Índice

INTRODUCCIÓN .................................................................................................................................11

CAPÍTULO 1. GESTIÓN DE LA SEGURIDAD Y NORMATIVAS .................................................................13
1.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN .................................................................14
1.2 METODOLOGÍA ITIL ......................................................................................................................16
   1.2.1 Estrategia del servicio .............................................................................................................17
   1.2.2 Diseño del servicio ..................................................................................................................18
   1.2.3 Transición del servicio ..........................................................................................................19
   1.2.4 Operación del servicio ...........................................................................................................20
   1.2.5 Mejora continua del servicio .................................................................................................20
1.3 LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL ................................21
1.4 NORMATIVAS UTILIZADAS PARA LA GESTIÓN DE LA SEGURIDAD FÍSICA ................................26
TEST DE CONOCIMIENTOS ............................................................................................................29

CAPÍTULO 2. ANÁLISIS DE LOS PROCESOS DE SISTEMAS ...............................................................29
2.1 PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN ............................30
2.2 CARACTERÍSTICAS FUNDAMENTALES DE LOS PROCESOS ELECTRÓNICOS ...........................31
   2.2.1 Estados de un proceso y ciclo de vida ......................................................................................33
   2.2.2 Comandos de control de procesos en sistemas Unix ..............................................................35
   2.2.3 Prioridades en los procesos Unix/Linux ..................................................................................36
2.3 SISTEMAS DE INFORMACIÓN EN LOS PROCESOS DE NEGOCIO ............................................38
2.4 FUNCIONALIDADES DE UN SISTEMA OPERATIVO PARA LA MONITORIZACIÓN Y GESTIÓN
   DEL CONSUMO DE RECURSOS ......................................................................................................39
   2.4.1 El Monitor del sistema en Linux ..............................................................................................39
   2.4.2 Monitorización mediante comandos en Linux ........................................................................41
   2.4.3 Gestión de recursos utilizados mediante comandos en Linux ..............................................43
   2.4.4 Monitorización en Linux con Nagios® ....................................................................................43
   2.4.5 Monitorización en sistemas Mac OS X ....................................................................................45
   2.4.6 Consumo de recursos .............................................................................................................49
   2.4.7 Principales procesos de servicios en Windows® .....................................................................50
   2.4.8 Principales procesos de servicios en Linux ............................................................................51
TEST DE CONOCIMIENTOS ............................................................................................................55

CAPÍTULO 3. DEMOSTRACIÓN DE LOS SISTEMAS DE ALMACENAMIENTO ....................................55
3.1 TIPOS DE DISPOSITIVOS DE ALMACENAMIENTO .......................................................................56
   3.1.1 Jerarquías de almacenamiento ...............................................................................................56
   3.1.2 La memoria principal ..............................................................................................................58
3.1.3 Jerarquías de almacenamiento ............................................................... 60
3.1.4 Sistemas NAS y SAN .............................................................................. 65
3.1.5 La tecnología RAID .............................................................................. 67
3.2 CARACTERÍSTICAS DE LOS SISTEMAS DE ARCHIVO ...................................... 68
  3.2.1 Singularidades de un sistema de archivos ............................................. 68
  3.2.2 Los archivos y directorios en Unix ..................................................... 70
  3.2.3 Nomenclatura y codificación de los archivos ....................................... 71
  3.2.4 Comparación de sistemas de archivos ................................................. 72
  3.2.5 Sistemas de archivos con journaling .................................................. 73
3.3 ORGANIZACIÓN Y ESTRUCTURA GENERAL DEL ALMACENAMIENTO ................ 74
  3.3.1 Implementación de sistemas de archivos .............................................. 74
  3.3.2 Particionamiento ............................................................................. 75
3.4 HERRAMIENTAS PARA LA GESTIÓN DE DISPOSITIVOS DE ALMACENAMIENTO .............. 77
  3.4.1 Herramientas para la gestión de discos en Linux (GParted) ..................... 77
  3.4.2 Utilidad de discos de Mac OS X .......................................................... 78
  3.4.3 Administrador de discos de Windows® .............................................. 79

TEST DE CONOCIMIENTOS ........................................................................... 81

CAPÍTULO 4. MÉTRICAS E INDICADORES DE MONITORIZACIÓN DE RENDIMIENTO DE SISTEMAS .......................................................... 83
4.1 USO DE MÉTRICAS E INDICADORES PARA LA MONITORIZACIÓN DE LOS SISTEMAS DE INFORMACIÓN ................................................................. 84
  4.1.1 Criterios y recomendaciones para la elección de un sistema de monitorización del rendimiento ................................................................. 85
4.2 OBJETOS DEL SISTEMA Y SUS INDICADORES ............................................. 86
  4.2.1 Monitor de rendimiento de Windows® 7 .............................................. 87
4.3 SELECCIÓN Y DEFINICIÓN DE INDICADORES ........................................... 88
  4.3.1 Crear un gráfico nuevo en el Monitor de rendimiento de Windows® 7 ........ 90
  4.3.2 Conjuntos de recopiladores de datos de Windows® 7 .............................. 92
4.4 ANÁLISIS DE LOS DATOS APORTADOS POR LOS INDICADORES .................... 95
  4.4.1 Monitor de confiabilidad en Windows® 7 .............................................. 95
4.5 CONSOLIDACIÓN DE INDICADORES .......................................................... 97
  4.5.1 Creación de alerts de contador de rendimiento en Windows® 7 ............ 98

TEST DE CONOCIMIENTOS ........................................................................... 104

CAPÍTULO 5. MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES ........................... 105
5.1 DISPOSITIVOS DE COMUNICACIONES ....................................................... 106
  5.1.1 La tarjeta de red .............................................................................. 107
  5.1.2 El repetidor y el hub ....................................................................... 107
  5.1.3 El switch ......................................................................................... 108
  5.1.4 Punto de acceso inalámbrico ............................................................ 109
  5.1.5 El router ......................................................................................... 109
5.2 PROTOCOLOS Y SERVICIOS DE COMUNICACIONES .................................... 110
5.3 PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES ................................................................. 112
5.4 PROCESOS DE MONITORIZACIÓN Y RESPUESTA .......................................................... 116
5.5 HERRAMIENTAS DE MONITORIZACIÓN DE PUERTOS Y SERVICIOS ..................................... 118
  5.5.1 Monitorización con Wireshark .......................................................... 118
5.6 HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS ....................................... 121
  5.6.1 Monitorización con Xymon .......................................................... 121
  5.6.2 Monitorización con Nagios® .......................................................... 124
  5.6.3 Monitorización con Cacti .......................................................... 128
5.7 SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD ......................... 134
5.8 GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO ....................................... 134
  5.8.1 Gestión de registros con rsyslog y LogAnalyzer ........................................ 135
TEST DE CONOCIMIENTOS .............................................................................. 143

CAPÍTULO 6. SELECCIÓN DEL SISTEMA DE REGISTRO ............................................................................. 143
6.1 REGISTROS, PERÍODOS DE RETENCIÓN Y NECESIDADES DE ALMACENAMIENTO ................. 144
6.2 REQUERIMIENTOS LEGALES EN REFERENCIA AL REGISTRO ................................................. 145
  6.2.1 La notificación de ficheros de carácter personal ............................................. 146
  6.2.2 Datos especialmente protegidos .................................................................. 147
  6.2.3 La calidad de los datos y su proporcionalidad ............................................... 147
  6.2.4 ¿Qué derechos tienen los ciudadanos sobre sus datos? .................................. 147
6.3 MEDIDAS DE SALVAGUARDIA PARA LA SEGURIDAD DEL SISTEMA DE REGISTROS .......... 148
  6.3.1 Propiedad de la información: restricciones de acceso ..................................... 148
  6.3.2 Identificador único de acceso .................................................................. 148
  6.3.3 El vaulting, backup remoto u offsite backup ............................................... 149
  6.3.4 La integridad de los datos ........................................................................ 151
6.4 ALTERNATIVAS AL ALMACENAMIENTO PARA LOS REGISTROS DEL SISTEMA ............... 151
  6.4.1 Recogida y tratamiento de datos .................................................................. 153
6.5 ALTERNATIVAS AL ALMACENAMIENTO PARA LOS REGISTROS DEL SISTEMA ............... 153
6.6 SELECCIÓN DEL SISTEMA DE ALMACENAMIENTO Y CUSTODIA DE REGISTROS .......... 156
TEST DE CONOCIMIENTOS .............................................................................. 159

CAPÍTULO 7. ADMINISTRACIÓN DEL CONTROL DE ACCESOS .......................................................... 159
7.1 REQUERIMIENTOS DE ACCESO A SISTEMAS DE INFORMACIÓN Y RECURSOS
  COMPARTIDOS ............................................................................................... 160
  7.1.1 Cuentas de usuarios .................................................................................. 160
  7.1.2 Cuentas de equipos ................................................................................... 161
  7.1.3 Cuentas de grupos .................................................................................... 162
7.2 CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS ...................................................... 163
7.3 CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS ...................................................... 165
7.4 PERFILES DE ACCESO ......................................................................................... 165
7.5 HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP .................................... 166
7.5.1 Paso 1: Instalar un servidor LDAP en Ubuntu Linux

7.5.2 Paso 2: Configurar el servidor LDAP

7.5.3 Paso 3: Agregar objetos a LDAP (unidades organizacionales de usuarios y grupos)

7.5.4 Paso 4: Agregar personas a la unidad organizacional (ou) users

7.5.5 Paso 5: Agregar grupos a la unidad organizacional (ou) groups

7.5.6 Herramientas LDAP: phpLDAPadmin

7.5.7 Herramientas LDAP: JXplorer

7.6 HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES

7.6.1 Identificador único de acceso

7.6.2 Identificación mediante certificado

7.7 HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO Y DE AUTENTICACIÓN SINGLE SIGN-ON

7.7.1 Herramientas de autenticación SSO: Kerberos

TEST DE CONOCIMIENTOS

SOLUCIONARIO DE LOS TEST DE CONOCIMIENTOS

ÍNDICE ALFABÉTICO