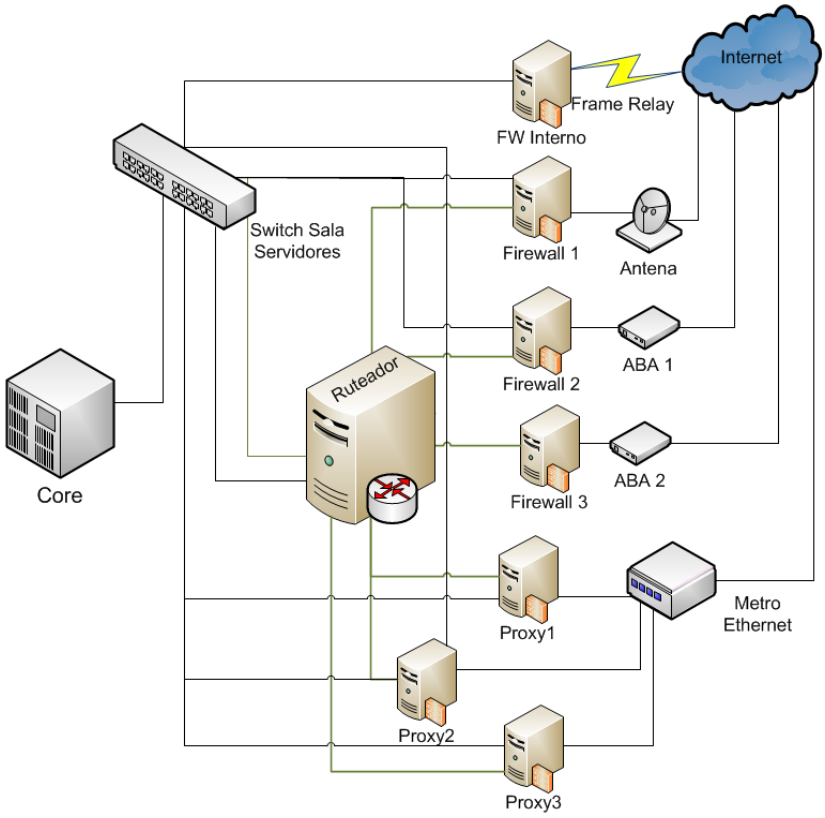

Figura 50. Esquema simplificado de las Redes de Datos del MPP Educación, elaborado por el autor.

Características del Diseño.

De acuerdo a las premisas de esta investigación, el diseño del sistema de seguridad para las redes de datos del MPP Educación deben poseer los siguientes elementos:

- Preventivo
- Correctivo
- De contingencia y recuperación
- Gestión del desempeño y la capacidad.
- Continuidad del servicio

En principio y basado en los antecedentes expuestos en el capítulo II del presente estudio, debería aproximarse al modelo de gestión de seguridad propuesto por Méndez (2006), el cual comprende un ciclo cerrado compuesto por los procesos de (1) Planificar, (2) Hacer, (3) Verificar y (4) Actuar, lo cual resulta un modelo simplificado de los resultados obtenidos por la investigación documental. El principal inconveniente de la propuesta es la dificultad de centrarse exclusivamente en la seguridad de redes de datos, tal como lo refieren Méndez (2006), Bolívar (2007) e inclusive Navarro (2007), la seguridad es un problema que debe afrontase de manera integral. Por lo que la presente propuesta presenta un diseño que incluye algunos tópicos relacionados no solamente con redes de datos, sino también con servidores, software y hardware, entre otros. Otra de las características del presente diseño, es la propiedad de mantenerse actualizado en todo momento, la dinámica de la seguridad es cambiante, por lo que la propuesta de seguridad también debe adaptarse a tales cambios.

El punto de partida para el diseño de seguridad fue CobiT 4.1, donde la Alineación CobiT 4.1, ITIL V3 e ISO/IEC 27002 permitirá relacionarlo con los dos restantes estándares, ITIL V3 e ISO/IEC 27002, todo esto enmarcado dentro del proceso administrativo que permita gestionar los procesos y ejercer el control y la respectiva retroalimentación que facilitará a su vez la actualización continua del sistema. **Debido al carácter proyectivo de la propuesta, la fase de dirección o puesta en práctica fue omitida**.

El resultado de la alineación de normas CobiT 4.1, ITIL V3 e ISO/IEC 27002 para el caso de específico del MPP Educación se puede observar en la Tabla 45.

Tabla 45. Base de normas internacionales utilizadas para el Diseño del Sistema de Seguridad para las Redes de Datos del MPP Educación.

Objetivo de Control CobiT 4.1	Procesos Administrativos Involucrados	Normas ITIL V3 Relacionadas	Normas ISO/IEC 27002 Relacionadas	
1. Seguridad de los sistemas (DS5): a. Seguridad de los sistemas de información	1. Organización	• SO 5.13 • SD 4.6.4 • SO 5.4	• 6.1.1 • 6.1.2 • 6.1.3	
	2. Planificación		• 5.1.1 • 6.1.5	
	3. Políticas y normas	• SO 5.14	• 9.1.6 • 9.2.1 • 13.2.1	• 13.2.3 • 15.3.2
	4. Control	• SD 4.6.5.1	• 10.4.1 • 10.10.1 • 10.10.2 • 10.10.4 • 10.10.5	• 10.10.6 • 12.4.1 • 12.5.1 • 15.2.2 • 15.3.1
b. Seguridad de las redes de datos	1. Planificación	• SO 5.5		
	2. Políticas y normas		• 9.2.3 • 11.4.1	
	3. Control	• SD5.10 • SD 4.6.5.2	• 11.4.3 • 11.4.5 • 11.4.6	• 11.6.2 • 11.7.1
c. Seguridad relacionada con los usuarios	1. Planificación			
	2. Políticas y normas	• SO 4.5	• 8.2.3 • 11.2.3 • 11.3.1	• 11.5.1 • 11.5.3 • 11.5.5
	3. Control	• DS5.4		

Objetivo de Control CobiT 4.1	Procesos Administrativos Involucrados	Normas ITIL V3 Relacionadas	Normas ISO/IEC 27002 Relacionadas
4. Desempeño y capacidad (DS3)	1. Planificación	• SD 4.3.5.1 • SD Apéndice J	
	2. Políticas y normas		• 5.1.1 • 6.1.5
	3. Control	• SD 4.3.5.4 • SD 4.4.5.1 • CSI 5.6.2 • SD 4.3.5.2	
5. Continuidad del servicio (DS4)	1. Planificación	• SD 4.5 • SD 4.5.5.1	
	2. Políticas y normas		
	3. Control	• CSI 5.6.1	• 6.1.7 • 14.1.5
6. Entrenar y educar a los usuarios (DS7)	1. Planificación		• 5.1.1 • 6.1.5
	2. Políticas y normas		
	3. Control		• 8.2.2

Nota: Elaborado por el autor.

Diseño del Sistema de Seguridad para las Redes de Datos del MPP Educación

Como resultado de lo anteriormente expuesto, se obtiene la Tabla 46, la cual en forma general resume el contenido del Sistema de Seguridad para las Redes de Datos del MPP Educación.

Tabla 46. Diseño del Sistema de Seguridad para las Redes de Datos del MPP Educación.

1. Seguridad de los sistemas: **a. Seguridad de los sistemas de información**	
1. Organización	**Creación de una estructura organizacional de seguridad de la información con las siguientes atribuciones:** • El diseño de planes preventivos, correctivos, de continuidad, de contingencia y recuperación. • Enunciado de políticas, normas y procedimientos de seguridad. • Monitoreo y elaboración de informes de seguridad. • Ofrecer asistencia técnica y asesoramiento en la investigación de accidentes de seguridad. • Realización de operativos de control sobre pistas de auditorías, controles de acceso físico. • Formación y sensibilización de los usuarios en materia de seguridad **Entre las funciones de esta unidad administrativa se tiene:** • Identificar los objetivos y metas pertinentes a la seguridad. • Formular, revisar y aprobar las políticas de seguridad. • Verificar la eficacia de la implementación de las políticas de seguridad. • Proporcionar una clara dirección y apoyo a las iniciativas de seguridad. • Proporcionar los recursos necesarios. • Aprobar la asignación de roles y responsabilidades de la seguridad de la información. • Asegurar que las actividades de seguridad sean ejecutadas. • Evaluar la información recibida del seguimiento y revisión de incidentes de seguridad, para recomendar las acciones pertinentes. • Soporte y mantenimiento adecuado de los sistemas operativos, actualizaciones, parches. • Gestión de licencias. • Contratación de soporte de tercer nivel para escalar los posibles

1. Seguridad de los sistemas: a. Seguridad de los sistemas de información	
1. Organización (Cont.)	problemas e incidentes de seguridad, obtener soporte. • Implementación de sistemas de seguridad, control y mantenimiento, así como la adecuación de medidas de seguridad física. • Distribución adecuada de las cargas de trabajo para garantizar la continuidad. • Mejoramiento del rendimiento de los equipos. • Planificación de la adquisición de nueva TI. • Planificación de cursos de adiestramiento. • Debe considerar el establecimiento de acuerdos con terceros, como por ejemplo, asesores externos o soporte de terceros, de manera que se pueda auditar y controlar las acciones de estas personas dentro de la estructura de TI de la organización.
2. Planificación	La planificación debe incluir: • Definición de la seguridad de información y de redes de datos. • Objetivos generales, alcance e importancia de la seguridad. • Declaración de la dirección sobre el apoyo a los objetivos y principios de seguridad. • Marco de referencia para establecer los objetivos de control, la estructura de evaluación y la gestión del riesgo. • Explicación de las políticas, principios, normas y requisitos de seguridad. • Definición de responsabilidades generales y específicas para la gestión de la seguridad. • Compendio de procedimientos detallados de seguridad. • Definir la información a ser protegida o confidencial. • Vigencia de la información confidencial. • Responsabilidades y acciones de las personas para evitar la divulgación no autorizada de información.

1. Seguridad de los sistemas: a. Seguridad de los sistemas de información	
2. Planificación (Cont.)	• Establecer la propiedad de la información. • Determinar el uso adecuado o permitido de la información confidencial. • Establecer los procedimientos de auditoría sobre la información confidencial. • Proceso de notificación y reporte de información no autorizada. • Los procedimientos para la destrucción de la información confidencial al término del acuerdo. • Las acciones previstas a ser tomadas en caso de infracción.
3. Políticas y normas	Enunciar políticas y normas relacionadas a: • Creación de un sistema de reportes de fácil acceso y disponibilidad que permita tanto al personal de operaciones, seguridad, usuarios e incluso terceras partes; notificar e informar cualquier debilidad del sistema o servicio. • Controles respecto al acceso a las áreas restringidas de TI • Supervisión de las condiciones medioambientales para evitar amenazas tales como incendios, inundaciones, humo, polvo, vibración, interferencia eléctrica y vandalismo, así como como la temperatura, humedad, iluminación, ventilación, entre otros. • Automatización de tareas repetitivas. • Revisión de actividades o procedimientos improvisados, las cuales por lo general se realizan para solventar problemas en el corto plazo, evitando que dicha práctica se instaure como norma. • Ejecución de auditorías frecuentes para asegurarse que el servicio funcione de manera satisfactoria. • Utilización de procedimientos de gestión de incidentes, como fuente de mejoras oportunas. • Mejorar las comunicaciones formales y regulares entre los responsables

1. Seguridad de los sistemas: a. Seguridad de los sistemas de información	
3. Políticas y normas (Cont.)	de la seguridad y la gestión de servicios. • Promover la educación de los operadores, con el objeto de apoyar sus actividades y se facilite el manejo de las TI, sobre todo en el caso de introducción de nuevas tecnologías a la organización.
4. Control	• Se debe realizar periódicamente los objetivos de control, los controles, las políticas, procesos, procedimientos y todos los demás componentes que forma parte de la seguridad de información y de redes de datos, con la finalidad de realizar ajustes y mejoras. Dicha revisión debe realizarla personal independiente al área que está bajo revisión. • Los controles de seguridad debe estar diseñado para respaldar y hacer cumplir las políticas, minimizando así las amenazas reconocidas e identificadas. • Se deben revisar periódicamente (según lo indicado en la fase de planificación) los registros o logs del sistema para determinar el grado de utilización de los servicios de parte de: Usuarios autorizados, operaciones autorizadas realizadas, intento de accesos no autorizados, alertas o fallas del sistema. • Se deben ejercer controles sobre las vulnerabilidades. • Incluir en los controles las pruebas de penetración. • Se debe utilizar la auditoría como principal herramienta de control. • Ejercer control sobre el software tanto operacional, aplicaciones, bibliotecas de programas, respaldo y restauración (control de versiones).

1.Seguridad de los sistemas: b. Seguridad de las redes de datos	
1.Planificación	La planificación debe incluir los siguientes aspectos: • La planificación inicial y la instalación de nuevas redes, así como el mantenimiento de su infraestructura física, mediante un servicio de diseño y transición de servicio. • Debe contar con soporte de tercer nivel, incluyendo actividades para la prevención de problemas de la red, como alternativa para escalar los problemas. • Se debería tener contratos de mantenimiento y soporte para los sistemas operativos de red, incluyendo gestión de parches y actualizaciones. • Monitorear el tráfico de red para identificar posibles fallas y congestionamiento de tráfico. • Reconfiguración o desvíos de tráfico para conseguir un mejor rendimiento, contribuyendo con la calidad del servicio. • Administración de la asignación de direcciones IP (DHCP), servicios de DNS. • Implementación, monitoreo y mantenimiento de los sistemas de detección de intrusos. • Evitar la denegación de servicios. • Actualización de la documentación necesaria para el mantenimiento de los sistemas de red.
2. Políticas y normas	Las políticas y normas deben incluir: • Identificar las redes y los servicios a los cuales se puede tener acceso. • Los procedimientos y autorizaciones para determinar quién tiene permiso de acceder a qué redes y servicios de red. • La gestión de controles y procedimientos para proteger el acceso a las conexiones de red y servicios de red. • Los medios utilizados para acceder redes y servicios de red. En relación a la protección de las líneas de telecomunicaciones se tiene los siguientes aspectos:

1.Seguridad de los sistemas: b. Seguridad de las redes de datos	
2. Políticas y normas (Cont.)	• Los cables de energía y de comunicaciones deben permanecer separados, para la prevención de interferencias. • Los cables de redes deben protegerse de interceptación no autorizada, evitando su exposición en áreas públicas. • Deben identificarse claramente los cables y equipos con la finalidad de minimizar los errores de manipulación. • Debe existir una lista de conexiones documentada para así reducir la posibilidad de errores. • Para los sistemas críticos, se debe: o Instalar conductos blindados y habitaciones o cajas cerradas en puntos de inspección o terminación. o Utilización de rutas alternativas o medios de transmisión que proporcionen la seguridad adecuada. o Utilización de escudos electromagnéticos para la protección de los cables de red. o Acceso controlado a los paneles de conexión y cuartos de cableado.
3. Control	Entre las medidas de control a implementar se tiene: • Identificación de los equipos de red. • Separación de la redes en grupos funcionales. • Aislamiento de los equipos de información sensibles. • Protección de los equipos informáticos móviles. • Ejercer controles sobre el tráfico de red, mediante la aplicación de restricciones a servicios de mensajería, transferencia de archivos, acceso interactivo (chat, video conferencia). • Evaluación de los incidentes de seguridad ocurridos, los cuales alimentarán las estadísticas para mejorar la gestión.

1.Seguridad de los sistemas: c. Seguridad relacionada con los usuarios	
1.Planificación	La planificación debe contemplar los siguientes aspectos: • Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI sean identificables de manera única. • Permitir que el usuario se identifique a través de mecanismos de autentificación. • Confirmar que los permisos de acceso del usuario al sistema sean los adecuados según la documentación escrita y de acuerdo a su ámbito de trabajo. • Asegurar que los derechos de acceso del usuario sean debidamente solicitados y aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. • Las identidades del usuario y los derechos de acceso se mantienen en un repositorio de datos centralizado. • Desplegar técnicas efectivas para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.
2. Políticas y normas	Se deben dictar políticas y normas relativas a: • Verificación de la identidad del usuario. • Procedimientos de otorgamiento, modificación y revocación de roles. • Procedimientos para el manejo de excepciones e incidentes. • Revisión periódica de los permisos otorgados. • Registro de los datos que identifiquen al usuario. • Registro de los grupos de usuarios. • Establecimientos de normas y procedimientos para la creación, uso y cambio de contraseñas. • Establecimiento de procesos disciplinarios para aquellos usuarios que compartan sus contraseñas.

1.Seguridad de los sistemas: c. Seguridad relacionada con los usuarios	
3. Control	El control debe garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia.

2.Desempeño y capacidad:	
1.Planificación	Los planes deben incluir: • Acuerdos de niveles de servicios: Se debe conocer las dimensiones del servicio requerido así como los tiempos de respuesta aceptable, por lo que se deben hacer consideraciones de la capacidad de respuesta de los equipos instalados, ancho de banda en relación al incremento en el consumo de tales servicios. • Diseñar, adquirir o modificar la configuración de los servicios en base a un diseño previamente propuesto, en función de equilibrar los costos con la implementación de alternativas adecuadas y rentables. • Se debe implementar técnicas de predicción que proporcionen la verificación de las capacidades de rendimiento del servicio. • Todos los cambios a realizar para garantizar la capacidad del servicio, deben seguir los procedimientos establecidos para la adquisición y actualización de TI.

2.Desempeño y capacidad:	
2. Políticas y normas	Las políticas y normas relativas a la gestión del desempeño y la capacidad, se encuentran enmarcadas dentro de las políticas generales de la seguridad de la información, las cuales deben estimular los controles y las auditorias para determinar el desempeño presente y futuro de los sistemas, para así medir la capacidad actual y planificar la capacidad futura acorde a las necesidades de la organización.
3. Control	Monitorear continuamente el desempeño y la capacidad de los recursos de TI, con el objetivo de: • Mantener y poner a punto el desempeño actual dentro de TI. • Permitir la elasticidad, contingencia, cargas de trabajo, tanto actuales como proyectadas, planes de almacenamiento y adquisición de recursos. • Permitir reportar la disponibilidad del servicio. • Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas. • Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados. • Medir el desempeño futuro, por lo que se deben efectuar periódicamente pronósticos de desempeño y capacidad de los recursos de TI para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. • Identificar el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

<table>
<tr><th colspan="2">3.Continuidad del servicio:</th></tr>
<tr><td>1.Planificación</td><td>La planificación tiene por objetivo el desarrollo de un marco de trabajo de continuidad de TI, facilitando la determinación de la fortaleza requerida por la infraestructura y contribuir guiar al desarrollo de planes de recuperación ante desastres y contingencias
La planificación de la continuidad se divide en cuatro etapas:

Primera Etapa Inicio:
Mantener actualizado los planes de continuidad de servicios alineados con los planes globales de continuidad de la organización.
Asegurarse que el plan de continuidad se mantenga vigente en relación a los cambios ocurridos en el contexto de la organización.
Realizar periódicamente el análisis de riesgos.
Proporcionar asesoramiento a todas aquellas áreas de la organización que puedan influir en la continuidad de TI.
Asegurarse que los mecanismos de adecuados de TI se materialicen en el momento indicado para así apoyar la continuidad de las operaciones.
Evaluar el impacto en los planes de continuidad de TI originados por cambios en los planes de prestación de servicios.
Garantizar que las medidas de continuidad de servicios se ajusten a costos razonables.
Negociar y acordar contratos con terceras partes para el suministro de insumos necesarios o apoyo de tercer nivel requeridos para los planes de recuperación.
Segunda Etapa – Requisitos y Estrategias:
Requisitos y Análisis del impacto de la organización: Tiene por finalidad medir el impacto que en la organización tiene la pérdida de servicios, por lo que se deben identificar los servicios más importantes.</td></tr>
</table>

3.Continuidad del servicio:	
1.Planificación (Cont.)	• Requisitos y análisis de riesgos: Este estudio determina la probabilidad de ocurrencia de un desastre de grandes dimensiones en la organización, conociendo así el grado de vulnerabilidad de la organización. **Tercera Etapa – Implementación:** Compuesto por una serie de planes técnicos, tales como: • Plan de respuesta emergencia: Permiten servir de interfaces entre los servicios de emergencia y las actividades relacionadas con la recuperación. • Plan de evaluación de daños: Contiene los datos de los contactos que realizan la valuación de daños, planes y procesos relacionados. • Plan de salvamento: Contiene información sobre los contactos de salvamento, planes y procesos relacionados. • Registro del plan vital: Contiene detalle de todos los registros vitales de información, los cuales son críticos para la organización, así como su ubicación. • Gestión de crisis y plan de relaciones públicas: Son planes que permiten manejar a los medios de comunicación y relaciones públicas. • Instalaciones y plan de servicios: Detalla el plan que permite salvaguardar las instalaciones necesarias para la continuidad del servicio. • Plan de seguridad: Muestra todos los aspectos de seguridad que deben ser administrados para la recuperación de los servicios en la organización. • Plan del personal: Muestran cómo se manejarán los problemas relacionados al personal durante el manejo del incidente. • Plan de comunicación: Muestra cómo todos aquellos aspectos de la comunicación serán administrados por aquellos entes involucrados durante la recuperación de un incidente grave. • Finanzas y administración: Contiene en detalle los procedimientos necesarios que permiten autorizar la erogación de los fondos necesarios para subsanar el incidente.

3.Continuidad del servicio:	
1.Planificación (Cont.)	Además de los planes anteriores, se requiere de un plan especial de contingencia que abarque las áreas ejecutivas, de manera que la alta gerencia se responsabilicen de la coordinación y la gestión de la crisis, el área de coordinación, correspondientes a los niveles ejecutivos medios, los cuales deben coordinar los esfuerzos de la recuperación, y finalmente el área de recuperación, representado por los equipos de trabajo que materializan la recuperación de los sistemas. Los planes de recuperación deben incluir validaciones que garanticen su funcionalidad y operatividad, por lo que se recomienda la realización de pruebas de simulación, parciales, completas y por escenarios. **Cuarta Etapa – Operación Continua:** Consiste en: • Educar y sensibilizar a la organización es los aspectos específicos de continuidad del servicio, asegurarse de la toma de conciencia en el personal de TI y hacerlo parte de su trabajo normal en base a que todos han sido entrenados para realizar las acciones que corresponden ante la ocurrencia de tales eventos. • Revisar todos los planes y procesos de recuperación para garantizar su actualización. • Realizar pruebas periódicas de los planes, sobre todo en aquellos casos que involucren cambios tecnológicos. • El proceso de gestión de cambios debe asegurar que los impactos de dichos cambios se reflejen en los planes de recuperación.

3.Continuidad del servicio:	
2. Políticas y normas	Están orientadas a brindar la capacidad y el desempeño requerido tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.
3. Control	Se divide en: • Mantenimiento del plan: Debido a las condiciones cambiantes de TI en la organización, se hace necesario mantener un proceso de actualización continua de los planes, por lo que se recomienda definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales. • Los planes de seguridad deben ser probados continuamente, para así demostrar su actualización y su eficacia. Así como también asegurar que todos los miembros del equipo de recuperación conozcan en detalle todos los procesos involucrados. • Actividades de Control: Análisis del impacto de las fallas de componentes: Identifica los puntos de fallo en los servicios de TI motivado por problemas de configuración, así mismo mide la validez de los procedimientos de recuperación. • Análisis de árbol de falla: Permite determinar la cadena de acontecimientos que causan una interrupción en los servicios de TI. Se identifican los eventos básicos, resultantes, condicionales y disparadores. • Análisis de fallas de servicios: Permite identificar las oportunidades de mejoras.

3.Continuidad del servicio:	
3. Control (Cont.)	• Observaciones técnicas: Es el resultado de un encuentro entre personal técnico especializado en soporte de TI, centrado en aspectos específicos de disponibilidad, busca controlar la ocurrencia de eventos en tiempo real a medida que ocurren.

4.Entrenar y educar a los usuarios:	
1.Planificación	La planificación del adiestramiento forma parte integral de la seguridad de la información y está contemplada a través de toda la propuesta, por lo que debe responder a cada plan en particular.
2. Políticas y normas	Con base a las necesidades de adiestramiento, deben formularse las políticas que permitan designar los a instructores debidamente calificados para organizar cursos con el tiempo suficiente, dicho adiestramiento debe ser sistematizado, incluyendo prerrequisitos, asistencia y evaluaciones.
3. Control	Al finalizar el adiestramiento, se deberá evaluar el contenido, la calidad, efectividad, percepción y retención del conocimiento, así como su costo y valor. Los resultados de esta evaluación definirán los planes futuros de adiestramiento.

Nota: Elaborado por el autor.

La tabla anterior integra las recomendaciones y normas internacionales establecidas por CobiT 4.1, ITIL V3 e ISO/IEC 27002, enmarcado dentro de un sistema administrativo que permite gerenciar todos los aspectos de la seguridad de la información y redes de datos. Así todos los eventos que puedan surgir relacionados con la seguridad, serán debidamente

atendidos. Además se cuenta con un continuo proceso de actualización y adaptación a los cambios que puedan surgir a través del tiempo.

A continuación en la Tabla 47, se exponen un conjunto de recomendaciones específicas para el tomando en cuenta las condiciones de seguridad encontradas dentro del MPP Educación:

Tabla 47. Recomendaciones al MPP Educación.

Recomendaciones al MPP Educación
1. Seguridad de los Sistemas: **a. Seguridad de los sistemas de información:** Con respecto a los controles establecidos para determinar posibles ataques en el MPP Educación, los registros o logs de los sistemas no son revisados con la meticulosidad que merecen, sin embargo, en los resultados obtenidos (ítem 14 del cuestionario), se registró que tales logs si son activados, por lo que este aspecto positivo debe ser reforzado. Otro de los aspectos positivos que actualmente existe en materia de seguridad en el MPP Educación, es la sincronización de los relojes del sistema, garantizando así la fidelidad de los reportes o logs del sistema, esta actividad debe ser mantenida y reforzada. El MPP Educación ha implementado algunos controles de acceso físico a las instalaciones de TI, por lo que se hace necesario reforzar estas iniciativas, según el resultado del ítem 37 del cuestionario. **b. Seguridad de las redes de datos:** La red datos del MPP Educación cuenta con los recursos de TI suficientes para prestar un adecuado servicio, sin embargo, debido a la inexistencia de políticas y normas relacionadas al tipo de datos que pueden circular por ellas, en un futuro cercano pueden el

tráfico de la red puede verse afectado negativamente. Así mimo se hace necesario adecuar la infraestructura de cableado de la red, según las normas dictadas para tal fin.

En cuanto al uso de dispositivos de red para el control de ataques e intrusiones, tal como los firewall el MPP Educación ha demostrado madurez, mediante la implementación de tales dispositivos, lo cual es uno de los aspectos que debe mantenerse y fortalecerse, así como los analizadores de tráfico de la red. Otro de los aspectos positivos encontrados (ítem 31 del cuestionario) es la identificación precisa de los equipos de red, así como la identificación de los sistemas sensitivos (ítem 32 del cuestionario).

c. Seguridad relacionada con los usuario:

Actualmente en el MPP Educación no existe un registro y control adecuado de usuarios y sus privilegios, por lo que se hace necesaria la implementación de tal registro en una base de datos, con una aplicación que permita realizar consultas. También se recomienda la realización de campañas de concientización a los usuarios con el fin de que conozcan sus derechos y responsabilidades asociadas al uso de privilegios en el sistema y sus contraseñas.

2. Desempeño y capacidad

A este respecto el MPP Educación carece de las mediciones necesarias para determinar tanto su capacidad actual como futura, por lo que es imposible realizar los cálculos necesarios para la implementación de planes y programas que garanticen la capacidad y la operatividad de los sistemas. Esta medición resulta fundamental para la prestación de un óptimo servicio, la cantidad de datos que circulan por la red generalmente se incrementa en la medida que el tiempo transcurre, esto debido a la implementación de nuevas aplicaciones, apertura de nuevos servicios, etc.

Recomendaciones al MPP Educación
3. Continuidad del servicio Con respecto a la gestión continuidad, el MPP Educación tiene un largo camino por recorrer, las recomendaciones anteriores servirán como punto de partida para esta labor. Actualmente no existen planes ni programas que garanticen la continuidad de las operaciones, así mismo los contratos de mantenimiento son inexistentes o se encuentran desactualizados.
4. Educar y entrenar a los usuarios El adiestramiento es una labor fundamental que debe ser reforzada dentro del MPP Educación, dicho adiestramiento no sólo deberá estar destinado a los operadores y administradores de los sistemas, sino también a los usuarios, para así potenciar sus capacidades y minimizar los riegos de errores humanos. En el MPP Educación se tiene la paradoja de realizar una efectiva detección de necesidades de adiestramiento, sin embargo, los cursos no son impartidos, por lo que se hace necesario resolver esta disonancia.

Nota: Elaborado por el autor.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se hace evidente que existe un serio problema de seguridad en las redes de datos del MPP Educación, presenta graves deficiencias desde el punto de vista organizacional, ya que no cuenta con una Dirección de Seguridad de la Información, así como tampoco de Auditoría de Sistemas, por lo que la responsabilidad de la seguridad recae en los operadores y administradores de los sistemas.

Así mismo no se han establecido las políticas, normas y procedimientos adecuados para el manejo de los incidentes de seguridad, esto acarrea serios inconvenientes a la hora de iniciar los procesos de recuperación luego de algún incidente.

En relación a las redes de datos, no se tienen estadísticas certeras que permitan medir la capacidad presente, mucho menos hacer cálculos para la capacidad requerida en el futuro, por lo que la continuidad de los servicios se encuentra gravemente comprometida.

En relación al registro y control de usuarios así como de sus privilegios dentro del sistema, se requiere la implementación de nuevos y mejores métodos de control, que permitan registrar los datos de los usuarios, la permisología, así como el historial de privilegios otorgados y revocados a través de toda su trayectoria como usuario del sistema. En este aspecto también se debe hacer énfasis en la necesidad de concientizar a los usuarios en relación a sus responsabilidades, el adecuado uso de contraseñas y las precauciones que debe tener respecto a las sesiones abiertas, esto puede lograr mediante el desarrollo de campañas informativas.

Los planes de continuidad de las operaciones se encuentran ausentes de la agenda de trabajo de seguridad en el MPP Educación, por lo que es imprescindible que se desarrollen lo antes posible, con el objeto de estar preparados para enfrentar cualquier incidente que en materia de seguridad se pueda presentar.

Finalmente se hace necesario crear conciencia, motivar y adiestrar al personal de operadores y administradores de TI en temas de seguridad, para potenciar sus capacidades y minimizar la ocurrencia de errores por fallas humanas, pero sobre todo, se requiere de la concientización de los niveles gerenciales para que incluyan en su agenda de trabajo los temas relativos a la seguridad de la información y de las redes de datos.

En relación a la investigación documental para determinar cuál de los estándares y mejores prácticas de seguridad es el más adecuado para la implementación de un sistema de seguridad, se obtuvo como resultado que no existe un mejor estándar que otro, sino que entre sí se complementan.

No resulta fácil la unificación de los criterios aportados por tales estándares, sin embargo, gracias a las nuevas investigaciones, aportes y recomendaciones de las instituciones que los promueven, se hace posible utilizar dichos estándares de manera integral.

En el caso de la presente investigación se analizaron CobiT 4.1, ITIL V3 e ISO/IEC 27002, de los tres estándares estudiados el más voluminoso, completo y el que aportó la mayor parte de las recomendaciones fue ITIL V3, seguido de ISO/IEC 27002, sin embargo, fue CobiT 4.1 el que sirvió de punto de partida, orientando así la elaboración de las recomendaciones finales, esto coincide con lo expuesto por IT Governance Institute (2008), en su Alineación CobiT, ITIL V3 e ISO/IEC 27002, donde recomienda utilizar CobiT e ISO /IEC 27002 para establecer qué debe hacerse, mientras ITIL V3, debe ser indica cómo hacerlo. Fue precisamente éste documento el que facilitó enormemente la unificación de los criterios aportados por las tres normas.

Es importante hacer énfasis que siendo CobiT 4.1 la norma utilizada como punto de partida para la formulación de las recomendaciones, se debe entender claramente las interrelaciones existentes entre los diversos objetivos de control para su correcta aplicación. En caso contrario, las recomendaciones finales pueden resultar insuficientes y poco efectivas.

Si bien en la investigación realizada a las condiciones de seguridad en las redes de datos del MPP Educación, resultaron ser deficientes, existen prácticas desarrolladas e implementadas que merecen se le den continuidad y se fortalezcan en lo futuro. Se observó que la seguridad de la red, aunque no es la óptima, posee mecanismos que le proporcionan al menos un mínimo de seguridad. El uso de dispositivos tales como *firewall* y *proxy*, está bastante desarrollada. Así mismo las iniciativas como la eliminación de virus en el propio servidor de correos contribuyen al control de malware que puede ser distribuido mediante la red, sin embargo pese a este esfuerzo, el resultado de la investigación de campo en el tema relacionado a la propagación del malware o virus arrojó resultados negativos.

Las redes de servidores no se encuentran separadas de la red de trabajo de los usuarios, contraviniendo así lo aconsejado por las mejores prácticas, sin embargo, se han realizado esfuerzos por crear VLAN o redes virtuales en cada piso del edificio sede del MPP Educación, lo cual contribuye a impedir la propagación de virus y gusanos, además aligeran la carga de trabajo de los suiches y *routers* de la red. Evitando así los puntos únicos de falla, en caso de presentarse algún problema con la red de un piso en particular, el servicio de red en los demás pisos no se vería afectado.

La infraestructura de la red del MPP Educación es bastante sólida, cuenta con tecnología que se puede considerar de punta, sin embargo esta característica por sí misma no garantiza la seguridad.

Las normas que pasaron a formar parte de la propuesta tienen su origen fundamentalmente en aquellas referidas a la seguridad de TI y en especial, las recomendaciones particulares para redes de datos.

La propuesta de seguridad formulada originalmente abarcaba tres aspectos relativos a: (1) La prevención de incidentes, (2) la corrección de posibles fallos y (3) la contingencia y recuperación en caso de afectación por incidentes de seguridad. Sin embargo, el estudio arrojó nuevos componentes a ser añadidos al trinomio anteriormente mencionado, se trata de: (4) La gestión del desempeño y la capacidad, la cual es pieza fundamental para medir los requerimientos actuales y prever las necesidades futuras, así como (5) la continuidad del servicio. Todos estos elementos permiten que los incidentes o fallos sean manejados de forma rutinaria, sin imprevistos, y con procedimientos comprobados que garanticen la pronta recuperación de los servicios y sistemas.

Otro aspecto interesante que se desprende de la presente investigación, es que en principio se enfocó a la seguridad como un problema técnico, que podía resolverse mediante la implementación de dispositivos, programas o herramientas tecnológicas. El resultado del estudio arrojó que la seguridad dista de ser problema técnico, es más bien un problema de gestión, de administración, por lo que envuelve procesos propios relativos a ésta, como lo son: La planificación, organización, dirección y control. Sin dicho mecanismo es imposible desarrollar un ambiente de seguridad adecuado dentro de la organización.

La tecnología es cambiante, las formas de ataque, las vulnerabilidades y los incidentes de seguridad también lo son, enfocar la seguridad como un tema de tipo técnico no resuelve el problema, ya que sólo se obtendría una solución temporal a los problemas, desactualizándose en la medida que transcurre el tiempo. La adecuada gestión de seguridad permite adaptarse a dichos cambios.

Si bien el principal tema del estudio fue la seguridad en las redes de datos, es imposible hablar de seguridad puntualizando sólo este aspecto, tal como lo indicaban los antecedentes del estudio, la seguridad debe ser visualizada holísticamente, integralmente. No puede centrarse sólo en los problemas específicos de la red, en los accesos físicos, en los equipos servidores, en las medidas contra incendio y catástrofes, en los procedimientos de recuperación, o en cualquier otro aspecto específico. La seguridad es un problema global y como tal debe ser afrontada, dejar de lado cualquiera de las aristas de la problemática de

seguridad en TI, sería como construir un coloso de acero con los pies de barro, en cualquier momento se corre el riesgo de la debacle. Por tal motivo la propuesta de seguridad de la presente investigación, aunque hizo énfasis en las redes de datos, también desarrolló otros aspectos que vienen a formar parte integral de la seguridad de TI.

Recomendaciones

El MPP Educación debería implementar muchas de las recomendaciones de seguridad expuestas en la presente investigación. Se hace imprescindible la creación de las unidades organizativas de seguridad de la información y de auditoría de sistemas, en su defecto esta última unidad pudiese ser sustituida por asesores externos. Una vez materializada la creación de estas unidades, se debería proceder a la formulación de objetivos, políticas, normas y procedimientos que regulen el tema de la seguridad de la información. Seguidamente, se debería iniciar cursos de adiestramiento para capacitar al personal operativo y a los administradores de sistemas en el adecuado uso de tales procedimientos. Así mismo se deben desarrollar campañas de concientización en materia de seguridad a los usuarios del sistema.

Iniciar esta tarea no es sencillo, por lo que se debe contar con el consentimiento y el apoyo de la Dirección de Administración y Servicios así como del propio Ministro del Poder Popular para la Educación.

Tal iniciativa debe ser liderada por la Dirección de Informática del MPP Educación, mediante informes, recomendaciones e incluso presentaciones con expertos en la materia donde asistan incluso los directores de las oficinas ministeriales.

Esta labor debe iniciarse lo antes posible, la seguridad así como la salud de los procesos organizacionales no puede esperar.

Debe realizarse porque los servicios de TI que ofrece el MPP Educación son indispensables para el normal desenvolvimiento de todas las actividades administrativas y académicas de educación inicial, básica y diversificada de la República Bolivariana de

Venezuela. Esto beneficiará a los usuarios de los sistemas, garantizando la continuidad y la calidad de los servicios prestados.

Como sugerencia, producto de la experiencia adquirida en la presente investigación, se tiene que los temas específicos de seguridad, tales como seguridad en las redes de datos, seguridad en los equipos servidores o en las bases de datos, deben ser tratados sólo cuando se tenga la certeza que exista un marco de seguridad global, previamente establecido, que la sustente. En este caso la investigación a desarrollar se encargaría de puntualizar y mejorar dichos aspectos específicos.

En caso de investigaciones específicas a los temas de seguridad en las redes de datos, enmarcadas dentro de la seguridad de TI globalmente aceptada e implementada en la organización, sería interesante desarrollar el conjunto de recomendaciones basadas en la Norma ISO/IEC 27033, profundizando así en estos temas. Lamentablemente no se contó con tales normas para el desarrollo de la presente investigación.

Así mismo y basado en los resultados del presente estudio, se pudiesen derivar otras investigaciones, tal como el desarrollo de un modelo de madurez para la seguridad de la información, destinado exclusivamente a organismos y entidades públicas de la República Bolivariana de Venezuela.

CAPÍTULO VI

LA PROPUESTA

Consideraciones generales

El presente capítulo está dedicado a la presentación de la propuesta resultante de la investigación, sus elementos más importantes así como la justificación y factibilidad de la misma.

Objetivo de la propuesta

Presentar un sistema de seguridad para las redes de datos del Ministerio del Poder Popular de Educación.

Justificación de la propuesta

Las condiciones de seguridad de redes de computadoras, así como de los sistemas de información en general del MPP Educación, según el estudio realizado, arrojó como resultado ser insuficiente, por lo que se hace necesaria la implementación de normas y estándares de seguridad que permitan mejorar la situación existente.

Beneficios de la propuesta

La propuesta tiene por finalidad beneficiar ampliamente los sistemas de información del MPP Educación, asegurando los datos existentes en sus repositorios así como la que circula libremente por la red, lo que repercutirá directamente en la mejora de los servicios prestados a los usuarios de dicho sistema.

Localización física y cobertura espacial

La propuesta se focaliza en las redes de datos y los sistemas de información del MPP Educación, ubicado en el Edificio Sede del Ministerio así como las 24 zonas educativas distribuidas en todos los estados de Venezuela, específicamente destinada a la Dirección de Informática del Ministerio del Poder Popular para la Educación (Ver Figura 52). Dicha propuesta está basada en las recomendaciones y estándares internacionales vigentes hasta el año 2011.

Figura 52. Organigrama Simplificado del MPP Educación

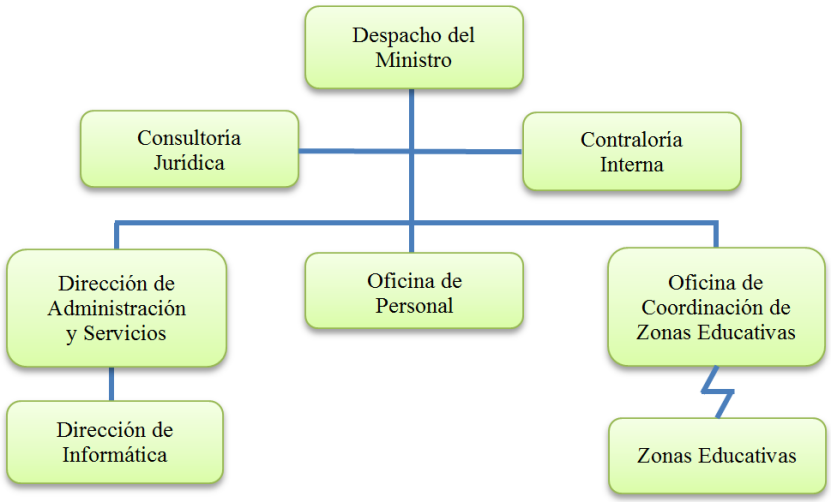

Figura 52. Organigrama simplificado del MPP Educación, donde se muestran las zonas educativas como entes desconcentrados. Elaborado por el autor.

Evaluación

La evaluación de la propuesta se realizó a través de la matriz DOFA (ver Tabla 48), la cual es una herramienta utilizada como método de diagnóstico en el ámbito de la planificación estratégica.

Tabla 48. Análisis DOFA de la propuesta presentada.

Fortalezas	Debilidades
El diseño del sistema de seguridad para las redes de datos está basado en tres normas y estándares internacionales, que fueron debidamente alineados por un organismo reconocido como lo es ISACA. Dichas normas han sido adaptadas a la realidad existente en el MPP Educación.	Como toda implementación de un nuevo sistema, existe la resistencia al cambio, de parte del personal, así como la falta de apoyo de los niveles gerenciales y las limitaciones presupuestarias que impidan la creación o modificación las estructuras organizacionales, adquisición de nuevas tecnologías, etc.
Oportunidades	**Amenazas**
Incrementar la seguridad de la información y las redes de datos del MPP Educación, lo cual redundará en la prestación de un mejor servicio, garantizando la continuidad los procesos y labores administrativas que tienen basados en los sistemas de información existentes.	Carencia de la madurez necesaria para aceptar los riesgos existentes y valorizar los cambios necesarios que deben llevarse a cabo para subsanar la problemática existente.

Nota: Elaborado por el autor.

Estudio de factibilidad o viabilidad.

Para la factibilidad de la presente propuesta se tomaron en cuenta los siguientes aspectos:

- Factibilidad institucional: La gerencia del MPP Educación debe convertirse en el motor que impulse los cambios necesarios para la implementación de las recomendaciones expuestas en el estudio.

- Factibilidad técnica: La implementación de la propuesta requiere que el recurso humano responsable de su puesta en práctica cuente con los conocimientos, habilidades, destrezas y experiencias necesarias para su materialización, así como la existencia o adquisición de la tecnología que le da soporte.
- Factibilidad operativa: Está relacionada con la estructura organizativa que permita la administración de los recursos involucrados en el diseño de seguridad. Esta actividad también está relacionada a las labores de adiestramiento continuo y concientización en materia de seguridad.

Descripción de la propuesta

La presente propuesta de seguridad para las redes de datos del MPP Educación tiene por característica ser de tipo (1) preventivo, (2) correctivo, (3) de contingencia y recuperación, (4) gestión del desempeño y la capacidad, (5) continuidad del servicio.

Otra de las características del presente diseño, es la propiedad de mantenerse actualizado en todo momento, la dinámica de la seguridad es cambiante, por lo que la propuesta de seguridad también debe adaptarse a tales cambios.

Además se hace necesario el énfasis en los aspectos de prevención, corrección, así como en contingencia y recuperación, garantizando los principios de seguridad como lo son: La confidencialidad, la integridad, disponibilidad, autentificación, autorización, auditabilidad, funcionalidad Vs. seguridad, privacidad y no repudio. El Diseño del Sistemas de Seguridad para las Redes de Datos del MPP Educación puede observarse gráficamente en la Figura 53.

Figura 53. Sistema del Sistema de Seguridad para las Redes de Datos del MPP Educación

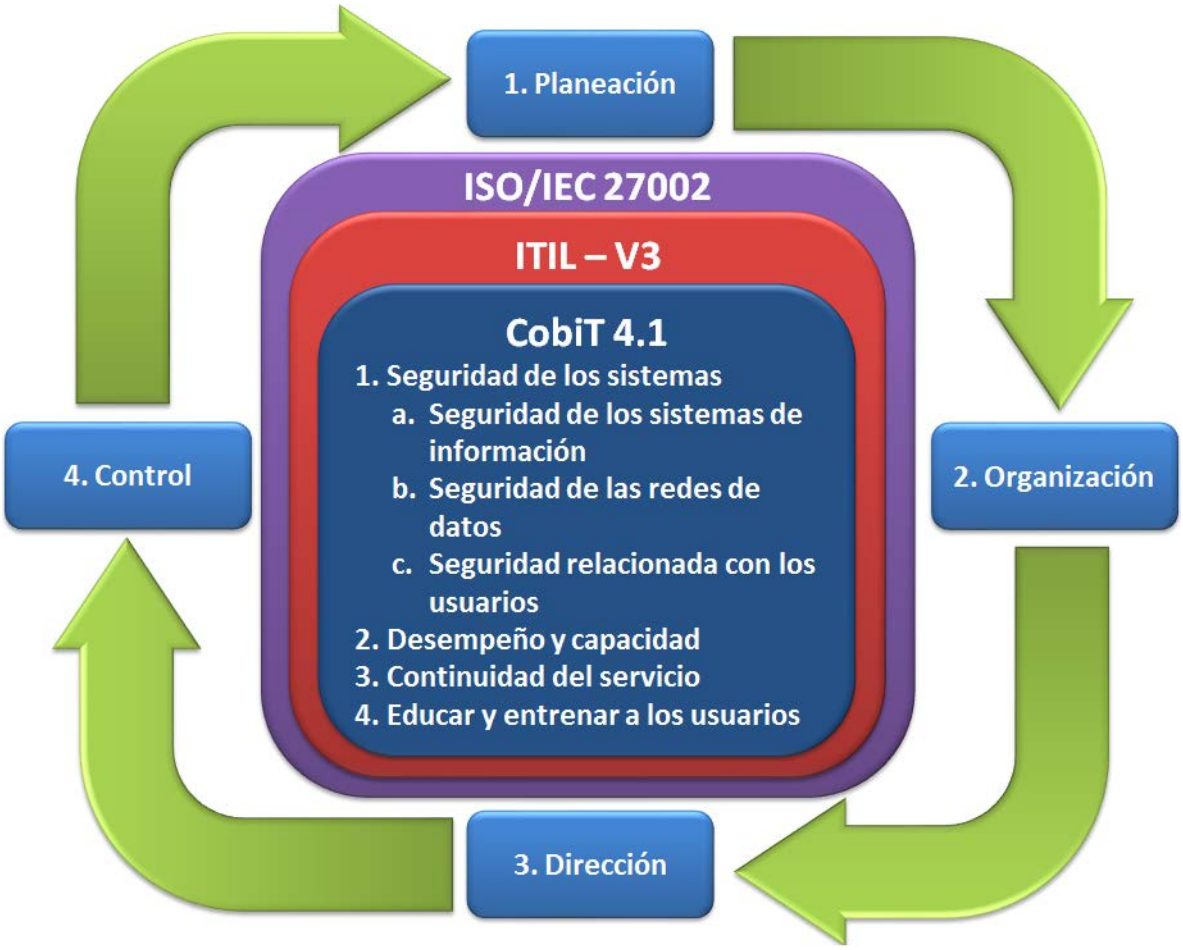

Figura 53. Sistemas de Seguridad para las Redes de Datos del MPP Educación, en la cual se integran CobiT 4.1, ITIL V3 e ISO/IEC 27002, dentro del marco de los procesos administrativos. Elaborado por el autor.

A continuación se expone en detalle en la Tabla 49, el Diseño del Sistemas de Seguridad para las Redes de Datos del MPP Educación:

Tabla 49. Diseño del Sistema de Seguridad para las Redes de Datos del MPP Educación.

1. Seguridad de los sistemas: **a. Seguridad de los sistemas de información**	
1. Organización	**Creación de una estructura organizacional de seguridad de la información con las siguientes atribuciones:** • El diseño de planes preventivos, correctivos, de continuidad, de contingencia y recuperación. • Enunciado de políticas, normas y procedimientos de seguridad. • Monitoreo y elaboración de informes de seguridad. • Ofrecer asistencia técnica y asesoramiento en la investigación de accidentes de seguridad. • Realización de operativos de control sobre pistas de auditorías, controles de acceso físico. • Formación y sensibilización de los usuarios en materia de seguridad **Entre las funciones de esta unidad administrativa se tiene:** • Identificar los objetivos y metas pertinentes a la seguridad. • Formular, revisar y aprobar las políticas de seguridad. • Verificar la eficacia de la implementación de las políticas de seguridad. • Proporcionar una clara dirección y apoyo a las iniciativas de seguridad. • Proporcionar los recursos necesarios. • Aprobar la asignación de roles y responsabilidades de la seguridad de la información. • Asegurar que las actividades de seguridad sean ejecutadas. • Evaluar la información recibida del seguimiento y revisión de incidentes de seguridad, para recomendar las acciones pertinentes. • Soporte y mantenimiento adecuado de los sistemas operativos, actualizaciones, parches. • Gestión de licencias. • Contratación de soporte de tercer nivel para escalar los posibles

1. Seguridad de los sistemas: a. Seguridad de los sistemas de información	
1. Organización (Cont.)	problemas e incidentes de seguridad, obtener soporte. • Implementación de sistemas de seguridad, control y mantenimiento, así como la adecuación de medidas de seguridad física. • Distribución adecuada de las cargas de trabajo para garantizar la continuidad. • Mejoramiento del rendimiento de los equipos. • Planificación de la adquisición de nueva TI. • Planificación de cursos de adiestramiento. • Debe considerar el establecimiento de acuerdos con terceros, como por ejemplo, asesores externos o soporte de terceros, de manera que se pueda auditar y controlar las acciones de estas personas dentro de la estructura de TI de la organización.
2. Planificación	La planificación debe incluir: • Definición de la seguridad de información y de redes de datos. • Objetivos generales, alcance e importancia de la seguridad. • Declaración de la dirección sobre el apoyo a los objetivos y principios de seguridad. • Marco de referencia para establecer los objetivos de control, la estructura de evaluación y la gestión del riesgo. • Explicación de las políticas, principios, normas y requisitos de seguridad. • Definición de responsabilidades generales y específicas para la gestión de la seguridad. • Compendio de procedimientos detallados de seguridad. • Definir la información a ser protegida o confidencial. • Vigencia de la información confidencial. • Responsabilidades y acciones de las personas para evitar la divulgación no autorizada de información.

1. Seguridad de los sistemas: a. Seguridad de los sistemas de información	
2. Planificación (Cont.)	• Establecer la propiedad de la información. • Determinar el uso adecuado o permitido de la información confidencial. • Establecer los procedimientos de auditoría sobre la información confidencial. • Proceso de notificación y reporte de información no autorizada. • Los procedimientos para la destrucción de la información confidencial al término del acuerdo. • Las acciones previstas a ser tomadas en caso de infracción.
3. Políticas y normas	Enunciar políticas y normas relacionadas a: • Creación de un sistema de reportes de fácil acceso y disponibilidad que permita tanto al personal de operaciones, seguridad, usuarios e incluso terceras partes; notificar e informar cualquier debilidad del sistema o servicio. • Controles respecto al acceso a las áreas restringidas de TI • Supervisión de las condiciones medioambientales para evitar amenazas tales como incendios, inundaciones, humo, polvo, vibración, interferencia eléctrica y vandalismo, así como como la temperatura, humedad, iluminación, ventilación, entre otros. • Automatización de tareas repetitivas. • Revisión de actividades o procedimientos improvisados, las cuales por lo general se realizan para solventar problemas en el corto plazo, evitando que dicha práctica se instaure como norma. • Ejecución de auditorías frecuentes para asegurarse que el servicio funcione de manera satisfactoria. • Utilización de procedimientos de gestión de incidentes, como fuente de mejoras oportunas. • Mejorar las comunicaciones formales y regulares entre los responsables

1. Seguridad de los sistemas: a. Seguridad de los sistemas de información	
3. Políticas y normas (Cont.)	de la seguridad y la gestión de servicios. • Promover la educación de los operadores, con el objeto de apoyar sus actividades y se facilite el manejo de las TI, sobre todo en el caso de introducción de nuevas tecnologías a la organización.
4. Control	• Se debe realizar periódicamente los objetivos de control, los controles, las políticas, procesos, procedimientos y todos los demás componentes que forma parte de la seguridad de información y de redes de datos, con la finalidad de realizar ajustes y mejoras. Dicha revisión debe realizarla personal independiente al área que está bajo revisión. • Los controles de seguridad debe estar diseñado para respaldar y hacer cumplir las políticas, minimizando así las amenazas reconocidas e identificadas. • Se deben revisar periódicamente (según lo indicado en la fase de planificación) los registros o logs del sistema para determinar el grado de utilización de los servicios de parte de: Usuarios autorizados, operaciones autorizadas realizadas, intento de accesos no autorizados, alertas o fallas del sistema. • Se deben ejercer controles sobre las vulnerabilidades. • Incluir en los controles las pruebas de penetración. • Se debe utilizar la auditoría como principal herramienta de control. • Ejercer control sobre el software tanto operacional, aplicaciones, bibliotecas de programas, respaldo y restauración (control de versiones).

1.Seguridad de los sistemas: b. Seguridad de las redes de datos	
1.Planificación	La planificación debe incluir los siguientes aspectos: • La planificación inicial y la instalación de nuevas redes, así como el mantenimiento de su infraestructura física, mediante un servicio de diseño y transición de servicio. • Debe contar con soporte de tercer nivel, incluyendo actividades para la prevención de problemas de la red, como alternativa para escalar los problemas. • Se debería tener contratos de mantenimiento y soporte para los sistemas operativos de red, incluyendo gestión de parches y actualizaciones. • Monitorear el tráfico de red para identificar posibles fallas y congestionamiento de tráfico. • Reconfiguración o desvíos de tráfico para conseguir un mejor rendimiento, contribuyendo con la calidad del servicio. • Administración de la asignación de direcciones IP (DHCP), servicios de DNS. • Implementación, monitoreo y mantenimiento de los sistemas de detección de intrusos. • Evitar la denegación de servicios. • Actualización de la documentación necesaria para el mantenimiento de los sistemas de red.
2. Políticas y normas	Las políticas y normas deben incluir: • Identificar las redes y los servicios a los cuales se puede tener acceso. • Los procedimientos y autorizaciones para determinar quién tiene permiso de acceder a qué redes y servicios de red. • La gestión de controles y procedimientos para proteger el acceso a las conexiones de red y servicios de red. • Los medios utilizados para acceder redes y servicios de red. En relación a la protección de las líneas de telecomunicaciones se tiene los siguientes aspectos:

1.Seguridad de los sistemas: b. Seguridad de las redes de datos	
2. Políticas y normas (Cont.)	• Los cables de energía y de comunicaciones deben permanecer separados, para la prevención de interferencias. • Los cables de redes deben protegerse de interceptación no autorizada, evitando su exposición en áreas públicas. • Deben identificarse claramente los cables y equipos con la finalidad de minimizar los errores de manipulación. • Debe existir una lista de conexiones documentada para así reducir la posibilidad de errores. • Para los sistemas críticos, se debe: o Instalar conductos blindados y habitaciones o cajas cerradas en puntos de inspección o terminación. o Utilización de rutas alternativas o medios de transmisión que proporcionen la seguridad adecuada. o Utilización de escudos electromagnéticos para la protección de los cables de red. o Acceso controlado a los paneles de conexión y cuartos de cableado.
3. Control	Entre las medidas de control a implementar se tiene: • Identificación de los equipos de red. • Separación de la redes en grupos funcionales. • Aislamiento de los equipos de información sensibles. • Protección de los equipos informáticos móviles. • Ejercer controles sobre el tráfico de red, mediante la aplicación de restricciones a servicios de mensajería, transferencia de archivos, acceso interactivo (chat, video conferencia). • Evaluación de los incidentes de seguridad ocurridos, los cuales alimentarán las estadísticas para mejorar la gestión.

1.Seguridad de los sistemas: c. Seguridad relacionada con los usuarios	
1.Planificación	La planificación debe contemplar los siguientes aspectos: • Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI sean identificables de manera única. • Permitir que el usuario se identifique a través de mecanismos de autentificación. • Confirmar que los permisos de acceso del usuario al sistema sean los adecuados según la documentación escrita y de acuerdo a su ámbito de trabajo. • Asegurar que los derechos de acceso del usuario sean debidamente solicitados y aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. • Las identidades del usuario y los derechos de acceso se mantienen en un repositorio de datos centralizado. • Desplegar técnicas efectivas para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.
2. Políticas y normas	Se deben dictar políticas y normas relativas a: • Verificación de la identidad del usuario. • Procedimientos de otorgamiento, modificación y revocación de roles. • Procedimientos para el manejo de excepciones e incidentes. • Revisión periódica de los permisos otorgados. • Registro de los datos que identifiquen al usuario. • Registro de los grupos de usuarios. • Establecimientos de normas y procedimientos para la creación, uso y cambio de contraseñas. • Establecimiento de procesos disciplinarios para aquellos usuarios que compartan sus contraseñas.

1.Seguridad de los sistemas: c. Seguridad relacionada con los usuarios	
3. Control	El control debe garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia.

2.Desempeño y capacidad:	
1.Planificación	Los planes deben incluir: • Acuerdos de niveles de servicios: Se debe conocer las dimensiones del servicio requerido así como los tiempos de respuesta aceptable, por lo que se deben hacer consideraciones de la capacidad de respuesta de los equipos instalados, ancho de banda en relación al incremento en el consumo de tales servicios. • Diseñar, adquirir o modificar la configuración de los servicios en base a un diseño previamente propuesto, en función de equilibrar los costos con la implementación de alternativas adecuadas y rentables. • Se debe implementar técnicas de predicción que proporcionen la verificación de las capacidades de rendimiento del servicio. • Todos los cambios a realizar para garantizar la capacidad del servicio, deben seguir los procedimientos establecidos para la adquisición y actualización de TI.

2.Desempeño y capacidad:	
2. Políticas y normas	Las políticas y normas relativas a la gestión del desempeño y la capacidad, se encuentran enmarcadas dentro de las políticas generales de la seguridad de la información, las cuales deben estimular los controles y las auditorias para determinar el desempeño presente y futuro de los sistemas, para así medir la capacidad actual y planificar la capacidad futura acorde a las necesidades de la organización.
3. Control	Monitorear continuamente el desempeño y la capacidad de los recursos de TI, con el objetivo de: • Mantener y poner a punto el desempeño actual dentro de TI. • Permitir la elasticidad, contingencia, cargas de trabajo, tanto actuales como proyectadas, planes de almacenamiento y adquisición de recursos. • Permitir reportar la disponibilidad del servicio. • Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas. • Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados. • Medir el desempeño futuro, por lo que se deben efectuar periódicamente pronósticos de desempeño y capacidad de los recursos de TI para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. • Identificar el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

3.Continuidad del servicio:	
1.Planificación	La planificación tiene por objetivo el desarrollo de un marco de trabajo de continuidad de TI, facilitando la determinación de la fortaleza requerida por la infraestructura y contribuir guiar al desarrollo de planes de recuperación ante desastres y contingencias La planificación de la continuidad se divide en cuatro etapas: **Primera Etapa Inicio:** • Mantener actualizado los planes de continuidad de servicios alineados con los planes globales de continuidad de la organización. • Asegurarse que el plan de continuidad se mantenga vigente en relación a los cambios ocurridos en el contexto de la organización. • Realizar periódicamente el análisis de riesgos. • Proporcionar asesoramiento a todas aquellas áreas de la organización que puedan influir en la continuidad de TI. • Asegurarse que los mecanismos de adecuados de TI se materialicen en el momento indicado para así apoyar la continuidad de las operaciones. • Evaluar el impacto en los planes de continuidad de TI originados por cambios en los planes de prestación de servicios. • Garantizar que las medidas de continuidad de servicios se ajusten a costos razonables. • Negociar y acordar contratos con terceras partes para el suministro de insumos necesarios o apoyo de tercer nivel requeridos para los planes de recuperación. **Segunda Etapa – Requisitos y Estrategias:** • Requisitos y Análisis del impacto de la organización: Tiene por finalidad medir el impacto que en la organización tiene la pérdida de servicios, por lo que se deben identificar los servicios más importantes.

3.Continuidad del servicio:	
1.Planificación (Cont.)	• Requisitos y análisis de riesgos: Este estudio determina la probabilidad de ocurrencia de un desastre de grandes dimensiones en la organización, conociendo así el grado de vulnerabilidad de la organización. **Tercera Etapa – Implementación:** Compuesto por una serie de planes técnicos, tales como: • Plan de respuesta emergencia: Permiten servir de interfaces entre los servicios de emergencia y las actividades relacionadas con la recuperación. • Plan de evaluación de daños: Contiene los datos de los contactos que realizan la valuación de daños, planes y procesos relacionados. • Plan de salvamento: Contiene información sobre los contactos de salvamento, planes y procesos relacionados. • Registro del plan vital: Contiene detalle de todos los registros vitales de información, los cuales son críticos para la organización, así como su ubicación. • Gestión de crisis y plan de relaciones públicas: Son planes que permiten manejar a los medios de comunicación y relaciones públicas. • Instalaciones y plan de servicios: Detalla el plan que permite salvaguardar las instalaciones necesarias para la continuidad del servicio. • Plan de seguridad: Muestra todos los aspectos de seguridad que deben ser administrados para la recuperación de los servicios en la organización. • Plan del personal: Muestran cómo se manejarán los problemas relacionados al personal durante el manejo del incidente. • Plan de comunicación: Muestra cómo todos aquellos aspectos de la comunicación serán administrados por aquellos entes involucrados durante la recuperación de un incidente grave. • Finanzas y administración: Contiene en detalle los procedimientos necesarios que permiten autorizar la erogación de los fondos necesarios para subsanar el incidente.

3.Continuidad del servicio:	
1.Planificación (Cont.)	Además de los planes anteriores, se requiere de un plan especial de contingencia que abarque las áreas ejecutivas, de manera que la alta gerencia se responsabilicen de la coordinación y la gestión de la crisis, el área de coordinación, correspondientes a los niveles ejecutivos medios, los cuales deben coordinar los esfuerzos de la recuperación, y finalmente el área de recuperación, representado por los equipos de trabajo que materializan la recuperación de los sistemas. Los planes de recuperación deben incluir validaciones que garanticen su funcionalidad y operatividad, por lo que se recomienda la realización de pruebas de simulación, parciales, completas y por escenarios. **Cuarta Etapa – Operación Continua:** Consiste en: • Educar y sensibilizar a la organización es los aspectos específicos de continuidad del servicio, asegurarse de la toma de conciencia en el personal de TI y hacerlo parte de su trabajo normal en base a que todos han sido entrenados para realizar las acciones que corresponden ante la ocurrencia de tales eventos. • Revisar todos los planes y procesos de recuperación para garantizar su actualización. • Realizar pruebas periódicas de los planes, sobre todo en aquellos casos que involucren cambios tecnológicos. • El proceso de gestión de cambios debe asegurar que los impactos de dichos cambios se reflejen en los planes de recuperación.

3.Continuidad del servicio:	
2. Políticas y normas	Están orientadas a brindar la capacidad y el desempeño requerido tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.
3. Control	Se divide en: • Mantenimiento del plan: Debido a las condiciones cambiantes de TI en la organización, se hace necesario mantener un proceso de actualización continua de los planes, por lo que se recomienda definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales. • Los planes de seguridad deben ser probados continuamente, para así demostrar su actualización y su eficacia. Así como también asegurar que todos los miembros del equipo de recuperación conozcan en detalle todos los procesos involucrados. • Actividades de Control: Análisis del impacto de las fallas de componentes: Identifica los puntos de fallo en los servicios de TI motivado por problemas de configuración, así mismo mide la validez de los procedimientos de recuperación. • Análisis de árbol de falla: Permite determinar la cadena de acontecimientos que causan una interrupción en los servicios de TI. Se identifican los eventos básicos, resultantes, condicionales y disparadores. • Análisis de fallas de servicios: Permite identificar las oportunidades de mejoras.

3.Continuidad del servicio:	
3. Control (Cont.)	• Observaciones técnicas: Es el resultado de un encuentro entre personal técnico especializado en soporte de TI, centrado en aspectos específicos de disponibilidad, busca controlar la ocurrencia de eventos en tiempo real a medida que ocurren.

4.Entrenar y educar a los usuarios:	
1.Planificación	La planificación del adiestramiento forma parte integral de la seguridad de la información y está contemplada a través de toda la propuesta, por lo que debe responder a cada plan en particular.
2. Políticas y normas	Con base a las necesidades de adiestramiento, deben formularse las políticas que permitan designar los a instructores debidamente calificados para organizar cursos con el tiempo suficiente, dicho adiestramiento debe ser sistematizado, incluyendo prerrequisitos, asistencia y evaluaciones.
3. Control	Al finalizar el adiestramiento, se deberá evaluar el contenido, la calidad, efectividad, percepción y retención del conocimiento, así como su costo y valor. Los resultados de esta evaluación definirán los planes futuros de adiestramiento.

Nota: Elaborado por el autor.

Recomendaciones finales.

A continuación en la Tabla 50, se exponen un conjunto de recomendaciones específicas tomando en cuenta las condiciones de seguridad encontradas dentro del MPP Educación:

Tabla 50. Recomendaciones al MPP Educación.

Recomendaciones al MPP Educación
1. Seguridad de los Sistemas: **a. Seguridad de los sistemas de información:** Con respecto a los controles establecidos para determinar posibles ataques en el MPP Educación, los registros o logs de los sistemas no son revisados con la meticulosidad que merecen, sin embargo, en los resultados obtenidos, se registró que tales logs si son activados, por lo que este aspecto positivo debe ser reforzado. Otro de los aspectos positivos que actualmente existe en materia de seguridad en el MPP Educación, es la sincronización de los relojes del sistema, garantizando así la fidelidad de los reportes o logs del sistema, esta actividad debe ser mantenida y reforzada. El MPP Educación ha implementado algunos controles de acceso físico a las instalaciones de TI, por lo que se hace necesario reforzar estas iniciativas. **b. Seguridad de las redes de datos:** La red datos del MPP Educación cuenta con los recursos de TI suficientes para prestar un adecuado servicio, sin embargo, debido a la inexistencia de políticas y normas relacionadas al tipo de datos que pueden circular por ellas, en un futuro cercano pueden el tráfico de la red puede verse afectado negativamente. Así mimo se hace necesario adecuar la infraestructura de cableado de la red, según las normas dictadas para tal fin. En cuanto al uso de dispositivos de red para el control de ataques e intrusiones, tal como los firewall el MPP Educación ha demostrado madurez, mediante la implementación de tales dispositivos, lo cual es uno de los aspectos que debe mantenerse y fortalecerse, así como los analizadores de tráfico de la red. Otro de los aspectos positivos encontrados es la identificación precisa de los equipos de red, así como la identificación de los sistemas

Recomendaciones al MPP Educación
sensitivos. **c. Seguridad relacionada con los usuario:** Actualmente en el MPP Educación no existe un registro y control adecuado de usuarios y sus privilegios, por lo que se hace necesaria la implementación de tal registro en una base de datos, con una aplicación que permita realizar consultas. También se recomienda la realización de campañas de concientización a los usuarios con el fin de que conozcan sus derechos y responsabilidades asociadas al uso de privilegios en el sistema y sus contraseñas.
2. Desempeño y capacidad A este respecto el MPP Educación carece de las mediciones necesarias para determinar tanto su capacidad actual como futura, por lo que es imposible realizar los cálculos necesarios para la implementación de planes y programas que garanticen la capacidad y la operatividad de los sistemas. Esta medición resulta fundamental para la prestación de un óptimo servicio, la cantidad de datos que circulan por la red generalmente se incrementa en la medida que el tiempo transcurre, esto debido a la implementación de nuevas aplicaciones, apertura de nuevos servicios, etc.
3. Continuidad del servicio Con respecto a la gestión continuidad, el MPP Educación tiene un largo camino por recorrer, las recomendaciones anteriores servirán como punto de partida para esta labor. Actualmente no existen planes ni programas que garanticen la continuidad de las operaciones, así mismo los contratos de mantenimiento son inexistentes o se encuentran desactualizados.

Recomendaciones al MPP Educación
4. Educar y entrenar a los usuarios El adiestramiento es una labor fundamental que debe ser reforzada dentro del MPP Educación, dicho adiestramiento no sólo deberá estar destinado a los operadores y administradores de los sistemas, sino también a los usuarios, para así potenciar sus capacidades y minimizar los riegos de errores humanos. En el MPP Educación se tiene la paradoja de realizar una efectiva detección de necesidades de adiestramiento, sin embargo, los cursos no son impartidos, por lo que se hace necesario resolver esta disonancia.

Nota: Elaborado por el autor.

REFERENCIAS BIBLIOGRÁFICAS

Fuentes Impresas

Aceituno, V. (2007). *Seguridad de la Información*. México. Limusa Noriega Editores.

Alexander, A. (2007). *Diseño de un Sistema de Seguridad de la Información*. Bogotá. Alfaomega Colombiana S.A.

Arias, F. (2006). *El Proyecto de Investigación, Introducción a la Metodología Científica*. (5ª Ed.). Caracas. Editorial Episteme.

Aycock, J. (2006). *Computer Viruses and Malware* .U.S. Springer.

Ballestrini, M. (2002). *Cómo se Elabora el Proyecto de Investigación*. (6ª Ed.).Caracas. BL Consultores Asociados, Servicio Editorial.

Bellovin, S., y Cheswick, W. (1994). *Network Firewalls. IEEE Comunications Magazine,* septiembre 1994.

Bolívar, M. (2007). *Seguridad de la Información dentro de la Banca Universal Venezolana.* Trabajo de grado de Maestría no publicado. Universidad Metropolitana. Caracas. Venezuela.

Brand, K., Boonen, H. (2007). *IT Governance based on CobiT 4.1 - A Management Guide*. itSMF International.

Caicedo, H. (2009). *Metro Ethernet: aplicación en el sector financiero venezolano*. Trabajo de grado de Especialización no publicado. Universidad Metropolitana. Caracas. Venezuela.

Chiavenato, I. (2006). Introducción a la Teoría General de la Administración. (7ª Ed.) . México. Mc Graw Hill Interamericana.

Chirilo, J. y Dalielyan, E. (2005). *Sun Certified Security Administrator for Solaris 9 & 10 Study Guide*. New York. McGraw-Hill.

Cioara, J., Minutella, D., Stevenson, H. (2008). *CCNA Exam Prep*. (2ª Ed.). U.S.

Cisco Networking Academy. (2010). *CCNA Security Course Booklet,* Version 1.0. Indianapolis. Cisco Press.

Clayton, J. (2002). *Diccionario Ilustrado de Telecomunicaciones*. Madrid. Mc Graw Hill.

Daswani, N., Kern, C. y Kesavan, A. (2007). *Fundations of Security, What Every Programmer Needs to Know*. New York. Apress.

De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van Der Veen, A.,Verheijen, T.(2008). *ITIL V3 Foundation Exam - The Study Guide*. Scotland. Van Haren Publishing.

Forouzan, B. (2002). *Transmisión de Datos y Redes de Comunicaciones*. (2ª Ed.). Madrid. McGraw Hill.

Groff, J. y Weinberg, P. (1998). *Guía de Sql*. Madrid. Mc Graw Hill.

Harris, S. (2003). *CISSP All in one exam guide*. (2da. Edición). Emerville, CA, McGraw Hill/Osborne.

Hernandez, R., Fernández, C., Baptista, M. (2010). *Metodología de la Investigación*. (5ª Ed.). México. McGraw-Hill.

Hurtado, J. (2010-a). *El Proyecto de Investigación, Comprensión holística de la metodología y la investigación*. (6ª Ed.).Caracas. Ediciones Quirón.

Hurtado, J. (2010-b). *Metodología de la Investigación, Guía para la comprensión holística de la ciencia*. (4ª Ed.). Caracas. Ediciones Quirón.

ISO 27002. (2005). *Information Technology Security Techniques. Code of Practice for Information Security Management ISO/IEC 27002:200*. Geneva.

ISO/IEC (2009). *International Standart ISO/IEC 27033-1 (Preview).* Switzerland.

IT Governance Institute. (2007). *CobiT 4.1*. EEUU

IT Governance Institute. (2008). *Alineando CobiT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio del negocio, un reporte para la gestión de ITGI y la OGC*. EEUU.

Jimeno, M., Perez, C., Mata, A., Pérez, J. (2008). *Destripa la Red, Hacking práctico*. Madrid. Ediciones Anaya Multimedia.

Johnson, A. (2009). *31 Days Before Your CCNA Exam*. (2ª Ed.). Indianapolis. Cisco Press.

Kendall, K. y Kendall, J. (2005). *Análisis y Diseño de Sistemas*. (6ª Ed.). México. McGraw Hill.

Laudon, K. y Laudon J. (2008). *Sistemas de Información Gerencial, Administración de la Empresa Digital.* (10ª Ed.). México. McGraw-Hill.

Llorens F., J. (2009). *Tecnología de Información: Gerencia de Servicios (basado en ITIL).* Caracas. Universidad Católica Andrés Bello.

Méndez, C. (2009). *Metodología, Diseño y Desarrollo de Procesos de Investigación con Énfasis en Ciencias Empresariales*. (4ª Ed.). México. Editorial Limusa.

Méndez, J. (2006). *Estudios de Metodologías para la Implantación de la Seguridad en Redes de Inalámbricas de Área Local*. Trabajo de Grado de Especialización no publicado, Universidad Metropolitana, Caracas, Venezuela.

Mishra, A. (2008). *Security and Quality of Service in Ad Hoc Wireless Networks*. New York. Cambridge University Press.

Navarro, A. (2007*). Metodología para la Gestión de Seguridad de Información en Venezuela*. Trabajo de grado de Especialización no publicado, Universidad Metropolitana, Caracas, Venezuela.

Office Government Commerce. (2008). *ITIL V3 Service Operation*. London. The Stationery Office.

Olifer, N., Olifer, V. (2009). *Redes de Computadores*. México. McGraw Hill.

Palacios, J. (2008). *Evaluación del Desarrollo de los Fundamentos Teóricos de Seguridad de la Información en la Banca Comercial y Universal de Venezuela*. Trabajo de grado de Maestría no publicado. Universidad Católica Andrés Bello, Caracas, Venezuela.

Palella, S. (2006). *Metodología de la Investigación Cuantitativa*. (2ª Ed.). Caracas. Fondo Editorial de la Universidad Pedagógica Experimental Libertador.

República Bolivariana de Venezuela. (1999). *Constitución*. *Gaceta Oficial de la República Bolivariana de Venezuela, N° 36.860*. Diciembre 30, 1999.

República Bolivariana de Venezuela. (2001). *Ley Especial Contra Los Delitos Informáticos*. Gaceta Oficial de La República Bolivariana de Venezuela, Nº 37.313, Octubre 30,2001.

República Bolivariana de Venezuela. (2004). *Decreto 3390. No. 38.095*, Diciembre 28, 2004.

Sabino, C. (2006). *Cómo Hacer una Tesis y Elaborar Todo Tipo de Escritos*. Caracas. Editorial Panapo de Venezuela.

Sabino, C. (2007). *El Proceso de Investigación*. Caracas. Editorial Panapo de Venezuela.

Sackett, G. (2002). *Manual de Routers Cisco*. Madrid. McGraw Hill.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes, Aplicaciones y Estándares.* (2ª Ed.). Madrid. Pearson Education, S.A.

Tanenbaum, A. (1997). *Redes de Computadoras*. (3ª Ed.). México. Prentice Hall Hispanoamérica, S.A.

Tanenbaum, A. (2003). *Redes de Computadoras*. (4ª Ed.). México. Prentice Hall Hispanoamérica, S.A.

Universidad Pedagógica Experimental Libertador UPEL (2006). *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*.(4ª Ed.). Caracas. Fondo Editorial de la Universidad Pedagógica Experimental Libertador.

Vyncke, E. y Paggen, C. (2008). *Lan Switch Security, What Hackers Know About Your Switches*. Indianapolis. Cisco Press.

Fuentes Electrónicas en Línea

Borghello, C. (2010). *Seguridad de la Información*. Recuperado en Noviembre 14, 2010, de http://www.segu-info.com.ar)

Guía de Seguridad de las TIC. (2009). No repudio. Recuperado en Diciembre 30, 2010, de https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/es/n/non_repudiation.htm.

ISO27000.es. (2011). ISO2700. Recuperado en Junio 07, 2011, de http://www.iso27000.es/iso27000.html#section3a

Ministerio del Poder Popular para la Educación. (2010). Visión y Misión. Recuperado en Noviembre 16, 2010, de http://me.gob.ve.

ANEXO A

CUESTIONARIO

Estimado encuestado

El presente cuestionario tiene por objeto recabar información para el desarrollo de la investigación titulada “Diseño de un Sistema de Seguridad para Redes de Datos del Ministerio del Poder Popular para la Educación”. El tiempo estimado para su realización es de aproximadamente 20 minutos.

El cuestionario es de carácter confidencial y anónimo, por lo que puede sentirse libre de expresar su opinión e ideas. La información que Ud. proporcione será expresada en la investigación en términos globales y no individualmente.

Las personas seleccionadas para responder este cuestionario, fueron elegidas por el tipo de actividad laboral que desarrolla dentro de la organización, debido a que se considera que Ud. puede aportar información valiosa al estudio, el cual redundará en mejores procesos y controles en el área de la seguridad de las redes de datos del MPP Educación.

Se solicita conteste cada pregunta con la mayor objetividad posible, no existe respuestas correctas o incorrectas, las preguntas se encuentran numeradas. El cuestionario consta de 34 preguntas de tipo cerrado, en la cual deberá marcar con una “X” la opción seleccionada, debe elegir sólo una opción.

Se le agradece su valiosa colaboración para el éxito del desarrollo de esta investigación.

ORGANIZACIÓN, POLÍTICAS Y PLANES DE SEGURIDAD

1. ¿Existe la estructura organizacional que sirva de apoyo a la seguridad de los sistemas y las redes de datos?

   ☐ Si ☐ No

2. ¿Existe la estructura organizacional que realice las funciones de auditoría de sistemas?

   ☐ Si ☐ No

3. ¿Existen políticas, normas y procedimientos, claramente establecidas, destinada a fortalecer la seguridad de los sistemas y las redes de datos?

   ☐ Si ☐ No

4. ¿Se diseñan planes y programas de seguridad, manteniéndolos actualizados?

   ☐ Si ☐ No

AMENAZAS

5. ¿Existen planes, programas y procedimientos que permitan el manejo de catástrofes tales como: Incendios, inundaciones, fallas eléctricas y ataques a los sistemas de TI?

   ☐ Si ☐ No

VULNERABILIDADES

6. ¿Se realizan planes que permitan controlar las vulnerabilidades?, entendiéndose por vulnerabilidad la probabilidad de sufrir un ataque en el corto plazo.

   ☐ Si ☐ No

7. ¿Se siguen las publicaciones referidas a las vulnerabilidades de los sistemas?

   ☐ Si ☐ No

GESTION DE USUARIOS

8. ¿Se tiene un registro detallado que incluya datos personales, roles así como de las transacciones realizadas por los usuarios del sistema? Entendiéndose por roles los privilegios que posee el usuario dentro del sistema.

☐ Si ☐ No

9. ¿Se tienen procedimientos detallados y escritos que regulen el otorgamiento de privilegios o roles?

☐ Si ☐ No

10. ¿Existen políticas o normas escritas y referidas al uso, cambio y responsabilidades asociadas con las contraseñas del sistema?

☐ Si ☐ No

AUDITORIAS Y REGISTROS (LOGS)

11. ¿Existen políticas y planes relativos a los procesos de auditoría y control en materia de seguridad de TI?

☐ Si ☐ No

12. ¿Se realizan auditoría de los sistemas de información?

☐ Si ☐ No

13. ¿Se utiliza la figura de auditores externos?

☐ Si ☐ No

14. ¿Usualmente se activan para su funcionamiento los avisos o logs de los sistemas? Entendiéndose por log, los archivos o registros que automáticamente son generados por el sistema para reportar fallos o ataques.

☐ Si ☐ No

15. ¿Se protegen los logs contra modificaciones maliciosas?

☐ Si ☐ No

16. ¿Se analizan los registros o logs de los sistemas en búsqueda de posibles intrusiones?

☐ Si ☐ No

17. ¿Se registran por medios manuales o automatizados, los eventos e incidentes que afectan la seguridad de las redes de datos y los sistemas?

☐ Si ☐ No

18. ¿Se utilizan analizadores de tráfico de red para determinar el tipo de protocolos que circulan por ésta?

☐ Si ☐ No

19. ¿Se utilizan sistemas de control de intrusos o IDS?

☐ Si ☐ No

20. ¿Se tiene un proceso automatizado que permita la sincronización de los relojes de los sistemas?

☐ Si ☐ No

VIRUS

21. ¿Se realizan periódicamente controles para impedir la propagación de códigos maliciosos o virus?

☐ Si ☐ No

CONTINUIDAD

22. ¿Se realizan mediciones periódicas que permitan prever el desempeño futuro, la capacidad o calidad del servicio de los sistemas o de la red de datos?

☐ Si ☐ No

23. ¿Se conoce en detalle los umbrales del servicio de red que permitan establecer cuáles son los valores normales de tráfico? Entendiéndose por umbrales, los niveles aceptables de tráfico previamente definido.

☐ Si ☐ No

24. ¿Existen planes o programas escritos y detallados que permitan garantizar la continuidad de los servicios de información y de las redes de datos?

☐ Si ☐ No

25. ¿Se tiene actualizado los contratos de mantenimiento de TI que permitan garantizar la continuidad del servicio?

☐ Si ☐ No

CONTINGENCIA Y RECUPERACIÓN

26. ¿Se han identificado por escrito los recursos críticos de TI que en caso de incidentes puedan afectar el normal desempeño de los procesos de la organización?

☐ Si ☐ No

27. ¿Se tienen planes detallados que describan los procedimientos a seguir para la recuperación y reanudación de los servicios de TI luego de la ocurrencia de un incidente?

☐ Si ☐ No

28. ¿Se tienen contratos con terceras partes específicamente para que sirvan de soporte en caso de requerir escalar problemas relacionados con la continuidad de las operaciones?

☐ Si ☐ No

SEGURIDAD EN LA REDES DE DATOS

29. ¿Se tienen planes relacionados a la instalación o ampliación de las redes de datos?

☐ Si ☐ No

30. ¿Se tiene documentada en detalle la arquitectura de red?

☐ Si ☐ No

31. ¿Se tienen identificado claramente y en detalle todos los equipos de red de la organización?

☐ Si ☐ No

32. ¿Los sistemas sensitivos se encuentran identificados?

☐ Si ☐ No

33. En caso de responder afirmativamente la pregunta anterior, ¿dichos sistemas se encuentran en redes separadas?

☐ Si ☐ No

34. ¿Se tienen normas claras y escritas que normen el tipo de información que puede transitar por la red de datos?

☐ Si ☐ No

35. ¿Se tienen por escrito las normas que regulen la disposición del cableado de red y de energía eléctrica?

☐ Si ☐ No

ACCESO FÍSICO

36. ¿Se tienen políticas escritas y claras que normen el acceso físico a la infraestructura e instalaciones de TI?

☐ Si ☐ No

37. ¿Se utilizan dispositivos de identificación que controlen el acceso físico a las instalaciones de TI, tales como tarjetas magnéticas, reconocimiento de medidas biométricas, etc.?

☐ Si ☐ No

ADIESTRAMIENTO

38. ¿Se realizan periódicamente detección de las necesidades de adiestramiento relacionados con la seguridad de la información y de las redes de datos?

☐ Si ☐ No

39. ¿Se realizan campañas de concientización sobre seguridad de TI a los usuarios del sistema?

☐ Si ☐ No

ANEXO B

CONSTANCIA DE VALIDACIÓN

CONSTANCIA DE VALIDACIÓN

Yo, ALBERTO RODRIGUEZ, titular de la Cédula de Identidad Nº _____, de profesión Sociologo, ejerciendo actualmente como DOCENTE, en la Institución UCAB.

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación.

En Caracas, a los 07 días del mes de JUNIO del año 2011

Firma

CONSTANCIA DE VALIDACIÓN

Yo, Raquel González, titular de la Cédula de Identidad Nº 11199155, de profesión Ingeniero de Sistemas, ejerciendo actualmente como Jefe de Redes y Telefonía, en la Institución Ministerio del Poder Popular para la Educación

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación.

En Caracas, a los 28 días del mes de Junio del año 2011

Raquel González

Firma

CONSTANCIA DE VALIDACIÓN

Yo, Pedro Nolasco Bonillo R., titular de la Cédula de Identidad Nº 10.868.538, de profesión Doctor en Ciencias de la Computación, ejerciendo actualmente como Evaluador, en la Institución Universidad Católica Andrés Bello.

Por medio de la presente hago constar que he revisado con fines de Validación del Instrumento (cuestionario), a los efectos de su aplicación.

En Caracas, a los 30 días del mes de Junio del año 2011

Bonillo Ronjs Pedro.

Firma

ANEXO C

COBIT 4.1, ESTRUCTURA Y DOMINIOS

Estructura de CobiT

Según Brand y Boonen (2007), la estructura de CobiT se puede representar en forma de cubo, tal como lo muestra la Figura 54, muestra tres puntos de vistas relacionados entre sí.

Figura 54. Representación del Cubo CobiT

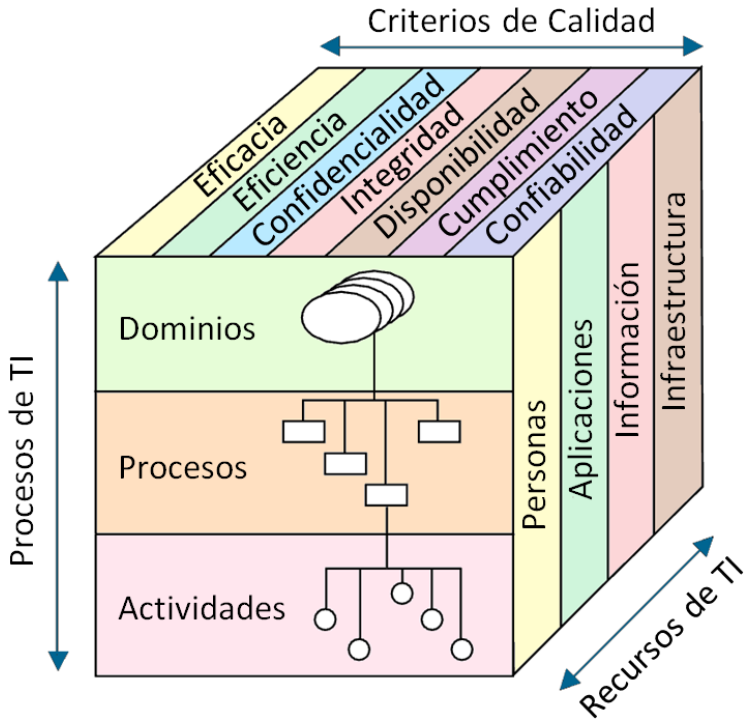

Figura 54. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 25)

Cada punto de vista se describe a continuación:

CobiT: Dominios y Procesos

Según Brand y Boonen (2007), los procesos de CobiT se han ordenado en cuatro campos distintos, que en conjunto forman un ciclo. Este ciclo ha sido incorrectamente comparado con el ciclo de la calidad de Deming, pero muestra una mejor concordancia con el ciclo de gestión según lo descrito por Hopstaken y Kranendonk en 1988. En su

publicación original Hopstaken y Kranendonk presenta los siguientes cuatro grupos de procesos:

- Estrategia, Modelado y Planificación
- Realización
- Entrega y Soporte
- Monitoreo y Corrección

La Estrategia, Modelado y Planificación proporcionan la monitorización y corrección de las normas o estándares de Realización, Entrega y Soporte, permitiendo a éstas ser evaluadas. En la fase de Monitoreo hay un doble ciclo de retroalimentación. En el primer ciclo, Realización, Monitoreo y Corrección, proveen de una retroalimentación en el orden adecuado para los resultados del proceso, en el segundo ciclo provee la Estrategia, Modelado y Planificación de los procesos con el aporte necesario para la mejora del siguiente ciclo, estas interacciones se pueden observar en la Figura 55.

Figura 55. Ciclo de Gestión

Figura 55. Adaptado de “IT Governance Base don CobiT 4.1 – A Management Guide”, por Bran y Boonen, 2007, (p. 26)

Los cuatro dominios de CobiT se pueden proyectar casi a la perfección en este ciclo de gestión, ver Figura 56.

Figura 56. CobiT Proyectado Sobre el Ciclo de Gestión

Figura 56. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 27)

Para cada dominio CobiT se tiene una serie de procesos que han sido identificados, estos se enumeran en la siguiente tabla:

Tabla 51. Aspectos de la Formulación del Problema

La siguiente tabla presenta los procesos de los cuatro dominios de gestión de CobiT.

Planificación y Organización (PO)	Entrega y Soporte (DS)
• PO1 Definir el plan estratégico de TI • PO2 Definir la arquitectura de la información • PO3 Determinarla dirección tecnológica • PO4 Definir procesos, organización y relaciones de TI • POS Administrar la inversión en TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO7 Administrar recursos humanos de TI • PO8 Administrar calidad • PO9 Evaluar y administrar riesgos de TI • PO10 Administrar proyectos	• DS1 Definir y administrar niveles de servicio • DS2 Administrar servicios de terceros • DS3 Administrar desempeño y capacidad • DS4 Garantizar la continuidad del servicio • DS5 Garantizar la seguridad de los sistemas • DS6 Identificar y asignar costos • DS7 Educar y entrenara los usuarios • DS8 Administrar la mesa de servicio y los incidentes • DS9 Administrar la configuración • DS10 Administrar los problemas • DS11 Administrar los datos • DS12 Administración del ambiente físico • DS13 Administración de las operaciones
Adquisición e Implementación (AI)	**Monitoreo y Evaluación (ME)**
• AI1 Identificar soluciones automatizadas • AI2 Adquirir y mantener el software aplicativo • AI3 Adquirir y mantener la infraestructura tecnológica • AI4 Facilitar la operación y el uso • AI5 Adquirir recursos de TI • AI6 Administrar cambios • AI7 Instalar y acreditar soluciones y cambios	• ME1 Monitorear y evaluar el desempeño de TI • ME2 Monitorear y evaluar el control interno • ME3 Garantizar cumplimiento regulatorio • ME4 Proporcionar gobierno de TI

Nota: Adaptado de “IT Governance based on CobiT 4.1 - A Management Guide”, por Brand y Boonen, 2007, (p. 28)

Descripción de los Dominios

Planificación y Organización (PO).

Según Brand y Boonen (2007), este ámbito abarca la estrategia y la táctica y se ocupa de la identificación de la forma en que mejor pueden contribuir a la consecución de los objetivos de negocio. La realización de la visión estratégica debe ser planeada, comunicada y administrada desde diferentes puntos de vista (por ejemplo, arquitectura de la información y la orientación tecnológica) y una adecuada organización e infraestructura tecnológica que la sustente.

Los procesos PO1 (Definición de un plan estratégico de TI), PO2 (Definir la arquitectura de la información), PO3 (Determinar la dirección tecnológica) y PO4 (Definir los procesos de TI, organización y relaciones) conforman el grupo estratégico que está en el centro del dominio del Plan Organizar (ver Figura 55). Estos cuatro procesos se ejecutan de forma interactiva e iterativa. Las elecciones realizadas en un proceso pueden influir en el resultado de los otros procesos. Los requisitos del negocio se introducen en el grupo estratégico, así como los requisitos externos.

Los resultados del grupo estratégico ingresan a PO5 (Gestión de la inversión en TI), PO6 (Comunicar objetivos de gestión y dirección) y PO7 (TI Gestión de recursos humanos). El cuadro de la derecha de la Figura 57 describe PO8 (Gestión de la calidad), PO9 (Evaluar y gestionar los riesgos de TI), PO10 (Gestión de proyectos) y el dominio ME (Monitoreo y Evaluación). Estos procesos han sido apartados porque son un recurso general que no pertenece únicamente al dominio de Planificar y Organizar, sino también a los procesos de otros dominios.

Figura 57. Estructura del Dominio de Planificación y Organización

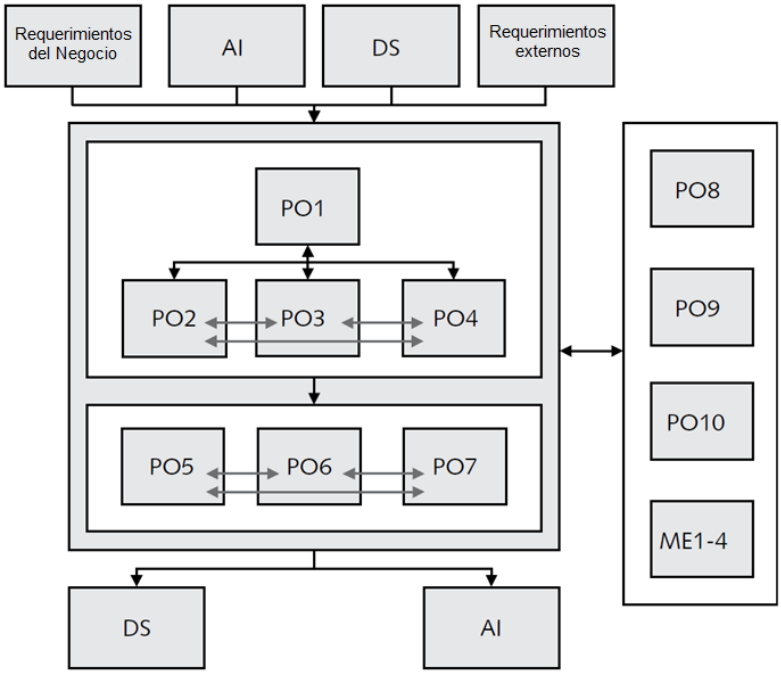

Figura 57. Se muestra el Dominio de la Planificación y Organización, AI = Adquisición e Implementación, DS = Entrega y Soporte, ME = Monitoreo y Evaluación, PO = Planificación y Organización. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 29)

Adquisición e Implementación (AI).

A fin de alcanzar las metas de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas, tanto como la aplicación e integración de los procesos de negocio. Además, para asegurarse el ciclo de vida de los sistemas existentes, este dominio cubre los cambios y el mantenimiento de dichos sistemas, ver Figura 58.

Basado en la información de la arquitectura y la tecnología, la dirección define dentro del dominio de Planificación y Organización los requerimientos de negocios y de fuentes externas, el proceso de AI1 (Identificar soluciones automatizadas) define los cambios necesarios en la infraestructura de TI. AI6 (Gestión de cambios) se asegura que dichos cambios se adecuen con las responsabilidades existentes.

Figura 58. Estructura del Dominio de Adquisición e Implementación

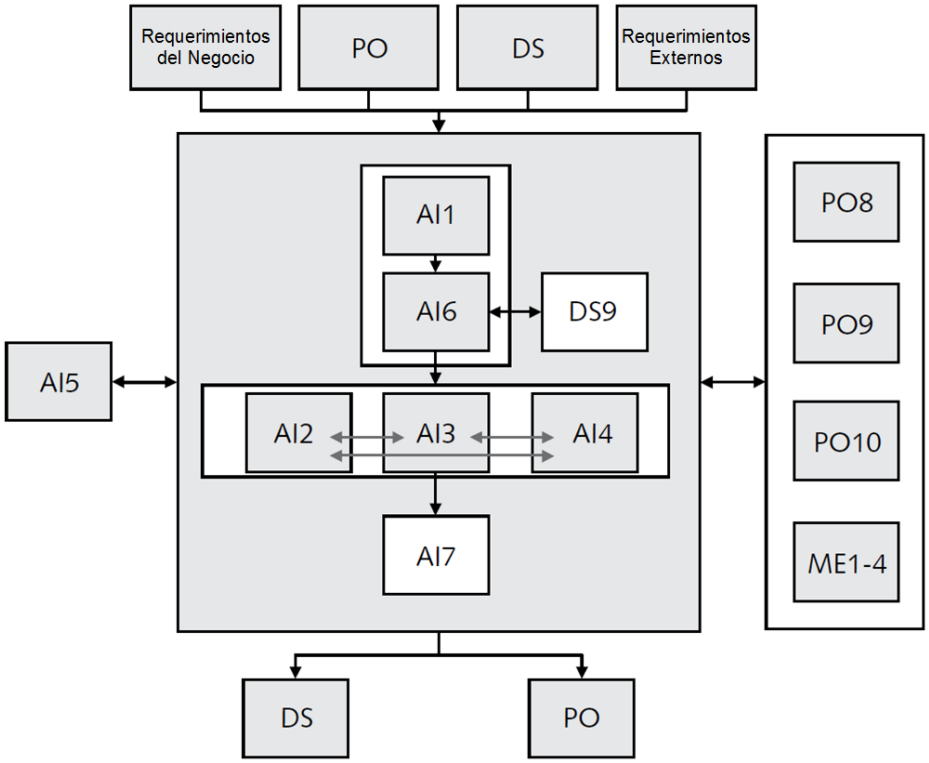

Figura 58. Se muestra el Dominio Adquisición e Implementación, AI = Adquisición e Implementación, DS = Entrega y Soporte, ME = Monitoreo y Evaluación, PO = Planificación y Organización. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 29)

El proceso de desarrollo de los procesos de AI2 (Adquirir y mantener el software aplicativo), AI3 (Adquirir y mantener la infraestructura de tecnología) y AI4 (Facilitar la operación y el uso) garantizar que, como resultado de estos procesos el sistema de información permanezca en funcionamiento. El proceso de AI7 (Instalación y acreditar soluciones y cambios) se encarga de la implementación sistemas dentro de su ambiente operacional. El proceso de AI5 (Adquirir recursos de TI) es un recurso general para los demás procesos de IA.

Debido a que el proceso DS9 (Administrar la configuración), tiene una relación directa con AI7 (Instalar y acreditar soluciones de cambios), se ha incluido en el dominio de Adquisición e Implementación.

El cuadro de la derecha de la Figura 58 describe PO8 (Administrar la calidad), PO9 (Evaluar y administrar riesgos de TI), PO10 (Administrar proyectos) y el dominio ME (Monitoreo y Evaluación). Estos procesos se distinguen porque son un recurso general que también son relevantes para la el dominio de la Adquisición e Implementación.

Entrega y Soporte (DS).

Según Brand y Boonen (2007), éste dominio se refiere a la prestación de los servicios requeridos, que van desde las operaciones tradicionales sobre aspectos de seguridad y continuidad hasta el adiestramiento del personal. Con el fin de prestar servicios, los procesos de apoyo necesarios se deben establecer. Este dominio incluye el procesamiento de los datos por los sistemas de aplicación, que con frecuencia se clasifican en los controles de aplicación, ver Figura 59.

El proceso DS1 (Definir y administrar niveles de servicio), es un proceso clave dentro de este dominio, porque está vinculado a la Entrega y Soporte de TI, mediante la definición de acuerdos de servicios. Dichos acuerdos influyen directamente en DS2 (Administrar servicios de terceros), ambos DS2 y DS1 están directamente relacionados con DS6 (Identificar y asignar costos), debido a las implicaciones financieras de ambos acuerdos de servicios.

DS1 (Definir y administrar niveles de servicio) proporciona el apoyo a los procesos DS11 (Administrar los datos), DS12 (Administración del ambiente físico) y DS13 (Administración de las operaciones) permiten establecer los adecuados criterios de desempeño, así como la cantidad y la calidad de los servicios prestados a ser evaluados.

DS8 (Administrar la mesa de servicio y los incidentes) proporciona un punto de contacto con los usuarios en relación a cualquier incidente con los sistemas operativos. DS10 (Administrar los problemas), se encarga que éstos sean resueltos profesionalmente.

Figura 59. Estructura del Dominio de Entrega y Soporte

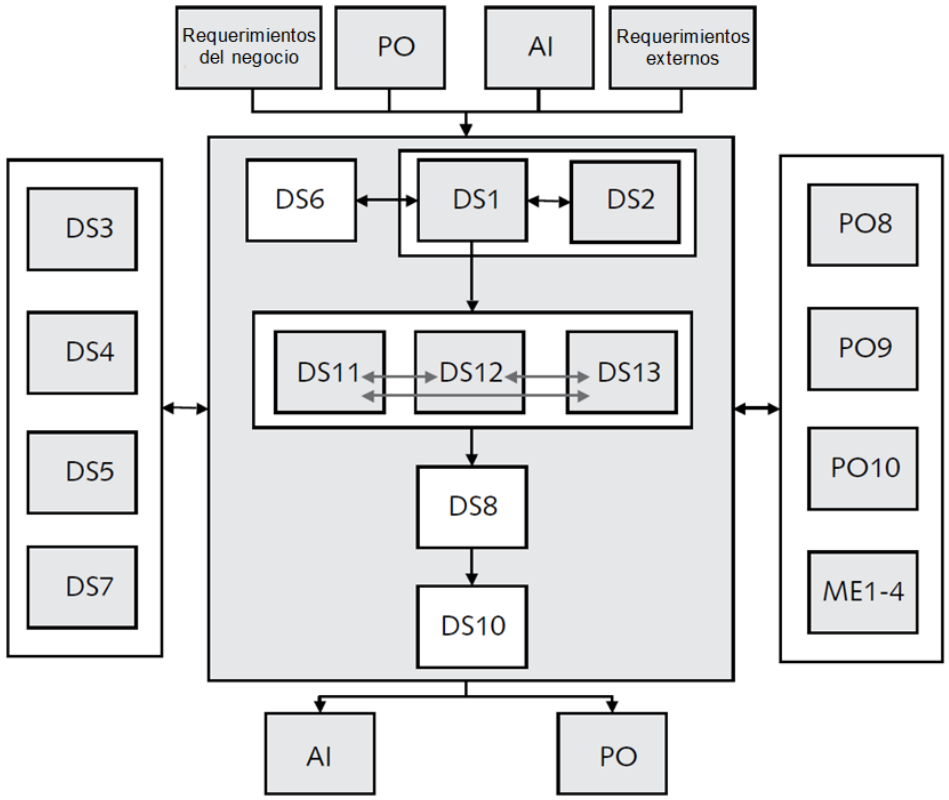

Figura 59. Se muestra el Dominio Entrega y soporte, AI = Adquisición e Implementación, DS = Entrega y Soporte, ME = Monitoreo y Evaluación, PO = Planificación y Organización. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 32)

Debido a que el proceso de DS9 (Administrar la configuración) tiene relación directa con IA6 (Administrar cambios), se le incluye en el dominio de Adquisición e Implementación).

Los procesos DS3 (Administrar desempeño y capacidad), DS4 (Garantizar la continuidad del servicio), DS5 (Garantizar la seguridad de los sistemas) y DS7 (Educar y entrenar a los usuarios) son incluidos en este dominio como apoyo a los procesos de éste ámbito.

El cuadro de la derecha de la Figura 59, describe PO8 (Administrar calidad), PO9 (Evaluar y administrar riesgos de TI), PO10 (Administrar los problemas) y el dominio Monitoreo y Evaluación (ME). Estos procesos han sido separados debido a que son recursos generales que son importantes para el dominio de Entrega y soporte.

Monitoreo y Evaluación (ME).

Según Brand y Boonen (2007), todos los procesos de TI necesitan ser evaluados regularmente, en cuanto a su calidad y el cumplimiento de los requisitos de control a través del tiempo. Este dominio guía la supervisión de los procesos de control dentro de la organización, garantizando la independencia de las auditorías internas, externas u obtenidas de fuentes alternativas, ver Figura 55.

ME1 (Monitorear y evaluar el desempeño de TI) es el principal proceso de control y evaluación. Mide todos los procesos con indicadores de comportamiento (Figura 60). También asegura que se tomen medidas correctivas. M2 (Monitorear y evaluar el control interno) supervisa y evalúa los objetivos de control interno. ME3 (Garantizar el cumplimiento regulatorio) asegura que la organización cumple con las leyes y reglamentos.

ME4 (TI Proporcionar gobierno de TI) proporciona para una buena gobernabilidad de TI dentro de la organización.

El cuadro de la derecha de la Figura 60 describe PO8 (Administrar la calidad), PO9 (Evaluar y administrar los riesgos de TI) y PO10 (Administrar proyectos). Estos procesos han sido apartados porque son un recurso general que también es relevante para el dominio de Monitoreo y Evaluación.

CobiT y los Recursos de TI

Según Brand y Boonen (2007), CobiT identifica cuatro clases de recursos de TI:

- Las personas: Los recursos humanos necesarios para planificar, organizar, adquirir, entregar, soportar, supervisar y evaluar los sistemas de información y servicios.

Figura 60. Estructura del Dominio de Monitoreo y Evaluación

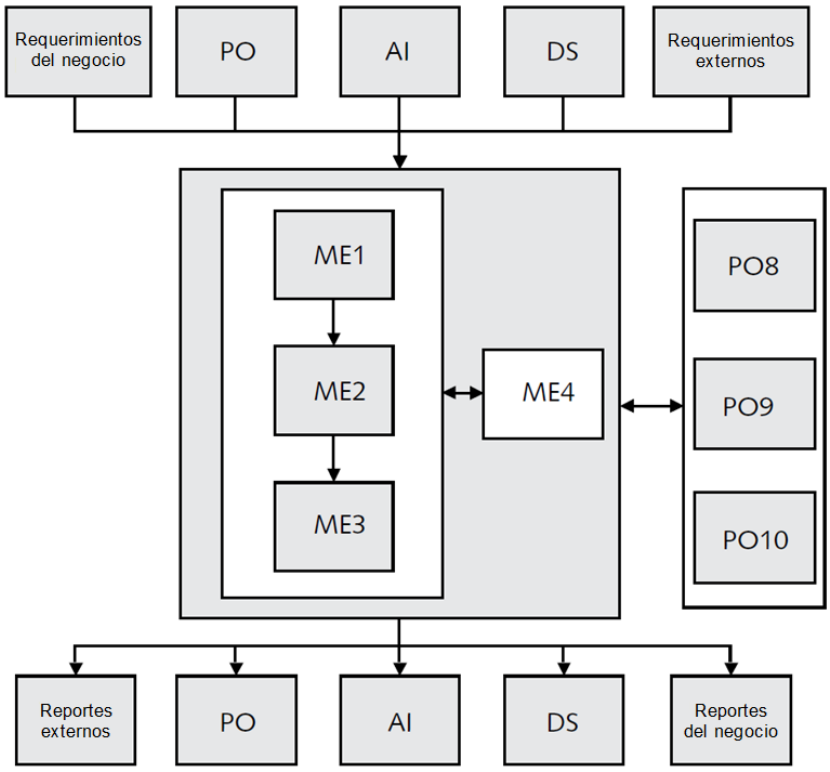

Figura 60. Se muestra el Dominio de Monitoreo y evaluación, AI = Adquisición e Implementación, DS = Entrega y Soporte, ME = Monitoreo y Evaluación, PO = Planificación y Organización. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 33)

- Aplicaciones: Los sistemas automatizados de usuario y manual de procedimientos que el proceso de la información.
- Información: Datos de entrada y salida de los sistemas de información, en cualquier forma utilizada por el negocio.
- Infraestructura: Tecnología e instalaciones que permitan la tramitación de las solicitudes.

Criterios de calidad

Un concepto para la cobertura de CobiT es que el control de las TI es abordado con miras a la información que se necesita para apoyar los requerimientos del negocio. Al establecer los criterios para la información, según Brand y Boonen (2007), CobiT analiza los modelos de referencia existentes y conocidos:

- Requisitos de calidad:
    - Calidad
    - Costo
    - Entrega
- Requisitos fiduciarios (Informe COSO):
    - Eficacia y eficiencia de las operaciones
    - Fiabilidad de la información
    - Cumplimiento de las leyes y reglamentos
- Requisitos de seguridad:
    - Confidencialidad
    - Integridad
    - Disponibilidad

El criterio de eficacia cubre el requisito de calidad, el aspecto de entrega de calidad se superpone al aspecto de la disponibilidad de los requisitos de seguridad y también la eficacia y la eficiencia. Por último, el aspecto de los costes de la calidad también está cubierto por la eficiencia.

Para los requisitos fiduciarios, ISACA (*Information Systems Audit and Control Association*), la cual es una organización internacional que dicta las pautas para el gobierno, el control, la seguridad y la auditoría de información, utiliza definiciones de COSO (*Committee of Sponsoring Organizations*), el cual a su vez dicta los pasos a seguir para el control interno, la eficacia y eficiencia de las operaciones y el cumplimiento de las

leyes, reglamentos y políticas existentes. Sin embargo, la fiabilidad de la información se amplió para incluir toda la información, no sólo la información financiera.

Con respecto a los requisitos de seguridad, CobiT identifica confidencialidad, integridad y disponibilidad como elementos claves, los cuales se utilizan universalmente para describir los requerimientos de seguridad de TI (ver Figura 61).

Figura 61. Transición de los Requerimientos a Criterios de Calidad

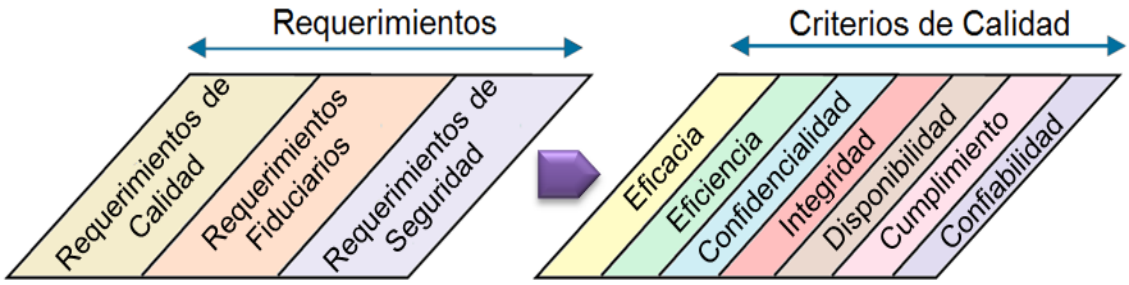

Figura 61. Adaptado de "IT Governance based on CobiT 4.1 - A Management Guide", por Brand y Boonen, 2007, (p. 35).

Según Brand y Boonen (2007), los criterios de calidad de CobiT se componen de:

- Efectividad: La medida en que la información sirve a los objetivos definidos.
- Eficiencia: La medida en que las actividades en relación con el suministro de información se llevan a cabo a un costo y esfuerzo aceptable.
- Confidencialidad: La medida en que los datos sólo están disponibles a un grupo bien definido de personas autorizadas.
- Integridad: La medida en que los datos se corresponde con la realidad.
- Disponibilidad: La medida en que un sistema o servicio está disponible para los usuarios previstos en el momento requerido.
- Cumplimiento: Es el grado en que los procesos están apegados a las leyes, los reglamentos y acuerdos contractuales.

- Confiabilidad: La medida en que se proporcione información adecuada para la gestión de las operaciones de la organización y el ejercicio de sus recursos financieros.

CobiT, como un instrumento para la regulación del entorno de TI, identifica los procesos dentro de los cuatro dominios necesarios para cumplir los criterios de calidad relevantes para la empresa, utilizando los recursos de TI necesarios.

CobiT como Marco de Gobierno de TI

CobiT como Marco de Control.

Según Brand y Boonen (2007), CobiT se centra en la gobernabilidad empresarial y la necesidad de mejorar los controles en las organizaciones. CobiT provee un marco para el control de TI y soporta los siguientes cinco requisitos para un marco de control:

- Proporcionar un enfoque de negocio más clara.
- Garantizar un proceso de orientación.
- Tiene buena aceptación entre las organizaciones.
- Define un lenguaje común.
- Ayudar a cumplir con los requisitos reglamentarios.

Área de negocios.

Según Brand y Boonen (2007), para proporcionar la información que la organización requiere para lograr sus objetivos, se necesita gestionar y controlar los recursos de TI como un conjunto estructurado de procesos para ofrecer los servicios de información necesarios.

- CobiT consigue el más agudo enfoque de negocio mediante la alineación de TI con los objetivos organizacionales.

- La medición del desempeño de TI deben centrarse en la contribución de TI para permitir y ampliar el negocio.
- CobiT con el apoyo de las métricas adecuadas enfocadas al negocio se puede utilizar para garantizar que el enfoque principal es la prestación de servicios y no de competencia técnica.

Proceso de Orientación.

Según Brand y Boonen (2007), esto garantiza que las actividades se organizan en procesos propios basada en las responsabilidades previamente identificadas. Por ejemplo, en la actualización de la página web de una organización, el contenido del sitio web se considerará publicado por la dicha organización y en consecuencia pesan sobre ésta las responsabilidades legales a que haya lugar. Por lo tanto, un proceso debe ser diseñado y alguien tiene que aprobar los cambios. Esto se conoce como cambio de gestión.

Cuando las organizaciones implementan CobiT, su enfoque está orientado a la transformación. Los incidentes y los problemas ya no desvían la atención del proceso. Las excepciones están claramente definidas en el marco de los procesos estándar. La definición de procesos, describe, asignar roles y responsabilidades que permiten a la organización mantener el control aún en circunstancias excepcionales.

Aceptabilidad General.

Según Brand y Boonen (2007), un marco de control abarca las mejores prácticas aceptadas a nivel mundial. Las mejores prácticas evolucionan con el tiempo mediante la inclusión de las aportaciones de personas con experiencia en la industria. A través de estos ciclos, dichas prácticas deben ser probadas, de esta forma las mejores prácticas se formalizan en un marco de trabajo.

- CobiT ha sido un estándar probado y aceptado mundialmente que permite aumentar la contribución de las TI para el éxito organizacional.

- El marco se sigue mejorando y desarrollando para adaptarse a las mejores prácticas que surgen.
- Los profesionales de TI de todo el mundo contribuyen con sus ideas y el tiempo a mejorar dichas prácticas mediante reuniones y encuentros periódicos.

Requisitos regulatorios.

Según Brand y Boonen (2007), el cumplimiento normativo es con frecuencia una tarea costosa. Es más fácil demostrar que se cumple si el marco de control se basa en las normas vigentes. Para los auditores también resulta más fácil revisar los controles, sobre todo cuando dichos controles están basados en un modelo globalmente aceptado.

- Las organizaciones necesitan constantemente mejorar el rendimiento de TI y demostrar un control adecuado sobre sus actividades de TI.
- Muchos administradores de TI, asesores y auditores recurren a CobiT como la respuesta de facto a los requerimientos regulatorios de TI.

Lenguaje Común.

Según Brand y Boonen (2007), con el tiempo las mejores prácticas tienden a adquirir carácter distintivo en cuanto a su terminología, esto permite facilitar la comunicación dentro de la organización, entre los compañeros de otras empresas y con las partes externas (terceros o consultores).

En el mundo actual de equipos multifuncionales e interdisciplinarios, los cuales con frecuencia son liderados por personas que no son conscientes de la magnitud de la implementación, debido a que sus conocimientos se encuentra en otra área de la organización, la coordinación dentro y entre los equipos de proyecto y las organizaciones pueden jugar un papel clave en el éxito de cualquier proyecto. CobiT como marco trabajo permite un lenguaje común de términos al proporcionar un glosario.

Principios de Gobierno de TI

El consejo de administración y la gestión ejecutiva son los responsables del gobierno de TI. Se trata de estructuras y procesos que dirigen a la organización hacia el logro de sus objetivos y se basa en cuatro principios, según Brand y Boonen (2007):

- Dirección y control
- Responsabilidad
- Rendición de cuentas
- Actividades de TI

Dirección y control.

La dirección y control son dos conceptos claves de la gobernabilidad de TI:

- Dirección: El gerente proveer de dirección para implementar los cambios. Para proporcionar una dirección efectiva, el gerente necesita entender el cambio que se pretende lograr, así el gerente dirige a otras personas para lograr el cambio.
- Control: Control asegura que el objetivo se logre evitando que se produzcan incidentes no deseados.

Responsabilidad.

El Director Ejecutivo es responsable en última instancia del control interno. Los altos directivos asignan la responsabilidad para el establecimiento de políticas específicas de control interno y procedimientos al personal responsable de las funciones de la unidad. El control interno es responsabilidad de cada miembro de la organización y debe ser una parte explícita o implícita de la descripción del cargo.

Rendición de cuentas.

Rendición de cuentas es la obligación de los empleados para contabilizar, informar, y explicar sus acciones sobre el uso de los recursos asignados a ellos. La administración es responsable ante la dirección de proveer de gobernabilidad, orientación y supervisión. Es

esencial que las personas conozcan cómo sus acciones contribuyen al logro de los objetivos. El ambiente de control se ve influenciado por los individuos a medida que reconocen que puede ser considerado responsable.

Actividades de TI

Las actividades de TI son eficaces cuando hay buen gobierno de TI.

Áreas de enfoque de Gobierno de TI.

Según Brand y Boonen (2007), las áreas de gobierno de TI se centran describir los temas que la dirección ejecutiva debe abordar para gobernar las TI dentro de las organizaciones, es por ello que CobiT provee un modelo de proceso genérico de gobierno de todas las funciones de TI, ver Figura 62.

Figura 62. Áreas de Enfoque de CobiT 4.1

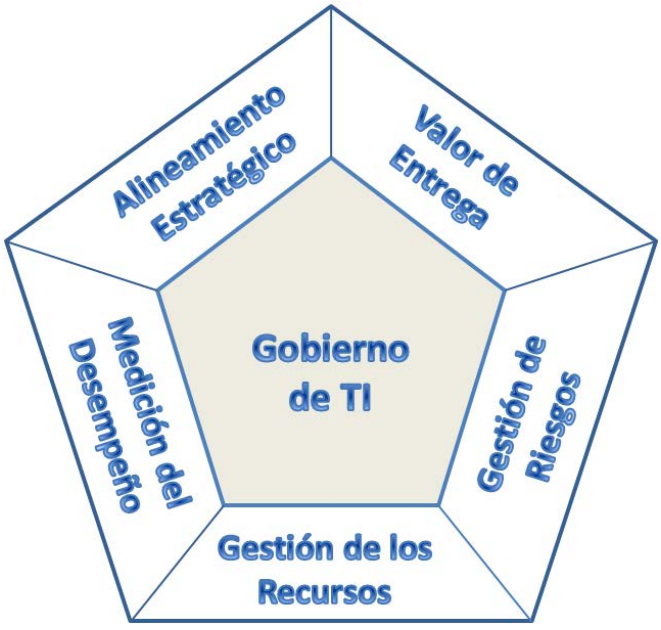

Figura 62. Adaptado de “IT Governance based on CobiT 4.1 - A Management Guide”, por Brand y Boonen, 2007, (p. 40).

- **Alineamiento Estratégico**: Se centra en garantizar la vinculación de la organización y los planes de TI, en la definición, mantenimiento, validación de la propuesta de valor de TI y en el alineamiento de las operaciones de TI con las operaciones de la organización.
- **Valor de Entrega**: Está relacionado a la ejecución de la propuesta de valor en todo el ciclo de entrega, asegurando que la tecnología ofrece los beneficios prometidos en consonancia con la estrategia, concentrándose en la optimización de costes y demostrar el valor intrínseco de la TI.
- **Gestión de Riesgos:** Requiere conocimiento de los riesgos por parte de los altos funcionarios de la empresa, comprensión del cumplimiento requisitos, normas y estándares, la transparencia acerca de los riesgos significativos para la empresa y la incorporación de las responsabilidades de gestión de riesgos en la organización.
- **Gestión de los Recursos**: Se refiere a la inversión óptima y la correcta gestión de los recursos críticos de TI tales como Recursos Humanos, aplicaciones, información e infraestructura.
- **Medición del Desempeño**: Rastrea y monitorea la implementación de estrategias, la terminación satisfactoria de los proyectos, el uso de recursos, rendimiento de los procesos y la prestación de servicios, utilizando, por ejemplo, cuadros de mando que traducen la estrategia en acción para alcanzar las metas mensurables más allá de la contabilización convencional.

ANEXO D

ITIL V 3.0

Definición de Servicio de Gestión

Según De Jong et al. (2008), ITIL se presenta como "buena práctica". Una buena práctica es un enfoque o método que se ha demostrado empíricamente. Las buenas prácticas puede ser un sólido respaldo para las organizaciones que quieren mejorar sus servicios de TI.

El ciclo de vida del servicio de ITIL se basa en el concepto de ITIL sobre "gestión de servicios" y "servicio" conceptos relacionados con "valor". Estos términos clave en la gestión del servicio se explican a continuación:

- **Gestión de servicios**: Es un conjunto de capacidades especializadas de la organización para proporcionar valor a los clientes en forma de servicios.
- **Servicio**: Es un medio que facilita la entrega de resultados satisfactorios a los clientes. Los resultados son posibles a partir de la realización de tareas y están restringidos por una serie de limitaciones, los servicios se mejoran al reducir las restricciones que existen sobre los mismos.
- **Valor**: El valor es el núcleo del concepto de servicio. Desde la perspectiva del cliente, el valor consiste en dos componentes fundamentales: utilidad y garantía. La utilidad es lo que el cliente recibe, y la garantía es la forma en que se preste.

Servicio de Gestión de la Tecnología

Según De Jong et al. (2008), la tecnología juega un papel importante en la gestión de servicios. Con la ayuda de herramientas, las tareas de gestión pueden ser automatizadas, como por ejemplo el uso de *Help Desk*, o herramientas de ayuda en la gestión y solución de incidentes.

Un conjunto integrado de servicios de tecnología de gestión debería incluir las siguientes funcionalidades:

- Soporte para todas las etapas del ciclo de vida.
- Soporte para el diseño de los servicios.

- Auto-ayuda y el control remoto.
- Un sistema integrado de gestión de configuración (*Configuration Management System* CMS).
- Tecnología para el descubrimiento, implementación, licenciamiento, diagnóstico y reportes.
- Cuadros de mandos.

La automatización es considerada para mejorar la utilidad y garantía de servicios debido a que:

- Simplificar los procesos al automatizarlos.
- Define claramente el flujo de trabajo, la asignación de tareas, la necesidad de información y las interacciones.
- En situaciones de auto-servicio, reducir la cantidad de usuarios en contacto tienen con los sistemas y procesos subyacentes.
- No toma a la ligera la automatización de las tareas e interacciones complejas.
- Descripción del ciclo de vida de servicio.

Según De Jong et al. (2008), ITIL V3 se aproxima a la gestión de servicios desde el punto de vista del ciclo de vida de un servicio. El ciclo de vida de servicio es un modelo de organización que ofrece información sobre:

- La forma en que se estructura la gestión de servicios.
- La manera en que varios componentes del ciclo de vida se vinculan entre sí.
- El impacto que los cambios en un componente tendrán sobre los demás y en el sistema de ciclo de vida completo del sistema.
- Por lo tanto, ITIL V3 se centra en el ciclo de vida del servicio y los componentes del servicio de gestión de manera que están vinculados. Los procesos y las funciones también se discuten en las fases del ciclo de vida.

Ciclo de vida de los servicios en ITIL V3

El ciclo de vida del servicio consta de cinco fases. Cada volumen de los libros fundamentales de ITIL describe cada una de estas fases.

Las cinco fases son:

1. Estrategia de Servicio: Corresponde a la fase de planificación estratégica de gestión de los servicios y su alineación con las estrategias de negocio. Según IT Governance Institute (2007), entre los procesos y funciones que la componen se encuentran:

- Gestión del servicio
- Ciclo de vida del servicio
- Activos del servicio y creación de valor
- Tipos y estructuras de proveedores de servicios
- Estrategia, mercados y oferta
- Gestión financiera
- Gestión del portafolio de servicios
- Gestión de la demanda
- Diseño organizacional, cultura y desarrollo
- Estrategia de aprovisionamiento
- Automatización e interfaces de servicios
- Herramienta para estrategias
- Desafíos y riesgos

2. Diseño del Servicio: Es la fase de diseño y desarrollo de servicios de TI, incluyendo la arquitectura, procesos, políticas y documentos. El objetivo del diseño es satisfacer las necesidades organizacionales actuales y futuras. Según IT Governance Institute (2008), entre los procesos y funciones que la componen se encuentran:

- Diseño balanceado
- Requisitos, indicadores, actividades y limitantes

- Arquitectura orientada al servicio
- Gestión de servicios de negocio
- Modelos de diseño de servicios
- Gestión del catálogo de servicios
- Gestión de niveles de servicios
- Capacidad y disponibilidad
- Continuidad de servicios de TI
- Seguridad de la información
- Gestión de proveedores
- Gestión de datos y de la información
- Gestión de aplicaciones
- Roles y herramientas
- Análisis de impacto en el negocio
- Desafíos y riesgos
- Paquete de diseño de servicios
- Criterios de aceptación de servicios
- Documentación
- Aspectos ambientales
- Marco de trabajo de maduración de procesos

3. **Transición del Servicio:** Es la fase de realización de los requisitos desde las etapas anteriores y la mejora de las capacidades para la transición hacia los nuevos servicios, modificando así la producción. Según IT Governance Institute (2007), entre los procesos y funciones que la componen se encuentran:

- Objetivos, principios, políticas, contexto, roles y modelos
- Planificación y soporte
- Gestión del cambio
- Activos del servicio y gestión de la configuración

- Liberación y distribución
- Validación y prueba del servicio
- Evaluación
- Gestión del conocimiento
- Gestionando las comunicaciones y el compromiso
- Gestión de partes interesadas
- Sistema de gestión de configuraciones
- Introducción por etapas
- Desafíos y riesgos
- Tipos de activos

4. **Operación del Servicio**. Esta fase permite lograr la efectividad y la eficiencia en la prestación del servicio y soporte, asegurando la satisfacción del cliente y del proveedor de servicios. Según IT Governance Institute (2007), entre los procesos y funciones que la componen se encuentran:

- Equilibrio en la operación del servicio
- Salud operacional
- Comunicación
- Documentación
- Eventos, incidentes y problemas
- Atención de requerimientos
- Gestión de accesos
- Monitoreo y control
- Gestión de la infraestructura y el servicio
- Gestión de instalaciones y del Data Center
- Seguridad física y de la información
- Mesa de servicios
- Gestión técnica de operaciones de TI y de aplicaciones

- Roles, responsabilidades y estructuras organizacionales
- Soporte tecnológico a la operación del servicio
- Gestionando los cambios, proyectos y riesgos
- Desafíos
- Guía complementaria

5. **Mejora Continua del Servicio (*Continual Service Improvement* CSI):** Esta fase permite crear y mantener el valor para el cliente a través de la mejora continua del diseño y la introducción de nuevos servicios y operaciones. Según IT Governance Institute (2007), entre los procesos y funciones que la componen se encuentran:

- Objetivos, métodos y técnicas
- Cambio organizacional
- Propiedad
- Drivers
- Gestión de niveles de servicios
- Medición del servicio
- Gestión del conocimiento
- Benchmarking
- Modelos, estándares y calidad
- Proceso de mejoramiento de los siete pasos CSI
- Retorno sobre la inversión (ROI) y aspectos de negocio
- Roles
- Matriz RACI
- Herramientas de soporte
- Implementación
- Gobierno
- Comunicaciones
- Desafíos y riesgos

- Innovación, corrección y mejoramiento
- Apoyo de las mejores prácticas a la mejora continua del servicio (CSI)
- Servicio de información

La Estrategia de Servicio es el eje principal del ciclo de vida del servicio (Figura 63), la cual impulsa todas las demás fases, ésta es la fase de formulación de políticas y el establecimiento de objetivos. El Diseño del Servicio, la Transición del Servicio y las fases de la Operación del Servicio se rigen por esta estrategia, su tema constante es el ajuste y el cambio. La fase de Mejora Continua del Servicio significa aprender y mejorar, abarca todas las fases del ciclo de vida de otros. Esto da inicio a la fase de programas de mejora y proyectos, les da prioridad sobre la base de los objetivos estratégicos de la organización.

Figura 63. Ciclo de Vida de los Servicios

Figura 63. Adaptado de “ITIL V3 Foundation Exam - The Study Guide”, por De Jong et al., 2008, (p. 10).

Contenido de ITIL V3

La Biblioteca ITIL V3 está compuesta por Según De Jong et al. (2008) por el Núcleo de Publicaciones, lo componen las cinco publicaciones de servicio del ciclo de vida:

- Estrategia de Servicio (SS *Service Strategy*)
- Diseño del Servicio (SD *Service Design*)
- Transición del Servicio (ST *Service Transition*)
- Operación del Servicio (SO *Service Operation*)
- Mejora Continua del Servicio (CSI *Continual Service Improvement*)

Cada libro incluye una fase del ciclo de vida del servicio y abarca varios procesos, funciones y actividades, que son descritos detalladamente en el libro donde se encuentran sus aplicaciones claves.

- Portafolio complementario:
    - Guía de introducción
    - Guías de elementos claves
    - Calificación de ayudas
    - Artículos
    - Glosario

Introducción a las funciones y procesos.

Según De Jong et al. (2008), en esta sección se ofrece una visión general de las funciones y procesos básicos que se incluyen en las cinco fases del ciclo de vida del servicio.

Los Procesos y Funciones se definen de la siguiente manera:

- **Procesos**: Es un conjunto estructurado de actividades encaminadas a lograr un objetivo determinado. Los procesos tienen entradas y salidas, sus resultados están orientados al cambio y utilizan la retroalimentación para corregir y mejorar sus dichos cambios. Los procesos son medibles, proporcionan resultados a los clientes y

siempre son generados por ciertos eventos particulares. Los procesos pueden ejecutarse a través de varias unidades organizativas.

- **Funciones**: Se puede definir como un equipo de personas y las herramientas que utilizan para llevar a cabo una o más actividades, especializándose en el cumplimiento de un tipo específico de trabajo y responsable con la finalidad de obtener resultados específicos. Las funciones tienen sus propias prácticas y su cuerpo de conocimientos propios. Las funciones pueden hacer uso de varios procesos.

Se puede estudiar cada proceso por separado para optimizar su calidad:

- El dueño del proceso es responsable de sus resultados.
- El administrador de procesos es responsable de la realización y la estructura del proceso e informa al dueño del proceso.
- Los agentes de proceso son responsables de las actividades definidas, y estas actividades se informa, al administrador de procesos.

Según De Jong et al. (2008), la gestión de la organización puede proporcionar el control básico de los datos manejados por cada proceso, en la mayoría de los casos los indicadores de desempeño y estándares se encontrarán previamente establecidos, para que así el supervisor de dichos procesos pueda tomar control de ellos.

El propietario de los procesos los evaluará mediante el uso de indicadores de rendimiento, para así determinar si satisface los estándares previamente acordados. Sin indicadores claros sería difícil determinar si los procesos están bajo control y si las mejoras previstas se están aplicando.

Los procesos se describen con frecuencia utilizando los procedimientos e instrucciones de trabajo:

- **Procedimiento**: Es una forma específica de llevar a cabo una actividad. Un procedimiento describe el "cómo", y también se puede describir "quién" ejecuta las

actividades. Un procedimiento puede incluir etapas para diferentes procesos. Los procedimientos pueden variar en función de la organización.

- **Conjunto de Instrucciones de Trabajo**: Definen detalladamente como una o más actividades en un procedimiento serán ejecutadas, utilizando para ello tecnología u otros recursos.

Cuando se define una organización, se establecen los roles y la descripción de los cargos:

- **Los roles** están compuestos por responsabilidades, actividades y la autoridad que ejerce una persona o grupo de personas, donde cada uno de ellos puede tener múltiples funciones.
- **Los cargos de trabajo** tradicionalmente se conocen como las tareas y responsabilidades que se asignan a una persona específica. Una persona en una posición particular que tiene un conjunto claramente definido de tareas y responsabilidades.

Según De Jong et al. (2008), las personas, procesos, productos y socios proporcionan la principal "maquinaria" de cualquier organización, pero sólo funcionan bien si dicha maquinaria está aceitada, la comunicación es un elemento esencial en cualquier organización. Si la gente no sabe acerca de los procesos o las instrucciones de uso correcto de las herramientas, los resultados pueden ser inesperados. Las estructuras formales de comunicación incluyen:

- Generación de informes: Informes internos y externos, dirigidos a la gestión y a los clientes, informes de avance del proyecto, las alertas, entre otros.
- Reuniones: Las reuniones oficiales del proyecto, reuniones regulares con objetivos específicos previamente establecidos.
- Sistemas en línea: Los sistemas de correo electrónico, salas de chat, buscapersonas, grupo de trabajo, los sistemas para compartir documentos, teleconferencias y servicios de reuniones virtuales.

- Tablones de anuncios: Se utilizan cerca de la máquina de café, a la entrada del edificio, en el restaurante de la compañía.

Es recomendable que todos en la organización comprendan el conjunto de procesos, proyectos, programas y portafolios, manejados por la organización.

- Proceso: Un proceso es un conjunto estructurado de actividades encaminadas a lograr un objetivo determinado.
- Proyecto: Un proyecto es una organización de carácter temporal, con las personas y otros recursos necesarios para lograr un objetivo.
- Programa: Un programa consta de una serie de proyectos y actividades que se planifican y gestionan en conjunto para lograr un conjunto general de objetivos relacionados.
- Portafolio o cartera: Es un conjunto de proyectos o programas que no están necesariamente relacionados entre sí, que manejado en conjunto permite el control, la coordinación y la optimización del portafolio en su totalidad. Una cartera de servicios es el conjunto completo de servicios que son administrados por un proveedor de servicios.

ANEXO E

SERIE ISO/IEC 27000

La Serie 27000.

Según ISO2700.es (2011), la serie 27000 se compone de los siguientes estándares:

ISO/IEC 27000.

Fue publicada en 1 de mayo del año 2009, proporciona una visión general de las normas que componen la serie 27000, a modo de introducción a los Sistemas de Gestión de la Seguridad de la Información, describen el proceso *Plan-Do-Check-Act*, además de otros términos y definiciones empleadas en toda la serie 27000.

ISO/IEC 27001.

Publicada el 15 de octubre de 2005, es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, su origen es la BS 7799-2:2002 (ya derogada), esta norma sirve para la calificación de los auditores externos de los SGSI de las organizaciones.

ISO/IEC 27002.

Vigente a partir del 1 de julio de 2007, se deriva de la norma ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describen los objetivos de control y los controles recomendados relativos a la seguridad de la información, no es certificable, contiene 39 objetivos de control y 133 controles que se agrupan en 11 dominios. Según IT Governance Institute (2008), el objetivo de este estándar es brindar información a los responsables de la implementación de seguridad de la información en las organizaciones. Los principios de esta norma sirven de punto de partida para la implementación de seguridad de la información y se basa en requisitos legales y en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en requisitos legales son:

- La protección y la no divulgación de datos personales
- Protección de la información interna
- Protección de los derechos de propiedad intelectual

Las mejores prácticas mencionadas en la norma incluyen:

- La política de seguridad de la información
- Asignación de la responsabilidad de seguridad de la información
- Escalamiento de problemas
- Gestión de la continuidad del negocio

Para la implementación de un sistema de gestión de seguridad de la información, se deben considerar los siguientes factores críticos de éxito:

- La política de seguridad, sus objetivos y actividades deben reflejar los objetivos de negocio.
- La implementación debe considerar los aspectos culturales de la organización.
- Se requiere del apoyo y compromiso de la alta dirección.
- Se requiere un conocimiento profundo de los requisitos de seguridad, evaluación del riesgo y gestión del riesgo.
- El marketing efectivo de la seguridad debe dirigirse a todo el personal, incluidos los miembros de la dirección.
- La política de seguridad y las medidas de seguridad deben ser comunicadas a terceros contratados.
- Los usuarios deben ser capacitados en forma adecuada.
- Se debería disponer de un sistema integral y balanceado para la medición del desempeño, que apoye la mejora continua de suministro de información.

El marco de seguridad para el desarrollo de un Sistema de Gestión de Seguridad de Información específico para la empresa debe contener:

- La política de seguridad
- Organización para la seguridad
- Clasificación de activos y su control
- Seguridad del personal

- Seguridad física y ambiental
- Comunicaciones y gestión de operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas
- Gestión de la continuidad del negocio
- Cumplimiento

ISO/IEC 27003.

Publicada el 01 de febrero de 2010, no es certificable. Es una guía centrada en los aspectos críticos que son imprescindibles para el diseño y la implementación exitosa de un SGSI según los lineamientos de la norma ISO/IEC 27001:2005. Esta norma describe el proceso de especificaciones desde su diseño hasta la puesta en práctica. Tiene su origen en el anexo B de la norma BS 7799-2 y en otros documentos publicados por el BSI.

ISO/IEC 27004.

Publicada el 7 de diciembre de 2009, no es certificable, es una guía para el desarrollo y la utilización de métricas y técnicas de medición que tienen por objeto establecer la eficacia de un SGSI y de los controles o grupos de ellos implementados según ISO/IEC 27001.

ISO/IEC 27005.

Publicada el 4 de junio de 2008, no es certificable, establece las directrices para la gestión del riesgo en la seguridad de la información, en conjunto con la norma ISO/IEC 27001 permite garantizar la seguridad de la información basada en un enfoque de gestión de riesgos.

ISO 27006.

Publicada el 1 de marzo de 2007, especifica los requisitos para la acreditación de entidades de auditoría y certificación de los sistemas de gestión de seguridad de la información, proviene de la revisión de la norma EA-1/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI) que en conjunto con ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) dicta los requisitos específicos relacionados con ISO 27001 y los SGSI. De esta manera ayuda a la interpretación de los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

ISO/IEC 27011.

Publicada el 15 de diciembre de 2008, es una guía de interpretación de la implementación y gestión de seguridad de la información en organizaciones que pertenecen al sector de las telecomunicaciones y que está basada en ISO/IEC 27002.

ISO/IEC 27033.

Es una norma de seguridad de redes, publicada el 10 de diciembre de 2009. Abarca desde conceptos generales, directrices de diseño e implementación de seguridad en redes, escenarios de referencia, aseguramiento de las comunicaciones mediante *gateways* de seguridad, aseguramiento de las comunicaciones mediante VPNs, convergencia de IP y redes inalámbricas. Esta norma, según ISO/IEC (2009), está estructurada siete partes individuales:

- **ISO/IEC 27033-1**: Es una guía general que describe conceptos básicos tales como gestión de seguridad en redes de datos, incluye una visión general, definiciones relacionadas, así como una orientación para identificar y analizar los riesgos de seguridad de la red mediante procesos de control. También sirve de introducción para el diseño de arquitecturas de buena calidad.

- **ISO/IEC 27033-2**: Describe los lineamientos para el diseño e implementación de seguridad en la red, define la calidad técnica de la arquitectura de red que se debe desarrollar para proporcionar seguridad a la misma, mediante la planificación, diseño e implementación basada en el uso de modelos o marcos arquitectónicos.
- **ISO/IEC 27033-3**: Permite definir los riesgos específicos, técnicas de diseño y problemas de control asociados a los escenarios de una red típica, está destinado al personal que participa en el diseño e implementación de aspectos arquitectónicos de seguridad en la red.
- **ISO/IEC 27033-4**: Norma las técnicas de diseño y los problemas de control para asegurar las comunicaciones entre redes que utilizan *gateways* o pasarelas de entrada/salida destinados a incrementar la seguridad, define riesgos específicos, técnicas de diseño y procedimientos de control.
- **ISO/IEC 27033-5**: Provee un marco de referencia destinado a las VPN o redes privadas virtuales, define los riesgos específicos, provee de técnicas de diseño y procedimientos de control.
- **ISO/IEC 27033-6**: Está destinada a normar todo lo relativo a la convergencia de IP, es decir, la convergencia de voz, datos y videos sobre la red de datos. Define sus riesgos específicos y dicta normas de control.
- **ISO/IEC 27033-7**: Está orientada a redes inalámbricas o *Wi-Fi*, define sus riegos específicos y los controles que deberían tener.

ISO/IEC 27799.

Publicada el 12 de junio de 2008, es una norma que sirve de guía para la interpretación y la aplicación de la norma ISO/IEC 27002 en el sector sanitario, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

ANEXO F

ALINEACIÓN COBIT 4.1, ITIL V3 E ISO/IEC 27002

Tabla 52. Alineación CobiT 4.1, ITIL V3 e ISO/IEC 27002

Según IT Governance Intitute (2008) la alineación de CobiT 4.1, en sus procesos de control DS5, DS3, DS4 y DS7 con ITIL V3 e ISO/IEC 27002 es la siguiente:

DS5 Garantizar la seguridad de los sistemas: La necesidad de mantener la integridad de la información y proteger los activos de TI precisa de un proceso de gestión de seguridad, lo que incluye establecer y mantener los roles, las responsabilidades, políticas, estándares y procedimientos de seguridad de TI. Además, realizar monitoreo de seguridad y pruebas periódicas e implementar acciones correctivas para identificar debilidades de seguridad o incidentes. Una gestión efectiva de seguridad protege todos los activos de TI para minimizar el impacto de vulnerabilidades de seguridad e incidentes en el negocio.

DS5 Garantizar la seguridad de los sistemas			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
DS5.1 Gestión de la seguridad de TI	• Ubicar la gestión de seguridad a alto nivel para cumplir con las necesidades del negocio	• SD 4.6 Gestión de seguridad de la información • SO 5.13 Gestión de seguridad de la información y la operación del servicio	• 6.1.1 Compromiso de la gerencia con la seguridad de la información • 6.1.2 Coordinación para la seguridad de la información • 6.2.3 Considerar la seguridad en los acuerdos con terceros • 8.2.2 Educación, entrenamiento y concientización en seguridad de información
DS5.2 Plan de Seguridad de TI	• Traducción de requerimientos de negocio, riesgo y cumplimiento en un plan de seguridad	• SD 4.6.4 Políticas, principios y conceptos básicos • SD 4.6.5.1 Controles de seguridad (cobertura a alto nivel, sin detalle)	• 5.1.1 Documento de la política de seguridad de la información • 5.1.2 Revisión de la política de seguridad de la información • 6.1.2 Coordinación para la seguridad de la información • 6.1.5 Acuerdos de confidencialidad

DS5 Garantizar la seguridad de los sistemas			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
			• 8.2.2 Educación, entrenamiento y concientización en seguridad de información • 11.1.1 Políticas de control de acceso • 11.7.1 Computación móvil y las comunicaciones • 11.7.2 Teletrabajo
DS5.3 Gestión de identidad	• Identificación de todos los usuarios (internos, externos y temporales) y su actividad	• SO 4.5 Gestión de acceso	• 5.1.1 Documento de la política de seguridad de la información • 5.1.2 Revisión de la política de seguridad de la información • 6.1.2 Coordinación para la seguridad de la información • 6.1.5 Acuerdos de confidencialidad • 8.2.2 Educación, entrenamiento y concientización en seguridad de información • 11.1.1 Políticas de control de acceso • 11.7.1 Computación móvil y las comunicaciones • 11.7.2 Teletrabajo
• DS5.4 Gestión de cuentas de usuario	• Gestión del ciclo de vida de las cuentas de usuario y privilegios de acceso	• SO 4.5 Gestión de acceso • SO 4.5.5.1 Peticiones de acceso • SO 4.5.5.2 Verificación • SO 4.5.5.3 Habilitar privilegios • SO 4.5.5.4 Monitorear el estado de la identidad • SO 4.5.5.5 Registro y seguimiento de accesos	• 6.1.5 Acuerdos de confidencialidad • 6.2.1 Identificación de riesgos relacionados con terceros • 6.2.2 Considerar la seguridad al tratar con los clientes • 8.1.1 Roles y responsabilidades • 8.3.1 Responsabilidades en el cese • 8.3.3 Eliminación de privilegios de acceso • 10.1.3 Segregación de funciones

DS5 Garantizar la seguridad de los sistemas			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
		• SO 4.5.5.6 Eliminar o restringir privilegios	• 11.1.1 Políticas de control de acceso • 11.2.1 Registro de usuarios • 11.2.2 Gestión de privilegios • 11.2.4 Revisión de derechos de acceso de usuarios • 11.3.1 Uso de contraseñas • 11.5.1 Procedimientos seguros de inicio de sesión • 11.5.3 Sistema de gestión de contraseñas • 11.6.1 Restricción de acceso a la información
• DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	• Pruebas proactivas de la implementación de seguridad • Acreditación oportuna • Reporte oportuno de eventos inusuales	• SO 4.5.5.6 Eliminar o restringir privilegios • SO 5.13 Gestión de seguridad de la información y la operación del servicio	• 6.1.8 Revisión independiente de la seguridad de la información • 10.10.2 Monitoreo del uso del sistema • 10.10.3 Protección de logs • 10.10.4 Logs de administrador y de operador • 12.6.1 Control de vulnerabilidades técnicas • 13.1.2 Reporte de debilidades de seguridad • 15.2.2 Verificación de cumplimiento técnico • 15.3.1 Controles de auditoría de sistemas de información
• DS5.6 Definición de incidente de seguridad	• Definición y clasificación de las características de los incidentes de seguridad	• SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) • SD 4.6.5.2 Gestión de brechas de seguridad e incidentes	• 8.2.3 Procesos disciplinarios • 13.1.1 Reporte de eventos de seguridad de información • 13.1.2 Reporte de debilidades de seguridad • 13.2.1 Responsabilidades y procedimientos • 13.2.3 Recolección de evidencia

DS5 Garantizar la seguridad de los sistemas			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
• DS5.7 Protección de la tecnología de seguridad	• Resistencia a la manipulación	• SO 5.4 Gestión y soporte de servidores	• 6.1.4 Proceso de autorización para las instalaciones de procesamiento de información • 9.1.6 Áreas de acceso público, despacho y recepción • 9.2.1 Ubicación y protección de equipos • 9.2.3 Seguridad del cableado • 10.6.2 Seguridad de los servicios de red • 10.7.4 Seguridad de la documentación de sistemas • 10.10.1 Logs de auditoría • 10.10.3 Protección de logs • 10.10.4 Logs de administrador y de operador • 10.10.5 Logs de fallas • 10.10.6 Sincronización de relojes • 11.3.2 Equipos desatendidos de usuario • 11.3.3 Políticas de escritorios y pantallas limpias • 11.4.3 Identificación de equipos en redes • 11.4.4 Protección de puertos de configuración y diagnóstico remoto • 11.5.1 Procedimientos seguros de inicio de sesión • 11.5.4 Uso de utilitarios del sistema • 11.5.5 Período de inactividad de sesión • 11.5.6 Limitación del tiempo de conexión • 11.6.2 Aislamiento de sistemas sensitivos • 11.7.1 Computación móvil y las comunicaciones • 11.7.2 Teletrabajo • 12.4.1 Control del software de operaciones • 12.6.1 Control de vulnerabilidades técnicas

DS5 Garantizar la seguridad de los sistemas			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
			• 13.1.2 Reporte de debilidades de seguridad • 13.2.3 Recolección de evidencia • 15.2.2 Verificación de cumplimiento técnico • 15.3.2 Protección de las herramientas de auditoría de Sistemas
• DS5.8 Gestión de llaves criptográficas	• Gestión del ciclo de vida de llaves criptográficas		• 10.8.4 Mensajería electrónica • 12.2.3 Integridad de mensajes • 12.3.1 Política de uso de controles criptográficos • 12.3.2 Gestión de llaves • 15.1.6 Regulación de controles criptográficos
• DS5.9 Prevención, detección y corrección de software malicioso	• Parches de actualización, control de virus y protección de malware		• 10.4.1 Controles contra código malicioso • 10.4.2 Controles contra código malicioso
• DS5.10 Seguridad de la red	• Controles para autorizar acceso y flujos de información desde y hacia las redes	• SO 5.5 Gestión de redes	• 6.2.1 Identificación de riesgos relacionados con terceros • 10.6.1 Controles de red • 10.6.2 Seguridad de los servicios de red • 11.4.1 Política de uso de los servicios de red • 11.4.2 Autenticación de usuarios para conexiones externas • 11.4.3 Identificación de equipos en redes • 11.4.4 Protección de puertos de configuración y diagnóstico remoto • 11.4.5 Segregación en redes

DS5 Garantizar la seguridad de los sistemas			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
			• 11.4.6 Control de conexiones en la red • 11.4.7 Control de enrutamiento en la red • 11.6.2 Aislamiento de sistemas sensitivos
• DS5.11 Intercambio de datos sensitivos	• Ruta confiable y controles de autenticación, constancia de recepción y no repudio		• 6.2.1 Identificación de riesgos relacionados con terceros • 10.6.1 Controles de red • 10.6.2 Seguridad de los servicios de red • 11.4.1 Política de uso de los servicios de red • 11.4.2 Autenticación de usuarios para conexiones externas • 11.4.3 Identificación de equipos en redes • 11.4.4 Protección de puertos de configuración y diagnóstico remoto • 11.4.5 Segregación en redes • 11.4.6 Control de conexiones en la red • 11.4.7 Control de enrutamiento en la red • 11.6.2 Aislamiento de sistemas sensitivos

Gestionar el desempeño y la capacidad: La necesidad de gestionar el desempeño y la capacidad de los recursos de TI requiere de un proceso para su revisión periódica, lo que incluye pronosticar necesidades futuras basándose en requerimientos de carga de trabajo, almacenamiento y contingencia. Este proceso provee la garantía de que los recursos de información que soportan los requerimientos del negocio estén disponibles en forma continua.

DS3 Gestionar el desempeño y la capacidad			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
• DS3.1 Planeamiento del desempeño y la capacidad	• Asegurar que las capacidades y los desempeños cumplen con los ANS	• SD 4.3.5.1 Gestión de la capacidad para el negocio • SD Apéndice J Contenido típico de un plan de capacidad • CSI 5.6.2 Gestión de la capacidad	• 10.3.1 Gestión de la capacidad
• DS3.2 Capacidad y desempeño actual	• Evaluación de los desempeños y capacidades actuales	• SD 4.3.5.2 Gestión de la capacidad del servicio • SD 4.3.5.3 Gestión de la capacidad de los componentes • SO 4.1.5.2 Notificación de eventos • SO 4.1.5.3 Detección de eventos • SO 5.4 Gestión y soporte de servidores • CSI 4.3 Mediciones del servicio	• 10.3.1 Gestión de la capacidad
• DS3.3 Capacidad y desempeño futuro	• Pronóstico de requerimientos de recursos • Tendencias de las cargas de trabajo	• SD 4.3.5.1 Gestión de la capacidad para el negocio • SD 4.3.5.2 Gestión de la capacidad del servicio • SD 4.3.5.3 Gestión de la capacidad de los componentes • SD 4.3.5.7 Modelamiento y tendencias • SD 4.3.8 Gestión de la información	• 10.3.1 Gestión de la capacidad

DS3 Gestionar el desempeño y la capacidad			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
• DS3.4 Disponibilidad de recursos de TI	• Provisión de recursos, contingencias, tolerancia a fallas y priorización de recursos	• SD 4.3.5.3 Gestión de la capacidad de los componentes • SD 4.3.5.4 Actividades de soporte de la gestión de capacidad • SD 4.4 Gestión de la disponibilidad • SD 4.4.5.1 Actividades reactivas de la gestión de la disponibilidad • SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad • SO 4.6.5 Gestión de la disponibilidad (actividades operativas) • CSI 5.6.1 Gestión de la disponibilidad	
• DS3.5 Monitoreo y reporte	• Mantenimiento y afinamiento de performance y capacidad; reporte de la disponibilidad de servicio al negocio	• SD 4.3.5.4 Actividades de soporte de la gestión de la capacidad • SD 4.3.5.5 Gestión y control de umbrales • SD 4.3.5.6 Gestión de la demanda • SD 4.4.5.1 Actividades reactivas de la gestión de la disponibilidad	

Garantizar la continuidad del servicio: La necesidad de proveer servicios continuos de TI requiere del desarrollo, mantenimiento y pruebas de planes de continuidad de TI, utilizar almacenamiento de respaldos fuera de las instalaciones y proporcionar entrenamiento periódico sobre el plan de continuidad. Un proceso eficaz de servicio continuo minimiza la probabilidad y el impacto de una interrupción de un servicio crítico de TI en funciones y procesos claves del negocio.

DS4 Garantizar la continuidad del servicio			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
• DS4.1 Marco de trabajo de continuidad de TI	• Enfoque consistente y corporativo a la gestión de continuidad	• SD 4.5 Gestión de continuidad de servicios de TI • SD 4.5.5.1 Etapa 1 – Inicio • CSI 5.6.3 Gestión de continuidad de servicios de TI	• 6.1.6 Relación con las autoridades • 6.1.7 Relación con grupos de interés especial • 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio • 14.1.2 Continuidad del negocio y evaluación de riesgos • 14.1.4 Marco de planificación de continuidad del negocio
• DS4.2 Planes de Continuidad de TI	• Planes individuales de continuidad • Análisis de impacto en el negocio • Resiliencia, procesamiento alternativo y recuperación	• SD 4.5.5.2 Etapa 2 – Requisitos y estrategia • SD 4.5.5.3 Etapa 3 – Implementación • SD Apéndice K Contenido típico de un plan de recuperación	• 6.1.6 Relación con las autoridades • 6.1.7 Relación con grupos de interés especial • 14.1.3 Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información
• DS4.3 Recursos críticos de TI	• Centrarse en la infraestructura crítica, resiliencia y priorización • Respuesta para diferentes períodos de tiempo	• SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad • SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio • 14.1.2 Continuidad del negocio y evaluación de riesgos

DS4 Garantizar la continuidad del servicio			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
• DS4.4 Mantenimiento del plan de continuidad de TI	• Control de cambios para reflejar los requerimientos cambiantes del negocio	• SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
• DS4.5 Pruebas del plan de continuidad de TI	• Pruebas regulares • Implementación del plan de acción	• SD 4.5.5.3 Etapa 3 – Implementación • SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
• DS4.6 Entrenamiento en el plan de continuidad de TI	• Entrenamiento regular para todas las partes involucradas	• SD 4.5.5.3 Etapa 3 – Implementación • SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
• DS4.7 Distribución del plan de continuidad de TI	• Distribución segura y adecuada a todas las partes autorizadas	• SD 4.5.5.3 Etapa 3 – Implementación • SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
• DS4.8 Recuperación y reanudación de los servicios de TI	• Planificación del período cuando TI se esté recuperando y reanudando servicios • Entendimiento del negocio y soporte a la inversión	• SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad • SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio • 14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información
• DS4.9 Almacenamiento externo de respaldos	• Almacenamiento externo de los medios críticos; documentación y recursos necesarios, en colaboración con los dueños de los procesos de negocio	• SD 4.5.5.2 Etapa 2 – Requisitos y estrategia • SO 5.2.3 Respaldo y restauración	• 10.5.1 Respaldo de la información
• DS4.10 Revisión postreanudación	• Evaluación regular de los planes	• SD 4.5.5.3 Etapa 3 – Implementación • SD 4.5.5.4 Etapa 4 – Operación continua	• 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio

Educar y entrenar a los usuarios: La educación efectiva de todos los usuarios de TI, incluidos a los que trabajan en TI, requiere identificar las necesidades de formación de cada grupo de usuarios, la definición y ejecución de una estrategia para una formación eficaz y la medición de los resultados. Un programa de formación eficaz aumenta el uso eficaz de la tecnología reduciendo los errores de usuario, aumentando la productividad e incrementando el cumplimiento de los controles clave, tales como las medidas de seguridad del usuario.

D7 Educar y entrenar a los usuarios			
Objetivo de Control CobiT **4.1**	**Áreas clave**	**Información de soporte ITIL V3**	**Información de Soporte ISO/IEC 27002:2005**
• DS7.1 Identificación de necesidades de educación y formación	• Programa de formación para cada grupo de empleados	• SO 5.13 Gestión de seguridad de la información y la operación del servicio • SO 5.14 Mejora de las actividades operativas	• 8.2.2 Educación, entrenamiento y concientización en seguridad de información
• DS7.2 Brindar educación y entrenamiento	• Identificar y nombrar instructores • Cronograma de entrenamiento		• 8.2.2 Educación, entrenamiento y concientización en seguridad de información
• DS7.3 Evaluación del entrenamiento recibido	• Evaluar la entrega del entrenamiento y mejoras futuras		