

<b>TEMA</b>	<b>PÁGINA</b>
<b>Introducción</b>	1
<b>Contexto</b>	2
<b>Estructura de la tesis</b>	3
<b>Capítulo 1.- Marco teórico</b>	4
1.1.- Seguridad informática	5
1.2.- Administración de la seguridad	8
1.2.1.- Definición de administración de la seguridad	8
1.3.- Definición de análisis de riesgos	9
1.3.1.- Tipos de análisis de riesgos	10
1.3.2.- Pasos a seguir para realizar un análisis de riesgo de tipo cualitativo	12
1.4.- Políticas de seguridad	14
1.4.1.- Principios fundamentales	15
1.4.2.- Ciclo de vida de las políticas de seguridad	15
1.5.- Plan de contingencias	17
1.5.1.- Definición de plan de contingencias	17
1.6.- Sistemas operativos para servidores	17
1.6.1.- Sistemas operativos de la familia Microsoft.	17
1.6.1.1.- Microsoft Windows Server	18
1.6.2.- Sistemas operativos de la familia Linux	19
1.6.2.1.- Comparativa entre distribuciones del sistema operativo Linux.	19
1.7.- Servidores web	20
1.7.1.- Comparativa entre Apache y IIS	21
1.8.- Manejadores de bases de datos	22
1.8.1.- Comparativa entre MySQL y PostgreSQL	22
1.9.- Plataformas de Hardware	23
1.9.1.- Comparativa del Hardware	23
<b>Capítulo 2.- Vulnerabilidades en aplicaciones web</b>	25
2.1.- Web	26
2.1.1.- XSS(Cross Site Scripting)	27
2.1.2.- CSRF(Cross Site Request Forgery)	27
2.1.3.- Inyección de código (Code Injection)	30
2.1.4.- Buffer overflow	31
2.2.- Bases de datos	33
2.2.1.- SQL Injection	33
<b>Capítulo 3.- Análisis de riesgos</b>	35
3.1.- Identificación de los activos	36
3.2.- Identificación de las amenazas y vulnerabilidades	36
3.3.- Determinación del impacto de la ocurrencia de una amenaza	38
3.4.- Identificación de controles	39
<b>Capítulo 4.- Recomendaciones para un servidor web y de bases de datos seguro</b>	41
4.1.- Recomendación del hardware	42
4.2.- Selección de plataformas	42
4.3.- Instalación y configuración de las plataformas	43
4.4.- Recomendaciones para la administración del servidor web y	44

de bases de datos	
4.5.- Recomendaciones de seguridad para aplicaciones que utilizan bases de datos	45
4.6.- Recomendaciones generales	46
<b>Capítulo 5.- Propuesta de políticas de seguridad</b>	49
5.1.- Políticas de seguridad física	50
5.2.- Políticas de cuentas	50
5.3.- Políticas de contraseñas	51
5.4.- Políticas de control de acceso (lógico y físico)	51
5.5.- Políticas de uso adecuado	51
5.6.- Políticas de mantenimiento	52
5.7.- Políticas de respaldos	52
5.8.- Sanciones	52
<b>Conclusiones</b>	54
<b>Anexo</b>	56
A.- Instalación de Ubuntu 9.04 Server	57
B.- Instalación de OpenSSH utilizando aptitude	59
C.- Instalación de Apache utilizando aptitude	61
D.- Instalación de MySQL utilizando aptitude	61
E.- Instalación de PHP utilizando aptitude	63
F.- Instalación de phpMyAdmin utilizando aptitude	64
G.- Configuración de UFW	65
H.- Configuración segura de Apache por medio de HTTPS	67
I.- Restricción de acceso de un usuario al home de otros usuarios	70
J.- Respaldo de archivos del sistema	72
K.- Configuración segura de PHP	74
<b>Glosario</b>	77
<b>Mesografía y bibliografía</b>	80

<b>TABLAS Y FIGURAS</b>	<b>PÁGINA</b>
<b>Tablas</b>	
Tabla 1.- Comparativa de Sistemas Operativos de la Familia Microsoft Windows Server	18
Tabla 2.- Comparativa de los sistemas operativos de la familia Linux: Fedora Core, Ubuntu Server, Red Hat Enterprise y SuSE Linux Enterprise Server	19,20
Tabla 3.- Comparativa de los servidores web: Apache y IIS	21,22
Tabla 4.- Comparativa entre los manejadores de bases de datos: MySQL y PostgreSQL	22,23
Tabla 5.- Comparativa de plataformas de Hardware	23,24
Tabla 6.- Características del servidor web del CDMIT	36
Tabla 7.- Características del hardware propuesto para el CDMIT	42
Tabla 8.- Selección de plataformas	43
<b>Figuras</b>	
Figura 1.1.- Contexto y relaciones de la seguridad	6
Figura 1.2.- Ciclo de la administración de la seguridad	8
Figura 1.3.- Modelo relacional simple	12

Figura 1.4.- Distribución mundial del uso de servidores web según Netcraft	21
Figura 3.1.- Estructura actual de la sección de cómputo del CDMIT	37
Figura 4.1.- Estructura propuesta para la sección de cómputo del CDMIT	46
Figura A1.- Pantalla de instalación de Ubuntu 8.04 Server	57
Figura A2.- Asistente de particionado de Ubuntu 8.04 Server	58
Figura A3.- Creación de particiones para Ubuntu 8.04 Server	58
Figura A4.- Proceso de instalación de Ubuntu 8.04 Server	59
Figura A5.- Selección de software de Ubuntu 8.04 Server	59
Figura A6.- Conexión remota al servidor por SSH	60
Figura A7.- Comprobación del Servidor web Apache	61
Figura A8.- Elección de contraseña de administrador para MySQL	62
Figura A9.- Inicio de sesión en el servidor MySQL	63
Figura A10.-Prueba de funcionamiento de PHP	64
Figura A11.-Cliente MySQL phpmyadmin	65
Figura A12.-Puertos permitidos por el Firewall	67
Figura A13.-Puerto 22 cerrado por el Firewall	67
Figura A14.-HTTPS funcionando	70
Figura A15.-Denegar el acceso de usuarios a directorios de otros usuarios	71
Figura A16.-Prueba de denegación de acceso al directorio de otro usuario	72