



UNAPPEC

UNIVERSIDAD APEC

Decanato de Ingenierías e Informática

Escuela de Informática

Tema:

Elaboración de un plan de continuidad de negocios para la disponibilidad en la plataforma web Moodle de la Universidad APEC, Santo Domingo, R. D., 2015.

Sustentantes:

Paula Rosario Ventura	2010 - 1724
Gabriel Antonio Tolentino Rosario	2011 - 0264
Leorge Artajerjes Jiménez Peralta	2009 - 2054

Asesor:

Ing. Santo Rafael Navarro

Trabajo de grado para optar por el Título de:

Ingeniero en Sistemas

Distrito Nacional, República Dominicana

LIBRO DE RESERVA
Este libro de reserva
NO debe ser sacado
de la Biblioteca.

INDICE

Índice de ilustraciones	VIII
Índice de tablas.....	XII
AGRADECIMIENTOS	XIII
DEDICATORIAS	XVI
INTRODUCCIÓN.....	XX
CAPITULO I. ASPECTOS GENERALES	22
1.1 Aspectos generales.....	23
1.2 Computación en la nube (Cloud Computing)	24
1.2.1 Ventajas.....	25
1.2.2 Desventajas	25
1.3 Características.....	27
1.4 Tipos de infraestructuras de nubes.....	27
RESUMEN.....	32
CAPITULO II. COMPONENTES DE LA NUBE	33
2.1 Clientes	34
2.2 Servicios de distribución.....	41
2.2.1 Infraestructura como servicio (<i>IaaS</i>)	41
2.2.2 Almacenamiento como Servicio (<i>DaaS</i>)	45
2.2.3 Comunicación como Servicio (<i>CaaS</i>)	45
2.2.4 <i>Hardware</i> como Servicio (<i>HaaS</i>).....	45

2.2.5	Software como Servicio (SaaS).....	48
2.2.6	Plataforma como servicio (PaaS).....	52
2.3	Internet – Protocolos.....	59
2.3.1	Transferencia de Estado Representacional (<i>REST</i>).....	63
2.3.2	Protocolo Simple de Acceso a Objetos (<i>SOAP</i>).....	67
2.3.3	Descripción de Servicios Web en Lenguas (<i>WSDL</i>).....	67
2.3.4	Descripción Universal, descubrimiento e integración (<i>UDDI</i>).....	69
2.3.5	Protocolo Simple de Administración de Redes (<i>SNMP</i>).....	70
2.3.6	Sistema de Archivos Comunes de Internet (<i>CIFS</i>).....	71
2.3.7	Capa de Conexión Segura (<i>SSL</i>).....	72
2.3.8	Seguridad de la capa de transporte (<i>TLS</i>).....	76
2.3.9	Estándar Avanzado de Encriptación (<i>AES</i>).....	77
2.3.10	Protocolo de Transferencia de Hipertexto (<i>HTTP</i>).....	77
2.3.11	Protocolo de Transferencia de archivos (<i>FTP</i>).....	78
2.3.12	Protocolo de Control de Transmisión (<i>TCP</i>).....	80
2.3.13	Protocolo de Internet (<i>IP</i>).....	80
2.3.14	Llamada de Procedimiento Remoto (<i>RPC</i>).....	81
2.3.15	Sistemas de Nombres de Dominio (<i>DNS</i>).....	82
2.4	Data Center.....	83
2.4.1	Niveles de centro de datos (<i>TIER</i>).....	84
2.4.2	Tipos de UPS.....	94
	RESUMEN.....	98
	CAPITULO III. SEGURIDAD EN LA NUBE.....	100
3.1	Seguridad en la nube.....	101

3.1.1	Características de la seguridad en la nube	101
3.1.2	Características de funcionamiento de las nubes	106
3.2	La seguridad	107
3.2.1	Seguridad como servicio.....	107
3.2.2	Seguridad del explorador.....	108
3.2.3	Autenticación	108
3.2.4	Perdida de gobernanza.....	108
3.2.5	Bloqueo de proveedor (<i>Provider Lock-In</i>)	109
3.2.6	Protección de los datos.....	109
3.3	La fundación para la nube	111
3.4	Las nubes utilizando funciones	118
3.5	Estándares	123
RESUMEN.....		129
CAPITULO IV. Entorno Virtual de Aprendizaje (EVA).....		131
4.1	Conceptualización.....	132
4.2	Tipos.....	133
4.3	Ventajas.....	135
4.4	Desventajas	136
4.5	Aplicación web Moodle.....	136
4.5.1	Conceptualización.....	136
4.5.2	Estructura	138
4.5.3	Interfaz de programación de aplicaciones (API)	139
4.5.4	Competencias.....	143

4.6 Tendencias presentes y futuras de los Entornos Virtuales de Aprendizajes	143
4.6.1 Panorama actual.....	143
4.6.2 Usuarios y casos de éxitos	144
4.6.3 Productos y Servicios	145
RESUMEN	146
CAPITULO V. INFRAESTRUCTURA TECNOLÓGICA	148
5.1 Conectividad	149
5.2 Seguridad y autenticación de usuario	150
5.2.1 Autenticación con Base de Datos Externa.....	151
5.2.2 Autenticación IMAP.....	151
5.2.3 Planificación de modelo de seguridad	152
5.3 Infraestructura	153
5.3.1 Infraestructura Virtual.....	153
5.3.2 Infraestructura de Servidores.....	153
5.3.3 Bases de Datos.....	154
5.4 Alimentación energética	160
RESUMEN	160
CAPITULO VI. PLAN DE CONINUIDAD DE NEGOCIO	162
FASE I: Análisis y evaluación de riesgos	163
6.1 Evaluación de riesgo	163
6.1.1 Desastres ambientales	163
6.1.2 Interrupciones organizadas o deliberadas	164
6.1.3 Fallas en servicios públicos	165

6.1.4	Fallas en los equipos o sistemas	165
6.1.5	Incidentes serios de seguridad	167
6.1.6	Otras situaciones de emergencia.....	168
6.2	Análisis de impacto del negocio	168
6.2.1	Procesos de negocio clave	169
6.2.2	Definición de períodos de tiempo objetivos de recuperación / RTO	169
6.2.3	Impacto financiero y operacional	171
6.3	Comunicaciones e IT.....	175
6.3.1	Especificaciones de IT y telecomunicaciones	176
6.3.2	Sistemas y procesos de información	178
6.3.3	Personal interno y lista de contactos de emergencia.....	179
6.3.4	Ingenieros de mantenimiento y personal clave de los proveedores...	180
FASE II: Selección de estrategias		181
6.4	Diseño de estrategias de continuidad	181
6.4.1	Estrategia de manejo del sitio alternativo	181
6.4.2	Respaldo y recuperación para sistemas IT	182
6.4.3	Respaldo y recuperación para sitios y equipos esenciales.....	183
6.4.4	Respaldo y recuperación para servicios al cliente	184
6.4.5	Respaldo y recuperación para información y documentación.....	185
6.4.6	Cubrimiento de seguros.....	186
6.5	Personal y proveedores claves	187
6.5.1	Organigrama funcional.....	187
6.5.2	Coordinador y delegado para cada área funcional	188
6.5.3	Personal clave e información de contactos de emergencia	188

6.5.4	Proveedores claves e información de contactos de emergencia .	189
FASE III: Desarrollo del Plan de Continuidad		191
6.5.5.1	Establecer el equipo de recuperación de desastres (DRT).....	191
6.5.5.2	Movilizar el equipo de recuperación del negocio (BRT).....	192
6.6 Documentos y procedimientos claves		192
6.6.1	Documentación y registros vitales para el negocio	192
6.6.2	Almacenamiento en sitio alternativo	193
6.6.3	Suministros de oficina.....	195
6.6.4	Procedimientos de manejo de los medios	196
6.6.5	Procedimientos de autorización en emergencia	196
6.6.6	Presupuesto para back-up y recuperación	197
6.7 Procedimientos de recuperación		198
6.7.1	Coordinar la preparación del lugar de recuperación	198
6.7.2	Traslado al centro de respaldo	199
6.7.3	Procedimiento de recuperación del Sistema Operativo	199
FASE IV: Pruebas y Mantenimiento		200
6.8 Pruebas y entrenamiento del plan		200
6.8.1	Revisiones periódicas	200
6.8.2	Ejercicios de entrenamiento.....	201
6.8.3	Pruebas técnicas	201
6.8.3	Mantenimiento	202
RECOMENDACIONES		203
CONCLUSIÓN		204
BIBLIOGRAFÍA.....		206

ANEXOS	211
Anexos, Capítulo I.....	212
Anexos, Capítulo III.....	213
Anexos Marco aplicativo, Capítulo VI.	215

Índice de ilustraciones

Ilustración 1. Nube privada.	29
Ilustración 2. Nube pública.....	30
Ilustración 3. Nube híbrida.	30
Ilustración 4. Nube de comunidad.	31
Ilustración 5. Resumen gráfico, Capítulo I.	32
Ilustración 6. El uso de servicios multimedia en la nube.....	35
Ilustración 7. Usuarios por servicio de almacenamiento en la nube.	36
Ilustración 8. Tráfico de red originado por usuarios hacia los centro de <i>data centers</i>.....	39
Ilustración 9. Proyección incremento del uso de servicios en la infraestructura <i>cloud</i>.....	41
Ilustración 10. Almacenamiento personal a nivel global en la nube.....	42
Ilustración 11. Almacenamiento personal en la nube en Latinoamérica.	43
Ilustración 12. Requerimientos para las aplicaciones en la nube en las empresas.	44
Ilustración 13. Ontología unificada de Cloud Computing.	46
Ilustración 14. Análisis de las infraestructuras de los <i>data centers</i> de proveedores de IaaS.....	48
Ilustración 15. Crecimiento del mercado XaaS.....	57
Ilustración 16. Usuarios de internet en el mundo.....	60
Ilustración 17. El incremento de usuarios en Internet se extiende cada año aún más.....	61
Ilustración 18. Arquitectura jerárquica de Internet.	62

Ilustración 19. Transferencia de estado representacional.	64
Ilustración 20. Servicio de datos REST en eXtreme Scale.	64
Ilustración 21. Verbos que permiten la comunicación entre HTTP y los servicios de RESTful.	66
Ilustración 22. Funcionamiento del protocolo SOAP.	67
Ilustración 23. Representación de conceptos definidos por documentos de WSDL.	68
Ilustración 24. <i>Los mensajes SAOP interrogan a UDDI.</i>	69
Ilustración 25. UDDI es un estándar para describir y descubrir servicios web. 70	
Ilustración 26. Infraestructura para intercambiar información de administración entre aplicaciones de consola.	71
Ilustración 27. Sistema de Archivos Comunes de Internet (CIFS), forma estándar de los usuarios compartir archivos a través de intranets e internet.	72
Ilustración 28. Autenticación SSL mutua.	75
Ilustración 29. Autenticación mutua y encriptación para protocolos fiables de la capa de Transporte (OSI).	76
Ilustración 30. Protocolo de transferencia de archivos.	79
Ilustración 31. Protocolo de Internet (IP).	80
Ilustración 32. Llamada de procedimiento remoto (RPC).	81
Ilustración 33. Sistema de nombre de dominio (DNS).	83
Ilustración 34. Diagrama de la Topología del Sistema Eléctrico de TIER 1.	86
Ilustración 35. Diagrama de la Topología del Sistema Eléctrico de TIER 2.	88
Ilustración 36. Diagrama de la Topología del Sistema Eléctrico de TIER 3.	90
Ilustración 37. Diagrama de la Topología del Sistema Eléctrico de TIER 4.	93
Ilustración 38. Línea interactiva (LI) UPS.	98
Ilustración 39. Modo de espera de Ferro.	98
Ilustración 40. Conversión Delta en línea.	98
Ilustración 41. Resumen gráfico, Capítulo II. Componentes de la Nube.	99
Ilustración 42. Safe zone.	104
Ilustración 43. Barracuda Web Security Flex Architecture.	107

Ilustración 44. La nube LTE, una red de banda ancha inalámbrica para seguridad pública.	110
Ilustración 45. Infraestructura de Seguridad en la Nubes.	113
Ilustración 46. Solución de seguridad para la nube y el centro de datos, con la integración de la plataforma <i>Deep Security</i>	120
Ilustración 47. Cyber-ataques a Skype, Nvidia, Xbox-life, entre otras compañías de IT.	121
Ilustración 48. Tendencias de ataques durante el 2014.	121
Ilustración 49. Motivos detrás de los ataques.	122
Ilustración 50. Top 10 de Cyber-ataques.	122
Ilustración 51. Entidades más atacadas.	123
Ilustración 52. Beneficios más valorados de la LFPDPPP.	127
Ilustración 53. Proporción de empresas que han incurrido en el incremento de costos de operación.	129
Ilustración 54. Resumen gráfico, Capítulo III.	130
Ilustración 55. Resumen gráfico, Capítulo IV.	147
Ilustración 56. Esquemmatización de la plataforma EVA, UNAPEC.	161
Ilustración 57. Diagrama de RPO y RTO.	170
Ilustración 58. Distribución jerárquica de los comités.	191
Ilustración 59. Estándares internacionales.	214
Ilustración 60. Modelo de organigrama.	216
Ilustración 61. Infraestructura tecnologica de UNAPEC, despues de la ejecuciion de un Plan de Continuidad de Negocios.	217
Ilustración 62. Proceso de descarga e instalación de los módulos de comunicación PHP.	222
Ilustración 63. Reparación de ramas disponibles, rastreo y chequeo de la versión.	222
Ilustración 64. Directorio <i>my.cnf</i> de MySQL para cambiar la ruta de almacenamiento por defecto al <i>innodb</i>	223
Ilustración 65. Interfaz gráfica de Moodle donde se elige un idioma para la instalación del mismo.	223

Ilustración 66. Chequeo de parámetros de correcta instalación de Moodle. ..	224
Ilustración 67. Creación de usuarios como administrador de cuentas y del sistema Moodle.	224
Ilustración 68. Creación de usuarios como administrador de cuentas y del sistema Moodle.	225
Ilustración 69. Configuración de la página frontal de Moodle. Requieren campos como el nombre completo de sitio, así como un nombre corto del mismo y un pequeño resumen.....	225
Ilustración 70. La administración de autenticación permite decidir cómo se desea configurar la registración de cuentas, si el usuario por su propia cuenta o si el por parte del administrador.....	226
Ilustración 71. Moodle instalado y configurado. Página de inicio de Moodle. .	226
Ilustración 72. Configuración para la creación de un nuevo curso.....	227
Ilustración 73. Descripción del curso y archivos a subir (PDF, Word, .JPG, etc.)	227
Ilustración 74. Se muestran más configuraciones para el curso a crear, como formato, apariencia, archivos y límites de tamaño de subida, acceso de invitado, grupos y roles asignados para quienes necesitan una descripción del rol de ese usuario.....	228
Ilustración 75. La opción para el formato permite especificar si se desea poner el curso como visible o no visible, también se especifica cuantas secciones se permiten a ese curso creado por tiempo definido. La apariencia configura que parámetros deseas tener en tu entorno virtual.	228
Ilustración 76. En <i>files and upload</i> puedo decidir qué tamaño de subida pueden los estudiantes y docentes subir al EVA, también presenta la opción de invitado para aquellos que pueden acceder al EVA temporalmente con o sin contraseña. La opción de grupo permite la interacción y realización de actividades en grupo.	229
Ilustración 77. Esta es la página con los parámetros del curso creado.	229
Ilustración 78. Esta es la página cuando accedemos al curso.	230

Índice de tablas

Tabla 1. Usuarios ante la tecnología de la nube. _____	37
Tabla 2. Tráfico y carga de trabajo en la nube. _____	44
Tabla 3. Tecnologías Cloud Computing en organizaciones. _____	52
Tabla 4. Segmentos más grandes del mercado de <i>Plataform as a Service</i> . ____	55
Tabla 5. Pronóstico del mercado PaaS. _____	56
Tabla 6. Acrónimos “as a service”. _____	59
Tabla 7. Estadística de la utilización de internet mundialmente. _____	60
Tabla 8. Distribución de los protocolos API y estilos. _____	65
Tabla 9. Fases del protocolo SSL. _____	74

AGRADECIMIENTOS

Gracias a Dios por permitir tener en mi camino, los mejores pilares, quienes han forjado la base perfecta para poder llegar a este punto tan importante en mi vida y prometerme seguir creciendo cada vez más, gracias a su apoyo incondicional, enseñanzas y el cariño irremplazable.

- Mis padres, *Guillermina A. Ventura* y *Ricardo A. Rosario*.
- Mis abuelos, *Yolanda Mora* y *Félix Ant. Ventura*.
- Mis tíos, *Félix A. Ventura*, *Jorge L. Quetglas* y *Elizabeth A. Ventura*.

Gracias a *José Arismendy Almonte*, *Belky M. Rodríguez*, *Milagros Contreras*, *Ingrid Pérez*, *Cecilia* y *Alba Rhina Hernández* por estar siempre presente y servir de zapata para mi vida personal y capacitación profesional. Tías, madrina, han sido mis mejores madres. ¡Gracias!

Agradezco a mi asesor, *Ing. Rafael Santo Navarro*, por su dedicación, esfuerzo y voluntad, por apoyarnos en todo momento y estar siempre presente, guiándonos durante la realización de este trabajo.

Gracias a quienes son más que profesores, han sido guías, instructores, maestros y amigos, *Alexander Almonte*, *Ramón María Gómez*, *Oswaldo Mota* y *José Joaquín Hernández*. Agradezco a mis compañeros de trabajo de grado, *Gabriel Tolentino* y *George A. Jiménez*, por aceptar, crecer y disfrutar en esta experiencia conmigo, a mis compañeros de la Universidad, que sin lugar a dudas siempre estuvimos juntos, en las buenas y en las malas, no solo hemos sido compañeros, hemos sido hermanos de trabajo, estudio, insomnio, proyectos y muchas otras aventuras que compartimos en el transcurso de estos 4 años juntos.

Jesús Ant. Martínez, gracias por tu apoyo incondicional, por estar siempre ahí para mí, enseñarme y aconsejarme durante este trayecto tan importante en mi vida. ¡Gracias!

Agradezco a quienes me han encaminado en el ámbito práctico, mi equipo de trabajo tecnológico, quienes han sido un libro abierto, gracias *Luis Félix García*, *Martín Feliz Cabrera*, *Ariel Isaac Moisés*, *Marlín Capellán* y *Jean Carlos Mejía*.

¡Gracias a todos!

Paula Rosario Ventura

AGRADECIMIENTOS

Expreso mi agradecimiento a Dios por poner en mi camino aquellos conocimientos claves para el entendimiento y la realización de esta investigación.

A mis padres, Jacinto Tolentino y María Magdalena, por el apoyo incondicional, sus enseñanzas, gran afecto y amor que me regalaron desde mis primeros pasos.

Mi hermano Gustavo Tolentino, influencia principal de adentrarme al mundo de los sistemas y la tecnología.

Mi mejor amigo de toda la vida, Emmanuel Santiago Iglesias, por enseñarme a no rendirme ante los obstáculos y cumplir mis metas por más imposibles que parezcan.

A mi maestro y mentor Eric Henoc Peña, por motivarme y guiarme en el mundo de las redes y la informática.

A mi asesor Rafael Santos Navarro, por orientarnos y guiarnos en la realización de este trabajo.

A Yasmin Alejandra, por su apoyo y amor incondicional en todo momento.

Mis compañeros de trabajo de grado, Paula Rosario y Leorge Jiménez, por ayudarme y apoyarme a completar la investigación de la tesis.

Por último, a mis familiares y amigos, por brindarme sus cariños y confianzas de tener las fuerzas de completar este trabajo.

Gabriel Tolentino

AGRADECIMIENTOS

En primer lugar antes que todo quisiera agradecer a Dios por haber estado siempre conmigo, guiándome a lo largo de mi carrera, dándome animo en los momentos de tristeza, fuerzas en los momentos de debilidad, perseverancia en los momentos de desesperanza y por brindarme una vida llena enseñanzas, experiencias y esperanza para un nuevo futuro.

Quiero agradecer a mis padres Gerges Leonte Jimenez y Rosa Elba Peralta porque sin ellos nada de esto habría sido posible, muchas gracias por estar siempre en todo momento, educándome, apoyándome, inculcándome en los buenos valores y sobre todo por ser un excelente ejemplo de vida a seguir. A mis familiares, hermanos Rossyger Z. Jimenez Peralta y Roger A. Jimenez Peralta, por ser parte importante en mi vida, así como los mejores hermanos que la vida me pudo dar, mis tíos y tías: Milagros Peralta, Altagracia Hilario, Rafael Lozada, Leda Jimenez y Wilson Jimenez por transmitirme su apoyo y motivación. A mis abuelos, primos y todos mis amigos que formaron del este trayecto que tuve que recorrer en mi vida.

A José Andrés Mezquita Fabián y Alan Maireni, por brindarme su amistad incondicional; gracias por escucharme y estar conmigo en todo momento. A Orlando Mezquita Gómez ya que sin su apoyo no hubiera podido terminar este trabajo de grado.

A mis compañeros de la universidad Eulises Mesa, Arturo Silva, Ángel Marcalle y Víctor Reyes por haberme seguido apoyando en el transcurso de la carrera.

Estoy sumamente agradecido con mis compañeros de trabajo de grado que estuvieron junto a mí caminando en este recorrido y acompañándome en la realización de este trabajo en todo momento. También estoy agradecido con nuestro asesor Santos Rafael Navarro por darnos una mejor visión de algunos puntos del trabajo y por habernos brindado su fuente de conocimiento para que este trabajo saliera a flote. Y finalmente estoy agradecido con todos los profesores de la universidad APEC, Por habernos brindado una excelente formación académica para el desarrollo y realización de este y futuros proyectos.

¡Mil gracias a todos!

George A. Jiménez

DEDICATORIAS

Es tiempo de retribuir un poco, le dedico mi trabajo de grado a quien empezó a caminar conmigo, a quien siempre estuvo ahí, quien guió mis primeros pasos, forjó en mí una dama, encaminó mi formación personal y capacitación profesional, inculcándome valores y principios, siempre como ejemplo del saber.

Te dedico mi trabajo, abuela querida, Yolanda Mora, eres por quien vivo y desvivo para hacer sentir orgullosa cada día de mi vida, espero que te sientas así. ¡Gracias!

Para ti...

Abuela.

Paula Rosario

DEDICATORIAS

El presente trabajo se lo dedico a mi madrina Caridad Sofía Fernández (fallecida), por su amor y cariño como una segunda madre.

Gabriel Tolentino

DEDICATORIA

Quiero dedicarle este trabajo de grado primero a Dios ya que sin el nada tiene sentido en mi vida y a cinco personas importantes en mi vida: mis padres, Gerges Leonte Jiménez y Rosa Elba Peralta quienes siempre han estado para mí, mi abuela, Carmen Luz, por todos sus cariños y consejos que me ha impartido en la vida y a mis tías Altagracia Hilario y Milagros Peralta que siempre me han brindado su amor y apoyo.

George A. Jiménez

Elaboración de un plan de continuidad de negocios para la disponibilidad
en la plataforma web Moodle de la Universidad APEC,
Santo Domingo, R. D., 2015.

INTRODUCCIÓN

La computación en la nube es una tecnología en constante crecimiento que se ha posicionado en un mercado competitivo con otras tecnologías tradicionales. Las empresas y los usuarios se ven beneficiados enormemente al tener alojados aplicaciones, archivos o máquinas virtuales en un servidor dedicado o compartido de un proveedor de servicios en la nube.

El servicio de internet y un host, son los requisitos mínimos, estos son los componentes necesarios para acceder a los recursos de servicios en la nube en cualquier parte del mundo, no obstante, el hecho de tener esta disponibilidad a través de internet, genera una gran ventaja pero también una desventaja, debido que la información es vulnerable y codiciada, representando un riesgo a compañías normatizadas.

Sin embargo, existe un estándar seguro y recomendable por la Organización Internacional de Estandarización (ISO) para evitar estos inconvenientes que podrían convertirse en pérdidas económicas y no recuperables para una organización.

La ISO define el estándar como ISO 22301 o también llamado Plan de Continuidad de Negocios, un plan analizado, preparado, revisado y con fines de ejecución en caso de un desastres y/o eventualidades perjudiciales para entidades.

En esta investigación se pretende integrar una nueva generación de las tecnologías, conocida como *Cloud Computing*, para mejorar la disponibilidad de web Moodle de la Universidad APEC, conocida como "Plataforma EVA", con el propósito de mantener los servicios de los clientes externos y sus operaciones.

Cloud Computing es un sistema de almacenamiento basado en la conectividad a internet y en *data centers* remotos, permitiendo la integración de servicios (*Software as a Service*, *Plataform as a Service* e *Infraestructure as a Service*) para desarrollar esta nueva tecnología.

La data tiene un papel fundamental en todos los *data centers*, respaldar la seguridad de la información debe ser el motivo principal de toda operación, para ello, se han elaborado técnicas de prevención y rápida recuperación de la información, dando lugar a los planes de continuidad de negocios.

La plataforma EVA será evaluada por factores críticos para determinar la capacidad de tener sus servicios disponibles ante cualquier desastre, la gobernabilidad, la gestión de la información, las políticas, regulaciones y los acuerdos con proveedores.

Se elaborará un Plan de Continuidad de Negocios (BCP) para garantizar una inmediata respuesta ante cualquier tipo de evento, basado en estándares (DR – BCP: ISO-IEC 24762 / NFPA 1600) y en las mejores prácticas.

CAPITULO I. ASPECTOS GENERALES

1.1 Aspectos generales

Hoy en día existen plataformas tecnológicas conocidas como Sistema de Gestión de Contenido de Aprendizaje (LCMS) que permiten la capacitación y certificación a distancia, por ejemplo: "Moodle" es una de las plataformas más utilizadas en todo el mundo, traducida a 86 idiomas, con más de 67,000 sitios registrados.

En el caso de la Universidad APEC, han implantado un Entorno Virtual de Aprendizaje (EVA), esta tiene como base esta aplicación web, Moodle (desarrollada en PHP "*opensource*"). Esta se utiliza para impartir cursos modulares basados en Internet que admiten una pedagogía del construccionismo social moderno, permitiendo al docente enseñar sin fronteras.

La universidad está presentando inconvenientes con la disponibilidad en los servicios cuando el tráfico está en su máxima capacidad. Actualmente, el Plan de Continuidad de Negocios no está implementado en el Entorno Virtual de Aprendizaje (EVA) de la Universidad APEC, pero este sistema podría ayudar al mejoramiento de la plataforma facilitando la administración del sistema, reduciendo los gastos de inversión y mantenimiento del espacio físico.

Los archivos que se suben al EVA son guardados en una caja de Red de Área de Almacenamiento (SAN), se almacenan alrededor de setenta a cien gigabytes por cuatrimestre y se realiza una copia de los datos para sacar la información del sistema. Actualmente, UNAPEC cuenta con más de 8,202 estudiantes¹, una universidad con una población estudiantil muy numerosa y que cada cuatrimestre incrementa significativamente.

La plataforma EVA no tiene ninguna función de ofrecer almacenamiento, debido a que su principio de creación ha sido la interacción docente-estudiante sin límites. Sin embargo, esto podría ser un desperfecto para aquellas mentes que solamente se mantienen en la función de lo que realiza una aplicación y puede que no vean una nueva funcionalidad para mejorar la plataforma. La aplicación web "Moodle" es adaptable y permite evolucionar, continuar mejorando su desempeño debido a la facilidad que brinda el "*opensource*", la plataforma EVA ha sido adaptada a las

¹Este valor fue tomado a finales del pasado año (2014), dado que UNAPEC incrementa su público estudiantil periódicamente, este valor es superior a la actual fecha.

necesidades de la universidad APEC, ¿no se ha vuelto una necesidad mantener los recursos bibliográficos del estudiante?

Además de estar ignorando una posible nueva funcionalidad, la plataforma ha estado presentado problemas por fallas de accesibilidad durante el tiempo pico (alto tráfico de usuarios) en semana de parciales, donde la situación se torna aún más complicada.

Entre las diversas interrupciones podemos especificar el acceso al EVA durante el mantenimiento a la base de datos, esta interrupción puede ser considerada como grave debido a que los estudiantes necesitan la plataforma disponible en un 98% del tiempo aproximadamente, para la realización de sus asignaciones o tomar exámenes.

Si este tipo de problema continúa presentándose sin ser transparente para el usuario, el EVA no sería un entorno virtual de aprendizaje eficaz. La plataforma no cuenta con un plan de continuidad de negocios que absorba esta falla, de acuerdo a lo expresado por el Ing. Ricardo Pérez, Encargado del departamento de Infraestructura.

No obstante, cuando están haciendo un mantenimiento a la aplicación Moodle, las materias del estudiante y del docente no se visualizan al momento de acceder al EVA. Para un profesor, que maneja grandes cantidades de materias, no poder encontrar a tiempo la materia en su entorno virtual para la asignación de una tarea o habilitar un examen, se traduce en pérdidas de tiempo y que a su vez genera pérdidas monetarias.

1.2 Computación en la nube (Cloud Computing)

En el libro *Computación para docentes*, aclara que la evolución de las tecnologías de la información y la comunicación está mostrando una fuerte tendencia a la conectividad, al abandonar paulatinamente el uso exclusivo de las computadoras de escritorio para sustituirlas por otros sistemas informáticos centrados en la conexión a internet desde diferentes dispositivos tales como los *Smartphone*, *netbooks* o *tablets*. En el marco de esta tendencia, el almacenamiento en la nube

comienza a ocupar un lugar destacado. Pero como toda implementación de un nuevo sistema, presenta ventajas y desventajas, como podemos ver:

1.2.1 Ventajas

Para José Juan Mora Pérez, el punto de vista de un usuario que contrata un servicio alojado en la nube, existen una serie de ventajas que debemos conocer antes de migrar a algún servicio de almacenamiento en la nube. Entre las ventajas podemos citar:

- a. Solo se paga por lo que se usa.** Esta característica genera un ahorro directo, ya que con el modelo de nube, no hay que repercutir conceptos como los costes de mantenimientos de *software* y *hardware* o las inversiones para la aplicación de infraestructura en caso de que nuestro negocio necesite crecer, solo se debe pagar por los recursos consumidos en la nube.
- b. Se reducen los tiempos de desarrollo del negocio.** Cuando nos planteamos utilizar un servicio en la nube solo debemos contratar el servicio con unos requerimientos mínimos para que pueda sostener la implementación del negocio que vamos a realizar y pagar más cuando el servicio comience a ser utilizado. Montar maquetas es un proceso sencillo y barato ya que no necesitamos realizar una inversión en infraestructura IT, únicamente contratamos un servicio en la nube, creamos maqueta y comprobamos si es viable la implementación del negocio, una vez terminada la prueba podemos o bien terminar el contrato del servicio o reducir los recursos contratados para reducir el coste del servicio.
- c. Se reduce los problemas derivados de una plataforma IT.** El usuario no debe preocuparse por problemas como la escalabilidad o las copias de respaldo, la nube se encarga de todo, por lo que la organización no tiene que emplear ni tiempo ni recursos en mantener una infraestructura para el Negocio. La organización se puede concentrar en el desarrollo del negocio.

1.2.2 Desventajas

1. La conectividad es una dependencia absoluta.
2. Inseguridad del control y la protección de la información.

Como podemos observar en la lista de posibilidades es más amplia que la de limitaciones. En la era de la conectividad, no podemos ignorar el impacto de estas nuevas herramientas; es más bien necesario que se conozcan y apliquen como recursos educativos interesantes para que nuestros alumnos puedan adquirir las competencias que le permitan desempeñarse adecuadamente en la sociedad de la información. (Caccurri, 2012)

En el libro "Capacity Planning IT" presenta las siguientes desventajas:

- a. **No controlar la localización de los datos.** Un servicio en la nube puede almacenar los datos en distintas localizaciones y el usuario del servicio no tiene control sobre donde están sus datos. Esta falta de control puede suponer un problema dependiendo del carácter de los datos, valor de la información y la legislación de cada país.
- b. **El usuario debe preocuparse por los SLA (acuerdos de niveles de servicio).** La única herramienta que el usuario posee para garantizar el servicio que está contratando son los acuerdos de niveles de servicio (SLA), con lo que se medirá la calidad del servicio.
- c. **Inversión en comunicaciones.** Otra de las desventajas de utilizar servicios en la nube es que las comunicaciones con la nube deben ser lo suficientemente fiables como para garantizar el acceso a los servicios contratados. Además de la disponibilidad, deben asegurarse que el caudal de acceso a los servicios en la nube la calidad necesaria para el desarrollo del Negocio. Las comunicaciones externas son sensiblemente más caras que las comunicaciones internas.
- d. **La información "podría" ser accedida por terceros.** La gestión del acceso a la información se puede delegar a un proveedor de servicios en la nube, un problema de seguridad en dicho proveedor pudiera ser accesible por otras personas.
- e. **Los recursos no son infinitos.** Una de las características de los servicios en la nube es la elasticidad de los recursos, el proveedor no dará recursos según nuestras necesidades pero debemos ser conservadores con esta idea ya que un proveedor de servicio no puede dar recursos ilimitados y se

pueden encontrar situaciones donde nuestras necesidades de negocio requieran más recursos y el proveedor no puede suministrar lo necesario, quedando atrapado en un servicio y obligando a migrar con otro proveedor, dicha medida suele tener un coste bastante elevado.

1.3 Características

Un servicio de *Cloud Computing* debe cubrir todas las necesidades, esta nueva tecnología ofrece únicas características que provoca una aceptación rápida, como son:

- **Amplio acceso a la red:** Pueden acceder a los datos desde cualquier lugar. Esta característica es sumamente importante para empresas distribuidas geográficamente.
- **Pooling de recursos:** Permite compartir los recursos entre diferentes usuarios, abaratando costes y ampliando la disponibilidad.
- **Escalabilidad y rapidez:** Permite añadir o eliminar recursos. Por parte de *software*, la flexibilidad que permite la *cloud computing* es muy alta, debido a que se pueden incorporar nuevas funciones para todos los usuarios de forma rápida.
- **Servicio medible:** Permite un acceso transparente, es decir, el usuario y el proveedor pueden apreciar el consumo real de los recursos, permitiendo que el pago se realice por la cantidad de veces que el servicio realmente es utilizado.

Los proveedores de *cloud* utilizan diferentes modalidades de pago, como son:

- Pago por disponibilidad
- Pago por uso
- Pago por paquetes escalables

1.4 Tipos de infraestructuras de nubes

Hasta ahora, ha habido una tendencia de las nubes a evolucionar a partir de las soluciones privadas para administrar la infraestructura local y la cantidad de solicitudes para asegurar la disponibilidad de los datos altamente solicitados.

Debido al hecho de que los centros de datos que inician las capacidades de las nubes utilizaron las características para propósitos internos, considerando la venta de las capacidades al público (las nubes públicas). Al momento de que los proveedores han adquirido la confianza en la publicación de esta tecnología y han expuesto las características de las nubes con soluciones híbridas de emergencia. Este movimiento de público/privada a través de soluciones combinadas a menudo se considera una evolución "natural" de estos sistemas, aunque no hay ninguna razón para que los proveedores no utilicen soluciones híbridas, una vez las tecnologías necesarias han alcanzado una posición suficientemente madura. (Caramirezbe, 2012)

Para Daniel Peña Valenzuela y Juan David Bazzani Montoya, en su libro "Aspectos legales de Computación en la Nube" los diferentes tipos de infraestructura de nubes son:

1.4.1 Nubes privadas

En la investigación documental "Computación en la nube: Sistema de base de datos y servicios a usuarios con enlace a internet" describe que las nubes privadas son generalmente propiedad de la respectiva empresa y/o arrendados. Las funcionalidades no son expuestas directamente al cliente, aunque en algunos casos con los servicios de *cloud computing*, las características mejoradas pueden ofrecer *software* como servicio desde el punto de vista del cliente.

Germread, expone algunas medidas de seguridad mínimas que se deben tener configuradas en una nube privada, como son:

- Utilización de privilegios mínimos.
- Uso de *firewalls*.
- NICs separados para la administración.
- Separar los recursos entre las distintas unidades de negocio o áreas de la organización.
- Delegar la seguridad de los accesos a la unidad de negocios para que a través de un portal de autoservicio, se auto-provisionen los recursos a fin de correr la aplicación o el servicio.

- Encriptar los datos y tener cuidado de cómo almacenar y administrar las llaves de encriptación que te permitan acceder a los datos almacenados en la nube.
- Utilizar tecnologías fuertes y establecidas de criptografía.
- Automatizar la operación de seguridad con servicios de monitoreo para identificar y actuar cuanto antes.



Ilustración 1. Nube privada.

Un buen ejemplo de nubes privadas sería un banco que almacene y maneje sus informaciones en una cloud interna, gestionando todos los servicios solo para satisfacer sus necesidades.

Además, un ejemplo "tangible" es la Universidad Europea de Madrid, quien ha migrado sus laboratorios virtuales a una nube privada de Microsoft.

Fuente: Imagen propia.

1.4.2 Nubes públicas

Las empresas pueden utilizar la funcionalidad de "cloud computing" de entidades que ofrecen su propio servicio a usuarios externos de la empresa. Proporcionando al usuario la capacidad real para explotar la característica de las nubes para sus propios fines o también permite a otras empresas externalizar sus servicios de dichos proveedores en la nube, reduciendo así los costes y el esfuerzo para construir su propia infraestructura. (Laguna, Marcano, Montilla, & Muñoz, 2012)

En el libro "Cloud Computing" dice que este modelo de implementación requiere de la articulación de una política de seguridad y protección de datos de gran exigencia por parte del proveedor.



Ilustración 2. Nube pública.

Fuente: Imagen propia.

1.4.3 Nubes híbridas

De acuerdo a la investigación documental "Computación en la nube" realizada en Venezuela (2012) "a pesar de que las nubes públicas permiten a las empresas a externalizar parte de su infraestructura a proveedores de *cloud*, donde al mismo tiempo, perdería el control sobre los recursos, la distribución, la gestión de código y datos. Las nubes híbridas consiste en un trabajo en común de infraestructuras, de nubes públicas y privadas con el fin de alcanzar un máximo de reducción de costos mediante la contratación externa, manteniendo el grado deseado de por ejemplo, el control sobre los datos confidenciales mediante el empleo de las nubes privadas locales."

Uno de los beneficios más importantes con las que cuenta este tipo de *cloud* es que ofrece una mejor seguridad y una protección superior de los activos de la información.



Ilustración 3. Nube híbrida.

El propósito de una nube híbrida es alcanzar reducción de costos máxima mediante una contratación externa.

Fuente: Imagen propia.

1.4.4 Nubes de comunidad

Normalmente los sistemas de nubes se limitan a la infraestructura local, es decir, los proveedores de las nubes públicas ofrecen su propia infraestructura a los clientes. Aunque el proveedor realmente podría vender la infraestructura de otro proveedor, las nubes no las infraestructuras desagregados para construir más grandes, estructuras transfronterizas.

Por ejemplo: "Las organizaciones más pequeñas pueden reunirse sólo para poner en común sus recursos para la construcción de una comunidad privada de nube. Como contraposición a esto, los revendedores, como Zimory² de mayo en común los recursos de nubes de diferentes proveedores y los revenden."



Ilustración 4. Nube de comunidad.

Tres diferentes empresas compartiendo recursos para elaborar una comunidad privada en la nube.

Fuente: Imagen propia.

² **Zimory:** Es una compañía de desarrollo de soluciones inteligentes para proporcionar facilidades en los procesos de la solución IaaS.

RESUMEN

Los entornos virtuales de aprendizaje o plataformas virtuales surgieron con por la necesidad de interconectar comunidades escolares, poder crear un banco de recursos, crear un lugar de colaboración y poder gestionar la enseñanza - aprendizaje sin fronteras. Debido a una necesidad, también ha surgido la computación en la nube, que está marcando la innovación dentro de las nuevas tecnologías, prestándose para ser la solución a grandes problemas de disponibilidad, costo, almacenamiento, entre otros.

¿Qué tan factible sería tener una plataforma virtual en la nube? Los recursos y la demanda se mantendrían en equilibrio, se garantiza la disponibilidad y la accesibilidad siempre que haya conectividad.

Resumen gráfico del Capítulo I. ASPECTOS GENERALES

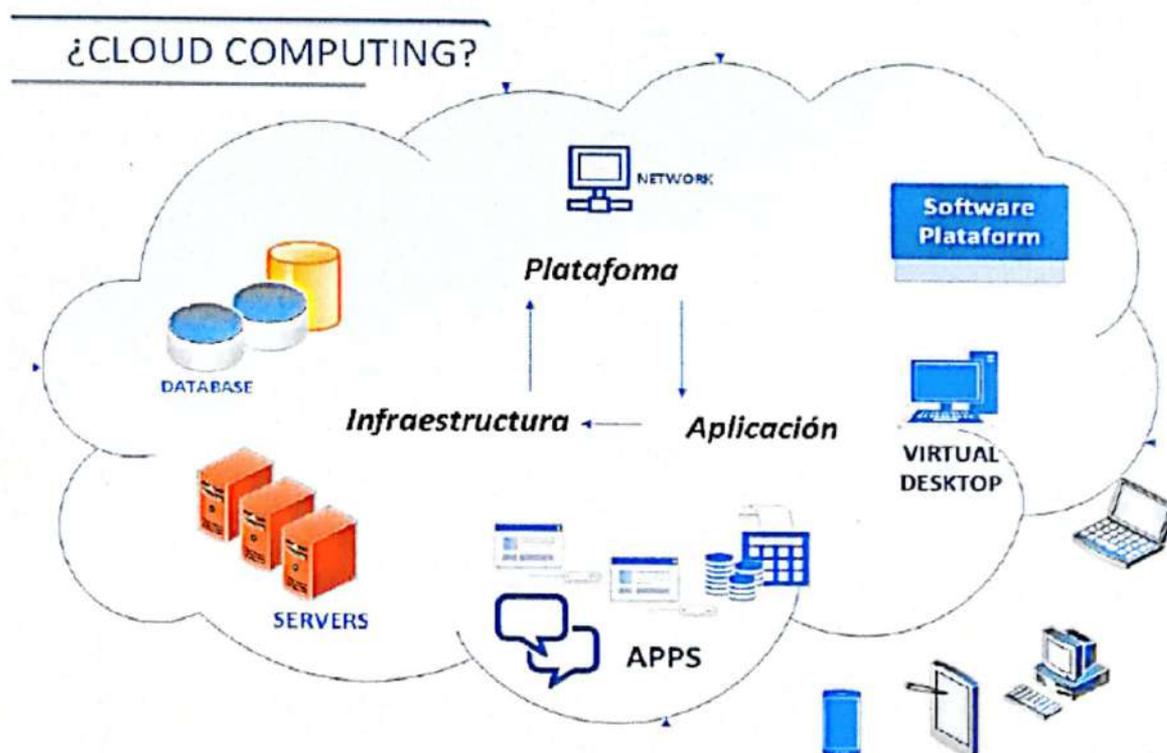


Ilustración 5. Resumen gráfico, Capítulo I.

Fuente: Imagen propia.

CAPITULO II. COMPONENTES DE LA NUBE

2.1 Clientes

La computación en la nube implica el uso de recursos informáticos que son ofertados por proveedores de *cloud*, son tratados en grandes *data center* remotos y entregan servicios a diferentes usuarios que acceden por medio de cualquier dispositivo con conexión internet.

Durante el 2015 *cloud computing* tendrá un público activo con más de 180 billones de usuarios aproximadamente, integrados a empresas como *Google*, *Microsoft*, *Salesforce*, *IBM* o *Amazon* que han integrado esta nueva tecnología.

Los proveedores obtienen ingresos económicos a nivel escalables, es decir, realizan inversiones en equipos informáticos, infraestructuras y centro de procesos de datos buscando recuperar los costos invertidos inicialmente y ganancias agregadas por los consumidores.

Esto trae ventaja para los clientes que no poseen grandes recursos económicos para invertir en una infraestructura tecnológica, pues los mismos prefieren pagar por un servicio con costos que varían debido a que las tarifas son pagadas por uso. Los clientes buscan satisfacer sus necesidades más simples de una manera flexible y escalable en su infraestructura.

La computación en la nube reúne todas estas características, siendo el modelo preferible por los mismos.

A partir del 2012 se ha visto un incremento excesivo en la utilización del *cloud*, tanto que las compañías han ido implementando estos servicios a su cartera de ofertas, garantizando resguardar las informaciones con una alta disponibilidad y acceso desde cualquier lugar con conexión.

En la siguiente gráfica se muestra el incremento porcentual desde octubre del 2012 en servicios multimedia en *cloud*.

Usuarios en Internet que utilizan servicios multimedia en la nube en el continente Americano, Octubre 2012

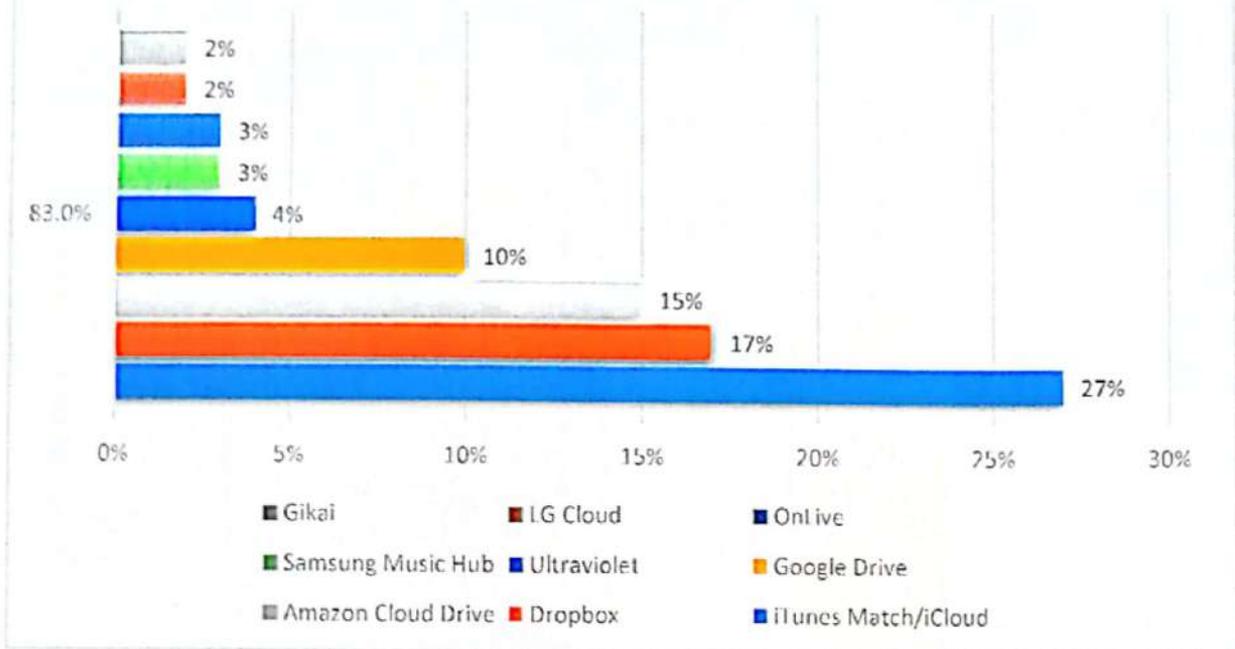


Ilustración 6. El uso de servicios multimedia en la nube.

El uso de los servicios multimedia en la nube ha beneficiado enormemente la compañía Apple durante octubre del 2012, siendo la compañía más solicitada por el uso de su aplicación iTunes ejecutada en la nube.

Fuente: (Ritcher, 2013)

La razón de que los usuarios han aceptado la tecnología *cloud* ha causado un incremento significativo la utilización de este tipo de almacenamiento en estos últimos años.

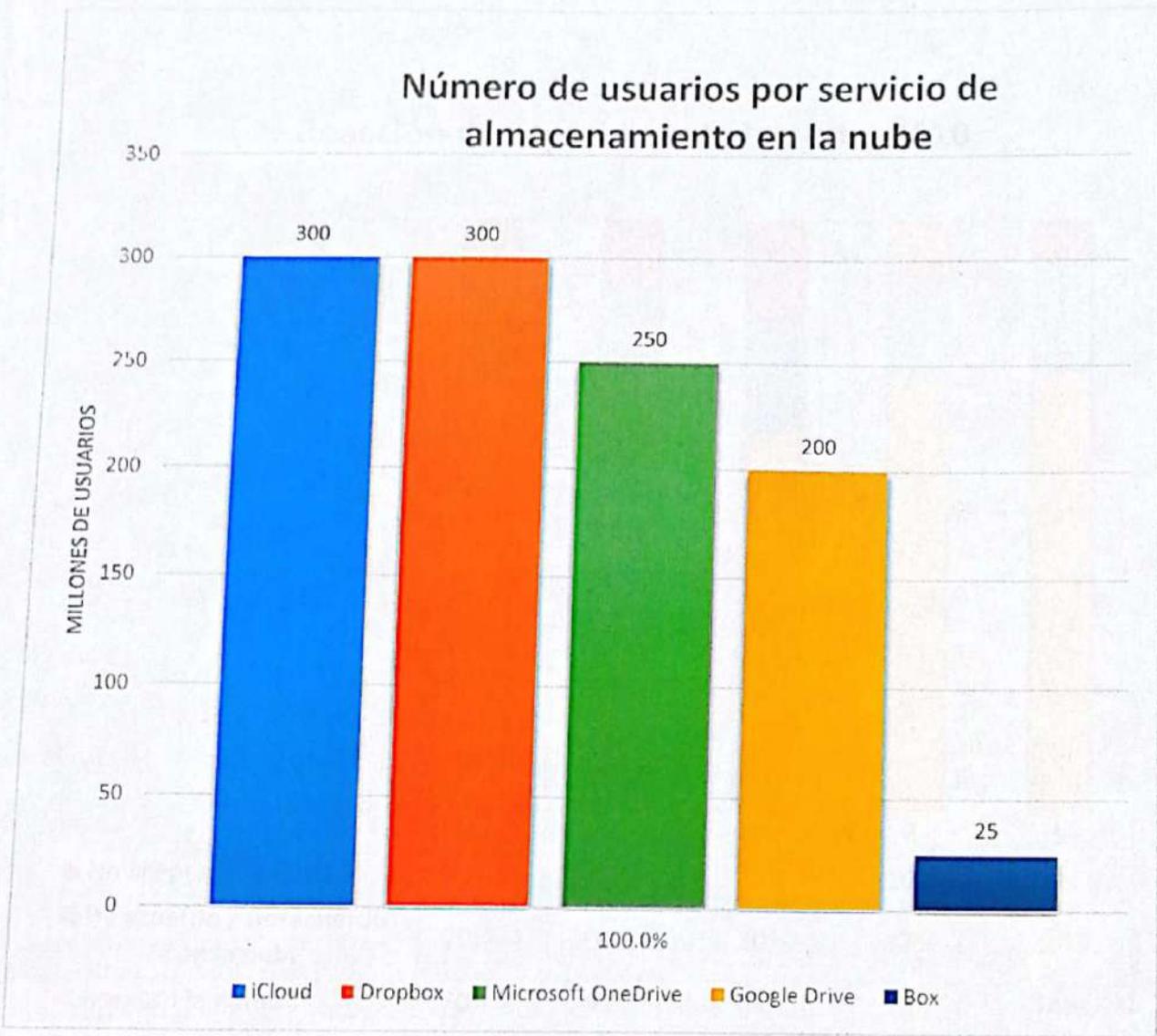
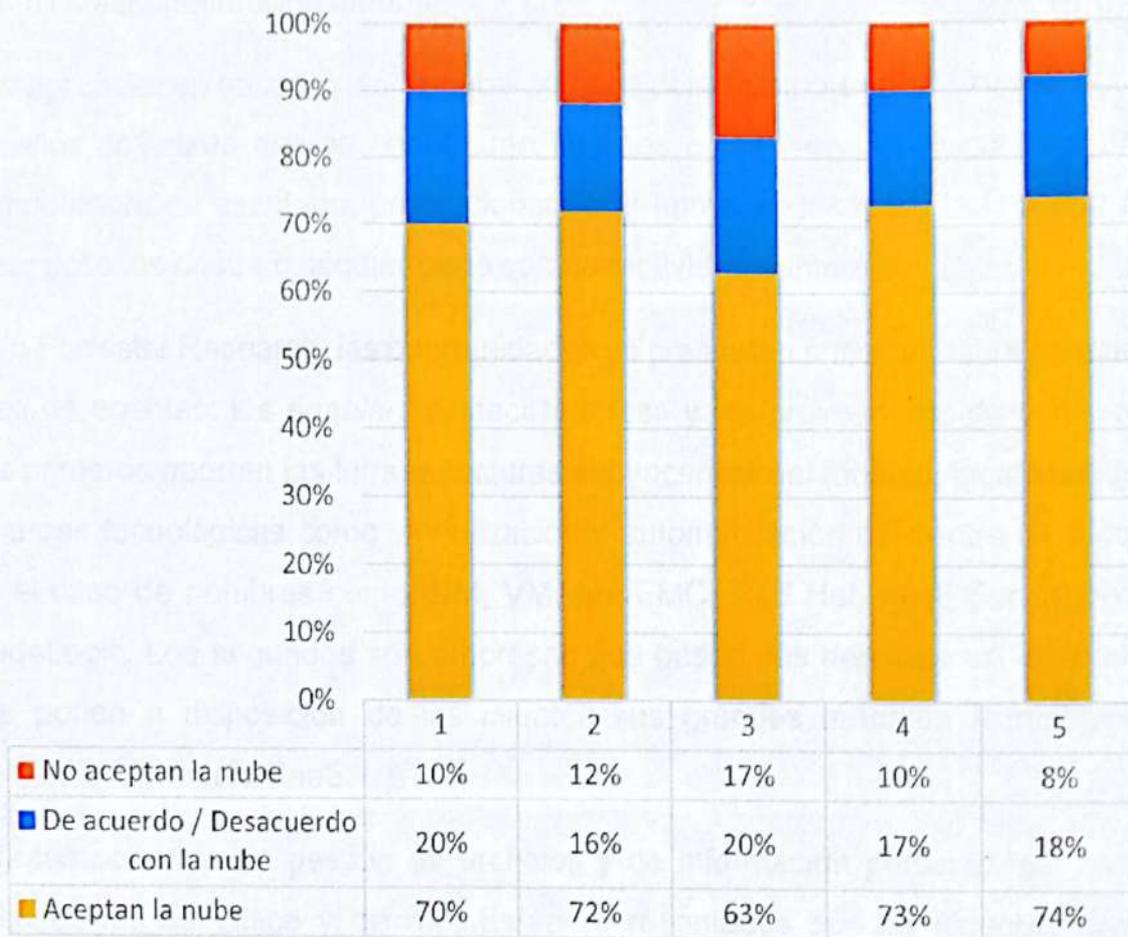


Ilustración 7. Usuarios por servicio de almacenamiento en la nube.

El número de usuarios por servicio de almacenamiento en la nube ha crecido enormemente, de manera que esta tecnología se ha diversificado y diferentes entidades tienen una plataforma que ofrece estos servicios.

Fuente: (Danova, 2014)

Reacción de usuarios ante la nube, 2010



Columna 1: Simplifica los procesos administrativos de TI.

Columna 2: Improvisa experiencia a usuarios finales.

Columna 3: Decebe los desafíos de TI en base a rendimiento.

Columna 4: Representa la reducción de costos de infraestructura.

Columna 5: Alivia las

■ Aceptan la nube ■ De acuerdo / Desacuerdo con la nube ■ No aceptan la nube

Tabla 1. Usuarios ante la tecnología de la nube.

Durante el 2010, más del 63% de los usuarios se acomodaron al uso de la tecnología en la nube, trayendo consigo grandes reducciones de costos e inversiones.

Fuente: (Cloud Hyper Market, 2010)

Las compañías operan de una manera más unida con sus clientes y proveedores, donde estos deben ser aún más competentes para resolver con urgencia a los cambios esta interacción amerita.

Las aplicaciones basadas en la nube se consideran como una alternativa hacia aquellos *softwares* que se encuentran internos en un servidor físico o en una computadora de escritorio, proporcionando el apoyo necesario y la facilidad de tener accesos desde cualquier parte con conectividad a internet.

Para Forrester Research, las oportunidades se presentan principalmente para dos tipos de agentes: los *enablers* o «facilitadores» y los proveedores de servicios. Los primeros aportan las infraestructuras subyacentes del modelo, focalizándose en áreas tecnológicas como virtualización y automatización del centro de datos. Es el caso de nombres como IBM, VMware/EMC, Red Hat, Intel, Sun, Citrix o BladeLogic. Los segundos son empresas que basan sus negocios en Internet y que ponen a disposición de los clientes sus grandes entornos tecnológicos siguiendo el modelo SaaS.

Ofrecen servicios de gestión de archivos y de información personal, así como aplicaciones de Office y de red. Están representados por los gigantes como Microsoft y Google que, fieles a su estrategia empresarial, se adelantan a toda tendencia tecnológica, incluso creando escuela para otros. Sin embargo, también han irrumpido con fuerza otros nombres como Amazon, Salesforce o *Rackspace*.” (Fundación de la Innovación Bankinter, 2010).

Las exigencias de los usuarios se vuelven cada vez más complejas, lo que obliga a los proveedores a expandir y modernizar sus *data center*.

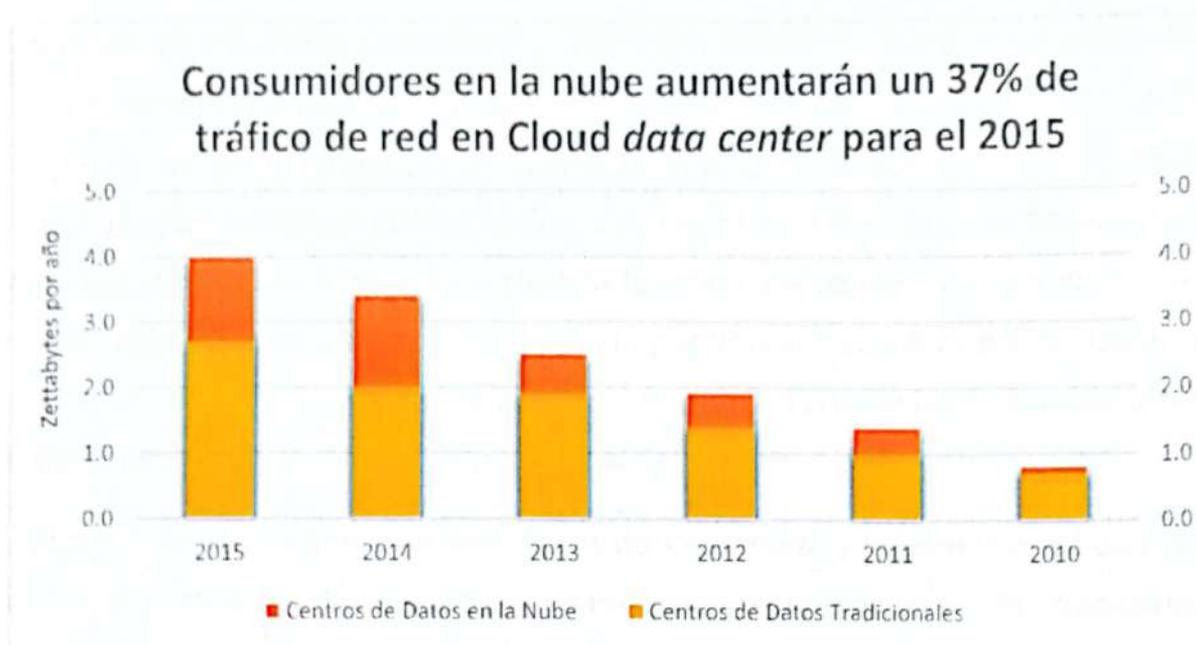


Ilustración 8. Tráfico de red originado por usuarios hacia los centro de *data centers*.

A medida que transcurre el tiempo, el tráfico de red, que será generado para el 2015 por los Data Center en la nube, significara un gran incremento por el uso de grandes, pequeñas y medianas empresas, así como de usuarios individuales.

Fuente: (Cisco Systems, Inc., 2011)

Sin embargo, la seguridad es un componente fundamental donde el cliente se detiene a ponderar antes de requerir un servicio en la nube. Los proveedores deben de asegurar la integridad de los archivos de los usuarios, de forma que no se comprometa el almacenamiento ni la carga/descarga de archivos. El cliente tiene derecho a conocer sobre los niveles de seguridad que el proveedor de *cloud computing* le ofrece, debe comprobar las medidas de seguridad, registros de acceso a los datos de los que tiene autoría y el proveedor es responsable de salvaguardar esa información.

La Agencia Española de Protección de Datos recalca que el proveedor de servicio de *cloud* debe comprometerse a garantizar la confidencialidad utilizando los datos sólo para los servicios contratados. Asimismo, debe comprometerse a dar instrucciones al personal que depende de él para que mantenga la confidencialidad.

También, es necesario pensar en los riesgos o catástrofes que puede presentar toda información o aplicación importante almacenada o ejecutada en la nube. Si el proveedor de servicios presenta una falla, la operatividad del negocio debe seguir un curso normal y como clientes, debemos tomar medidas preventivas para este tipo de inconvenientes. Una medida factible para conservar la disponibilidad del servicio y los datos, implementando la portabilidad de información, donde el cliente transfiere todos los datos y aplicaciones de un proveedor de servicio *cloud* a otro, o incluso a la infraestructura actual del cliente.

Actualmente, los clientes se benefician de los recursos de *Amazon (Cloud)* de diferentes formas, tales como: planes de recuperación ante desastres, infraestructura de escritorio virtual y control en los tiempos picos donde el usuario demanda mayores recursos de los que pueda ofrecer *Amazon*.

La compañía *Salesforce*³ desarrolló un sistema de gestión de recursos de clientes (*CRM*) ha pedido, impulsando la tecnología de *SaaS* para ofrecer más tarde la solución de *PaaS* de *Force.com*. Otros proveedores importantes están siguiendo estrategias similares comenzando por un mercado que ellos conocen y aumentan sus ofertas a medida que se sienten más cómodos con la plataforma *cloud*.

Cuando consideras adquirir un servicio hacia la nube es de suma importancia concentrarse en las capacidades del mundo real y los beneficios que ofrece trasladarse a ese modelo computacional, así como los riesgos que conlleva.

Esto es particularmente significativo en áreas de *IaaS* y *PaaS* donde muchos de la más vasta gama de productos, tales como el *Windows Azure*⁴ y *Blue Cloud* de *Microsoft* e *IBM* respectivamente, se encuentra en desarrollo constante para entregar resultados satisfactorios a sus clientes día tras día.

³ *Salesforce* (1999): Empresa informática dedicada a la venta de *software* para negocios, orientada a *CRM* (*Customer relationship management*).

⁴ *Windows Azure*: Es una plataforma como servicio donde se alojan aplicaciones para que se ejecute sobre su infraestructura hasta servicios de comunicación segura, esta se encuentra alojada en *Microsoft*.

2.2 Servicios de distribución

La computación en la nube nos brinda varios servicios de los cuales se puede elegir el que más conveniente para las necesidades y al mercado el cual se dirige. Los servicios de distribución de *cloud computing* se dividen en:

2.2.1 Infraestructura como servicio (*IaaS*)

El Instituto Tecnológico Metalmeccánico (AIMME) explica que *IaaS* consiste en la externalización de las máquinas de proceso de datos, como son: servidores, dispositivos de almacenamiento, enrutadores, entre otros. Gracias a la virtualización (separación física entre la infraestructura y el lugar donde transcurren las operaciones) se puede pagar por el consumo de recursos.

Las soluciones de *IaaS* dan la ventaja a la empresa de acceder a una serie de recursos informáticos que les resulta difícil económicamente de implementar en su compañía. Esta solución se caracteriza por tener un entorno en la nube, donde se paga por el uso de los dispositivos, las PYMEs utilizan este tipo de servicio por ser un modelo escalable y económico.



Ilustración 9. Proyección incremento del uso de servicios en la infraestructura *cloud*.

De acuerdo a la proyección del incremento de los servicios en la infraestructura de la nube a pesar de que SaaS está siendo más utilizado. Los servicios aumentarán un 59%, 28% y 13% respectivamente para el 2018.

Fuente: (Cisco Systems, Inc., 2014)

Otra característica del *IaaS* es que ofrece servidores dedicados. Los mismos permiten a las compañías tener conexiones más seguras y amplia diversidad de servidores para una gestión centralizada de la organización o alojamiento de aplicaciones, que no tendrían muchos beneficios y eficacia si estos se encontraran en un servidor compartido. *IaaS* también brinda sistemas de almacenamiento para las empresas con bases de datos grandes y medianas. Se debe tener en cuenta que el proveedor debe cumplir la ley de protección de datos 126-02 establecida por INDOTEL⁵ para los archivos que resguarde. Existen proveedores que ofrecen este tipo de almacenamiento y se comprometen con dicha ley de protección de datos para fortalecer los derechos del usuario y darle a conocer de manera confiada que sus archivos son importantes activos para su organización o para uso personal.

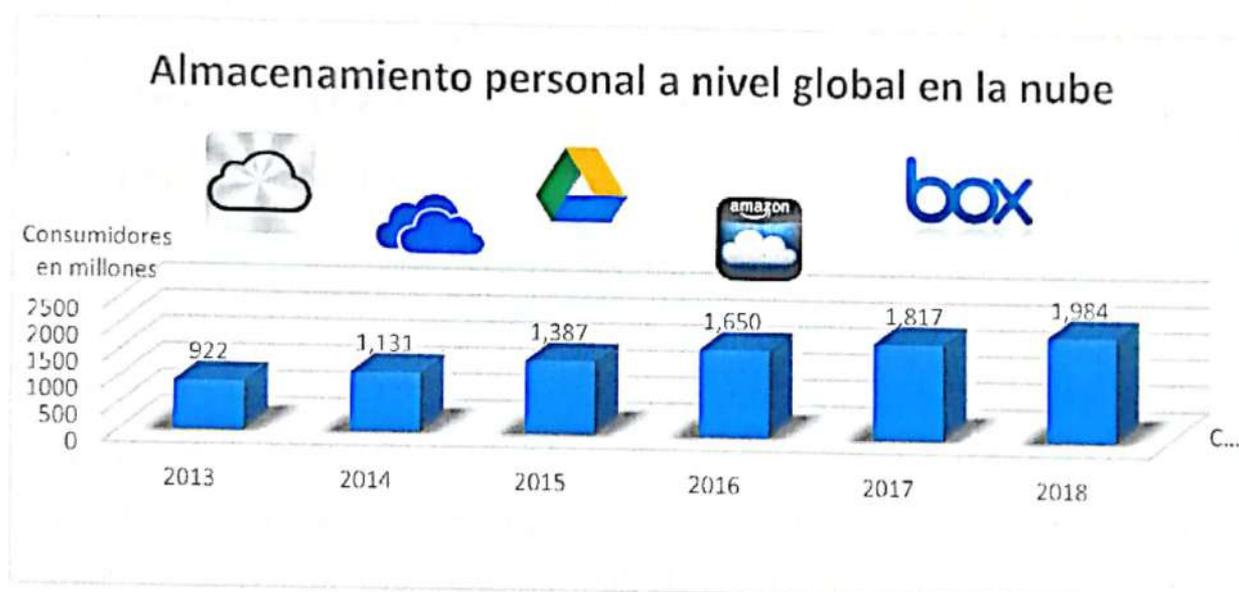


Ilustración 10. Almacenamiento personal a nivel global en la nube.

A nivel global, el almacenamiento en la nube seguirá ascendiendo para los próximos 3 años, favoreciendo aquellas compañías que ofrecen servicio de almacenamiento en la nube.

De acuerdo a CISCO y sus estadísticas de computación en la nube, para el 2018, el 53% de los usuarios de Internet usaran el almacenamiento en la nube. De la misma forma, la prestigiosa compañía de telecomunicaciones estima que para ese

⁵ INDOTEL: Organismo del Estado Dominicano, creado por la Ley General de las Telecomunicaciones (153-98) que regula y supervisa el desarrollo del mercado de las telecomunicaciones.

año casi un tercio de los usuarios que navegan en Internet habrán adoptado este tipo de servicio en toda Latinoamérica.



Ilustración 11. Almacenamiento personal en la nube en Latinoamérica.

En Latinoamérica, el incremento se verá de igual forma reflejado para el 2018.

Fuente: (Cisco Systems, Inc., 2014)

El recurso de las redes en *IaaS* da la conformidad de poder monitorear, gestionar y administrar las opciones de red de los servidores contratados de forma más fácil. Es posible indicar la velocidad del puerto que deseamos, así como también el ancho de banda, balanceo de carga, calidad de servicio y la configuración de seguridad de estos recursos de red. Una ventaja muy importante de la infraestructura como servicio es que podemos crear nubes privadas, que para estos casos, se prepararía al departamento de tecnología de la organización para proporcionar una configuración adecuada y sencilla. CISCO ha hecho un análisis con un *software* de análisis de tráfico de red en compañías que utilizan servicios *cloud*, y la cantidad de paquetes que viajan a través del internet por la demanda de estos servicios va en aumento cada año. Este tipo de análisis, le dio una ventaja a la compañía de telecomunicaciones para poder clasificar las velocidades necesarias que las compañías deben de adquirir para un correcto funcionamiento de aplicaciones que se manejan en la nube.

Tráfico en la nube y carga de trabajo

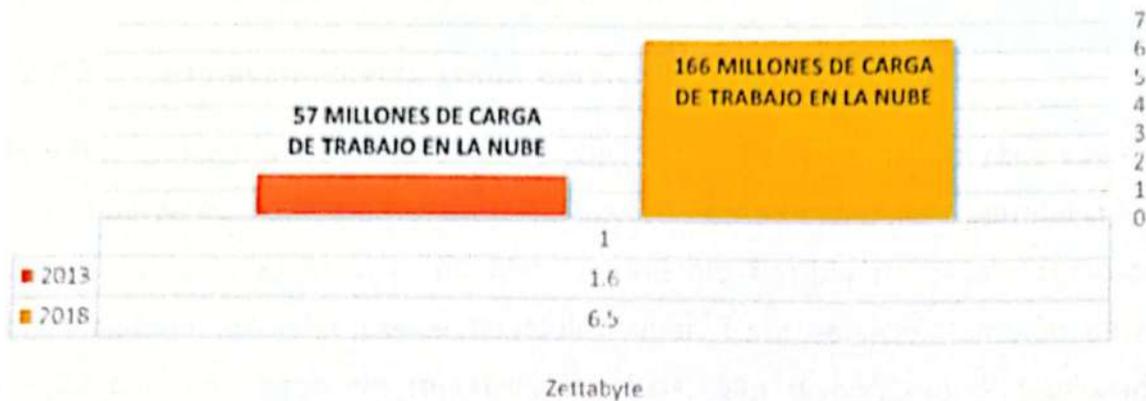


Tabla 2. Tráfico y carga de trabajo en la nube.

Sobre el 78% de las cargas de trabajos basada en la nube se verán incrementadas para el 2018.

Fuente: (Cisco Systems, Inc., 2015)



Ilustración 12. Requerimientos para las aplicaciones en la nube en las empresas.

Los requerimientos para aplicaciones en la nube van desde servicios básicos a servicios avanzados, ofreciendo un límite de velocidad en descargas, subidas y un rango definido en latencias.

Fuente: (Cisco Systems, Inc., 2014)

De acuerdo a Fons Gómez, las características y servicios que *IaaS* tienen sus propios términos como servicio, como son:

2.2.2 Almacenamiento como Servicio (DaaS)

De modo análogo a los recursos computacionales se proporcionan recursos de almacenamiento de datos. El *DaaS (Data Storage as a Service)* permite a los usuarios obtener el servicio de almacenamiento flexible en discos remotos donde pueden acceder desde cualquier lugar. Éste servicio, también debe cumplir con una serie de requisitos básicos: alta disponibilidad, fiabilidad, rendimiento, replicación y la consistencia de los datos.

2.2.3 Comunicación como Servicio (CaaS)

Esta capa proporciona servicios de comunicaciones a todas las capas o como servicio independiente. El servicio debe cumplir ciertos requisitos, garantizando la calidad del servicio, que incluye la seguridad de la red, la disponibilidad, el ancho de banda (preferiblemente dedicado) y supervisión directa a la red. El audio y la videoconferencia es solo un ejemplo de aplicaciones en la nube que se benefician de *CaaS (Communication as a Service)*.

2.2.4 Hardware como Servicio (HaaS)

El extremo inferior del modelo de capas de la computación en nube es el *hardware* (físico), que forma la columna vertebral de cualquier oferta de servicios de *cloud computing*.

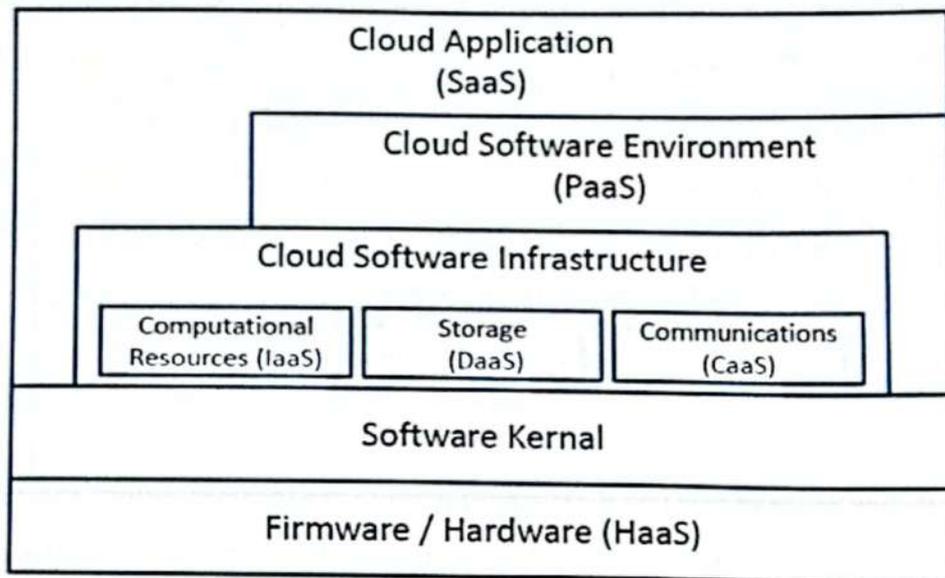


Ilustración 13. Ontología unificada de Cloud Computing.

El modelo de la computación en la nube presenta la infraestructura como servicio compuesta por capas entre las que se incluyen las comunicaciones, el almacenamiento y los recursos computacionales.

Fuente: (CloudTek University, 2009)

Según un estudio publicado por IHS Technology en su página web, explica que: Dicho estudio realizado por IHS encontró la Infraestructura como Servicio (*IaaS*) en el mercado con un valor de poco más de US\$4 mil millones para el año 2013. Amazon, Microsoft, e IBM se encontraron para dar cuenta de más de la mitad de los ingresos *IaaS* en ese mismo año. Google estuvo ausente de las estimaciones de cuota de mercado de dicho año, dado que sólo presentó su oferta en ese diciembre. Sin embargo, debido a la escalabilidad de la empresa, la infraestructura del *data center* existente y los recursos disponibles para la inversión, IHS sospecha que la compañía estará entre los primeros del top 5, en los mejores proveedores de servicios del mercado para el 2014.

Otros proveedores importantes que analiza el informe (tanto en términos de ingresos y centro de datos) son AT&T, British Telecom, CenturyLink, Hewlett-Packard, Internap, Rackspace, Verizon Terremark y VMware.

En cuanto a la presencia de estos 12 suplidores y sus centros de datos, IHS encontró que en conjunto tienen más de 100 *data center IaaS* habilitados en todo el mundo. Existen zonas especialmente densas de centros de datos para estos importantes proveedores, como son: California, Texas, Virginia, Reino Unido, Países Bajos y Singapur. Las ubicaciones y los números de instalaciones para cada proveedor puede variar mucho, todo depende del modelo de negocio global de las empresas, ya sea por alojamiento de telecomunicaciones, colocación o Internet.

IaaS es actualmente sólo una pequeña porción de la TI de la empresa del mercado total de servicios en la nube. Por el momento, la mayor parte de los ingresos que provienen de la nube es a causa de *SaaS*, que en esencia puede ser cualquiera de la suscripción y el *software* basado en web del mercado. A pesar de su tamaño relativamente pequeño, *IaaS* es un mercado de rápido crecimiento, con importantes implicaciones para el mercado de la infraestructura del *data center*. A medida que más empresas se mueven a un modelo *IaaS*, habrá una necesidad para la reducción de los *data center* empresariales, lo que significa una base de clientes muy diferente para los proveedores de equipos de centro de datos como UPS, refrigeración, bastidores, PDU, etc.

Los proveedores de servicios de nube brindan un reporte de la Infraestructura como servicio y sus *data center* hasta el año 2014, dan una nueva perspectiva sobre la *IaaS* en el mercado. El estudio presenta una evaluación precisa del tamaño del mercado mediante la estimación de los ingresos provenientes de los servicios de Infraestructura por los principales 12 proveedores a este mercado.



Infrastructure as a Service Data Centers



© 2014 IHS

Ilustración 14. Análisis de las infraestructuras de los *data centers* de proveedores de IaaS.

Los Data Center como servicio se han expandido en todo los continentes, teniendo 122 Data Center con capacidades IaaS.

Fuente: (Cruz, IHS Technology, 2014)

En definitiva, la infraestructura como servicio da la oportunidad a las empresas de una alternativa, arrendando el *hardware* y la tecnología necesaria para realizar las actividades de la empresa, cuando las necesidades de construir una infraestructura tecnológica exceden el pago por uso.

2.2.5 Software como Servicio (SaaS)

AIMME explica que es la distribución de aplicaciones a través de Internet mediante un navegador web, pagando en base al consumo. La información, el proceso de datos y los resultados están alojados en la empresa proveedora de Tecnologías de la Información y la Comunicación.

SaaS promete aplicaciones como servicio, las cuales pueden acceder varios usuarios a través de un navegador web con conexión hacia Internet, o incluso cualquier aplicación que haya sido desarrollada para cumplir tal función. Gracias a este tipo de servicio de distribución, no es necesario instalar y ejecutar el *software* en el servidor o PC físico, trayendo consigo ventajas en la disminución de costos en soporte técnico y mantenimiento hacia el *software*.

Las características de este servicio son en parte similares a la *IaaS* (Infraestructura como servicio), son accesibles a través de internet y son alojados en servidores gestionados por la compañía proveedora. La diferencia entre estos servicios es que su pago se realiza por cuota en vez de hacerlo por uso. Sin embargo, existen otras características que el cliente debe tener en cuenta al momento de adquirir el servicio.

La compañía *Salesforce* y su *software* de gestión de relaciones con clientes (CRM) en la nube utiliza una peculiaridad importante en su *software* ofrecido como servicio, la importación y exportación de datos, regala facilidades al usuario del ingreso al sistema importando datos, así como la salida de ellos exportando datos. Es necesario que el SaaS cuente con un Acuerdo de Nivel de Servicio (SLA), de esta manera, el usuario puede saber las garantías o limitaciones que posee al utilizar la aplicación con el servicio. Por último, es recomendable que el *software* sea auto-formativo, es decir, sea intuitivo con el usuario, sea especializado en el área para evitar costos innecesarios, tenga manuales y videos tutoriales online para facilitarle el uso al usuario.

Google Apps, *Microsoft Office 365*, *Salesforce* y *Lotus Live* de IBM son algunos de los *software* como servicios que ofrecen estas compañías en nubes públicas y privadas.

Es sustancial concretar los siguientes aspectos al momento de considerar un acuerdo fijo con el servicio de *software* en la nube:

- **Topología de transacción:** Este tipo de servicio se suscribe vía electrónica por lo que una configuración exacta de la empresa que se suscribe utiliza un *software* con licencia por uso.
- **Mantenimiento:** El cliente debe estar consciente de que la prestación del servicio recibido tenga calidad y no exista ninguna falla por falta de mantenimiento.
- **Nivel de servicio:** Si el sistema es escalable, el *SaaS* no tendrá ningún tipo de problema de entregar servicios a múltiples usuarios, del mismo modo, se necesita acordar alta disponibilidad para obtener respuesta rápida con la aplicación en la nube.
- **Protección de datos y seguridad del negocio:** Es necesario identificar si la aplicación en la nube está certificado por la ley de protección de datos vigente en el país de residencia, además de las certificaciones internacionales.

La compañía *Salesforce*, compañía global de computación en la nube, tiene su historia con el servicio de *software* en la nube. Así lo expresa el libro: “Las reglas de la victoria: Cómo transformar el caos y el conflicto”.

Salesforce.com empezó a funcionar intentando convencer a las empresas grandes y pequeñas para que emplearan su *software* de base de datos de relaciones de clientes basado en la red, accediendo al mismo por una cuota mensual, en vez de comprar el *software* en propiedad a su proveedor habitual, en discos o para descargarlo de la red, e instalarlo en sus propios ordenadores. La venta de soluciones de «*software* como servicio» no era una idea absolutamente nueva. Otras 10 compañías habían intentado y habían fracasado; pero *salesforce.com* consideraba que tenía una posición única y que estaba bien preparada para alcanzar el éxito en este sector. Durante toda esta fase, las grandes empresas que encabezaban el sector del *software* en propiedad, con ventas de muchos miles de millones de dólares, criticaban tanto el modelo de negocio del *software* como servicio, como la capacidad de *salesforce.com* para llevarlo adelante con éxito. Dicha empresa empezó a crecer rápidamente, al cabo

de pocos años se alcanzó un avance importante, cuando se ganó el respeto y los contratos, después de varias instituciones financieras grandes e influyentes. Entonces, cuando las ventas anuales de *salesforce.com* se aproximaban a los 500 millones de dólares anuales y se esperaba que llegarían a los 1,000 millones de dólares a los pocos años, las grandes empresas de la competencia se inquietaron. Llegaron a la conclusión de que aquel mercado era importante para ellas, y anunciaron públicamente que se disponían a entrar de manera agresiva en el mercado del *software* como servicio, descrito por Gimian & Boyc en el 2008.

No es algo nuevo que el SaaS provee grandes ingresos económicos para los proveedores de servicios y para las compañías que contratan este servicio. En el año 2010, pudo generar más de 10 billones de dólares. De acuerdo a Torres Viñals no es sencillo responder a la pregunta de qué cuota de mercado tiene actualmente este tipo de servicios. En un artículo reciente de la revista "*The Economist*" se daban las siguientes cifras: el *Software* como Servicio habría podido generar, durante el año 2010, unas ventas de más de 11 billones de dólares, mientras que la Plataforma como Servicio podría rondar los 300 millones de dólares y la capa de la Infraestructura como Servicio, aún resulta difícil de dimensionar, aunque seguro que son millones los ordenadores que dan apoyo a esta industrialización de la informática.

Actualmente, uno de los servicios más utilizados es SaaS, siendo un servicio primario en muchas compañías y organizaciones debido a que tiene una mayor demanda que cualquier otro en la nube, como se representa estadísticamente en la siguiente tabla:

Tecnologías de computación en la nube utilizadas en organizaciones, 2011-2014

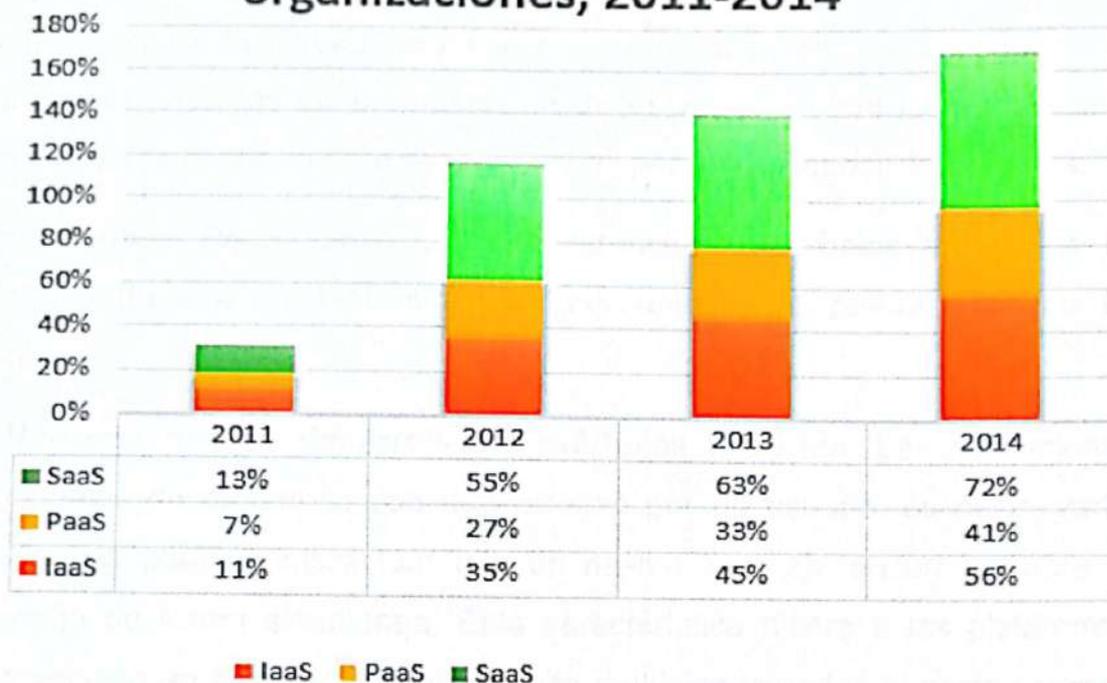


Tabla 3. Tecnologías Cloud Computing en organizaciones.

La gráfica representa el servicio de software en la nube como la de mayor demanda entre los años 2011-2014.

Fuente: (Skok, n.d.)

2.2.6 Plataforma como servicio (PaaS)

El Instituto Tecnológico Metalmeccánico define el *PaaS* como la distribución de herramientas y *software* necesarios para el desarrollo de aplicaciones en equipos distribuidos.

El servicio *PaaS* promete una solución basada en plataformas de aplicaciones, donde aquellas herramientas de desarrollo se encuentran alojadas en la nube accediendo a ellas por medio de un navegador web. Con la ayuda de este servicio, muchos desarrolladores podrán crear aplicaciones web y *software* de aplicaciones sin necesidad de tener instalado algún programa adicional en las computadoras (compiladores) y posteriormente se podrá ejecutar dicha aplicación sin necesidad de algún permiso administrativo. Los Entornos de Desarrollos Integrados (*IDE*)

incorporan lenguajes de programación tradicionales y lenguajes de programación web.

Se prefiere utilizar la plataforma como servicio para desarrollar aplicaciones a través de herramientas de programación de escritorio, donde las aplicaciones desarrolladas se importan para ser ejecutadas por un proveedor de servicios.

Las plataformas *PaaS* tienen ciertas diferencias funcionales entorno a las plataformas de desarrollo comunes o tradicionales. Se puede distinguir las siguientes:

- **Herramientas de desarrollo de múltiples usuarios:** Las herramientas tradicionales de desarrollo son usadas solo por un usuario, es decir, varios usuarios no pueden interactuar con un mismo lenguaje en un *software* de desarrollo de forma simultánea. Esta característica difiere a las plataformas como servicio en la nube, ya que permite múltiples usuarios al mismo tiempo, donde cada usuario puede tener un sinnúmero de proyectos activos.
- **Escalabilidad para el soporte de múltiples usuarios:** Normalmente esta característica no es muy inquietante para desarrolladores y se deja gestionada por administradores de sistemas cuando se trabaja un proyecto. La escalabilidad en *PaaS* debe estar estrechamente relacionada a la solución que se trabaja, tomando en cuenta el balanceo de carga y la disponibilidad a la hora de integrar nuevos usuarios al proyecto.
- **Gestión integrada:** El monitoreo es una característica importante cuando se tiene una plataforma en la nube, algo que no era muy común es que cuando se trabajaba en desarrollos tradicionales de *software*, solo se monitoreaba la aplicación cuando presentaba algún error o falla en el sistema. Como *PaaS* se ejecuta en la nube y es necesario la conexión a internet para acceder, es importante saber cómo se encuentra la plataforma entorno a factores de tráfico de red, múltiples usuarios, rendimiento, etc.
- **Pago por uso:** Al igual que *IaaS*, su pago se realiza por la cantidad de veces que se utiliza el servicio.

Algunos ejemplos de plataformas como servicio son: *Google App Engine*, que actualmente añadió Java como lenguaje soportado, también están el caso de *Force* de *Salesforce* o el *Azure* de *Microsoft*, son algunos de los más importantes en la actualidad. Otros que están entrando en la competitividad con ellos son *Bungee Connect*, *LongJump*, basado en Java/Eclipse y *WaveMaker*, que son plataformas de desarrollo basadas en java y alojado en Amazon EC2.

PaaS ofrece beneficios que están cada vez más actualizados, adaptándose a las necesidades de los usuarios permitiendo que una mayor cantidad de personas puedan mantener, desarrollar y ejecutar aplicaciones web y de *software*.

Hoy en día, para crear aplicaciones web se necesitan de desarrolladores expertos con habilidades especializadas, algunas habilidades fundamentales, como son: desarrollo del *frontend* en el cliente (JavaScript / Dojo), desarrollo del *backend* en el servidor (Java / J2EE) y administración de sitios web.

El potencial que permite la plataforma como servicio para que los desarrolladores puedan crear aplicaciones web y *software* sin necesidad de un experto, se ha convertido en una de las principales ventajas de este servicio.

El mercado de la plataforma como servicio va en aumento, siempre y cuando existan nuevas tendencias para crear tecnologías más sofisticadas. Con ello, la portabilidad de una plataforma a la nube y el acceso a ella desde cualquier parte donde exista una conexión a Internet, resultando más económica y simple, lo que hace *PaaS* competitivo en el mercado contra las plataformas tradicionales. Según un artículo del 2012 publicado por *Gartner*, una empresa de consultoría e investigación de tecnologías de la información con sede en *Stamford, Connecticut*, Estados Unidos, afirma que en el 2011 la plataforma como servicio alcanzó una cifra de 900 millones, y que la misma seguirá en aumentos increíbles para años posteriores. "Plataforma como servicio (*PaaS*) y sus ingresos está en camino de alcanzar los US\$1.2 mil millones en 2012, frente a US\$900 millones en 2011, según *Gartner, Inc.* El mercado experimentará un crecimiento consistente con los ingresos *PaaS* en todo el mundo con un total de US\$1,5 mil millones en el 2013, y en crecimiento a US\$2.9 mil millones en el 2016.

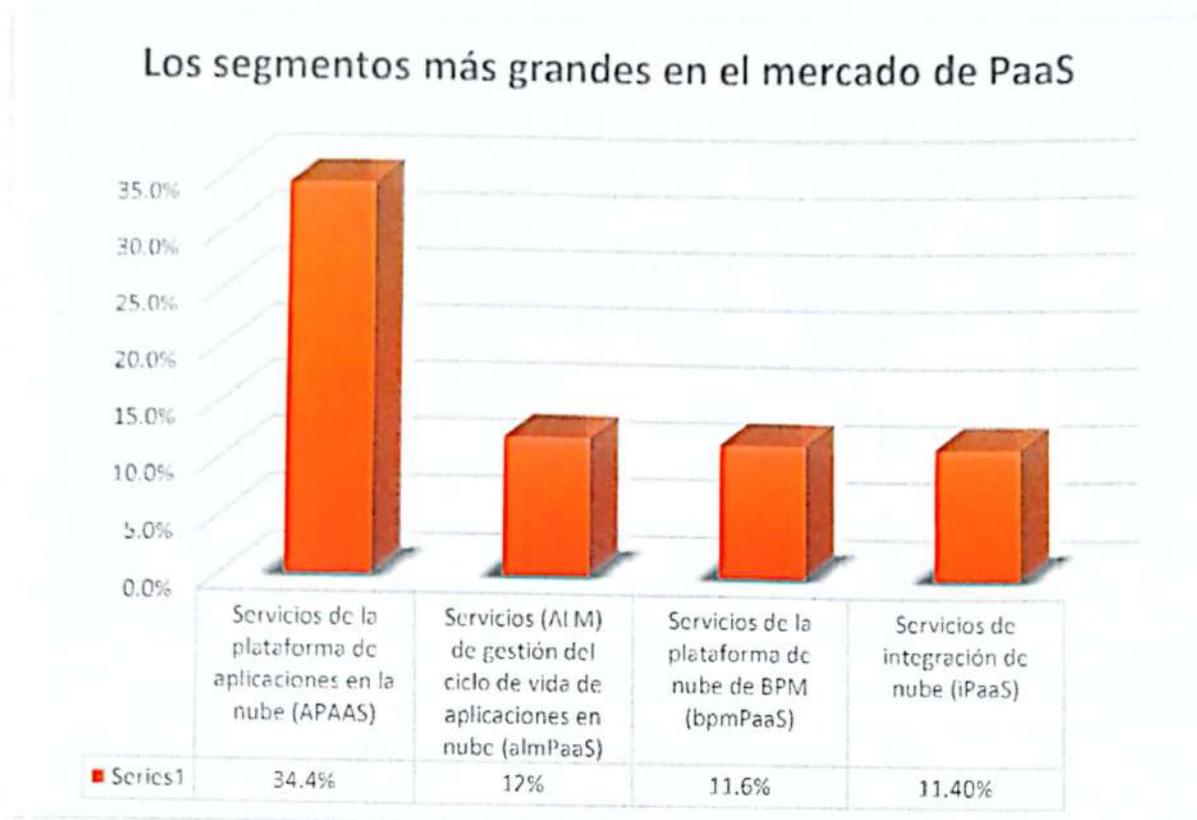


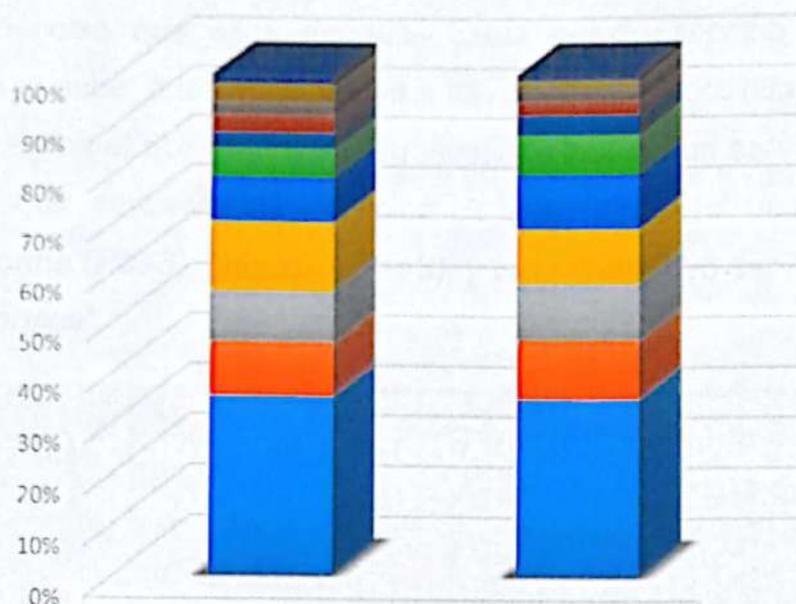
Tabla 4. Segmentos más grandes del mercado de *Plataforma as a Service*.

Los servicios APAAS representa el segmento más grande del mercado PaaS, contando con el 34.4% de la totalidad.

Fuente: Imagen propia.

Gartner predice que el gasto potencial en tecnologías *PaaS* es un promedio de US\$360 millones por año entre 2011 y 2016. *Natis* expresa que todos los desarrolladores de *software* están invirtiendo estratégicamente en el mercado de *PaaS*, a pesar de los ingresos de mercado proyectados. "La infraestructura de aplicaciones, y en este caso como servicio (*PaaS*), siempre ha jugado un papel central en el establecimiento de las normas, arquitecturas y las mejores prácticas en los mercados de *software* empresarial. Los vendedores esperan que su liderazgo en el mercado de *PaaS* crezca de manera vertiginosa para traducirlo a ecosistemas eficaces, desarrolladores y soluciones de tecnologías *PaaS* está incrustado en muchos otros tipos de servicios en la nube donde todos los principales canales de oportunidad y el ingreso directo en el mercado de *PaaS* subestima groseramente la importancia de esta parte de la arquitectura de nube." (STAMFORD, 2012)

Pronóstico del mercado PaaS, 2011-2016



	2016	2011
■ Portal de Servicios Horizontal en la Nube(Portal PaaS)	2%	1%
■ Servicios de Base de Datos en la Nube (dbPaaS)	4%	2%
■ Servicios MOM en la Nube	7%	2%
■ Servicios Analíticos de Negocios en la Nube (baPaaS)	4%	3%
■ Servicios de Gobernanza para Aplicaciones en la Nube	3%	4%
■ Servicios MFI en la Nube	6%	8%
■ Servicios de Seguridad de Aplicaciones en la Nube	9%	11%
■ Servicios de Integración en la Nube (iPaaS)	14%	11%
■ Plataforma de Servicios BPM en la Nube(bpmPaaS)	10%	11%
■ Servicio ALM en la Nube (almPaaS)	11%	12%
■ Plataforma de Servicios para Aplicaciones en la Nube (aPaaS)	35%	35%

Tabla 5. Pronóstico del mercado PaaS.

Pronóstico de crecimientos del mercado de plataforma como servicio en la nube entre los años 2011 al 2016.

Fuente: (Gartner, Inc., 2012)

Otro servicio que ha venido surgiendo es "Todo como servicio" (XaaS), facilitando la flexibilidad para los usuarios de personalizar sus entornos computacionales, embarcando las experiencias que ellos desean. Este tipo de servicio es dependiente del todo en la nube, a la vez confiable a través de la conectividad a internet para ganar con éxitos el acepto de los usuarios. Todo como un servicio es un término general que envuelve los servicios de Infraestructura (IaaS), Software (SaaS), Plataforma (PaaS), Negocio (BaaS), y todo aquel otro servicio con las palabras "as a service".

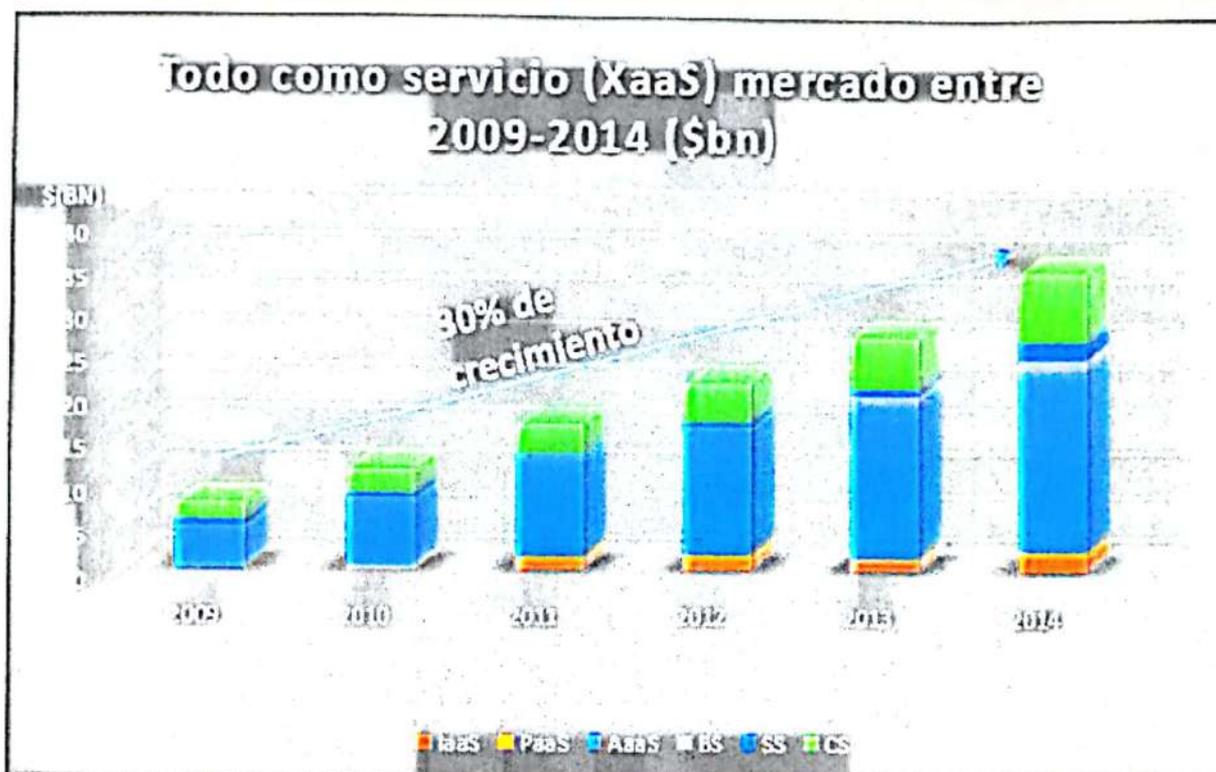


Ilustración 15. Crecimiento del mercado XaaS.

El mercado de XaaS ha aumentado un 30% de crecimiento entre los períodos 2011 - 2014.

Fuente: (FabriQate, 2011)

Como el mundo de la nube es una realidad, que hoy en día beneficia a usuarios y empresas, existen muchos otros servicios que han incursionado en ese mundo, obteniendo gran aceptación por parte de usuarios e ingresos económicos por parte de compañías. Como son:

Acrónimos as a service	Términos originales
AaaS	<i>Architecture as a Service</i>
BaaS	<i>Backup as a Service</i>
BaaS	<i>Business as a Service</i>
CaaS	<i>Communications as a Service</i> <i>Compliance as a Service</i> <i>Content as a Service</i> <i>Crimeware as a Service</i> <i>Computing as a Service</i> <i>CRM as a Service</i>
DaaS	<i>Data as a Service</i> <i>Data Warehousing as a Service</i> <i>Data Mining as a Service</i> <i>Database as a Service</i> <i>Development as a Service</i> <i>Desktop as a Service</i> <i>Document Management as a Service</i>
EaaS	<i>Ethernet as a Service</i> <i>ERP as a Service</i> <i>Email as a Service</i>
FaaS	<i>Framework as a Service</i>
GaaS	<i>Globalization as a Service</i>
HaaS	<i>Hardware as a Service</i> <i>Humans as a Service</i>
HCMaaS	<i>Human Capital Management as a Service</i>
HRaaS	<i>Human Resources as a Service</i>
IaaS	<i>Information as a Service</i> <i>Infrastructure as a Service</i> <i>Integration as a Service</i> <i>Identity as a Service</i>
LaaS	<i>Lending as a Service</i>

Acrónimos as a service	Términos originales
MaaS	<i>Malware as a Service</i> <i>Manufacturing as a Service</i> <i>Mashups as a Service</i> <i>Media as a Service</i>
OaaS	<i>Organization as a Service</i> <i>Optimization as a Service</i> <i>Operations as a Service</i>
QaaS	<i>Queue as a Service</i>
SaaS	<i>Security as a Service</i> <i>Storage as a Service</i>
TaaS	<i>Testing as a Service</i>
UaaS	<i>UI as a Service</i>
VaaS	<i>Voice as a Service</i>

Tabla 6. Acrónimos “as a service”.

Fuente: Imagen propia.

2.3 Internet – Protocolos

Internet es el motor principal para acceder a la nube y que la misma representa el 38% de la población mundial, aproximadamente 3 mil millones de usuarios. El hecho de que se pueda acceder al *cloud computing* vía Internet y por múltiples dispositivos, lo hace sencillo y sin muchos requisitos para la accesibilidad. Sin embargo, los países en vía de desarrollo, que no tienen un acceso total a Internet o el mismo es limitado, representa una desventaja para dos tercios de la población mundial, de acuerdo a informaciones publicadas por una organización sin fines de lucro fundada por Mark Zuckerberg, llamada “internet.org” que busca conectar al 100% de la población mundial a Internet. Cuando la cifra llegue a su máximo, el modelo de computación en la nube desplazará muchas tecnologías tradicionales.

WORLD INTERNET USAGE AND POPULATION STATISTICS JUNE 30, 2014 - Mid-Year Update						
World Regions	Population (2014 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2014	Users % of Table
Africa	1,125,721,038	4,514,400	297,885,898	26.50%	6498.60%	9.80%
Asia	3,996,408,007	114,304,000	1,386,188,112	34.70%	1112.70%	45.70%
Europe	825,824,883	105,096,093	582,441,059	70.50%	454.20%	19.20%
Middle East	231,588,580	3,284,800	111,809,510	48.30%	3303.80%	3.70%
North America	353,860,227	108,096,800	310,322,257	87.70%	187.10%	10.20%
Latin America / Caribbean	612,279,181	18,068,919	320,312,562	52.30%	1672.70%	10.50%
Oceania / Australia	36,724,649	7,620,480	26,789,942	72.90%	251.60%	0.90%
WORLD TOTAL	7,182,406,565	360,985,492	3,035,749,340	42.30%	741.00%	100.00%

Tabla 7. Estadística de la utilización de internet mundialmente.

Estadística de la población mundial de Internet dividida en regiones mundiales. En la estadística se presenta un estimado de población del 2014, usuarios en internet durante el 31 de diciembre del año 2000 y la data que utilizaron en ese día. El crecimiento de todas las regiones dio una totalidad de 741.0% desde el 2000 al 2014, representando el 100% de los usuarios.

Fuente: (Miniwatts Marketing Group, 2014)

Cantidad de usuarios de Internet distribuidos por regiones mundiales - 2014

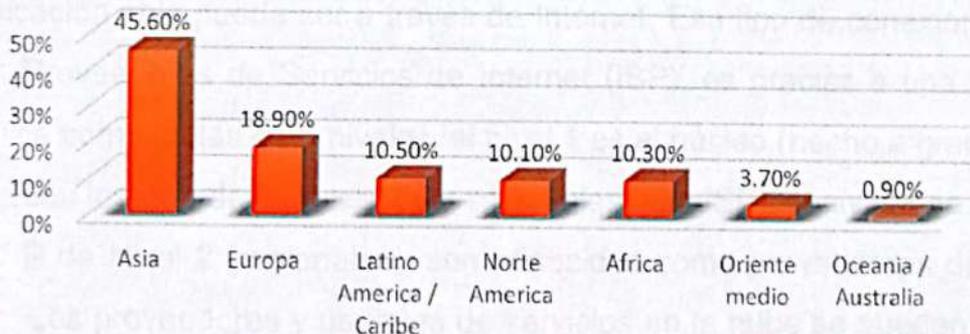


Ilustración 16. Usuarios de internet en el mundo.

Para el 31 de diciembre del 2014, existían 3, 079, 339,857 usuarios de Internet. El porcentaje de usuarios de Internet la lidera el continente Asiático, con casi un 50% de usuarios, representa la mitad de usuarios a nivel mundial.

Fuente: (Miniwatts Marketing Group, 2014)

USUARIOS DE INTERNET POR REGIONES GEOGRAFICAS

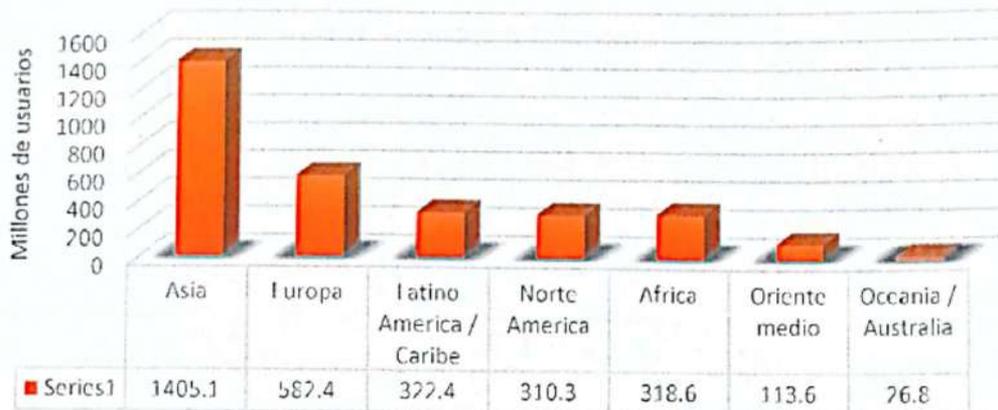


Ilustración 17. El incremento de usuarios en Internet se extiende cada año aún más.

Asia posee 1,405 millones de usuarios de Internet, en ella se encuentra la mayor demanda de usuarios de Internet.

Fuente: (Miniwatts Marketing Group, 31)

Los proveedores de servicios de Internet juegan un rol muy importante para establecer comunicación entre los proveedores de *cloud* y el usuario, esta comunicación solo puede ser a través de Internet. Ese tipo de conexión ofrecido por los Proveedores de Servicios de Internet (ISP), es gracias a una topología jerárquica compuestas de 3 niveles, el nivel 1 es el núcleo (hecho a gran escala), nivel 2 (son los grandes proveedores regionales), los ISP del nivel 3 se conectan a los ISP de Nivel 2 (regionales), son conocidos como proveedores de Internet locales. Los proveedores y usuarios de servicios en la nube se pueden conectar a través de un proveedor de nivel 1, ya que cualquier ISP la habilita conexión a Internet. El libro *Handbook of Enterprise Integration* explica que los ISPs de nivel superior cobran los del nivel más bajo: Los ISP de *Tier 1* cobran a los regionales (ISP *Tier 2*). Por supuesto, los ISP locales les cobran a los clientes residenciales y corporativos individuales por el acceso. En base a esta clasificación, un ISP *Tier 1* puede llegar a todas las demás cadenas en Internet sin tener que comprar la

conexión desde cualquier otra red. Sin embargo, una red de nivel 2 puede hacer *peering* con otras redes, pero todavía tienen que comprar la conexión a un *Tier 1* y así poder llegar a algunos puntos de la Internet. Un nivel 3 ISP debe adquirir conexiones de otros ISPs para acceder a Internet.

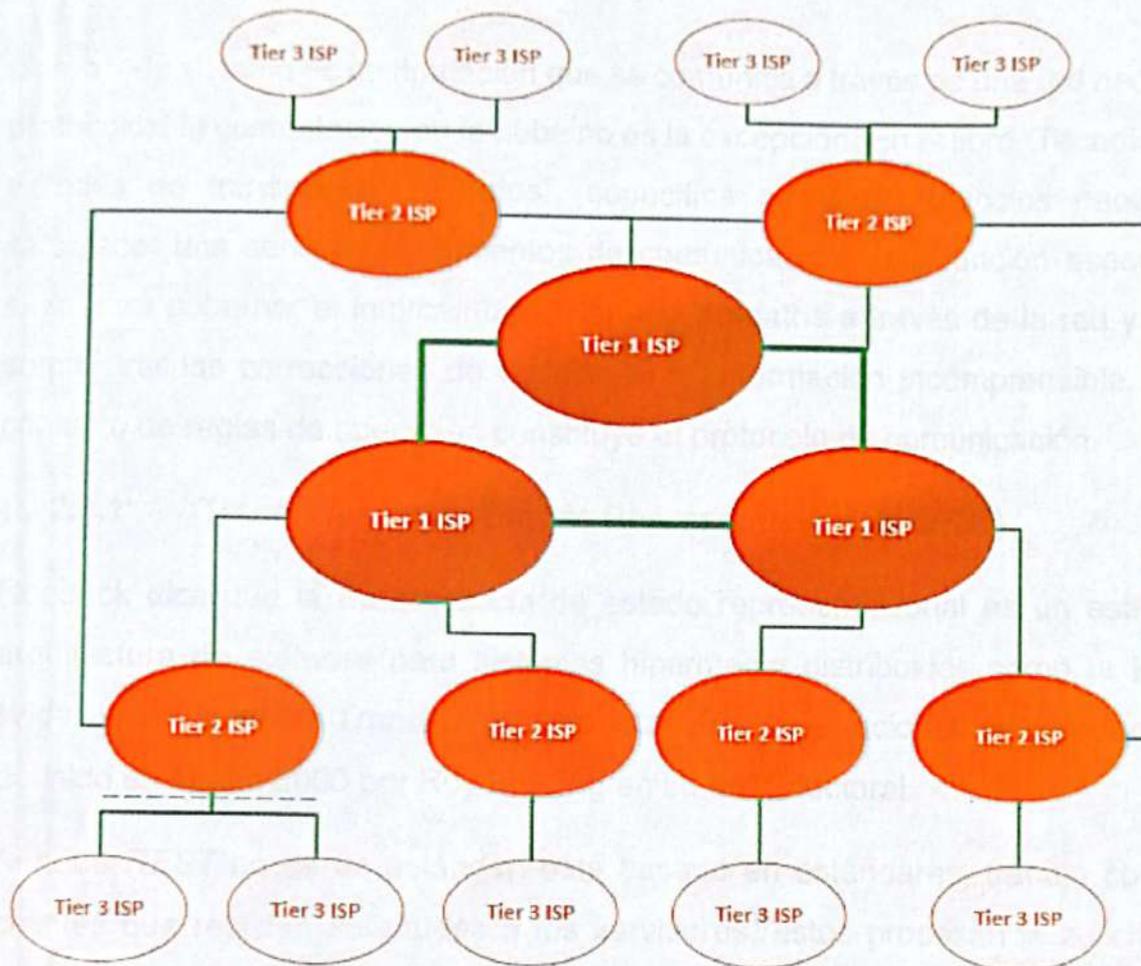


Ilustración 18. Arquitectura jerárquica de Internet.

La arquitectura jerárquica del internet presenta los TIER 1 como los más centralizados y los más independientes de cualquier otro TIER.

Fuente: (Hashem Sherif, 2010, p. 66)

Los *ISP* deben asegurarse de que la calidad de conexión entre los proveedores *cloud computing* y el usuario sea la más óptima posible, donde el rendimiento de las operaciones de la organización no se vean afectadas por baja velocidad en los enlaces o sobrecarga de ellos. Menken expresa en su libro que una empresa tiene que asegurarse de que su proveedor de servicios Internet (*ISP*) les proporciona

una conexión sin interrupciones. La cantidad de ancho de banda disponible de los *ISPs* tiende a variar dependiendo la hora del día. Para minimizar los problemas relacionados con la conexión, una empresa debe asegurarse de que tienen un vínculo de calidad con alta velocidad que le asegure la disponibilidad a la empresa.

Como todo sistema de computación que se comunica a través de una red necesita protocolos, la computación en la nube no es la excepción. En el libro "Tecnologías y redes de transmisión de datos", especifica que los protocolos necesitan establecer una serie de lineamientos de comunicación cuya función específica sirva para gobernar el intercambio ordenado de datos a través de la red y para suministrar las correcciones de errores en la información incomprensible. Este conjunto de reglas de operación constituye el protocolo de comunicación.

2.3.1 Transferencia de Estado Representacional (*REST*)

Roebuck dice que la transferencia de estado representacional es un estilo de arquitectura de *software* para sistemas hipermedia distribuidos como la *World Wide Web*. El término Transferencia de estado representacional fue introducido y definido en el año 2000 por Roy Fielding en su tesis doctoral.

Aunque *REST* no es un estándar, está basado en estándares, trabaja con los clientes que realizan solicitudes a los servidores, estos procesan la solicitud y responden a las mismas. Estas solicitudes y respuestas son construidas con la transferencia de representación de recursos, por ejemplo, un documento que captura lo común o algún estado anterior de un recurso. Un cliente puede incluso estar en transición entre aplicaciones de estado o descanso. Un cliente en estado de descanso está disponible a interactuar con su usuario, pero no crea carga y el almacenamiento por cliente no consume en los servidores o en la red. El cliente inicia enviando solicitudes cuando esté listo para hacer transiciones a un nuevo estado. Mientras uno o más solicitudes son relevantes, el cliente es considerado a estar en transición. La representación de cada aplicación en estado contiene enlaces que quizás sean usados la próxima vez que el cliente escoja iniciar una nueva transición. *Amazon, eBay, Facebook, Youtube, Yahoo!* utilizan este

protocolo, usando *HTTP* como un túnel de llamadas, también conocido como *Plain Old XML over HTTP* o *POX/HTTP*.

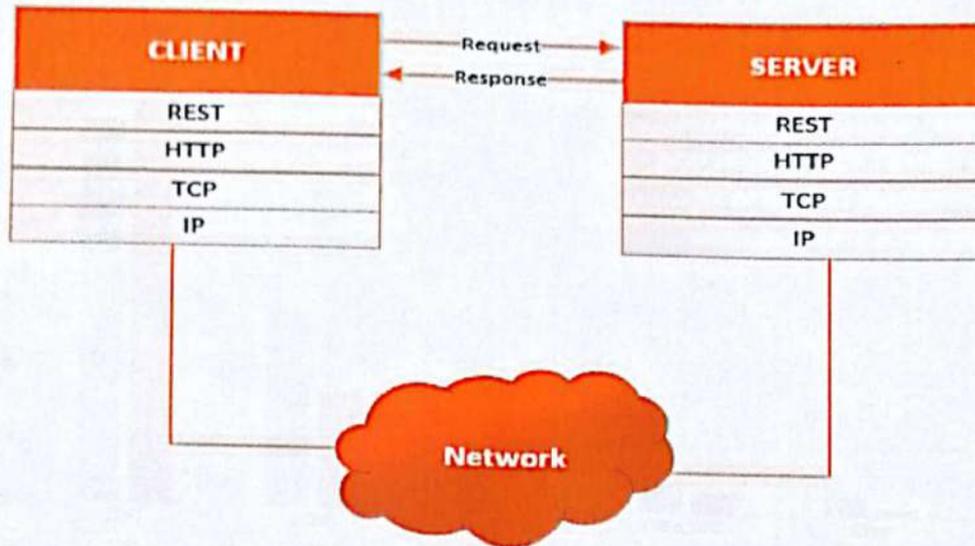


Ilustración 19. Transferencia de estado representacional.

Imagen que muestra la interacción de solicitud y respuesta entre el servidor y el cliente. Una vez la comunicación se haya establecido, podrá acceder a los recursos del servidor de forma inmediata.

Fuente: Imagen propia.

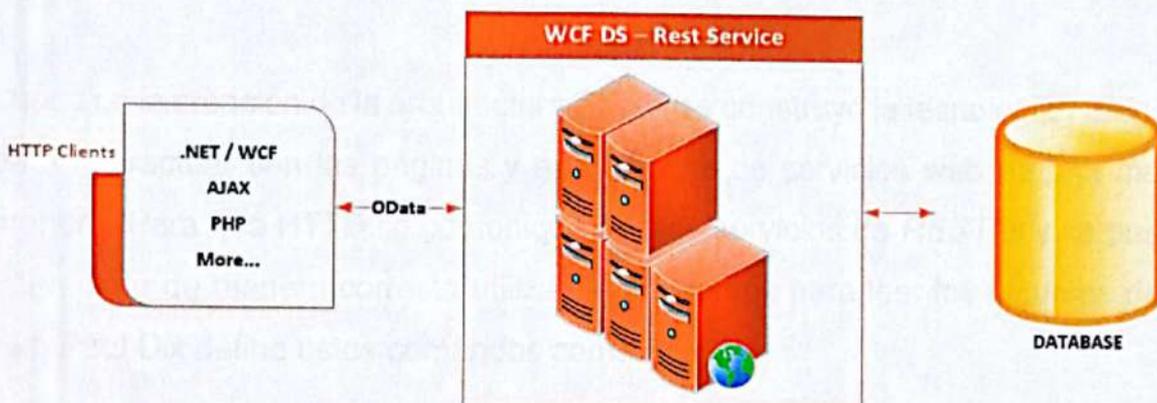


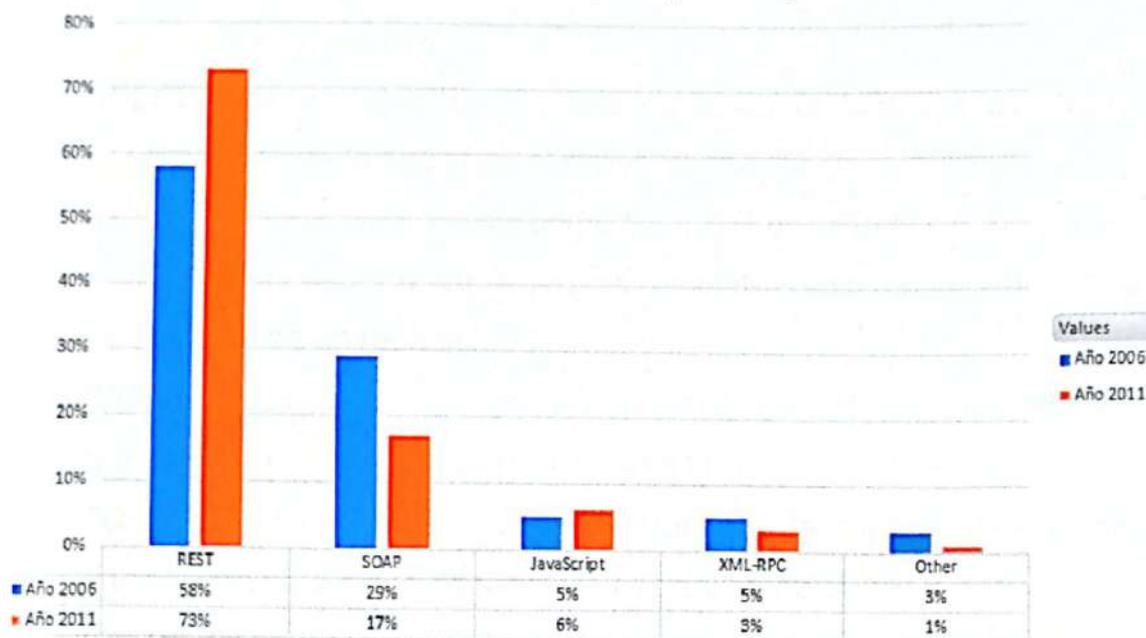
Ilustración 20. Servicio de datos REST en eXtreme Scale.

Aquí se muestra como la data es enviada al REST service y al DATABASE para su correcto funcionamiento. El servidor con servicios de REST sincroniza la data de archivos PHP, .NET, etc. con la base de datos.

Fuente: (IBM, 2009)

Año 2006 Año 2011

REST Vs. SOAP: Simplicity wins again



Distribution of API protocols and styles

Based on directory of 3,200 web APIs listed at ProgrammableWeb.

REST Vs. SOAP

Tabla 8. Distribución de los protocolos API y estilos.

Para el año 2011, el protocolo REST se consolidó como el de mayor ventaja frente a los demás protocolos de estilos.

Fuente: (Musser, 2011)

Luego de la creación de la arquitectura *REST*, se construyó la tecnología *RESTful*, para interactuar con las páginas y aplicaciones de servicios web de una mejor manera. Para que HTTP se comuniquen con los servicios de *RESTful* y se pueda interactuar de manera correcta utiliza ciertos verbos para leer los recursos de la red, Paul Dix define estos comandos como:

- **GET:** Es una petición de lectura de un recurso específico. Se recupera la información que es identificado por el *URI*.
- **POST:** Es una petición que incluye una entidad (algunos datos) que el servidor debe aceptar. Se puede utilizar para anotar un recurso existente (como añadir un comentario a una lista de comentarios), añadiendo de datos, o, simplemente, el suministro de datos a algún proceso backend.

- **PUT:** El método *PUT* coloca un recurso a un *URI* específico. La solicitud incluye los datos y especifica que el servidor debe almacenar los datos en virtud de la solicitud *URI*.
- **DELETE:** Elimina el recurso a una especificada *URI*. Sin embargo, la operación se puede anular en el servidor.
- **HEAD:** Funciona exactamente como *GET*, con una diferencia. No devuelve el recurso actual. En su lugar, se devuelve sólo la información del encabezado de un recurso.
- **OPTIONS:** Es un método para la obtención de información sobre las operaciones que se pueden realizar en un recurso.
- **CONNECT:** Se utiliza con un proxy que tiene la capacidad de cambiar dinámicamente a modo de túnel (es decir, un túnel SSL).
- **TRACE:** Envía una solicitud de un mensaje de retorno. A pesar de que la solicitud se envía al servidor de destino, proxys a menudo responden en su lugar. Esta característica permite a un atacante enumerar los servidores proxy en línea.

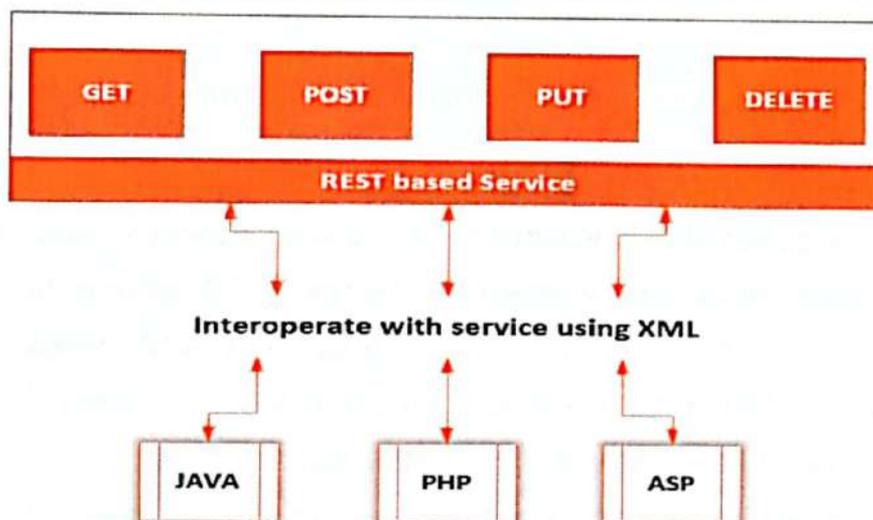


Ilustración 21. Verbos que permiten la comunicación entre HTTP y los servicios de RESTful.

Para la comunicación de los verbos HTTP y los servicios de RESTful, los servicios que usan XML inter operan en el flujo de comunicación.

Fuente: Imagen propia.

2.3.2 Protocolo Simple de Acceso a Objetos (SOAP)

Hausman, Gunderloy & Tittel proporcionan un método para traducir objetos, junto con sus métodos y propiedades, en XML que pueden ser enviados a través de HTTP, HTTPS encriptado y seguro, u otros protocolos. Debido a que SOAP se basa en XML, los servicios web pueden ser utilizados por muchos vendedores y clientes diferentes. En la siguiente ilustración se muestra el funcionamiento de este interesante protocolo.

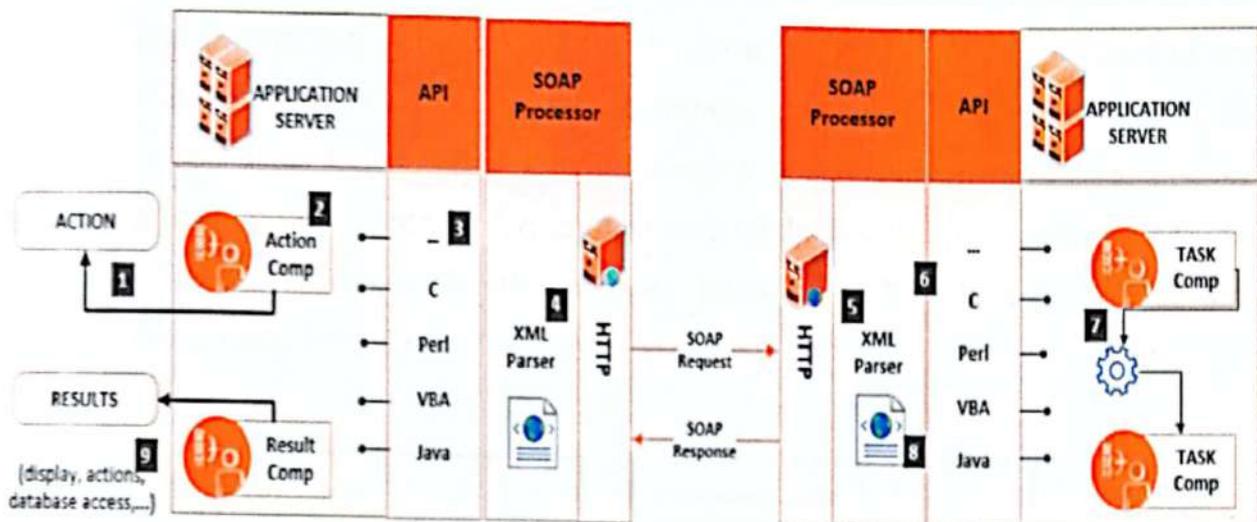


Ilustración 22. Funcionamiento del protocolo SOAP.

En la imagen se muestra el funcionamiento del protocolo SOAP desarrollándose de la siguiente manera: Una acción es llamada para la ejecución del protocolo, luego el servidor SOAP compila una acción, esa acción será determinada dependiendo del API que se quiera llamar (C, JAVA, VBA, etc...). El mismo, verifica el mensaje descifrándolo e invocando el tipo de API necesario. Una vez realizado, se crea un mensaje en formato XML y se envía por algún protocolo de transferencia de texto. La respuesta se genera de manera inversa, mostrando los resultados deseados, ya sea por acceso a la base de datos, acciones, etc.

Fuente: (Moscatelli, 2001)

2.3.3 Descripción de Servicios Web en Lenguas (WSDL)

Bhuvanewari & Sujatha describen los servicios Web en lenguas como un lenguaje basado en XML que proporciona un modelo para describir servicios Web.

WSDL es un formato XML para describir servicios de red como un conjunto de puntos finales que operan en los mensajes que contienen información orientado al procedimiento.

Las operaciones y mensajes se describen de forma genérica y posteriormente ambos son fusionados como protocolo de red. Los elementos que intervienen se relacionan y son combinados como puntos finales o también llamado servicios. Cuando se creó el lenguaje WSDL en el año 2000, se inició con la versión 1.0, sin embargo, no había sido oficialmente formalizado hasta marzo del 2001 con la que fue llamada WSDL 1.1. Entre la 1.0 y la 1.1 no se realizaron ningún tipo de cambios para ambas versiones. Más tarde, en junio del 2003, El *World Wide Web Consortium* abreviado como W3C, estuvo trabajando con la versión 1.2, donde expresaban que eran más fácil y flexible para desarrolladores que la versión anterior. Finalmente, en junio del 2007, la versión 1.2 fue renombrada a la 2.0 y fue definida como recomendación.

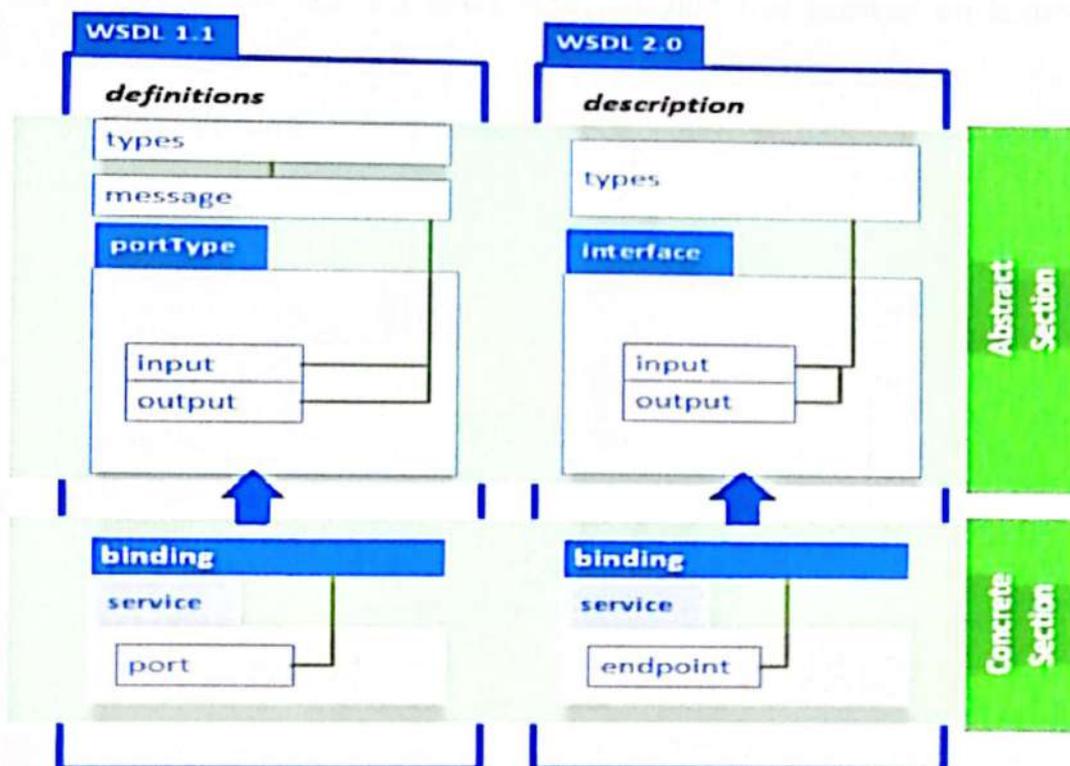


Ilustración 23. Representación de conceptos definidos por documentos de WSDL.

La imagen representa las diferencias entre versiones WSDL, presentando importantes ventajas y comprensión en los datos en la última versión creada (WSDL 2.0).

Fuente: (Bhuvaneswari & Sujatha, 2011)

2.3.4 Descripción Universal, descubrimiento e integración (UDDI)

Es un registro del lenguaje de marcas extensible (XML), basado en la plataforma independiente para empresas de todo el mundo para mostrarse a sí mismos en Internet y contiene un mecanismo para registrar y localizar aplicaciones de servicios web. UDDI fue propuesto originalmente como un servicio Web núcleo standard, diseñado para ser cuestionado por mensajes SOAP y proporcionar acceso a documentos, conjunto con Descripción de Servicios Web en Lenguas (WSDL) que describen los enlaces de protocolo y formatos de mensaje requerido para interactuar con los servicios web que figuran en su directorio, de acuerdo a Roebuck.

Además Roebuck dice que un registro de empresas UDDI consta de tres componentes, los cuales son:

- **Páginas blancas:** Contacto, dirección e identificadores conocidos.
- **Páginas Amarillas:** La categorización industrial basada en taxonomías estándar.
- **Páginas Verdes:** Información técnica sobre servicios expuestos por el negocio.

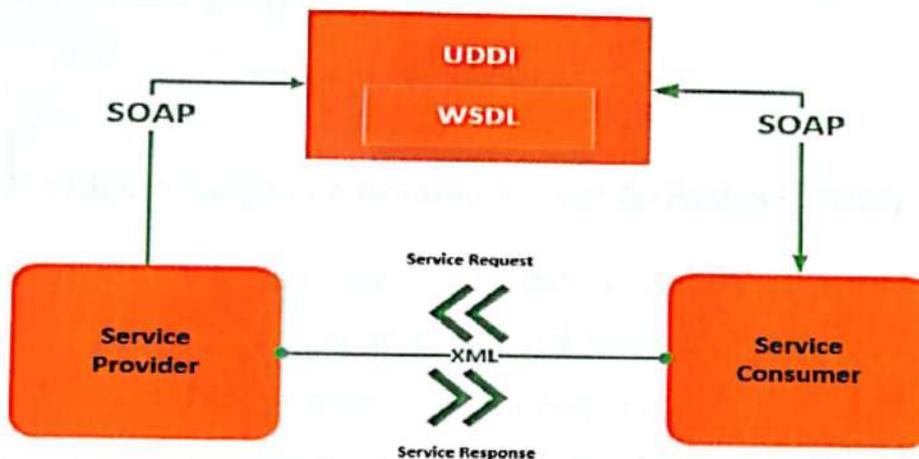


Ilustración 24. Los mensajes SAOP interrogan a UDDI.

UDDI está diseñado para ser interrogado por los mensajes SOAP. Este protocolo interactúa con el registro de lenguajes UDDI para localizar aplicaciones API y mostrarse a sí mismo a Internet.

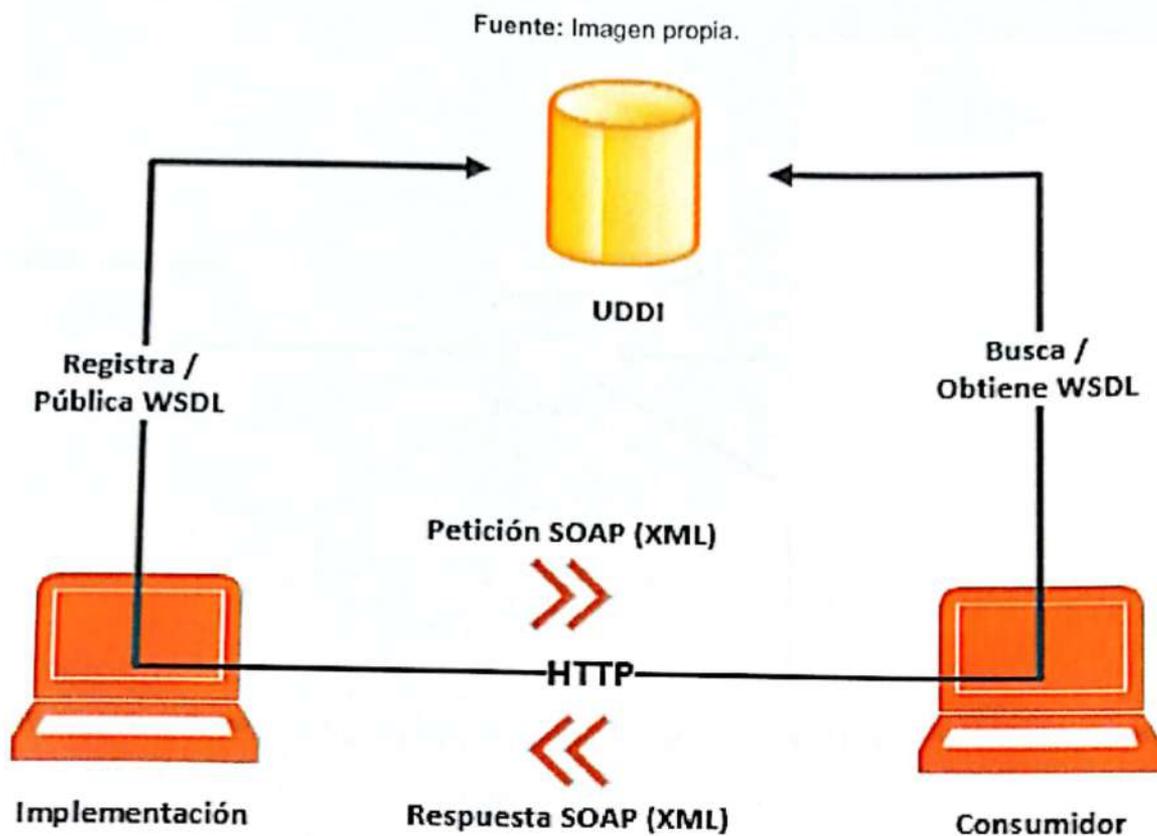


Ilustración 25. UDDI es un estándar para describir y descubrir servicios web.

Quando se realiza una petición SOAP, el registro y la publicación WSDL se coloca en el registro de lenguajes UDDI, como respuesta SOAP, el consumidor busca y obtiene el WSDL por el mismo registro.

Fuente: (Fabiang, 2008).

2.3.5 Protocolo Simple de Administración de Redes (SNMP)

El libro "Windows Server 2008: instalación, configuración y administración" define SNMP como el protocolo estándar de internet para intercambiar información de administración entre aplicaciones de consola de administración, como por ejemplo: *HP Openview*, *Novell NMS*, *IBM NetView* o *Sun Net Manager*, y entidades administradas. Además, explica que entre las entidades administradas pueden encontrarse hosts, enrutadores, puentes y concentradores.

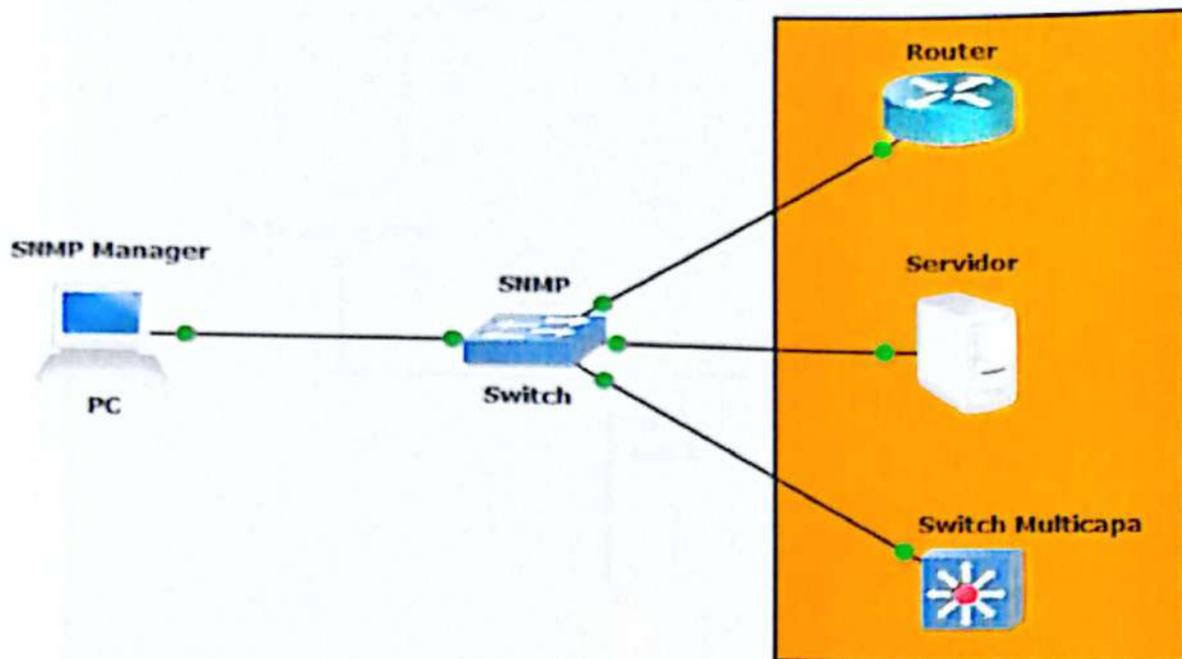


Ilustración 26. Infraestructura para intercambiar información de administración entre aplicaciones de consola.

La imagen muestra la administración para intercambiar información de administración de manera remota y centralizada entre apps de consola a equipos dentro de la red LAN.

Fuente: (Morimoto, Noel, Droubi, Mistry, & Amaris, 2010).

2.3.6 Sistema de Archivos Comunes de Internet (CIFS)

Javvin Technologies Inc. dice que es una versión mejorada de *Microsoft Server Message Block (SMB)*, siendo la manera estándar en que los usuarios de computadoras comparten archivos a través de intranets e Internet. CIFS permite la colaboración a través de Internet mediante la definición de un protocolo de acceso a archivos remoto que es compatible con la forma en que las aplicaciones comparten datos en servidores de archivos y disco de red local. CIFS se ejecuta a través de *TCP/IP*, utiliza Dominio global de Internet Servicio de Nombres (*DNS*) para la escalabilidad y está optimizado para soportar conexiones de acceso telefónico de velocidades más lentas comunes en Internet.

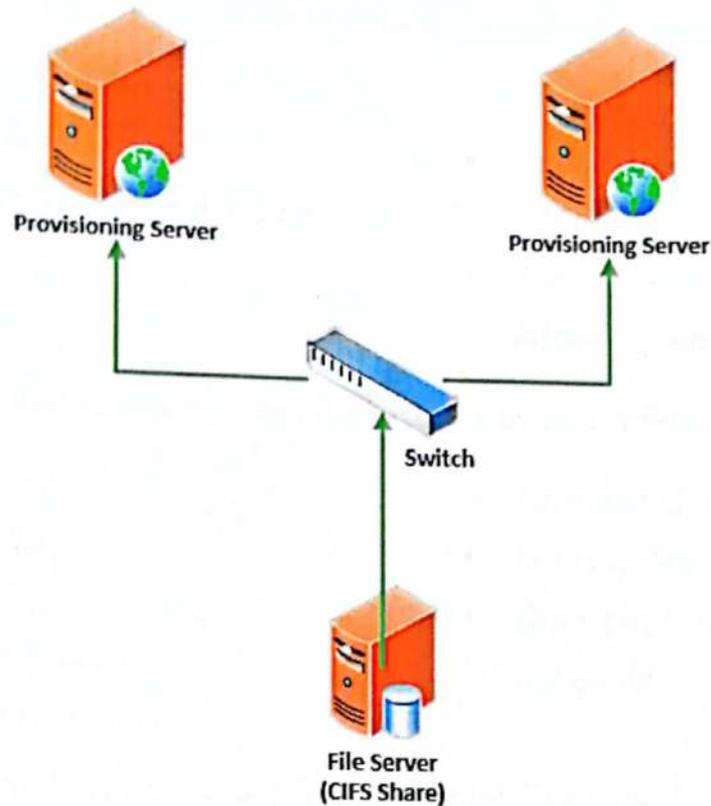


Ilustración 27. Sistema de Archivos Comunes de Internet (CIFS), forma estándar de los usuarios compartir archivos a través de intranets e internet.

Con el protocolo CIFS se mantienen los archivos compartidos en la red LAN. Con algún otro servidor provisional o enrutador, se pueden conectar a la misma red local para acceder y compartir esos recursos a través de Internet.

Fuente: (Javvin Technologies Inc., 2005)

2.3.7 Capa de Conexión Segura (SSL)

“SSL (*Secure Sockets Layer*), traducido literalmente como “capa segura de sockets”, es un protocolo desarrollado por la empresa Netscape para la transmisión privada vía internet de documentos. SSL utiliza una clave privada para encriptar la información transmitida a través de la conexión. Los navegadores web más actuales y difundidos, Netscape e Internet Explorer, soportan ambos el sistema, así como muchos servidores Web. SSL se utiliza para transmitir información confidencial de los usuarios”. (Desongles Corrales & Moya Arribas, 2006)

Actualmente, SSL trabaja con otros navegadores web muy populares, como por ejemplo:

- *Google Chrome*
- *Mozilla Firefox* (versión 1.0 en adelante)
- *Opera* (versión 7.0 en adelante)
- *Apple Safari* (versión 1.2 en adelante), entre muchos otros.

También existen servidores web que manejan estos certificados, como son:

- *Apache*
- *Microsoft IIS*
- *Microsoft SQL Server 2005*
- *IBM HTTP Server*
- *Oracle HTTP Server*
- *Microsoft Outlook*
- *Lotus Notes*
- *Qualcomm Eudora* (versión 6.2 en adelante), etc.

La suite de aplicaciones de *Visual Basic* (*Visual Basic for Applications*) no está exenta de utilizar el certificado, ofreciendo altos niveles de seguridad a desarrolladores.

El protocolo SSL utiliza la norma X.509, un estándar creada por la UTHH Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T).

La organización explica la norma de la siguiente forma:

“Define los marcos de certificados de clave pública y certificados de atributos, donde el marco de certificados de clave pública es la base de la especificación para los diferentes componentes que entran en una infraestructura de este tipo y para los procedimientos de validación, con la revocación de estos certificados.”

En el libro “Administración y gestión de una red de área local”, se detallan las fases de cómo trabaja el protocolo SSL, las cuales son:

Fase 1	El navegador solicita una página a un servidor seguro. La petición queda identificada por el protocolo https en vez de http, utilizado en páginas no seguras. A continuación, navegador y servidor negocian las capacidades de seguridad que utilizarán a partir de ese momento.
Fase 2	Seguidamente, se ponen de acuerdo en los algoritmos que garanticen la confidencialidad, integridad y autenticidad.
Fase 3	En una tercera fase, el servidor envía al navegador su certificado de norma X.509 que contiene su clave pública y, si la aplicación lo requiere, solicita a su vez el certificado del cliente.
Fase 4	A continuación, el navegador envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para cifrar los datos que se hayan de intercambiar como seguros. El envío de esta clave se hace cifrándola con la clave pública del servidor que extrajo previamente de su certificado.
Fase 5	Finalmente, se comprueba la autenticidad de las partes implicadas y, si el canal ha sido establecido con seguridad, comenzarán las transferencias de datos.

Tabla 9. Fases del protocolo SSL.

Fuente: (Abad Domingo, 2005)

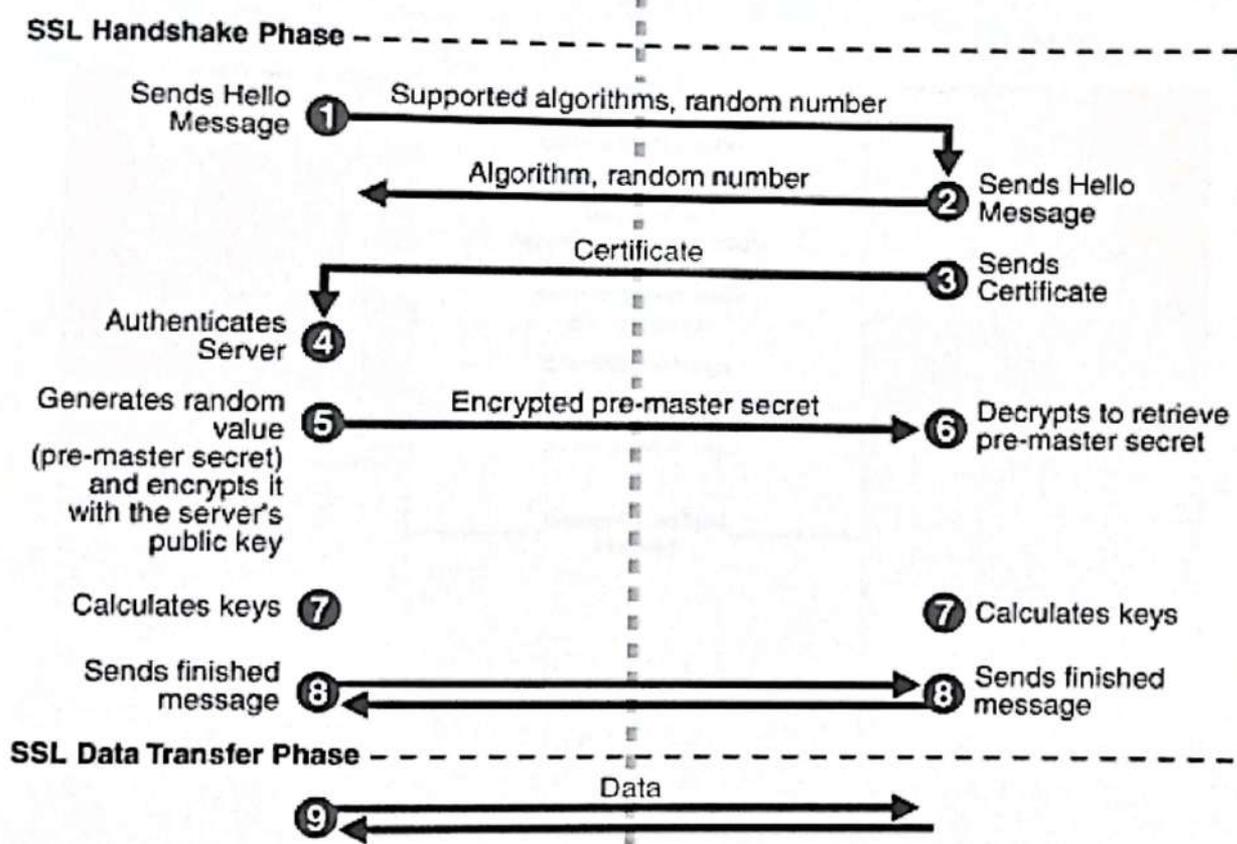
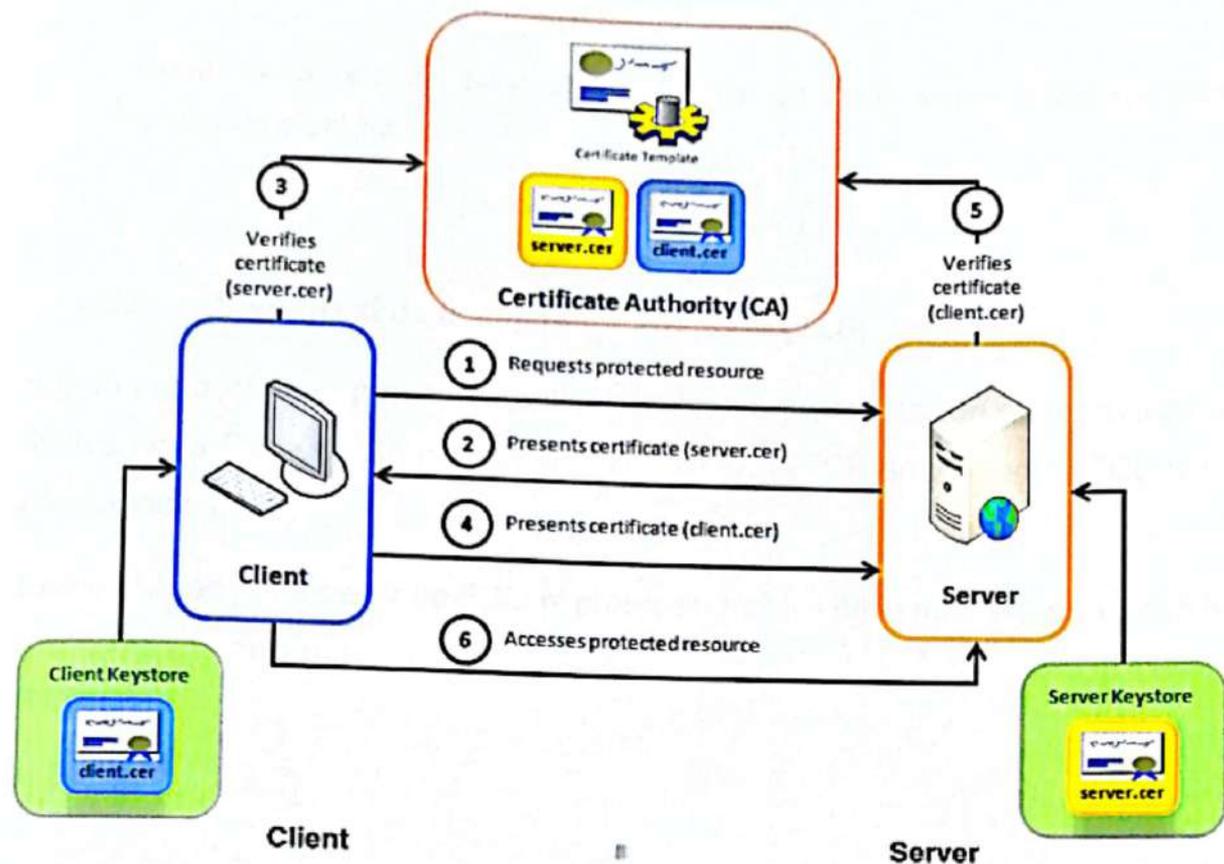


Ilustración 28. Autenticación SSL mutua.

En las imágenes, el cliente solicita un recurso, al presentarse el certificado del servidor y del cliente, una validación de ambos certificados es realizada por la

entidad autoritaria del servidor. Finalmente, se tiene acceso a los recursos informáticos del servidor.

Fuente: (Abad Domingo, 2005)

2.3.8 Seguridad de la capa de transporte (TLS)

“Es un protocolo que provee autenticación mutua y encriptación para protocolos fiables de la Capa de Transporte del Modelo OSI (TCP en el modelo TCP/IP).” (Fernández, 2008)

Como TLS es predecesor de SSL, el protocolo trabaja de la misma forma y con la misma norma descrita.

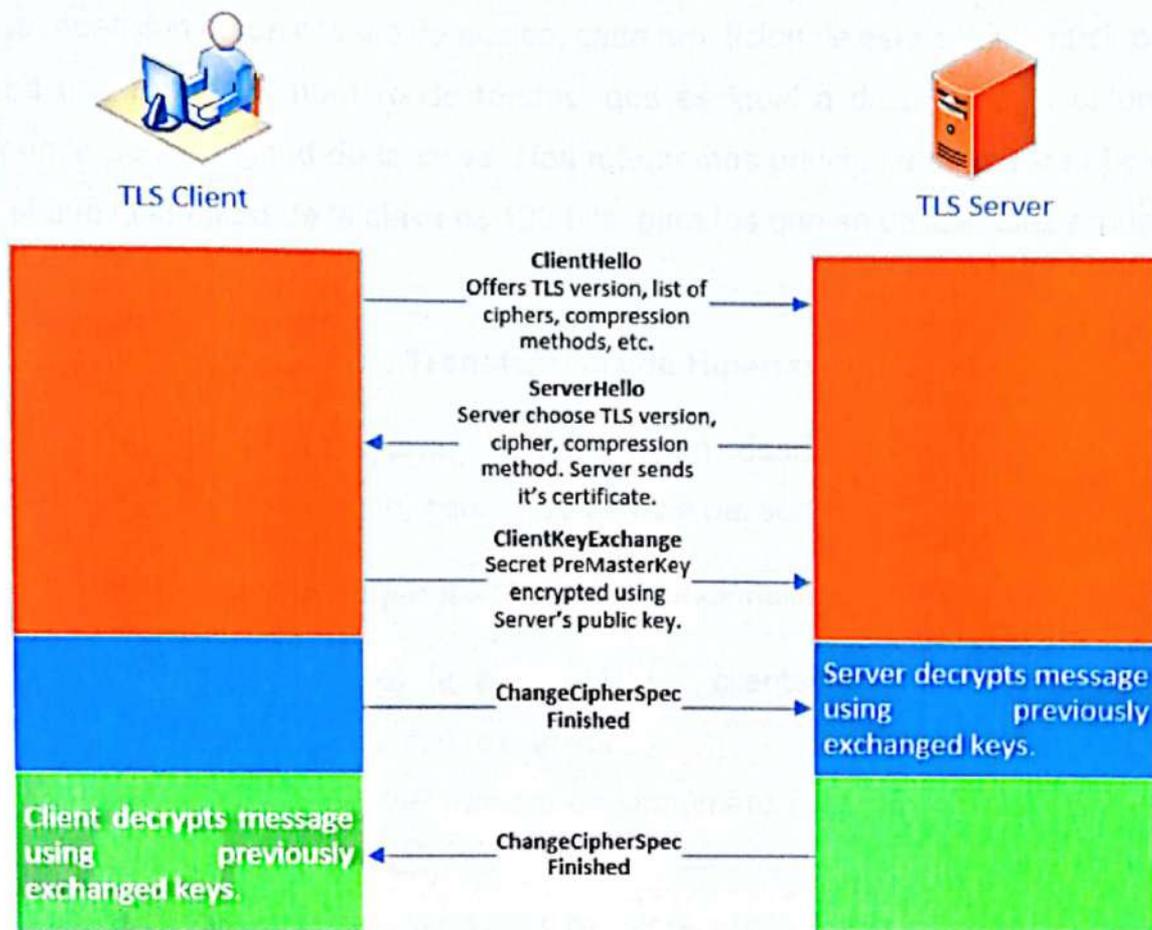


Ilustración 29. Autenticación mutua y encriptación para protocolos fiables de la capa de Transporte (OSI).

El proceso TLS ofrece un paquete ClientHello, que tiene información de la versión, métodos de compresión, lista de cifrados, etc. por parte del cliente. El servidor, le

ofrece un *ServerHello* donde escoge la versión, el método de compresión y el cifrado a utilizar. El mismo envía el certificado al cliente. El *ClientKeyExchange* es una llave encriptada que genera el cliente usando una llave pública del servidor. Por último, el *ChangeCipherSpec* es utilizado para descifrar el mensaje entre el cliente y el servidor.

Fuente: (Fernández, 2008)

2.3.9 Estándar Avanzado de Encriptación (AES)

El libro *Cryptography and Secure Communication* explica que AES es un cifrado de bloques que, en su forma preferida, utiliza longitudes de datos de 128 bits y longitudes de clave de 128, 192 o 256 bits. El procedimiento de cifrado consiste en la repetición de un cálculo de núcleo, cada repetición de este cálculo núcleo se llama una ronda. El número de rondas, que es igual a diez, doce, o catorce, depende de la longitud de la clave. Nos referiremos principalmente para el caso en el que la longitud de la clave es 128 bits, para los que se utilizan diez rondas.

2.3.10 Protocolo de Transferencia de Hipertexto (HTTP)

“Es utilizado para transportar la información desde donde se encuentra almacenada hasta el usuario, constituye la base del servicio WWW.”

El protocolo se caracteriza por las siguientes funcionalidades:

- Está formado por la modalidad de cliente/servidor, siguiendo una estructura de solicitud respuesta.
- El protocolo *TCP/IP* maneja un sinnúmero de protocolos dentro de la capa de transporte.
- HTTP se utiliza para enviar y recibir recursos de textos por el puerto 80, esta función es útil para mostrar los textos e informaciones de las páginas web que solicitamos.

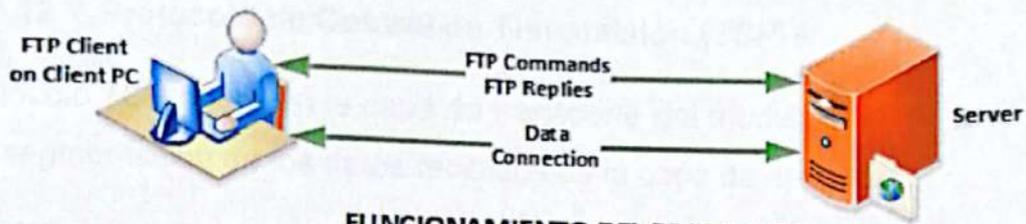
2.3.11 Protocolo de Transferencia de archivos (*FTP*)

En el ejemplar de Windows Server 2008 R2 define el protocolo de transferencias de archivos (*FTP*) como uno de los servicios más antiguos disponibles para transferir archivos entre sistemas.

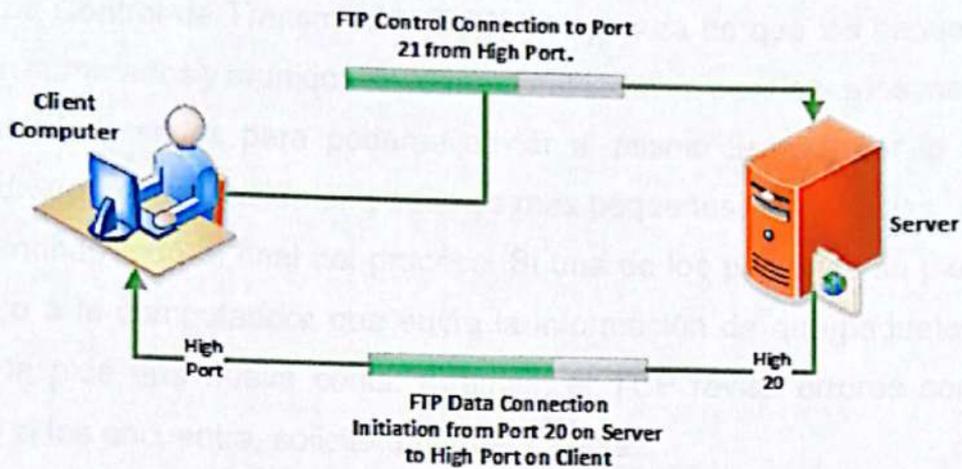
El funcionamiento del protocolo *FTP* Bobillier lo describe con dos host: Uno funcionando como cliente y otro como servidor. Anteriormente, el modo de conexión cliente-servidor es activo, donde dos conexiones son establecidas, una para la transmisión de comandos y otro para la escucha de datos. Con la transmisión de comandos, se abre una conexión en el puerto 21, y con la escucha de datos se especifica que puerto se utilizará para recibir los envíos del servidor. Tradicionalmente, los clientes *FTP* trabajaban en modo activo, donde la sesión se establecía en el puerto 21 del servidor y los datos se enviaban por iniciativa del servidor desde el puerto 20 a un puerto cualquiera del cliente.

Por otro lado, el libro Linux: Administración del sistema y explotación de los servicios de red dice que cuando el cliente establece un inicio de sesión con el servidor *FTP*, se establece una conexión en modo pasivo entre ellos. Este modo apareció para corregir esta situación mediante el establecimiento de dos sesiones por el cliente, el puerto utilizado para los datos es uno cualquiera que lo anuncia el servidor en modo comando y lo utiliza el cliente para abrir la sesión de datos.

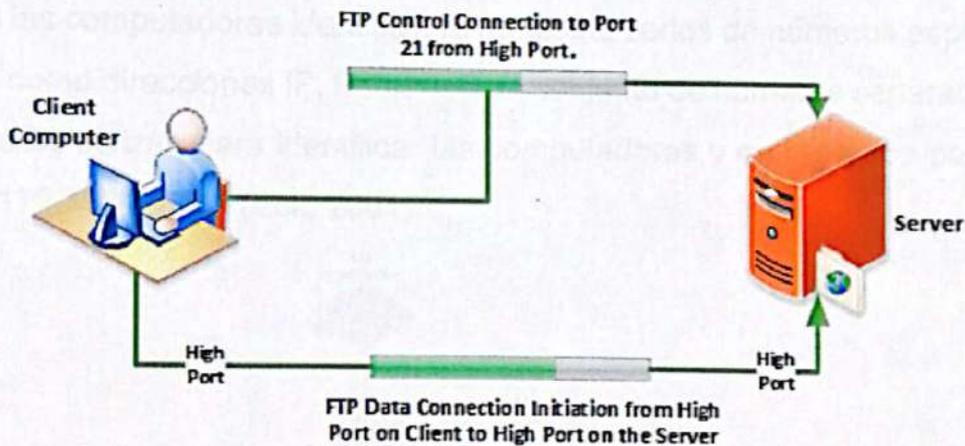
Además, si la conexión o sesión permanece abierta, el usuario puede usar el programa cliente para ejecutar comandos *FTP* que repercutan los archivos que están en el servidor. Además, estará en manos de permisos con autorizaciones, los archivos que pueden ser editados o incluso movidos a otros directorios. Utilizando el mismo protocolo se pueden hacer funciones de descargas desde el servidor, subir archivos hacia el servidor, cambiar permisos de archivos y/o directorios, etc.



FUNCIONAMIENTO DEL PROTOCOLO



MODO ACTIVO



MODO PASIVO

Ilustración 30. Protocolo de transferencia de archivos.

El funcionamiento del FTP es simple, se solicita una conexión mediante comandos y el servidor da respuesta al cliente. Una vez se hayan validados las informaciones se establece la conexión del cliente al servidor. En el modo activo la conexión de la data se inicia por el puerto 20 en el servidor. El pasivo es de una manera diferente, ya que el puerto que utilice para comunicarse con el servidor puede ser el puerto 21 o el puerto 20, cualquiera a utilizarse de manera automática.

Fuente: (Eck, 2001)

2.3.12 Protocolo de Control de Transmisión (TCP)

El protocolo TCP opera en la capa de transporte del modelo OSI, se caracteriza por la segmentación de los datos recibidos de la capa de aplicación.

Michael Eck, en su libro *La Internet: por dentro y por fuera* dilucida que el Protocolo de Control de Transmisión (TCP) se asegura de que los paquetes se encuentren numerados y reunidos de forma apropiada, en ocasiones los mensajes son demasiado grandes para poderse enviar al mismo tiempo, por lo que el protocolo divide la información en paquetes más pequeños, enviándolas una por una y ordenando todo al final del proceso. Si una de los paquetes se pierde, el TCP le dice a la computadora que envíe la información de que paquete se ha perdido y le pide una nueva copia. Además, el TCP revisa errores con cada paquete, y si los encuentra, solicita una nueva copia.

2.3.13 Protocolo de Internet (IP)

"Permite a las computadoras identificarse mediante series de números especiales conocidos como direcciones IP. Estas son un conjunto de números separados por puntos que se utilizan para identificar las computadoras y entregar los paquetes (ejemplo, 172.16.152.5)." (Eck, 2001)

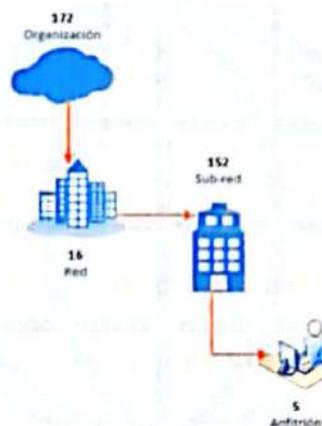


Ilustración 31. Protocolo de Internet (IP).

Imagen que muestra la comunicación e identificación de un cliente hacia su organización ubicada en la nube mediante una dirección IP.

Fuente: Imagen propia.

El protocolo IP trabaja en conjunto con el TCP, para formar el stack de protocolos TCP/IP, estos protocolos son más utilizados debido a que las direcciones IP identifican el host y el TCP es utilizado para la segmentación y recomposición de paquetes en la red.

2.3.14 Llamada de Procedimiento Remoto (RPC)

Atelin y Dordoigne, explican que la llamada de procedimiento remoto (RPC) permite la implantación de aplicaciones cliente/servidor, ya sea para una administración remota o en el marco de algunas aplicaciones como NFS.

“RPC funciona mediante la publicación de un puerto de mapeo de punto final (puerto 135) en un servidor que ejecuta servicios RPC. Este puerto es el encargado de dirigir los clientes para asignarle dinámicamente puertos de alta gama por los servicios. Estos puertos pueden ser cualquiera de los puertos TCP / IP en el rango de 1,024 a 65,536, en función de la asignación al azar por el servicio de mapas de puntos finales RPC.” (Noel, 2007)

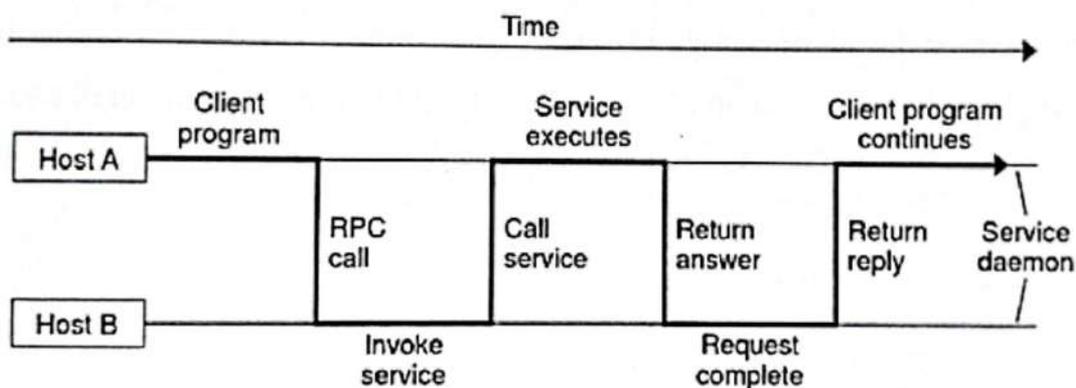


Ilustración 32. Llamada de procedimiento remoto (RPC).

En la imagen, se muestra el Host A que es el programa cliente, donde realiza una llamada RPC. El host B recibe la llamada e invoca el servicio. Luego, el servicio es llamado y posteriormente ejecutado. La respuesta es regresada y completa la solicitud. Después de completar la solicitud, la respuesta de retorno es enviado y el cliente continúa utilizando el programa. Ya en esta fase, el puerto se encuentra con la sesión conectada y lista para el envío de data de aplicaciones.

Fuente: (ORACLE, 2012).

2.3.15 Sistemas de Nombres de Dominio (DNS)

En el libro Redes de computadoras, se aclara que la esencia del DNS es la invención de un esquema de nombres jerárquico basado en dominios y un sistema de base de datos distribuido para implementar este esquema de nombres. El DNS se usa principalmente para relacionar los nombres de host y destinos de correo electrónico con las direcciones IP, pero también puede usarse con otros fines. El DNS se define en los RFCs 1034 y 1035. En el momento en que una persona solicita acceder a una página web, el host buscará de manera jerárquica la traducción de la dirección con aquella IP que la página tenga sincronizada. Cuando la dirección IP se haya encontrado, la solicitud llegará a la máquina o servidor destino ligados al dominio en específico.

Además, Tanenbaum explica que la forma en que se utiliza el DNS es la siguiente. Para relacionar un nombre con una dirección IP donde un programa de aplicación llama a un procedimiento de biblioteca llamado resolvidor, y le pasa el nombre como parámetro. El resolvidor envía un paquete UDP a un servidor DNS local, que después busca el nombre y devuelve la dirección IP al resolvidor, que entonces lo devuelve al solicitante. Una vez que tiene la dirección IP, el programa puede establecer una conexión TCP con el destino, o enviarle paquetes UDP.

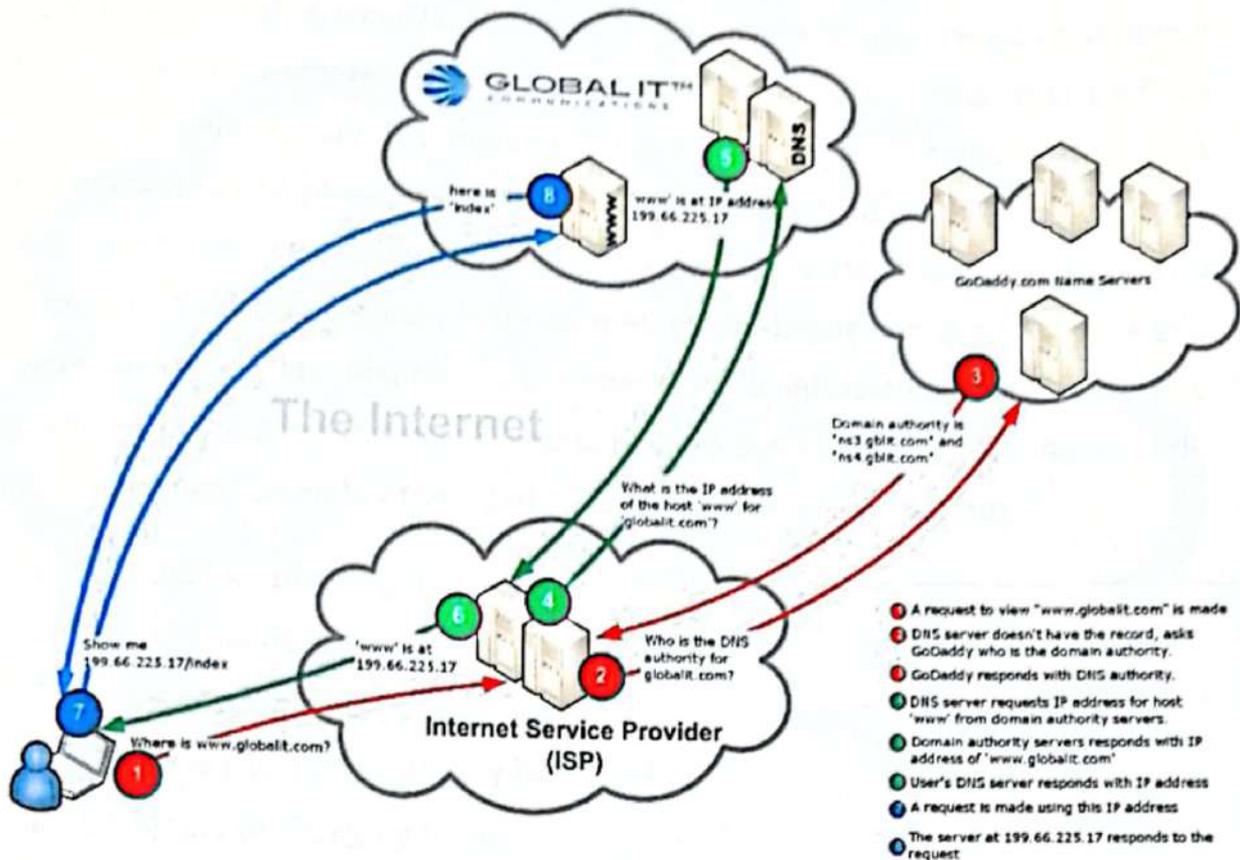


Ilustración 33. Sistema de nombre de dominio (DNS).

El usuario solicita acceder a una página web (www.unapec.edu.do, por ejemplo). La solicitud viaja a través de la red pública del internet y llega hasta los servidores DNS públicos, una vez ahí, el servidor sabe a dónde redirigir y envía la solicitud hacia el servidor DNS de UNAPEC. Una vez la solicitud haya sido recibida, el DNS de UNAPEC convierte la información del nombre a una dirección IP para validar que sea el nombre de dominio de la solicitud recibida. Mediante procesos de enrutamiento y autorizaciones, una respuesta es enviada al usuario de inmediato, donde la página es visualizada y accedida por el mismo.

Fuente: Imagen propia.

2.4 Data Center

Es un espacio centralizado para las operaciones de equipos de una organización, almacenando, administrando y difundiendo sus datos de manera cuidadosa. Los *Data Center* alojan los sistemas más críticos de una red y son importantes para la continuidad de las operaciones diarias.

Según el libro "*Data Center Fundamentals*", estas son algunas recomendaciones importantes que se debe de tener en cuenta cuando se planifica crear un *Data Center*: "Debido a que los centros de datos albergan recursos críticos de computación, las empresas deben hacer arreglos especiales con respecto tanto a las instalaciones que albergan el equipo y el personal necesario para una operación de 24 por 7. Estas instalaciones están dispuestas a apoyar una alta concentración de los recursos del servidor y la infraestructura de red. Las demandas planteadas por estos recursos, junto con la criticidad del negocio de las aplicaciones, crean la necesidad de abordar las siguientes áreas:

- Capacidad de energía.
- Capacidad de enfriamiento.
- Cableado.
- Controles de temperatura y humedad.
- Sistemas de Fuego y humo.
- Seguridad física: sistemas de acceso restringido y vigilancia.
- Espacio de rack y suelos técnicos.

2.4.1 Niveles de centro de datos (TIER)

De acuerdo al libro "*The Green and Virtual Data Center*" los TIER son desarrollados por el *Uptime Institute* y entrega a las empresas una forma estandarizada de medir el retorno de inversión (*ROI*) y el rendimiento a fin de determinar la disponibilidad de una instalación. Estas normas están compuestas de 4 niveles. Teniendo en cuenta que dentro de una instalación determinada, diferentes salas o zonas pueden tener diferentes niveles de protección.

Además, el libro "*TIER Classifications Define Site Infrastructure Performance*" explica la prueba de confirmación de rendimiento con el impacto operativo en cada uno de los 4 niveles de TIER, los cuales son:

TIER 1: Es la disponibilidad y es la implementación de menor costo, puede ser visto como el nivel menos fiable, debido al hecho de que los componentes de

capacidad no son redundantes, así como la vía de distribución es de un solo camino, si se produce un corte de energía importante o algún desastre, su equipo tiene más probabilidades de estar fuera de servicio, ya que no existen sistemas de copia de seguridad.

- El trabajo planificado requerirá la mayoría o la totalidad de la infraestructura del lugar, con sistemas que se apagan los equipos informáticos que afectan a los sistemas y usuarios finales.
- Una interrupción imprevista o fracaso de cualquier sistema de capacidad, componente de la capacidad, o elemento de distribución impactarán el equipo de cómputo.

El impacto operativo:

- El espacio es susceptible de interrupción, tanto planificada y actividades no planificadas, errores de funcionamiento o fallos espontáneos de los componentes de infraestructura del lugar causarán una interrupción *data center*.
- La infraestructura del lugar debe estar completamente cerrada sobre una base anual para realizar con seguridad necesaria preventiva trabajos de mantenimiento y reparación para prevenir desastres/interrupciones/fallos.
- Situaciones de urgencia pueden requerir paradas más frecuentes. Si no se realiza regularmente mantenimiento aumenta significativamente el riesgo de una interrupción no planificada, así como la gravedad del consecuente fracaso.

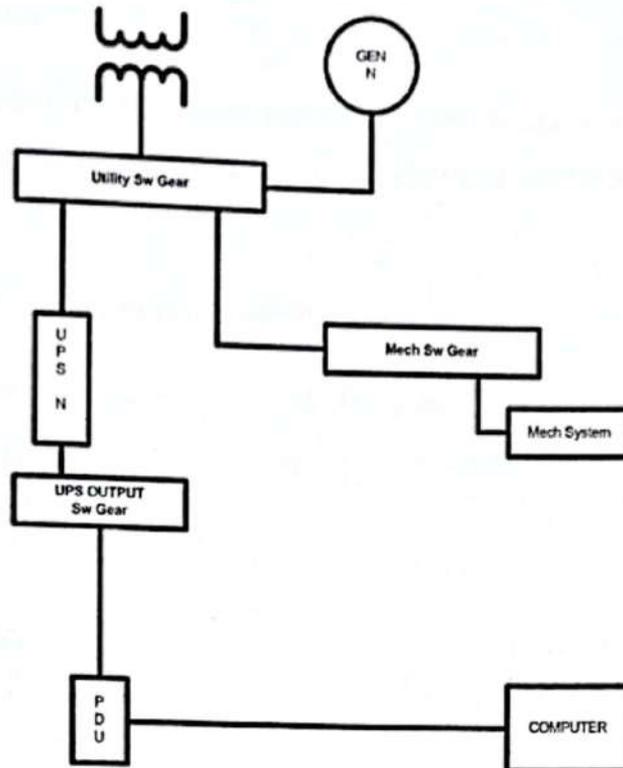


Ilustración 34. Diagrama de la Topología del Sistema Eléctrico de TIER 1.

Este diagrama ilustra los conceptos básicos de distribución eléctrica TIER 1. El computador está conectado al PDU (una regleta grande). El PDU va conectado al UPS, y el UPS se encuentra conectado a la fuente de energía eléctrica y/o una planta eléctrica.

Este diagrama no debe ser interpretado para representar una topología del sistema eléctrico estándar ni compatible o una solución de cumplimiento de cualquier conjunto particular de requisitos. Certificación de los TIER requiere la aplicación coherente de los conceptos de nivel a todos los subsistemas críticos relevantes que componen la infraestructura de datos del sitio central.

Fuente: (Pitt Turner IV, Seader, Renaud, & Bill, 2008)

TIER 2: Los TIER 2 son mucho más fiables que los centros de datos del TIER 1 a pesar de que pueden estar sujetos a problemas con el tiempo de actividad. Para alcanzar el nivel 2, la instalación tiene que cumplir con los criterios del TIER 1, así como garantizar que todos los componentes de capacidad son totalmente redundante.

El requisito fundamental:

- Un centro de datos TIER 2 tiene componentes de capacidad redundantes y una vía de distribución única, no redundante al servicio del equipo de cómputo.

La prueba de confirmación de la realización:

- Componentes de capacidad redundantes pueden ser retirados de servicio en una base planificada sin causar que cualquiera de los equipos informáticos quede cerrado.
- Extracción de las rutas de distribución de servicio para el mantenimiento u otra actividad requiere corte de corriente de los equipos informáticos.
- Una interrupción imprevista, fallo o fracaso de cualquier elemento del sistema de capacidad o distribución impactarán los equipos informáticos.

El impacto operativo:

- El espacio es susceptible de interrupción de ambas actividades planificadas y los eventos no planificados. Errores de funcionamiento o fallas espontáneas de componentes de la infraestructura del sitio pueden causar una interrupción del centro de datos.
- La infraestructura del sitio debe estar completamente cerrada sobre una base anual para realizar con seguridad el mantenimiento preventivo y reparación. Situaciones de urgencia pueden requerir paradas más frecuentes. Si no se realiza regularmente mantenimiento aumenta significativamente el riesgo de interrupción no planificada, así como la gravedad de la insuficiencia consecuentes.

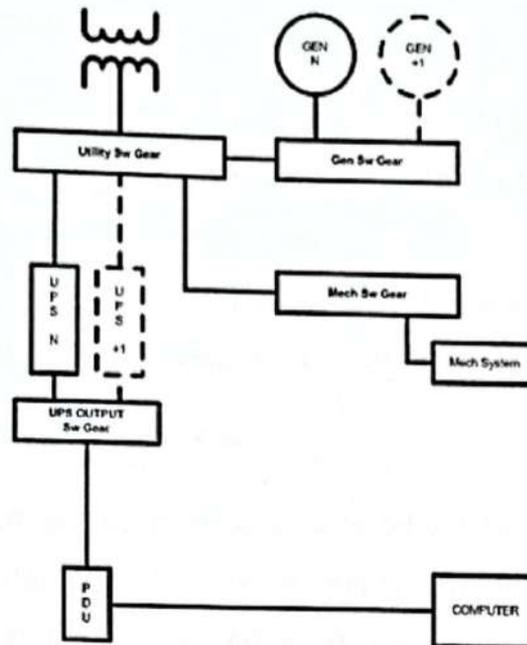


Ilustración 35. Diagrama de la Topología del Sistema Eléctrico de TIER 2.

Este diagrama ilustra un concepto de distribución eléctrica básico TIER 2.

El diagrama muestra los mismos elementos de distribución eléctrica TIER 1 pero con redundancia de UPS y plantas eléctricas. En caso que un UPS o planta eléctrica no se encuentre en servicio, el otro empezara a funcionar inmediatamente.

Tenga en cuenta el equipamiento adicional (redundante) necesarios para pasar de nivel 1 al Nivel 2. Este diagrama no debe ser interpretado para representar una topología del sistema eléctrico estándar ni compatible o una solución de cumplimiento de cualquier conjunto particular de requisitos.

Fuente: (Pitt Turner IV, Seader, Renaud, & Bill, 2008)

TIER 3: Para los TIER 3, los centros de datos se observan con frecuencia como las soluciones más rentable para medianas y grandes empresas, con alta disponibilidad, lo que garantiza un tiempo mínimo de recuperación ante desastres. El TIER 3 tiene que cumplir con todos los requisitos de los niveles 1 y 2, así como velar por todo el equipo de alimentación dual y tiene múltiples enlaces ascendentes. Algunos centros ofrecen equipos totalmente resistentes a fallos. Este nivel es generalmente considerado como de nivel 3+ en el mercado.

Los requisitos fundamentales:

- Un centro de datos concurrentemente mantenido tiene componentes con capacidad redundante y varias rutas de distribución que están al servicio de los equipos informáticos.
- Todo el equipo de TI es de doble potencia e instalado correctamente para que sea compatible con la topología de la arquitectura del sitio.

La prueba de confirmación de la realización:

- Cada uno de los componentes de la capacidad y los elementos de las rutas de distribución pueden ser retirados de servicio en una base planificada sin afectar cualquiera de los equipos informáticos.
- Una interrupción imprevista, fracaso de cualquier sistema de capacidad, elemento de un componente de capacidad o distribución tendrán un impacto negativo en los equipos informáticos y los datos.
- Hay suficiente capacidad instalada permanentemente para satisfacer las necesidades del sitio cuando los componentes redundantes se han retirado de servicio.

El impacto operativo:

- El espacio es susceptible de interrupción de las actividades planificadas. Errores de funcionamiento o fallas espontáneas de componentes de la infraestructura del sitio pueden causar una interrupción el ordenador.
- Mantenimiento de la infraestructura planificada del lugar se puede realizar mediante el uso de los componentes de capacidad redundantes y rutas de distribución para trabajar con seguridad en el equipo restante.
- Para establecer mantenibilidad concurrente del sistema de distribución de energía crítica entre el SAI y el equipo de cómputo, TIER 3 requerirá que todo el *hardware* tenga entradas de alimentación dual según la definición de tolerante a errores de alimentación, conformidad con las especificaciones del Instituto, Versión 2.0. Los dispositivos de transferencia, como los interruptores de punto de uso, deben ser

incorporados para equipo de cómputo que no cumpla con esta especificación.

- Durante las actividades de mantenimiento, el riesgo de interrupción puede ser elevado. Este estado de mantenimiento no derrota la calificación Nivel alcanzado en las operaciones normales.

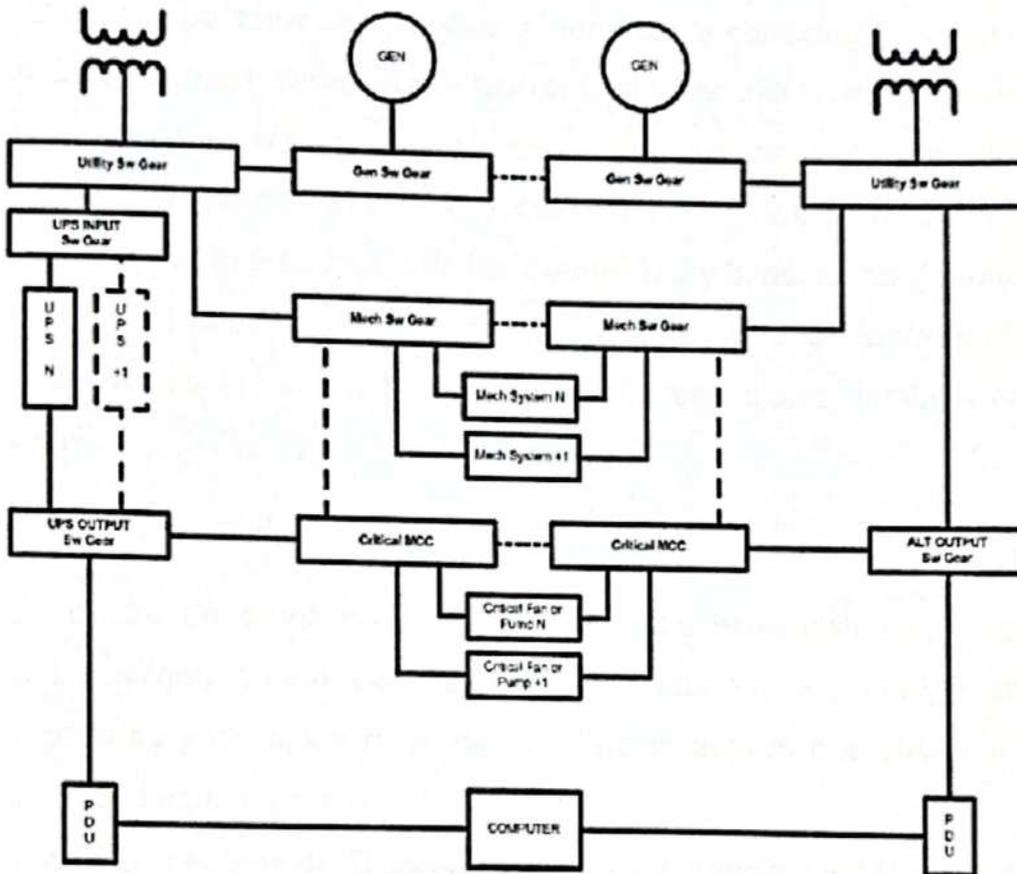


Ilustración 36. Diagrama de la Topología del Sistema Eléctrico de TIER 3.

Este diagrama ilustra un concepto de distribución eléctrica TIER 3, donde se muestra los dispositivos informáticos conectados por dos regletas, cada una de las regletas van conectado a la salida del UPS, uno funcional y otro como Back-up. También posee sistemas críticos y la redundancia va aplicada a cada elemento básico de la distribución eléctrica. La única desventaja es que la redundancia en UPS se encuentra en uno de los PDU, el otro se encuentra solo para ser activado como salida alterna.

Tenga en cuenta el equipamiento adicional (redundante) necesarios para pasar de nivel 2 al Nivel 3. Este diagrama no debe ser interpretado para representar una topología del sistema eléctrico estándar ni compatible o una solución de

cumplimiento de cualquier conjunto particular de requisitos. Certificación de TIER requiere la aplicación coherente de los conceptos de nivel a todos los subsistemas críticos relevantes que componen la infraestructura de datos del sitio central.

Fuente: (Pitt Turner IV, Seader, Renaud, & Bill, 2008)

TIER 4: Un centro de datos de nivel 4 es generalmente considerada la opción más cara para las empresas, debido a que todo el equipo incluye climatización (*HVAC*), servidores, almacenamiento, enfriadores y enlaces ascendentes, debe ser resistente a fallos totalmente, siendo el más robusto de los TIER. Estos centros se adhieren a todos los requisitos de los niveles 1, 2 y 3, así como garantizar que todo el equipo es completamente resistente a fallas. Esto se logra mediante la creación de copias físicas de todos los equipos esenciales, también conocido como N + N.

El requisito fundamental:

- Un centro de datos con tolerancia a fallos tiene sistemas físicamente aislados que tienen cada uno redundancia en sus componentes de capacidad y múltiples rutas de distribución activos que sirven al mismo tiempo al equipo de cómputo.
- Todos los equipos de TI tienen el doble de potencia y están correctamente instalado para ser compatible con la topología de la arquitectura del sitio.

La prueba de confirmación de la realización:

- Un solo fallo de cualquier sistema de capacidad, componente de la capacidad, o elemento de distribución no tendrá impacto en el ordenador.
- El sistema en sí responde de forma automática (auto-cura) a un fracaso para prevenir una mayor repercusión en el sitio.
- Cada uno de los componentes de la capacidad y los elementos de las rutas de distribución pueden ser retirados de servicio en una planificada base sin afectar a ninguno de los equipos informáticos.

- Los sistemas complementarios y rutas de distribución deben ser aislados físicamente el uno del otro (compartimentada) para evitar cualquier caso sencillo de impactar de manera simultánea ambos sistemas o caminos.
- Se requiere un enfriamiento continuo para la continua disponibilidad.
- Tiene capacidad suficiente para satisfacer las necesidades del sitio cuando los componentes redundantes o rutas de distribución han sido retirados del servicio.

El impacto operativo:

- El sitio no es susceptible a la interrupción de un solo acontecimiento imprevisto.
- El sitio no es susceptible a la interrupción de cualquier planificada actividad de trabajo.
- Con el fin de establecer mantenibilidad concurrente del sistema de distribución de energía crítica entre los UPS y los equipos informáticos, los TIER 4 requieren todo el *hardware* para tener entradas de alimentación duales como se define por la Tolerancia a fallos de alimentación conforme.
- El mantenimiento de la infraestructura del sitio puede ser realizada por los componentes redundantes y la capacidad de distribución en caminos para trabajar de forma segura en el equipo restante.
- Durante las actividades de mantenimiento, el riesgo de interrupción puede ser elevado, debido a que se cierra una ruta y los equipos informáticos se exponen a una aumento del riesgo de interrupción debe ocurrir una falla en el camino restante. Este estado de mantenimiento no derrotar a la calificación de Nivel alcanzado en las operaciones normales.
- El funcionamiento de la alarma de incendios, extinción de incendios, o el suministro de energía característica de emergencia (EPO) puede causar una interrupción centro.

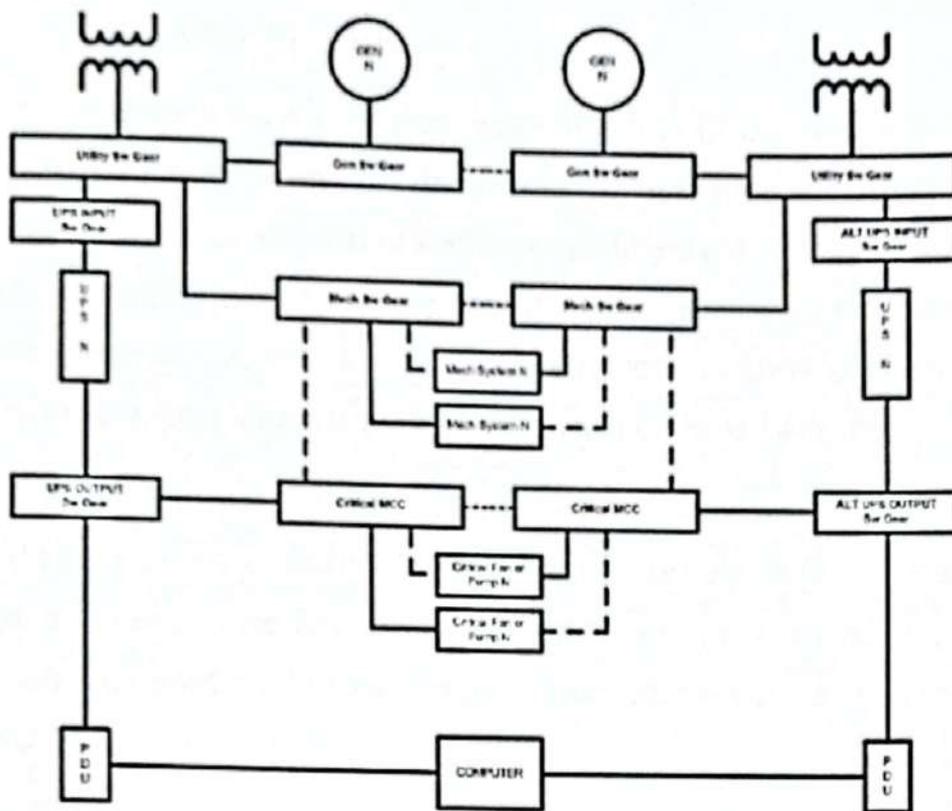


Ilustración 37. Diagrama de la Topología del Sistema Eléctrico de TIER 4.

Este diagrama ilustra un concepto de distribución eléctrica TIER 4, donde cada equipo informático conectado a cada equipo de distribución eléctrica de manera redundante.

Tenga en cuenta el equipamiento adicional (redundante) necesarios para pasar de nivel 3 a TIER 4. Este diagrama no debe ser interpretado para representar una topología del sistema eléctrico estándar ni compatible o una solución de cumplimiento de cualquier conjunto particular de requisitos.

La omisión de los módulos SAI redundantes no cambiaría la calificación TIER 4. Certificación de Nivel requiere la aplicación coherente de los conceptos de nivel a todos los subsistemas críticos relevantes que apoyan la sala de ordenadores.

Fuente: (Pitt Turner IV, Seader, Renaud, & Bill, 2008)

2.4.2 Tipos de UPS

Una fuente de alimentación ininterrumpida (UPS), se utiliza principalmente para proporcionar una fuente de energía de reserva a importantes equipos informáticos de sobremesa. Actuando como una interfaz entre la red eléctrica y las aplicaciones sensitivas, proveyendo carga eléctrica continua para equipos electrónicos independientemente del estado de la red eléctrica. El UPS entrega una libre alimentación de voltaje libre de cualquier disturbio de la red eléctrica.

La importancia de un UPS es sencilla, un disturbio o falla en la alimentación eléctrica de los equipos electrónicos por solo unos segundos puede afectar miles o millones de operaciones básicas en la organización, el resultado de esta falla puede resultar en pérdida de data con peligrosas consecuencias entorno al costo como pérdida de producción.

Los diversos tipos de sistemas de alimentación ininterrumpida (UPS) y sus atributos, suelen confusión en la industria de los *data centers*. Numerosos malentendidos sobre los sistemas de UPS se generan cuando los diferentes tipos de topologías de UPS son debidamente identificados, topología UPS indicando la naturaleza básica del diseño, como son:

➤ **Conversión Simple**

De acuerdo al libro "Data Center Handbook" en un diseño de conversión simple, el poder de corriente alterna (CA) de entrada se utiliza para alimentar directamente el equipo crítico conectado.

Sin embargo, puede haber algo de regulación de voltaje hecho dentro de las UPS a cualquiera "buck" (inferior) o "impulso" (subir) al subir la tensión a un nivel que sea aceptable para las cargas. Algunos UPS simples de conversión diseñan fuente de alimentación a las cargas críticas a través de un inductor en serie o un lineal o Ferro transformador resonante, por lo tanto, dar "línea para cargar" el aislamiento y la protección transitoria. UPS simples de conversión suelen requerir un circuito de carga de batería por separado para asegurarse de que la batería se quede cargada adecuadamente para soportar la carga crítica cuando se le solicite.

➤ **UPS en modo de espera**

Geng en el libro "Data Center Handbook" explica que un UPS en modo de espera se encuentra frecuentemente en aplicaciones de pequeña potencia, tales como computadora de escritorio u oficina en casa o la protección de cine en casa. Para estas aplicaciones, alguna protección transitoria y respaldo de batería corta son los impulsores principales, así como de bajo costo. Los sistemas de reserva funcionan haciendo pasar energía de la red desde la entrada directa a la salida, a través de sólo un dispositivo de conmutación, tal como un interruptor estático o pequeño relé.

Cuando el voltaje de entrada de CA está dentro del nivel de tolerancia de la especificación de tensión de salida del SAI (normalmente de - 15 a + 10%), el UPS permanece en este modo, como un dispositivo de paso muy eficiente. Si hay un suministro de luz o grande oscilación de tensión, el inversor del UPS se enciende y los interruptores de conmutación internos a la fuente de respaldo (batería) por el poder.

El UPS en modo de espera diseña hasta que se pierda la tensión de entrada de CA, y luego cambiar a la operación de la batería, así que siempre hay una "transferencia" o tiempo de conmutación, donde la tensión de salida va a 0V.

➤ **Línea interactiva (LI) UPS**

"La línea interactiva de UPS (LI) se encuentra en muchas aplicaciones, desde la oficina, en el hogar, el respaldo del piso de la fábrica hasta TI, e incluso en algunos equipos de procesamiento.

Sistemas LI vienen en un número de diferentes arquitecturas de energía básica, sin embargo, todas siguen el mismo principio que van a regular el voltaje AC entrante a una cierta especificación de tensión de salida, lo que permite un rango de voltaje de entrada más ancho que el diseño del sistema de espera. Al hacer esto, ellos son un poco menos eficaces que el de espera, pero ofrecen el beneficio de la batería, por lo tanto, tiene una operación de posible bajada de tensión o sobre las condiciones de voltaje. Las diferentes formas en que los sistemas de LI

regulan el rango de tensión en el funcionamiento continuo del inversor en paralelo con la utilidad de tener un sencillo transformador de tomas de conmutación que cambia a un modo buck o impulso, basado en la tensión de entrada. Los sistemas que operan su inversor para regular la tensión son menos eficientes que los modelos de conmutación de derivación. Además, suelen proporcionar una tensión de salida que se regula más ligera." (Geng, 2014)

➤ **Modo de espera de Ferro**

En el libro *Electrical Power Quality* explica que el UPS Standby-Ferro fue una vez la forma dominante de UPS en el rango de 3 a 15 kVA. Este diseño depende de un transformador de saturación especial que tiene tres bobinados (conexiones eléctricas). El camino de alimentación primaria es de entrada de CA, a través de un interruptor de transferencia, que cruza por el transformador y la salida.

En caso de un fallo de alimentación, el interruptor de transferencia se abre, y el inversor recoge la carga de salida. En el diseño de Standby-Ferro, el inversor se encuentra en modo de espera y se activa cuando la potencia de entrada falla y se abre el interruptor de transferencia. El transformador tiene capacidad especial "Ferro resonante", que proporciona la regulación de tensión limitada y la forma de onda de salida. El aislamiento de los transitorios de potencia de CA suministrado por el transformador Ferro es tan bueno como o mejor que cualquier filtro disponible, pero el transformador Ferro crea una severa salida de distorsión de la tensión y transitorios que puede ser peor que una conexión de CA pobre. El Standby-Ferro genera una gran cantidad de calor debido a que el transformador resonante Ferro es inherentemente ineficiente. (Dixit & Yadav, 2010)

➤ **Doble conversión en línea**

Curtis explica que esta tecnología utiliza la combinación de una doble conversión (AC a CC y de CC a CA) al circuito de alimentación, que alimenta continuamente la carga para proporcionar acondicionamiento de protección de energía y corte de luz eléctrica. Con el rectificador / inversor (doble conversión) UPS, la potencia de entrada se convierte primero en DC, donde el suministro normal de potencia

alimenta el rectificador y la carga de corriente alterna se suministra continuamente por la salida del inversor. La alimentación de CC se utiliza para cargar las baterías y operar de forma continua al inversor en cualquier condición de carga requerida. El inversor convierte la parte posterior de alimentación de CC a la corriente alterna. Hay una ruta de bypass estático instantánea donde cualquier componente falla en el circuito de alimentación rectificador / inversor (el interruptor de bypass estático es parte del sistema de UPS, que puede ser interno o en un armario separado, dependiendo del tamaño del sistema).

➤ **Conversión Delta en línea**

"La conversión delta UPS en línea está disponible para cargas de 5 kVA o más. En este tipo de UPS, el inversor suministra la tensión de carga, pero en lugar del rectificador cargar las baterías como en los UPS de doble conversión, la conversión delta utiliza convertidores bidireccionales que están conectados a una batería.

Estos se convierten de AC a DC y de nuevo a la CA con una mínima pérdida de energía. Los convertidores están conectados en serie entre la fuente de alimentación y la carga. También compensan las diferencias entre la tensión de salida requerida y el voltaje de la utilidad. La distorsión armónica se reduce y aumenta la eficiencia energética.

La conversión delta en línea UPS tiene las mismas características de salida que la doble conversión en línea, pero la conversión delta reduce las pérdidas de energía y costos. La calidad de la potencia de entrada de los UPS de conversión delta también es mejor, especialmente en los tamaños kVA más grandes." (Hordeski, 2005)

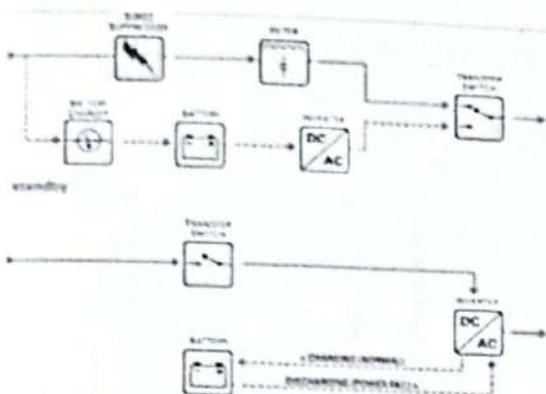


Ilustración 38. Línea interactiva (LI) UPS.
Fuente: (Whitman & Mattord, 2011)

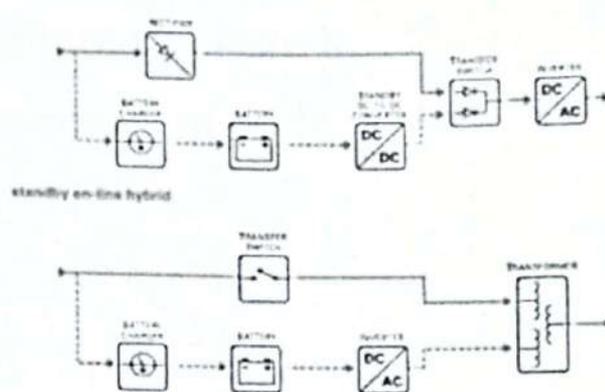


Ilustración 39. Modo de espera de Ferro.
Fuente: (Whitman & Mattord, 2011)

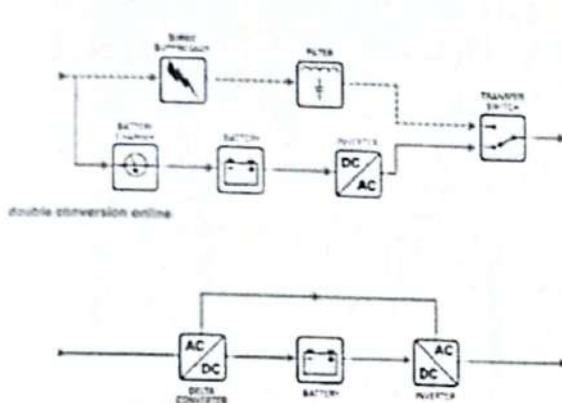


Ilustración 40. Conversión Delta en línea.
Fuente: (Whitman & Mattord, 2011)

LEYENDA

-  Inversor
-  Batería
-  Filtro
-  Interruptor de transferencia
-  Cargador de batería
-  Supresor de sobre-tensiones
-  Transformador

RESUMEN

Los servicios de la computación en la nube van en constante evolución, y a medida que esta tecnología se desarrolla va adquiriendo nuevos servicios y se va integrando a empresas que requieran de esos servicios. Los clientes siempre irán orientados a pequeñas, medianas y grandes empresas que requieran una solución de migrar su infraestructura, *software* y/o plataforma a la nube. Los protocolos son necesarios para entender el idioma entre el servidor y el cliente a través de la red y una vez entendidas, su comunicación se habrá establecido para el uso del *cloud computing*. Los Data Center deben contar con redundancia a nivel eléctrico o niveles de TIER para que su trabajo se realice ininterrumpidamente en caso de apagones. Los UPS ayudan a sostener los niveles de TIER como energía alterna.

Resumen gráfico, Capítulo II.

Estructura de los componentes de la Nube

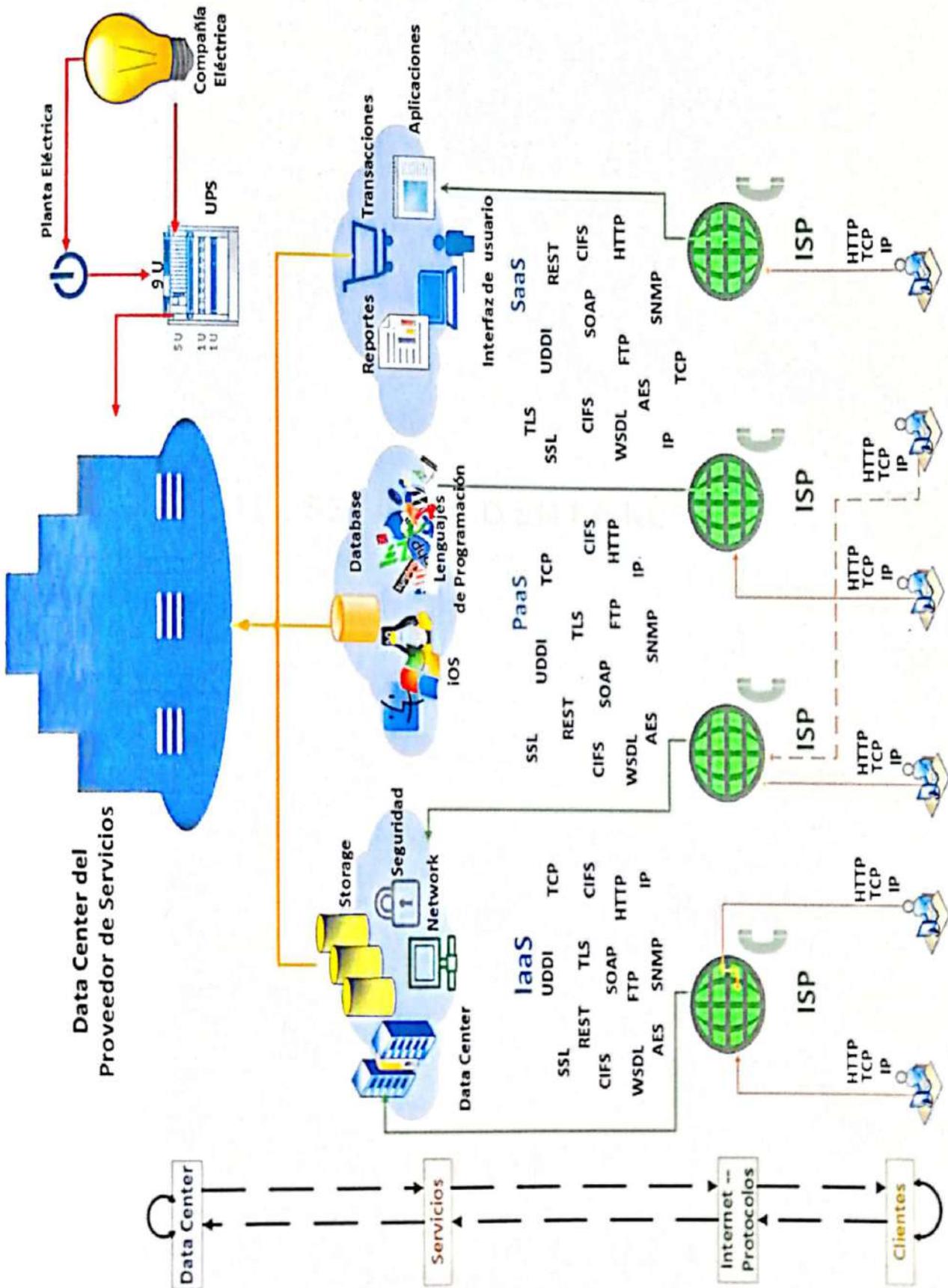


Ilustración 41. Resumen gráfico, Capítulo II. Componentes de la Nube.

Fuente: Imagen propia.

CAPITULO III. SEGURIDAD EN LA NUBE

3.1 Seguridad en la nube

3.1.1 Características de la seguridad en la nube

La seguridad es la protección de la infraestructura computacional e información de sistemas específicos. También, se podría decir que es una disciplina que estipula los procedimientos, normas, técnicas y métodos destinados a conseguir un sistema de información seguro.

En el libro "*Securing the Cloud*", aclara que una buena manera de visualizar la computación en la nube, a manera de ejemplo, como un paisaje que ya ofrece un gran valor y los servicios, pero que aún no está en la etapa de Ricinos de Oro, donde las necesidades de computación de cada cliente son recibidos por una solución justa. Como un nuevo paradigma para la computación, es que la nube presenta retos aún, ya que esta tecnología es nueva en el mercado y todavía no se ha utilizado a su máxima capacidad. No todos los modelos de las nubes que hoy en día se implementan (público, mixto, privado y de la comunidad) son apropiadas para cada servicio, cada servicio al cliente, o todos los inquilinos. Asimismo, no es rentable para todos los proveedores de la nube implementar alta seguridad u ofrecer garantía al mismo nivel de la seguridad. Sin embargo, el *cloud computing* es convincente, es una tendencia de rápido crecimiento, y está obligando a importantes avances en las tecnologías de soporte.

En este libro se expone a algunos de los problemas de seguridad común:

- **Fiabilidad y disponibilidad de la red:** Es uno de los ejes clave para la computación en las nubes y servicios en la nube. Desde una nube pública el proveedor debe abordar el potencial de pérdida catastrófica con conectividad a la red troncal de Internet. La misma preocupación debe ser una consideración primaria para los consumidores de servicios informáticos que confían en infraestructuras críticas para la nube. Existen preocupaciones similares para las nubes privadas:

- **Privacidad y Datos:** Los datos no podrán permanecer en el mismo sistema, en el mismo centro de datos, o dentro de los sistemas del mismo proveedor de nube. Posiblemente, los datos pueden incluso ser almacenado en otro país, incurriendo en una gran preocupación.
- **Control de Datos:** Que un usuario u organización determinan si puede ser llevadero en almacenamiento o procesamiento de datos que pertenecen a otros. Como mínimo, los datos deben cifrar en la granularidad de los archivos que pertenecen a los usuarios u organizaciones determinadas.
- **Viabilidad de los proveedores de la nube:** Los proveedores de la nube son relativamente nuevos en el negocio, hay preguntas sobre la viabilidad del proveedor y su compromiso. Esta preocupación se agrava cuando un proveedor requiere que los inquilinos usen un estándar no basada en interfaz de programación de aplicaciones (API), efectuando así un *lock-in* (impidiendo un arrendatario en la migración a un proveedor alternativo).
- **Los Incidentes de Seguridad:** Los inquilinos y los usuarios necesitan saber qué información del proveedor compartirá cuando se presente un incidente. Esta preocupación está relacionada con preguntas sobre la transparencia que los proveedores pueden ofrecer a los procesos de seguridad, procedimientos y políticas internas.
- **Recuperación de Desastres y Empresariales:** Los inquilinos y usuarios de continuidad debe entender cómo pueden seguir sus propias operaciones y servicios si el entorno de producción subyacente está sujeta a un desastre.
- **Sistemas de vulnerabilidades y riesgo de ataques conocidos:** Todo el *software*, *hardware* y equipos de red está sujeta a la exposición de nuevas vulnerabilidades. Algunos componentes pueden plantear mayores riesgos basado en una historia de vulnerabilidades y *exploits*. Los inquilinos no pueden tolerar las vulnerabilidades específicas o áreas de riesgo por un sin número de razones. Una nube específica puede estar sujeta a nuevo tipos de ataques o puede ser inmune a los tipos de ataques comunes.

- **Cumplimiento de la normativa o legislativa:** Es difícil de utilizar nubes públicas cuando sus datos están sujetos a restricciones legales o el cumplimiento normativo. La construcción de una nube que pueda ser certificada, representa un reto a la actual etapa de conocimiento de nubes y mejores prácticas.

Por otra parte, el libro "*Seguridad informática de Aguilera López*", nos da a conocer los tipos de seguridad informática, dando a conocer que se divide en 4 tipos, las cuales son:

- **La seguridad pasiva:** Está constituida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión, por motivos de incidentes de seguridad y permite la recuperación del sistema. A estas medidas se le conocen como corrección.
- **La seguridad activa:** Los mecanismos y procedimientos que permiten prevenir y detectar riesgos para la seguridad del sistema de información constituyen la seguridad activa. Al igual que los mecanismos de seguridad pasiva, la seguridad activa se aplica a la parte física y a la parte lógica del sistema de información y en todo caso pueden ser físicos y lógicos.
- **La seguridad física:** Protege elementos físicos de la empresa u organización, tales como el *hardware* y el lugar donde se realizan las actividades (edificio o habitaciones).
- **La seguridad lógica:** Es aquella que abarca la protección del *software* y de los sistemas operativos, que en definitiva, es la protección directa a los datos y la información.

La seguridad en las nubes se define como la seguridad lógica que funciona en servidores virtuales comunicados a través de internet. Dicha seguridad representa una novedad para las empresas pues está aplicada a la tecnología de *cloud computing*. Para las empresas, la computación en la nube ofrece una gran

variedad de servicios rentables y aplicaciones, las mismas son “userfriendly” (fáciles de usar).

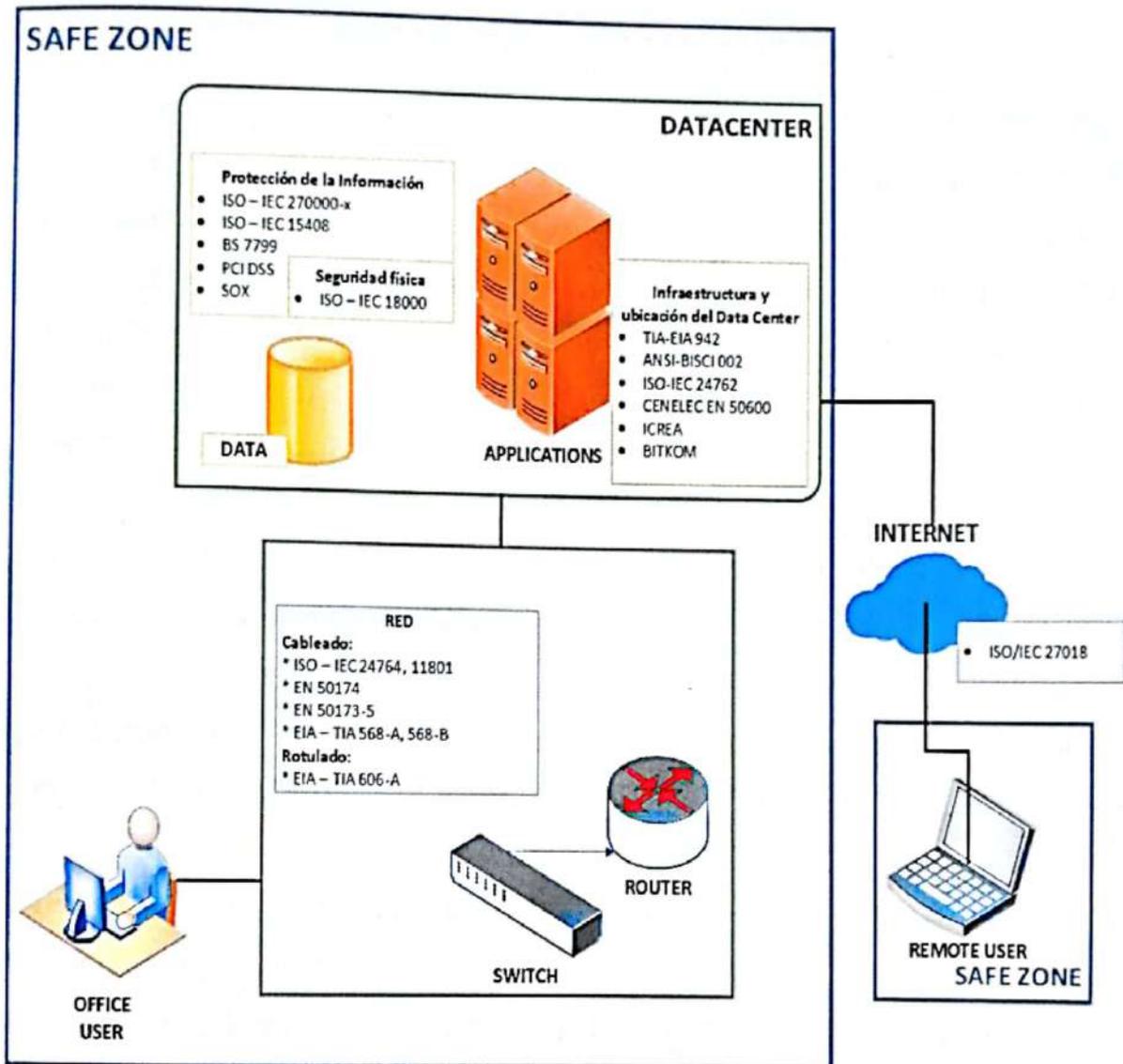


Ilustración 42. Safe zone.

La imagen explica las zonas que deben permanecer seguras al ofrecer servicios de computación en la nube, con el conjunto de estándares que cada una de las partes debe cumplir para garantizar la seguridad.

Fuente: Imagen propia.

La seguridad en las nubes ofrece mayor velocidad de detección de intrusos, información más completa de las amenazas y el bloqueo de las mismas. Su fuerza radica en las actualizaciones de archivos de patrones en menor tamaño a tiempo real. Gracias a esto, la información pueda estar siempre seguro en cualquier situación.

Aguilera López explica que el esqueleto de *Cloud Computing* es la Web 2.0, debido a que muchas las empresas por seguridad no almacenan sus datos ni alojan sus servidores web en su propia localidad, sino que contratan los servicios que ofrecen grandes centros de datos del país o del extranjero. Incluso puede ser que la empresa solamente mantenga terminales que trabajan como clientes con un servidor alojado en un data center de Alemania o Texas, que es el que tiene el *software* y se encarga de la gestión y conservación de la información.

Además, en el libro "Seguridad informática" (2010), la autora destaca diferentes características de la seguridad en la computación en la nube, tales como:

- **Reducción de Inversión de capital y costes operativos:** Sería la consolidación del número de servidores utilizados y activación de los equipos virtuales en la medida que la empresa los necesite.
- **Incremento de la agilidad empresarial:** Se ofrecen nuevos servicios de forma rápida y sencilla.
- **Escalabilidad inmediata:** Activación y desactivación de los equipos virtuales cuando sea necesario.
- **Acceso desde cualquier lugar y en cualquier momento:** Se ofrecen servicios empresariales a los usuarios que están en la oficina, en casa o que estén utilizando cualquier dispositivo móvil.

Cabe destacar que la computación en la nube no necesita instalarse en la maquina sino que esta funciona solamente por conexión a internet, por lo tanto, la información estará segura en la web, disminuyendo los riesgos de catástrofes o

amenazas que pueda causar la pérdida de la información, ya que la información es vital para cualquier empresa u organización.

3.1.2 Características de funcionamiento de las nubes

La nube se refiere básicamente a una aplicación cliente/servidor que se ejecuta en Internet y en las *intranets* TCP/IP. Como tal, las herramientas de seguridad y los enfoques discutidos son importantes para la nube.

En el tema “Nube escala, patrones y la eficiencia operativa” del libro de Winkler, especifica que al entrar en un centro de datos que aloja una infraestructura en la nube, se dará cuenta el inmenso tamaño del espacio y el ruido abrumador que viene de incontables ordenadores con el mismo rack todos bien cableados y al final, buscan lo mismo. Escala masiva, un aspecto disciplinado y patrones repetidos son tres cualidades de exitosas implementaciones en la nube. Estas cualidades, obviamente, no son única de la nube, pero contribuyen a las ventajas del modelo de nube. Mediante el desarrollo de patrones repetidos adecuadas y ponerlas en práctica en un escala masiva, usted ganará las ventajas de costos en todas las fases del ciclo de vida de la nube.

A partir de la adquisición y construcción de salida a las operaciones, los costos pueden ser minimizados a través de simplificaciones. Estas mismas ventajas se benefician la seguridad.

La seguridad de *cloud computing* puede ser mejor de lo que se cree, debido a que los proveedores pueden proporcionar recursos para resolver las dificultades de seguridad al que muchos usuarios no pueden enfrentar o evitar. Sin embargo, aún es un factor crítico para las informaciones vitales de una empresa u organización.

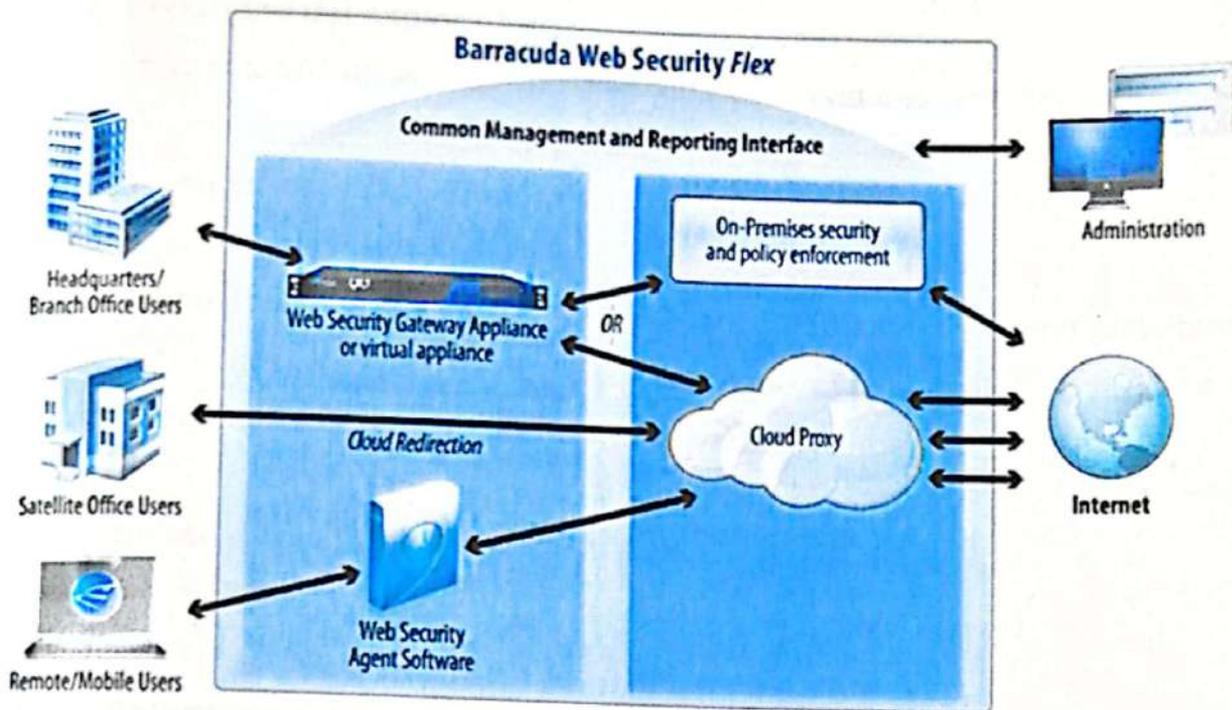


Ilustración 43. Barracuda Web Security Flex Architecture.

Para la barracuda web security flex, el usuario interactúa con el agente software, con un re-direccionamiento hacia la nube o con un security Gateway para filtrar y chequear las listas de accesos que se tienen permitidos a la nube. Toda esa solicitud es procesada al cloud proxy o dependiendo de las políticas de seguridad y administración del mismo, será dirigido al encargado de seguridad informática de la empresa para tomar las medidas necesarias.

Fuente: (Globenet International, 2015)

3.2 La seguridad

3.2.1 Seguridad como servicio

En la computación en la nube, la seguridad es proporcionada por los proveedores. Existen dos métodos para resguardar la seguridad. Como son:

- Primer método: El cliente/usuario puede cambiar las formas de entrega incluidos en los servicios en nube.
- Segundo método: Los proveedores *cloud* brindan seguridad como un servicio agregado.

3.2.2 Seguridad del explorador

Para la computación en la nube son utilizados los servidores remotos, los equipos de los usuarios son utilizados solo para la entrada y salida de operaciones y para realizar la autenticación de la información en el *cloud*.

Normalmente los usuarios utilizan un navegador web estándar como plataforma de acceso a la nube, esto puede ser clasificado por diferentes tipos, para la encriptación de datos y la autenticación del host, existen:

- Software como Servicio (SaaS)
- Aplicaciones web o web 2.0 *Transport Layer Security* (TLS)

3.2.3 Autenticación

El cimiento fundamental para el control del acceso en la nube es la autenticación, es lo más importante debido a que todos los datos en internet son accesibles para aquel que tenga las informaciones para validarse.

El Modulo de Plataforma Confiable (TPM) ofrece un método de cifrado para los sistemas de autenticación, como los nombres de usuario y contraseñas. Además de este módulo, existe un estándar para la autorización de usuarios como un sistema de seguridad para la comunicación (tiempo real) entre el cliente y el proveedor. (McAfee, Inc., 2014)

3.2.4 Perdida de gobernanza

El cliente accede a que el *Cloud Provider* tenga el control en un sinnúmero de operaciones que afectan la seguridad de la plataforma e información. Además, dependiendo el acuerdo por el tipo de servicio, el proveedor tiende a no brindar estos servicios, pudiendo dejar huecos en las defensas de seguridad.

3.2.5 Bloqueo de proveedor (*Provider Lock-In*)

Alacot Torres, explica que la interoperabilidad entre las plataformas ha mejorado pero las API's para *Cloud Computing* siguen siendo esencialmente propietarias, o al menos no han sido objeto de una normalización activa. La preocupación por la dificultad de extracción de los datos de la nube es uno de los principales factores de desconfianza en muchas organizaciones para la migración de *Cloud Computing*.

En su trabajo, *Implantación de una plataforma de Cloud Computing*, dice que el lock-in de clientes/usuarios puede ser atractivo para los proveedores de *Cloud Computing*, pero los usuarios son vulnerables a los aumentos de precios, a los problemas de fiabilidad o incluso a la salida del negocio de los proveedores. La solución "obvia" es la estandarización de las API para que un desarrollador de SaaS pueden desplegar servicios y datos a través de múltiples proveedores de *Cloud Computing* para evitar que el fallo de una sola empresa, se lleve todas las copias de datos de los clientes/usuarios consigo.

3.2.6 Protección de los datos

La computación en la nube pone en riesgo la protección de datos para los usuarios y sus proveedores. En muchos casos, ocasiona dificultades para el proveedor (en el rol del controlador de la información) para asegurar la efectividad práctica del manejo de los datos y la transición para la transferencia de los datos.

Existen certificaciones para resguardar la seguridad en el procesamiento de datos, controles y actividades. Un ejemplo sería la certificación SAS70⁶. Además, hay que tener presente que el transporte de datos por internet contienen paquetes de señuelos y malware, para provocar que el usuario en actividades desconocidas delictivas.

⁶ SAS70 (Statement on Auditing Standards No. 70): Norma de auditoría ampliamente reconocido que proporciona orientación sobre la auditoría de los controles internos de una organización de servicio e informar los procesos de información financiera de sus clientes. SSAE 16 sustituye SAS 70 en 2011. (Rouse, 2015)

En la gráfica se pueden apreciar todos los componentes básicos para sostener la seguridad basada en *cloud*.

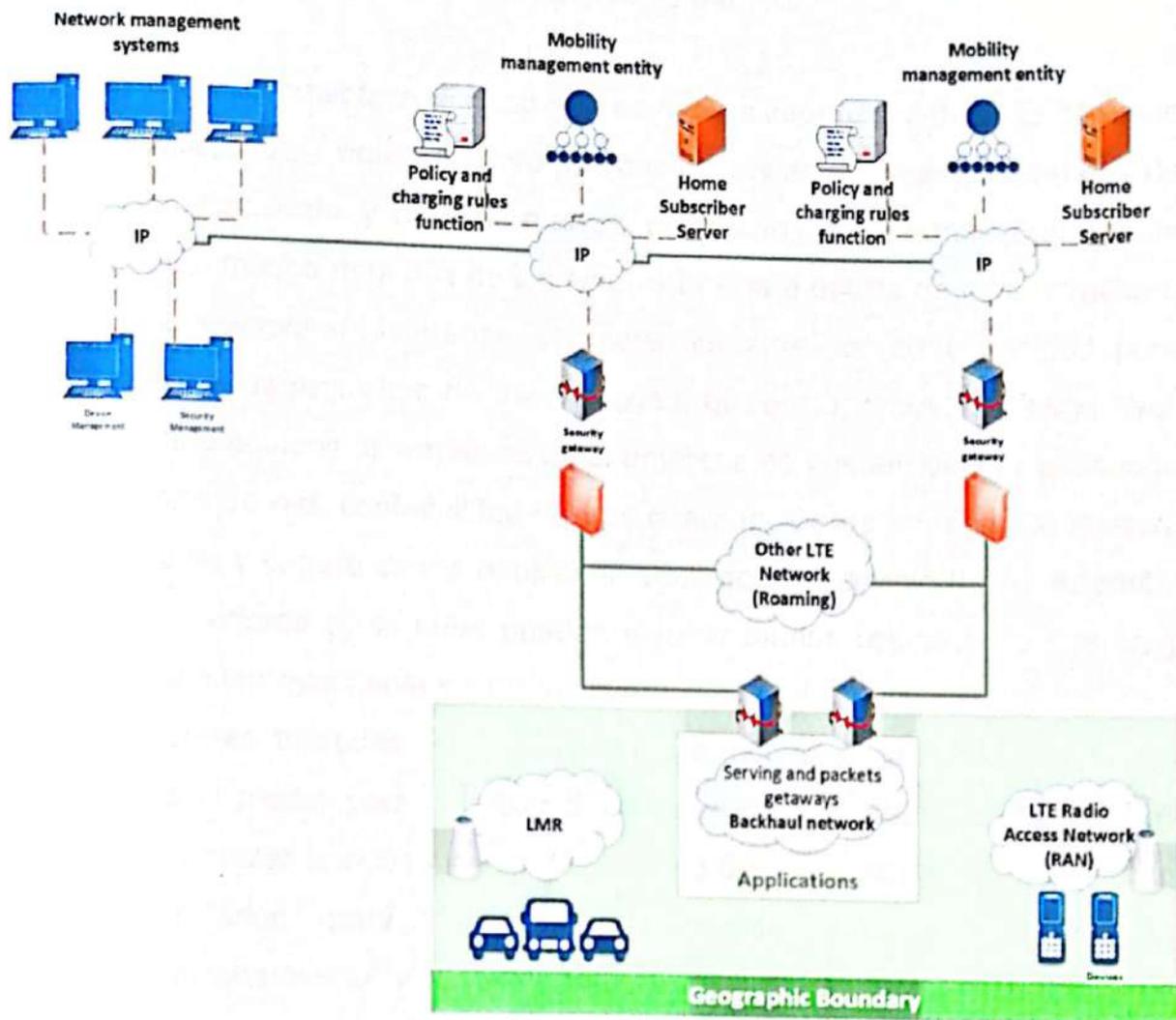


Ilustración 44. La nube LTE, una red de banda ancha inalámbrica para seguridad pública.

En la imagen se presenta el centro de operaciones de red de un proveedor de servicios, capaces de configurar, administrar y manejar los equipos informáticos a nivel de seguridad y de red. Luego se analizan y coordinan las políticas y reglas que se aplicaran a la red. Estas políticas se configuran en el security Gateway. Se encuentra un back-up como plan alternativo de estas políticas en caso de recuperación ante desastre. Por último, la tecnología LTE da servicios a dispositivos móviles.

Fuente: (Wendt, 2012)

3.3 La fundación para la nube

Las piezas tecnológicas subyacentes para la construcción de la infraestructura en la nube pueden ser clasificadas de la siguiente manera:

- **Cloud Infrastructure:** Es una infraestructura informática definida como un conjunto de equipos informáticos (servidores, componentes de almacenamiento y de red) que se organizan para permitir crecimiento gradual mucho más allá de los niveles típicos a escala de infraestructura. Estos componentes deben ser seleccionados por su capacidad para soportar los requisitos de escalabilidad, eficiencia, robustez y seguridad. Muchos equipos informáticos de la empresa no pueden ofrecer adecuado soporte de red, confiabilidad u otras cualidades para entregar de manera eficiente y segura contra el nivel de acuerdos de servicio (SLA). Además, los servidores de la nube pueden resultar menos costosos de operar, y pueden ser más fiable sin discos internos en cada servidor.
- **Las redes basadas en IP:** En la infraestructura de la nube, la red sirve como el medio para conectar a los usuarios a la nube, así como para interconectar la nube interna. Un modelo de empresa de redes cubre las necesidades para formar una eficiente y segura "nube de aprovisionamiento y operación". Múltiples interruptores en *datapaths* convierten en puntos únicos de fallo (SPOF) y el costo compuesto de varias maneras. Aunque la optimización puede señalar a un solo unificado de red, la seguridad es requerida para que la red pueda dividir o virtualizar y así efectúe la separación entre diferentes clases de tráfico.

Aunque la creación de redes puede llegar a ser más plano, se debe esperar para ver múltiples redes paralelas con el fin de apoyar la seguridad. Algunos de éstos gestionan la plataforma a partir de datos públicos y tráfico de servicio, otros son necesarios para los patrones de escala. Estas redes adicionales implican un costo adicional, pero por el precio, también te dan separación física y seguridad superior.

- **Virtualización:** Con profundas raíces en la informática, la virtualización se utiliza para dividir un único servidor físico en múltiples máquinas virtuales, o un único recurso físico (como almacenamiento o redes) en múltiples virtuales. La virtualización permite consolidación de servidores con una gran flexibilidad de utilización. Para la computación en nube, virtualización tiene un gran valor en la puesta en marcha rápida y clausura de servidores. El *software* de virtualización en la nube, también presenta una perspectiva dinámica y visión unificada de la utilización de recursos y la eficiencia de las operaciones de TI en la nube. La virtualización permite a las primarias de la tecnología lograr ingresos rentables para la utilización del servidor y fortalece el apoyo a la separación entre múltiples arrendatarios en *hardware* físico. La virtualización no es la única manera de lograr estos beneficios, pero sus ventajas lo convierten en el método de elección.
- **Software:** Permite gestionar, aprovisionar, desarrollar los servicios, contabilidad, y la seguridad relacionado a todos los aspectos de la infraestructura en la nube. Es fundamental que la misma sea capaz de cumplir dinámicamente las políticas de separación, aislamiento, seguimiento y composición de servicios. Los patrones regulares de infraestructura en la nube activan el *software* para automatizar las tareas proporcionando elasticidad y cambio de forma para presentar los servicios que se componen de servidores, máquinas virtuales, almacenamiento, servicios, y otros componentes de TI. Con el *software*, podemos automatizar el aprovisionamiento y desaprovisionamiento.
- **Servicio de Interfaces:** La interfaz de servicio entre el proveedor y el consumidor es un diferenciador clave para la nube. Representa un contrato que cumplir para la propuesta de valor de los *SLAs* y condiciones de precios. Es, en gran parte, esta interfaz que hace que las nubes se destacan como nuevo. Se convierte en un valor competitivo y permite la competencia entre los proveedores. Con la adición de las interfaces de auto-servicio, se ganan nuevas optimizaciones. Los clientes de la nube pueden dedicarse recursos de la nube en una de forma automatizada sin

tener que actuar como un impedimento. Almacenamiento y otros recursos que se expresan a través de interfaces gráficas que el usuario puede manipular para definir y posteriormente crear la infraestructura de TI virtual. Solo necesita un navegador web y una tarjeta de crédito, y ya es libre para construir su propio centro de datos virtual. (Council)

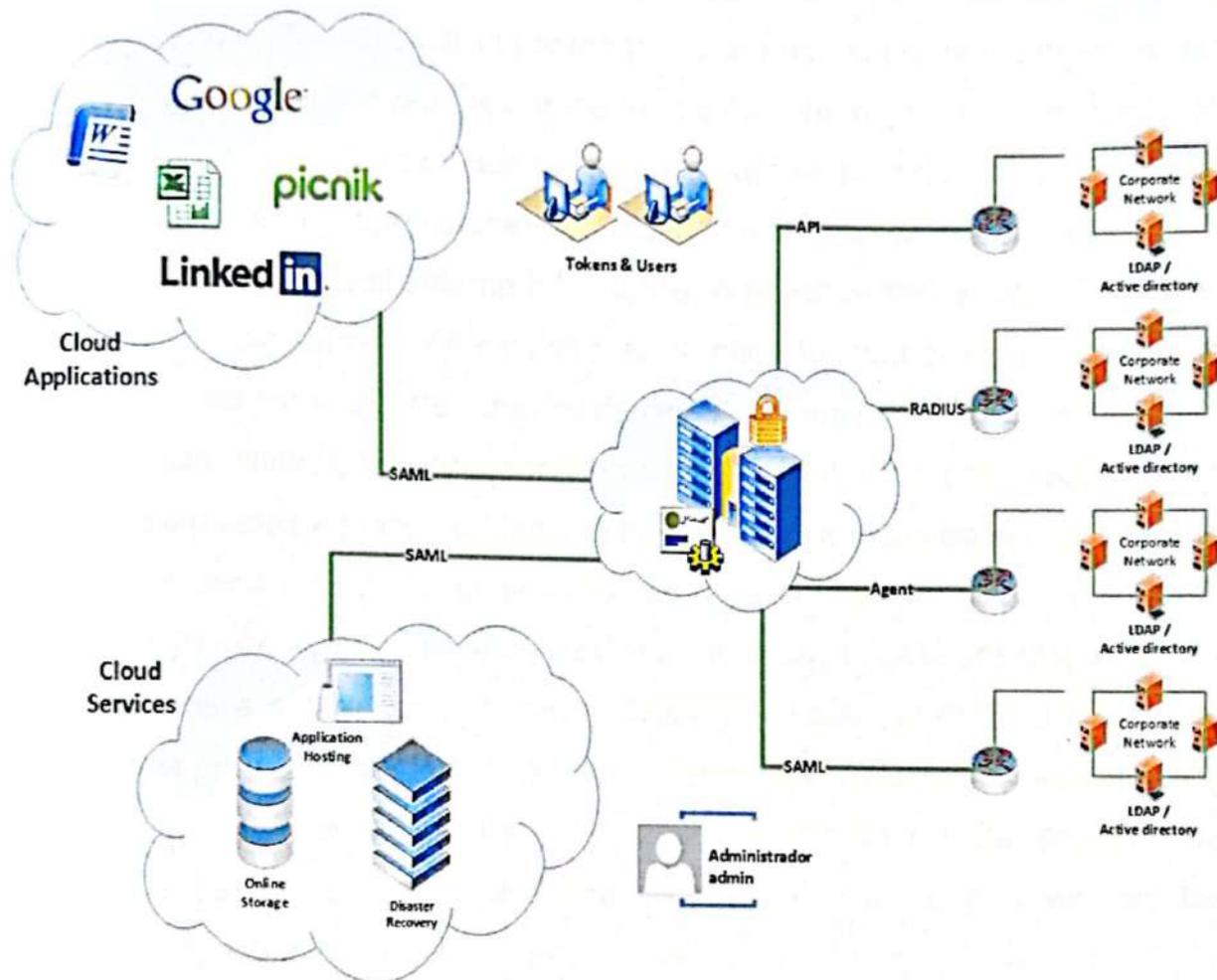


Ilustración 45. Infraestructura de Seguridad en la Nubes.

Cuando los usuarios ejecutan una aplicación en la nube primero son llamados por el SAML para conocer la autenticación del usuario y posteriormente ser autorizados. Más tarde, la solicitud pasa por el Internet, la cual es solicitada a un agente, un servidor RADIUS o un API, dependiendo cual tenga instalado. El Active Directory o LDAP chequea en sus registros las informaciones del usuario para ser validadas. Una vez sean validadas como accesibles, el usuario es libre de utilizar los servicios en la nube de manera segura.

Fuente: (Gemalto N.V., n.d.)

En el ejemplar de "Security for Cloud Computing: 10 Steps to Ensure Success" explica que las preocupaciones de seguridad y privacidad cuando utilizan los servicios de *cloud computing* son similares a las de servicios no tradicionales en la nube, las preocupaciones son amplificadas por el control externo sobre los activos de la organización y el potencial de la mala gestión de esos activos. La transición a la computación en nube pública implica una transferencia de responsabilidad y control para el proveedor de la nube sobre la información, así como el sistema que componen, anteriormente estaban bajo el control directo de la organización. La transición suele ir acompañado de pérdida de control directo sobre la gestión de las operaciones y también una pérdida de influencia sobre las decisiones tomadas en el entorno informático. A pesar de esta pérdida inherente de control, un consumidor de servicios en la nube todavía tiene que asumir la responsabilidad por el uso de servicios de *cloud computing* con el fin de mantener la conciencia situacional, sopesar alternativas, establecer prioridades, y los cambios de efectos en la seguridad y la privacidad que están en el mejor interés de la organización. El consumidor logra esto al asegurar que el contrato con el proveedor y su acuerdo de nivel de servicios asociados (*SLA*) tiene disposiciones apropiadas para la seguridad y la privacidad. En particular, el *SLA* debe ayudar a mantener la protección legal de la privacidad en relación a los datos almacenados en los sistemas del proveedor. El consumidor también debe asegurar la integración adecuada de los servicios de *cloud computing* con sus propios sistemas de gestión de seguridad y privacidad.

La computación en la nube representa un área muy dinámica en el momento actual, con nuevos proveedores y nuevas ofertas que llegan todo el tiempo. Hay una serie de riesgos de seguridad asociados a la nube que debe ser abordado adecuadamente, como son:

- **La pérdida de la gobernabilidad.** Para las implementaciones de la nube pública, los consumidores ceden necesariamente control al proveedor de la nube a través de una serie de cuestiones que puedan afectar a la seguridad. Al mismo tiempo, los acuerdos de nivel de servicio (*SLA*) en las nubes no

- pueden ofrecer un compromiso de proporcionar tales capacidades por parte del proveedor de la nube, lo que deja huecos en las defensas de seguridad.
- **Ambigüedad y Responsabilidad.** Dado que el uso de los servicios de computación en la nube se extiende sobre el consumidor y las organizaciones de proveedores, la responsabilidad de los aspectos de la seguridad se puede transmitir a través de ambas organizaciones, con el potencial de partes vitales de las defensas para quedar sin vigilancia si hay una falta de asignación de responsabilidad claramente. La división de responsabilidades entre las organizaciones de consumidores y proveedores puede variar según el modelo que se utiliza (por ejemplo *IaaS* frente *SaaS*).
 - **Fallo de aislamiento.** Arrendamientos múltiples y recursos compartidos están definiendo las características del *cloud computing* pública. Esta categoría de riesgo cubre el fracaso de los mecanismos que separan el uso de almacenamiento, la memoria, enrutamiento e incluso la reputación entre los diferentes arrendatarios (por ejemplo, los llamados ataques de los huéspedes de salto).
 - **Dependencia de un proveedor.** La dependencia de los servicios propios de un proveedor de la nube en particular podría dar lugar a que el consumidor sea atado a ese proveedor. Servicios que no soportan la portabilidad de las aplicaciones y los datos a otros proveedores aumentan el riesgo de los datos y la falta de disponibilidad del servicio.
 - **Cumplimiento y riesgos legales.** La inversión en el logro de la certificación (por ejemplo, estándares de industrias o los requisitos reglamentarios) se puede poner en riesgo por la migración de utilizar la computación en nube, si el proveedor de la nube no puede presentar pruebas de su propio cumplimiento de los requisitos pertinentes o si el proveedor de la nube no permite auditoría del consumidor de la nube. Es la responsabilidad del consumidor en la nube comprobar que el proveedor tiene certificaciones adecuadas en el lugar, pero también es necesario que el consumidor este claro acerca de la división de las responsabilidades de seguridad entre el consumidor y el proveedor. Del mismo

modo, es importante asegurarse de que las responsabilidades del consumidor puedan utilizarse correctamente al utilizar los servicios de *cloud computing*.

- **Manejo de incidentes de seguridad.** La detección, notificación y gestión posterior de las brechas de seguridad es una preocupación para los consumidores que están confiando en proveedores para manejar estos asuntos.
- **Vulnerabilidad en la interfaz de gestión.** Las interfaces de administración del consumidor de un proveedor en la nube pública, suelen ser accesibles a través de Internet y median el acceso a grandes conjuntos de recursos que proveedores de hosting tradicionales, por lo tanto, representan un mayor riesgo, especialmente cuando se combina el acceso remoto y las vulnerabilidades de los navegadores web.
- **La protección de datos.** *Cloud computing* presenta varios riesgos de protección de datos para los usuarios y los proveedores de la nube. Las principales preocupaciones son las exposiciones o publicaciones de los datos sensibles, poca disponibilidad de los datos o la pérdida. En algunos casos, puede ser difícil para el consumidor (en el papel de controlador de datos) comprobar efectivamente las prácticas de manipulación de datos del proveedor y así estar seguro de que los datos se maneja de una manera legal. Este problema se agrava en los casos de múltiples transferencias de datos, por ejemplo, entre los servicios de nube federados.
- **Comportamiento malicioso de la información privilegiada.** Los daños causados por las acciones maliciosas de iniciados que trabajan dentro de una organización puede ser sustancial, dado el acceso y las autorizaciones que puedan tener. Esto se ve agravado en el entorno de *cloud computing* ya que dicha actividad podría ocurrir dentro de uno o dos organizaciones de consumidores y la organización proveedora.
- **El fracaso empresarial del proveedor.** Estos fallos podrían hacer los datos y aplicaciones esenciales para el negocio del consumidor disponible.
- **Indisponibilidad del servicio.** Esto podría ser causado por una serie de factores, de equipos o fallas de *software* en el centro de datos del proveedor a

través de las fallas de las comunicaciones entre los sistemas de consumo y los servicios de proveedores.

- **Eliminación de datos inseguros o incompletos.** Las solicitudes para eliminar recursos de la nube, por ejemplo, cuando un consumidor cancela el servicio con un proveedor, puede no resultar en cierta limpieza de los datos. La eliminación adecuada y oportuna de datos también puede ser imposible (o deseable desde la perspectiva del consumidor), ya sea porque las copias adicionales de los datos se almacenan pero no están disponibles, o porque el disco que desea borrar también almacena datos de otros clientes. En el caso de múltiples clientes y la reutilización de los recursos del *hardware*, esto representa un riesgo mayor para el consumidor que es el caso del *hardware* dedicado.

Mientras que la seguridad está por encima de los riesgos que deben tratarse, el uso de la computación en la nube ofrece oportunidades para la innovación en el aprovisionamiento de servicios de seguridad que mantienen la perspectiva de mejorar la seguridad general de muchas organizaciones. Los proveedores de servicios de *cloud computing* deben ser capaces de ofrecer servicios avanzados de apoyo a la seguridad y a la privacidad debido a sus economías de escala y capacidades de automatización, potencialmente una bendición para todas las organizaciones de consumidores, en especial para aquellos que han limitado el número de personal con habilidades avanzadas de seguridad.

Al considerar un cambio a utilizar la computación en la nube, los consumidores deben tener una clara comprensión de los posibles beneficios de la seguridad, los riesgos asociados y establecer expectativas realistas con su proveedor de la nube.

Hay que tener en cuenta los modelos de prestaciones de servicios (Infraestructura como Servicio (*IaaS*), Plataforma como Servicio (*PaaS*) y Software como Servicio (*SaaS*) ya que cada modelo trae diferentes requisitos y responsabilidades de

seguridad. Además, cada norma asume un papel importante para mejorar la seguridad en la nube.

3.4 Las nubes utilizando funciones

La seguridad en las nubes tiene como función proteger los datos e informaciones alojados en un servidor virtual en la nube. Esto permite el desempeño de la iteración del usuario con dicha tecnología de una manera eficaz y privada, sin interrupciones. (Reis, Seguridad para la nube y virtualización para DUMMIES, 2013)

En el libro Seguridad para la nube y virtualización para DUMMIES, el uso de la informática en la nube ha aumentado enormemente y ha generado todo un nuevo modelo empresarial. Ofrece a las empresas la posibilidad de modificar la disponibilidad de sus recursos informáticos de manera rápida, fácil y barata, además de adaptarse a las exigencias de los recursos informáticos dinámicos. De modo que ¿Cómo se protegen las empresas frente a los peligros específicos de la nube? ¿Cómo se asegura una empresa de que sus datos en la nube tengan el mismo nivel de protección que cuando se accede a ellos y se almacenan en su propio centro de datos?

Los proveedores de servicios en la nube quieren que tus datos estén seguros. Les interesa que emplees las herramientas apropiadas para proteger tus aplicaciones virtuales en servidores virtuales de las máquinas virtuales de otras organizaciones que se ejecutan en la misma máquina anfitriona o están almacenadas en el mismo espacio.

Estas funciones han de permitirte supervisar y bloquear las amenazas que puedan surgir de otras aplicaciones virtuales. También debería ser posible proteger aplicaciones específicas o archivos y directorios confidenciales.

Daniel Reis, explica que en el mundo compartido de la nube, tus datos están más expuestos porque circulan por redes compartidas y se guardan en dispositivos de almacenamiento compartidos con los datos de otros clientes de la nube. Además, la ubicación de tus datos almacenados puede cambiar en base a muchos factores que se hallan fuera de tu control. El hecho es que un proveedor de servicios en la nube puede trasladar, y trasladará, tus aplicaciones virtuales entre anfitriones físicos y tus datos de un entorno de almacenamiento a otro.

Es posible que el movimiento de datos dé lugar a problemas puesto que pueden quedar restos legibles de tus datos en una antigua ubicación de almacenamiento.

Para proteger los datos que viajan por redes compartidas y son almacenados de manera compartida, es necesario adoptar un enfoque que se centre más en los datos. Trata de emplear un componente de seguridad que te permita establecer directivas de acceso y almacenamiento de datos en la nube (esto también puede funcionar en tu propio centro de datos).

Asimismo, sírvete del cifrado para garantizar que los datos no puedan ser leídos cuando circulen o sean almacenados en la nube. Este sistema te permite establecer y hacer cumplir directivas para la protección de datos mediante un servidor de directivas que te pertenece y el cual controlas. Se trata en parte de utilizar claves para cifrar y descifrar datos, con derechos definidos de acceso a las claves y los datos de acuerdo con las directivas de tu empresa.

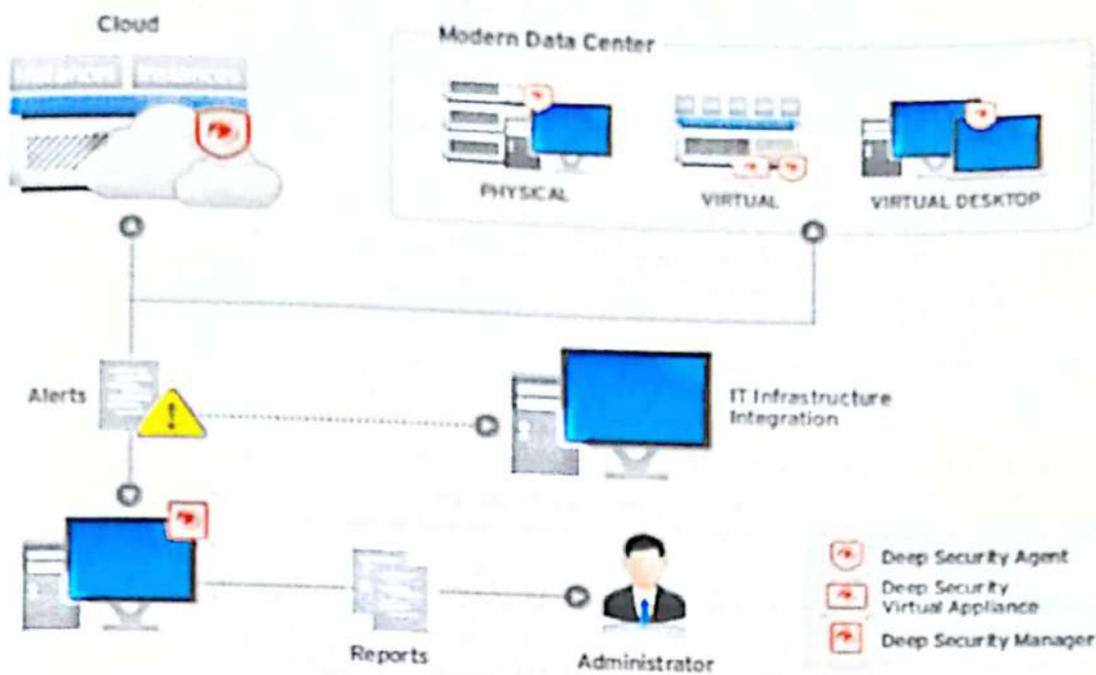


Ilustración 46. Solución de seguridad para la nube y el centro de datos, con la integración de la plataforma *Deep Security*.

La imagen muestra la seguridad para un Data Center en la nube. La nube se encuentra asegurada con agentes Deep security, que es seguridad basada en virtualizaciones. Esa nube está compuesta por equipos informáticos físicos y PC de escritorios virtualizados, asegurados por agentes y administradores Deep security. Las alertas generadas por la infraestructura en la nube y de IT son enviadas como reportes al administrador, donde luego puede tomar una decisión con respecto al problema.

Fuente: (Trend Micro, n.d.)

La página web HACKMAGEDDON, ha ofrecido estadísticas sobre cyber-ataques que se han producido desde los años 2012 hasta la fecha y ha afectado muchas de grandes compañías tales como Skype, Nvidia, Xbox-life, entro muchos otros. Dicha gráfica muestra la tendencia del 2014 y comparando con años anteriores, se muestra mucho más estable. Paolo Passeri, dueño y fundador de la página web, soporta nuestro argumento afirmando que el impacto de la disminución de hacktivismo y la principal atención de los medios hacia las violaciones masivas caracterizan el pasado año 2014.

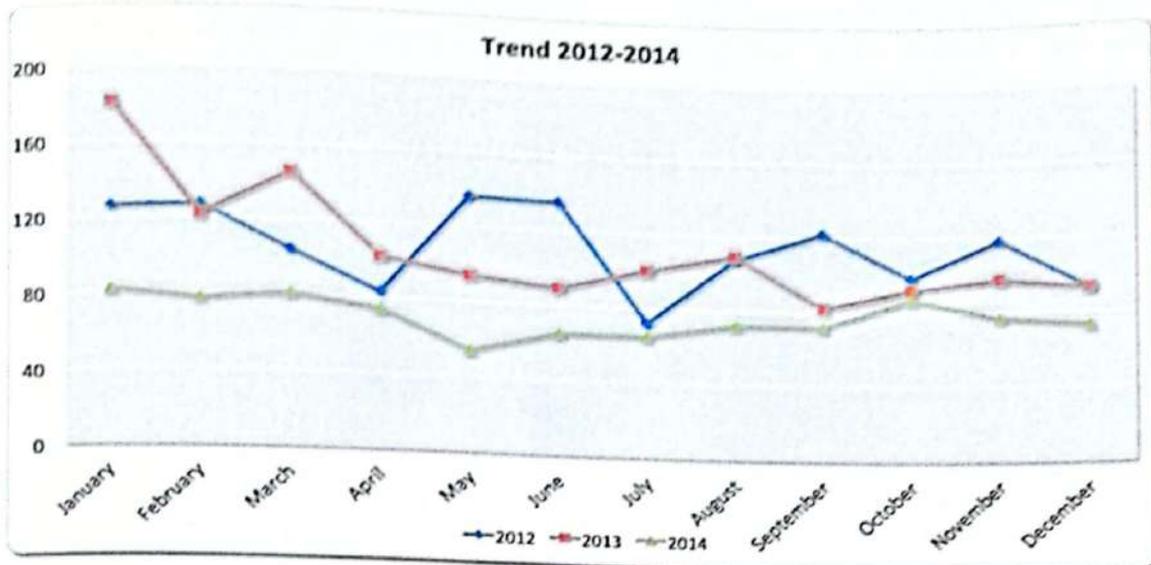


Ilustración 47. Cyber-ataques a Skype, Nvidia, Xbox-life, entre otras compañías de IT.

Fuente: (Passeri, HACKMAGEDDON, 2015)

Muestra la tendencia de los ataques realizado durante los 12 meses del 2012, 2013 y 2014, observando claramente que el año 2013 fue el más afectado por ataques informáticos a grandes empresas.

Estas tendencias en ataques se ha profundizado cada vez más en los últimos 12 meses del año 2014, provocando descubrimientos de nuevos ataques y a la seguridad a nuevas brechas reveladas.

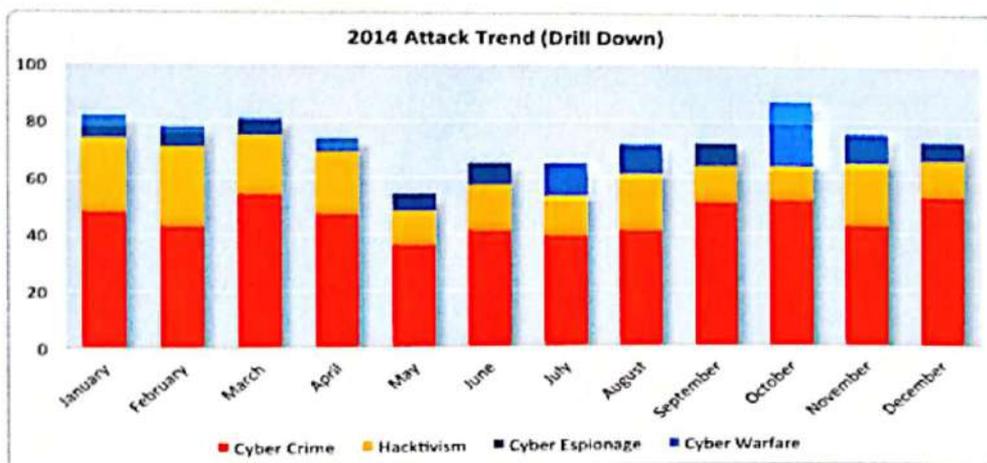


Ilustración 48. Tendencias de ataques durante el 2014.

La imagen muestra que el cyber crime ha aumentado considerablemente en el año 2014, siendo uno de los ataques más realizado durante ese año.

Fuente: (Passeri, HACKMAGEDDON, 2015)

Estas brechas impulsan a generar más ataques, y más si estas son accesibles.

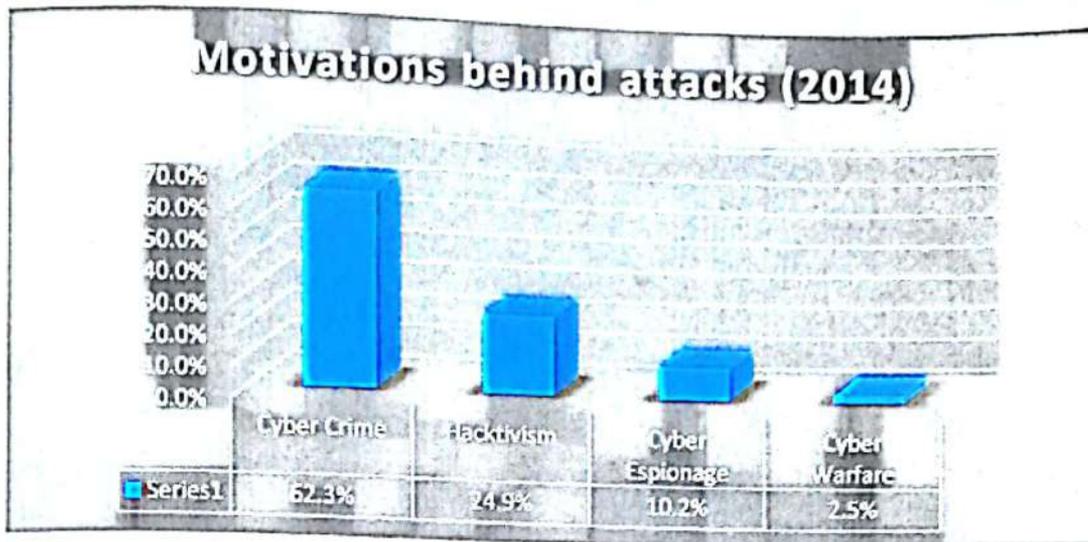


Ilustración 49. Motivos detrás de los ataques.

La gráfica muestra que el 62.3% de los hackers usan el cyber crime, siendo el que lidera para el 2014.

Fuente: (Passeri, HACKMAGEDDON, 2015)

No obstante, siempre hay más técnicas de ataques que se destacan más que otras por ser más eficaces y tener mayor dominio sobre ciertas vulnerabilidades.

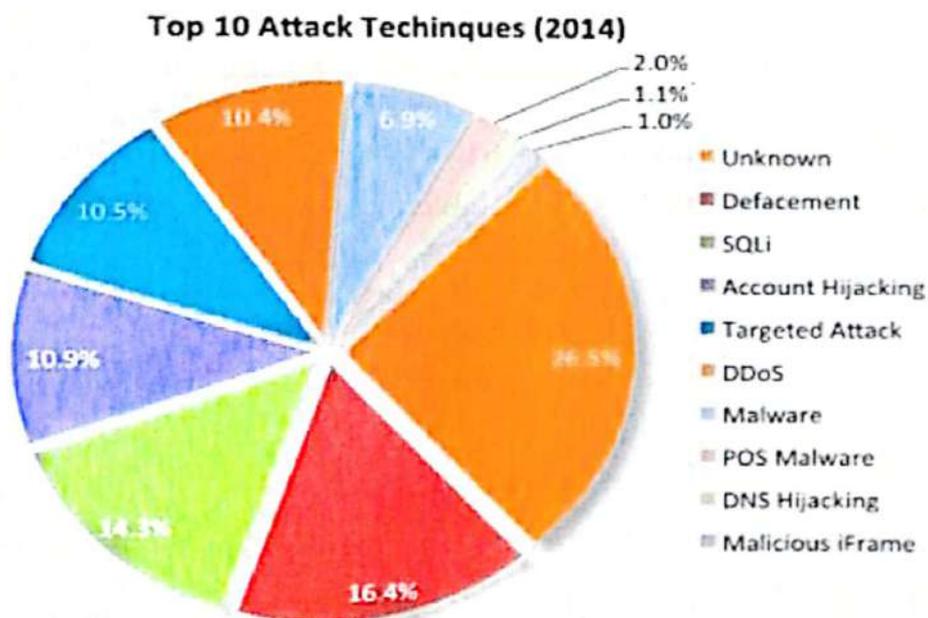


Ilustración 50. Top 10 de Cyber-ataques.

Entre el top 10 de los ataques más realizados en el 2014, se encuentran el defacement o desfiguración de algún sistema informático y el otro es liderado por nuevos ataques que hoy en día se desconocen.

Fuente: (Passeri, HACKMAGEDDON, 2015)

Y como siempre, existen sectores que son más propensos a recibir ataques que otros. En la siguiente gráfica se encuentra el Top 10 de las entidades más atacadas durante el año 2014.

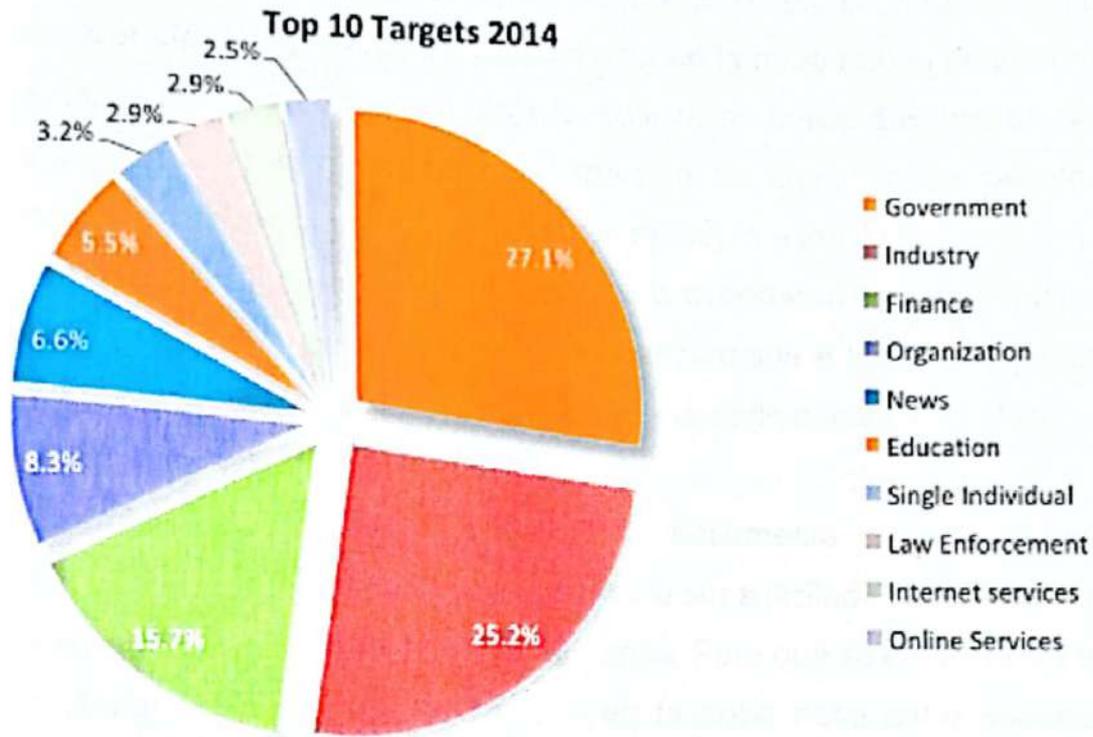


Ilustración 51. Entidades más atacadas.

En la gráfica se muestra que el gobierno ha sido el sector más vulnerable dentro del top 10 de los objetivos atacados para el 2014, representando el 27,1% de ataques recibidos.

Fuente: (Passeri, HACKMAGEDDON, 2015)

3.5 Estándares

Conocemos el estándar como un protocolo o una regla a la que hay que regirse para que se use repetidamente. Actualmente, Microsoft conoce su primer estándar de seguridad en la nube, la ISO/IEC 27018. Con el estándar definido, debe operar debajo los siguientes principios:

- **Consciencia de los proveedores:** Los proveedores no deben utilizar los datos personales de los usuarios que se reciben para fines publicitarios o de

marketing a menos que se le especifique al cliente. Del mismo modo, cuando el cliente se registra a los servicios de la nube del proveedor, está sometido a tener un servicio libre de publicidad o marketing sin que sus datos estén envuelto en ellos.

- **Control:** Clientes tienen control explícito sobre su propia información usada.
- **Transparencia:** Los proveedores de servicio en la nube deben de informar a los usuarios donde su data está alojada, este compromiso describe el uso de los subcontratistas para procesar información de identificación personal y asumir compromisos claros sobre cómo se manejan esos datos.
- **Comunicación:** En caso de una brecha, los proveedores deben de notificar a sus clientes sobre la brecha de seguridad encontrada e informarlo mediante un reporte completo, a la vez el proveedor debe darle continuidad al incidente y responder por ello.
- **Auditoría:** La realización de una auditoría documenta la conformidad del servicio con el estándar, posteriormente puede ser solicitada por el cliente para llevar sus propias obligaciones reglamentarias. Para que se cumpla esta parte del estándar, el proveedor de servicio en la nube debe estar sometido a revisiones anuales de terceros.

La página web de TREND MICRO presenta que existen amenazas persistentes avanzadas (APT) y los ataques dirigidos han demostrado su capacidad para penetrar en las defensas de seguridad estándar y permanecer ocultos durante meses mientras sustraen datos valiosos o llevan a cabo acciones destructivas. Muchas de las empresas en las que confía son algunos de los objetivos principales: instituciones financieras, organizaciones sanitarias y grandes minoristas, entre otros. En 2011, PC World detectó un aumento del 81% en los ataques de hackers avanzados y dirigidos a equipos y, según los resultados de una investigación de Verizon en 2012, se alcanzó la asombrosa cifra de 855 incidentes de seguridad cibernética y 174 millones de registros atacados. Según el estudio Ponemon sobre los costes de la ciberdelincuencia en Estados Unidos realizado en 2012 con 56 grandes empresas, se producen 1,8 ataques con éxito

en cada organización a la semana, lo que conlleva un coste medio en ciberdelincuencia de 8,9 millones de dólares por organización. Estos ciberataques son:

- **Sociales:** dirigidos a personas específicas con ingeniería social y malware avanzado.
- **Sofisticados:** aprovechan vulnerabilidades, aplican controles de puerta trasera, roban y utilizan credenciales válidas.
- **Sigilosos:** se ejecutan en una serie de sigilosos movimientos indetectables para la seguridad estándar o se ocultan entre miles de registros de eventos recopilados diariamente.

La solución ideal pasa por interconectar toda su infraestructura de seguridad en una defensa personalizada y adaptable, ajustada a su entorno particular y a sus atacantes específicos. Esto le permitiría no solo detectar y analizar estos ataques, sino también combatir a los atacantes. Nuestra solución Custom Defense es una plataforma de protección frente a amenazas especializadas que supervisa la red para detectar malware de día cero, comunicaciones maliciosas y comportamientos de ataque que resultan invisibles para las defensas de seguridad estándar. Ejecuta código sospechoso en un entorno seguro y controlado que se puede optimizar para el rendimiento y configurar para eludir las técnicas de los hackers que buscan soluciones para el aislamiento de procesos. Le ayuda a definir el riesgo, el origen y las características del ataque. Además, proporciona información práctica de forma exclusiva que permite contener y solucionar el ataque y, posteriormente, adaptar y reforzar su protección frente a otros ciberataques. (Trend Micro, n.d.)

En la Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General explica que desde el punto de vista de la innovación y la competitividad, la privacidad y la seguridad deben

ser detonadores de aquéllas, generando la confianza necesaria. Se trata, por tanto, de que la regulación en materia de privacidad y la seguridad permitan el desarrollo de la tecnología, sin que la innovación y la competitividad supongan renunciar a derechos y, en particular, el derecho fundamental a la protección de datos personales. La privacidad y la seguridad son paradigmas que están en constante evolución, debido entre otros aspectos a que fundamentalmente la tecnología y la sociedad lo hacen igualmente. Es decir, se produce una interrelación que hace que los cambios tecnológicos y sociales influyan en la percepción que tenemos de la protección de datos personales, la privacidad y la seguridad, y de manera inversa, estas tres últimas pueden influenciar en su caso el desarrollo tecnológico y social. El cómputo en la nube, como una de las tecnologías innovadoras que más atraen la atención de todas las partes, es un claro ejemplo de cómo la protección de datos, la privacidad y la seguridad no pueden ser consideradas como algo estático, sino que deben irse adecuando de manera que estén en equilibrio con los cambios que se producen día a día. Esta circunstancia exige que la seguridad deba ser tomada en consideración en atención al estado de la tecnología, entre otros factores.

En el libro *“Encuesta Nacional sobre Protección de Datos Personales (2012)”*, entre los beneficios más valorados de la Ley Federal De Protección de Datos Personales en Posesión de Particulares (LFPDPPP), los participantes en la encuesta respondieron lo siguiente:

“En el caso de México, resulta relevante tomar en consideración la Encuesta Nacional sobre Protección de Datos Personales (2012) que en el apartado relativo a los costos y beneficios de cumplir con la LFPDPPP señala que en promedio, el 29% de los entrevistados (siendo la base de entrevistas un total de 4729) considera que no es difícil cumplir con la LFPDPPP y que entre los beneficios de dicho cumplimiento se encuentran, por una parte, la mayor confianza de los clientes y proveedores y, por otra parte, el mejor posicionamiento de mercado.

En cuanto a los costos de cumplimiento, poniendo foco en este caso en la autorregulación pero sirviendo también para calcular los costos de implementación de un Sistema de Gestión de Datos Personales (SGDP), la Manifestación de Impacto Regulatorio (MIR) expone determinados datos estadísticos con base en los cuales se estima que “en una micro y pequeña empresa se invertirían un total de 220 horas en instaurar un SGDP, mientras que en una mediana y grande empresa se invertirían 700 horas”, siendo el 99% micro y pequeñas empresas y el 1% medianas y grandes empresas, de acuerdo con la información estadística del Censo Económico 2009 elaborado por el INEGI. Además, el sueldo promedio por hora de un profesional, según un estudio de tendencias de empleo profesional realizado en el primer trimestre de 2013 por la Secretaría del Trabajo y Previsión Social, es de \$64.6 pesos por lo que “el monto total de la implementación de un SGDP por unidad económica el cual asciende a \$14,212 pesos para las micro y pequeñas empresas y \$45,220 para medianas y grandes empresas”, de manera que “el costo total de la implementación de un SGDP es de \$30,876,866,827 pesos” considerando el número total de empresas.”

Beneficios más valorados de la LFPDPPP

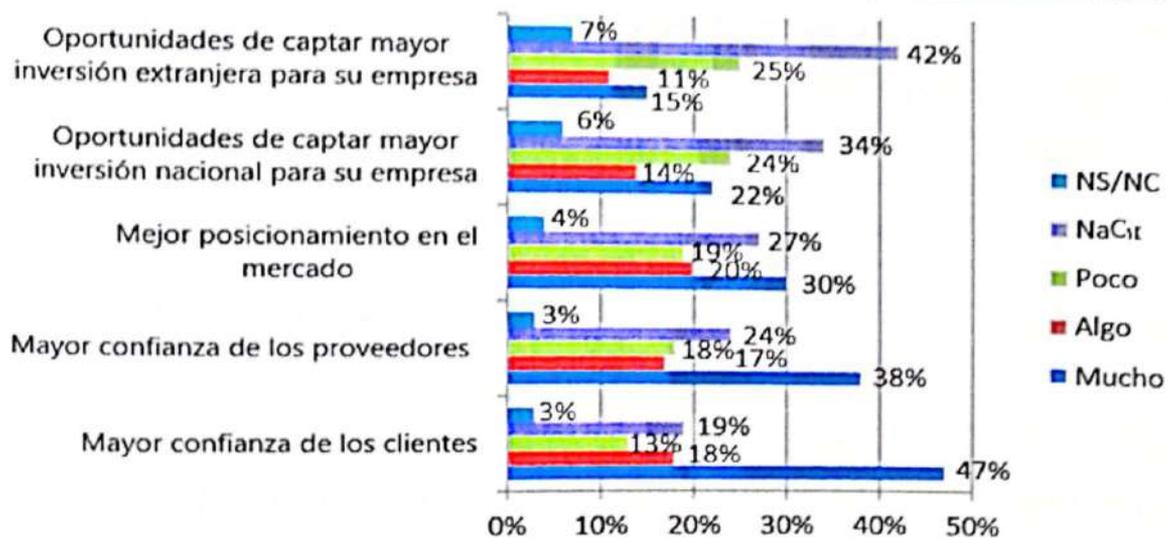


Ilustración 52. Beneficios más valorados de la LFPDPPP.

En la encuesta realizada por el cuerpo normativo de México, revelaron que los beneficios generados en gran porcentaje son la mayor confianza en el cliente y en

los proveedores. Estos porcentajes reflejan la importancia que radica proteger los datos de los usuarios.

Fuente: Encuesta Nacional sobre Protección de Datos Personales (2012).

En materia de medidas de seguridad, según la MIR de impacto moderado con análisis de impacto en la competencia, por lo que se refiere al "grupo o industria al que beneficia la regulación" se estima que el número promedio de registros en una base de datos con información personal es de 18,285 aproximadamente y el costo que tendría una vulneración es de \$3,770,656 pesos, además del impacto negativo en la reputación, de manera que el beneficio unitario de adoptar un esquema de autorregulación es de \$4,963,310 pesos y al multiplicarlo por el número efectivo de unidades económicas el beneficio total anual de la regulación sobre parámetros de autorregulación vinculante en protección de datos personales asciende a \$10,552,996,039,152 pesos. Se destaca que la mayoría de las empresas consideren que la LFPDPPP no supone una oportunidad para captar mayor inversión nacional o extranjera, lo que debería ser tomado en consideración ya que generar confianza a través del cumplimiento de una normatividad sobre protección de datos personales es uno de los factores que puede incrementar el número de clientes, máxime si se piensa en clientes que están establecidos en la Unión Europea o en otras regiones o países que también tienen normatividad en la materia. (Comisión Federal de Mejora Regulatoria, 2014)

En los Parámetros de Autorregulación en Materia de Protección de Datos Personales cabe señalar que sólo un promedio del 13% de las empresas entrevistadas había incurrido en un incremento de costos de operación como consecuencia de la entrada en vigor de la LFPDPPP. Y de entre este porcentaje, en mayor medida las empresas que han visto incrementado dichos costos de operación son las financieras y de telecomunicaciones. Es posible, por tanto, afirmar que el cumplimiento de la normatividad sobre protección de datos personales no es una barrera u obstáculo para las empresas mexicanas además

de que supone que éstas puedan ser competitivas incluso con las de otros países que también cuentan con normatividad en la materia. En este sentido, la citada encuesta proporciona los siguientes datos:

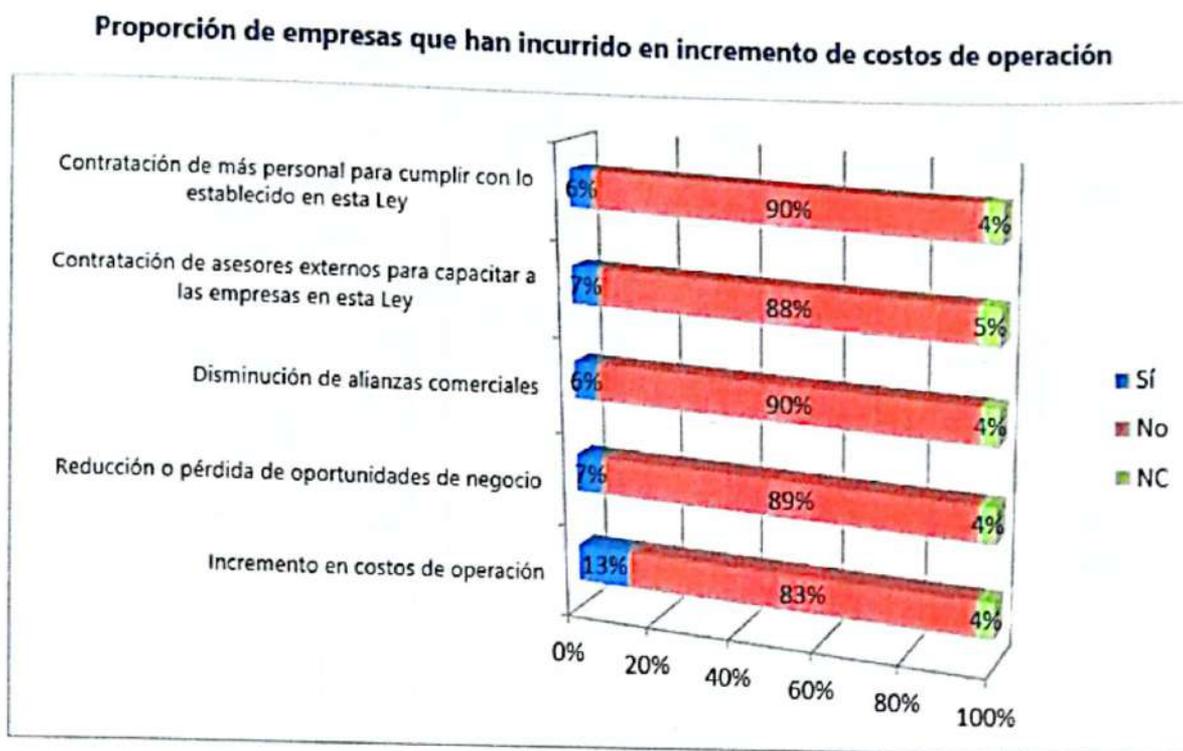


Ilustración 53. Proporción de empresas que han incurrido en el incremento de costos de operación.

Las estadísticas muestran claramente que cumplir con la normativa de protección de datos no incurre en incremento de costos, disminución de alianzas comerciales y otros factores.

Fuente: Encuesta Nacional sobre Protección de Datos Personales (2012).

RESUMEN

El estándar ISO/IEC 27018 constituye los controles principales que permiten proteger la privacidad, directrices fundamentadas en la norma ISO/IEC 27002 (mejores prácticas para la seguridad de la data) y objetivos de control para la protección de la información de identificación personal (PII). Microsoft Azure ha adoptado este estándar.

Resumen gráfico, Capítulo III.

Seguridad en la nube

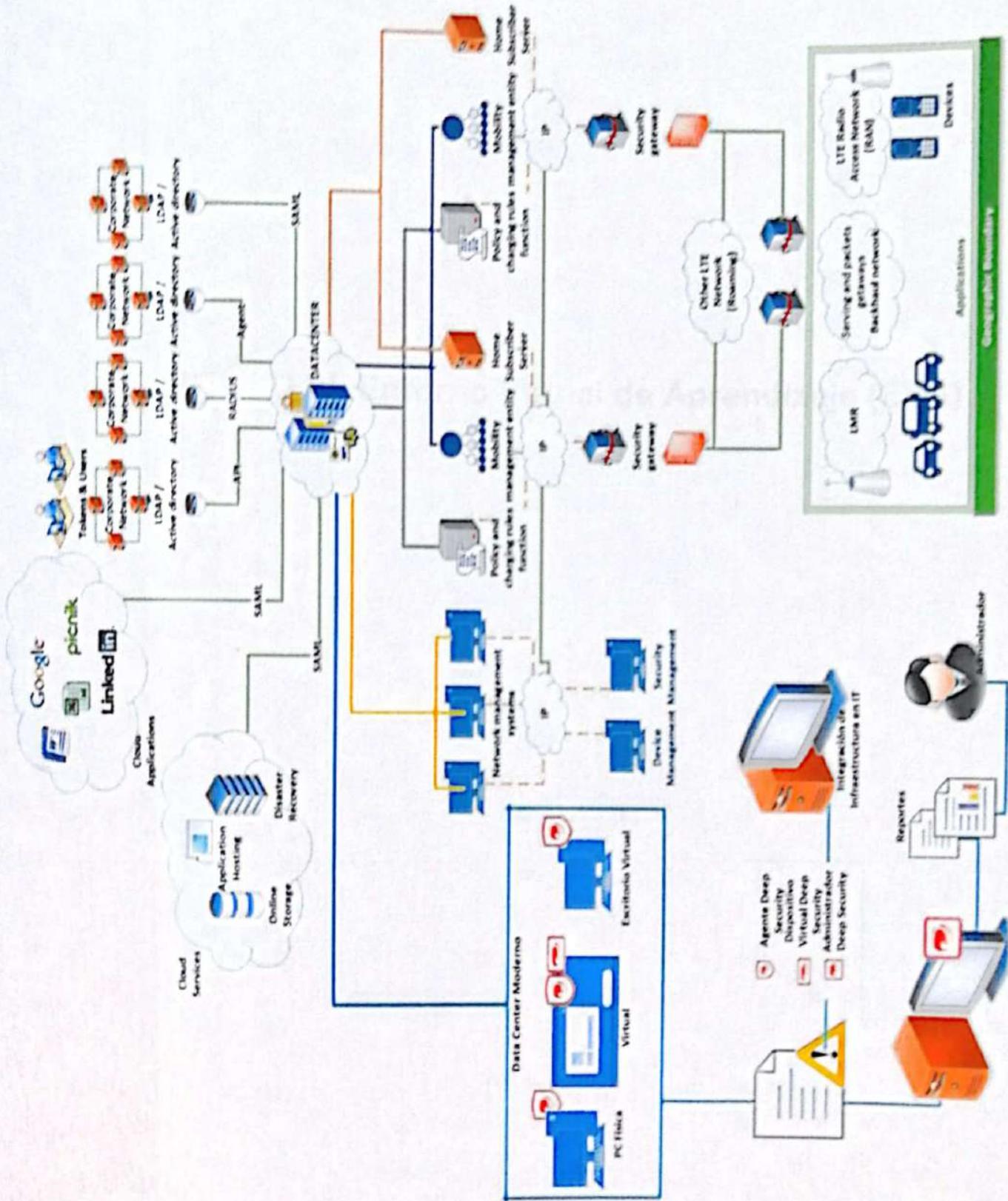


Ilustración 54. Resumen gráfico, Capítulo III.
Fuente: Imagen propia.

CAPITULO IV. Entorno Virtual de Aprendizaje (EVA)

4.1 Conceptualización

Un Entorno Virtual de Aprendizaje (EVA) es una herramienta que habilita un espacio con accesos restringidos, pensado y diseñado para que las personas que acceden a él para desarrollar asignaturas, facilitando la educación a distancia. Lo más importante del EVA, es el "aula virtual", esta permite que se impartan uno o varios cursos didácticos al mismo tiempo, de manera interactiva a distancia, creando numerosas facilidades de capacitación sin fronteras.

La página web, XARXATIC, explica que el "aula virtual" no es más que un entorno de aprendizaje, consta de una plataforma o *software* a través del cual el ordenador permite la facilidad de dictar las actividades en clases, de igual forma permitiendo el desarrollo de las actividades de enseñanzas y aprendizajes habituales que requerimos para obtener una buena educación. A través de ese entorno el alumno puede acceder y desarrollar una serie de acciones que son las propias de un proceso de enseñanza presencial tales como conversar, leer documentos, realizar prácticas, formular preguntas al docente, trabajar en equipo, etc. Todo ello de forma simulada sin que utilice una interacción física entre alumnos y docentes.

En el artículo "Entornos virtuales de aprendizaje en la escuela: tipos, modelo didáctico y rol del docente" describe que el contexto socio-cultural contemporáneo, caracterizado por la presencia ubicua y el uso intensivo de las Tecnologías de la Información y la Comunicación (TIC), coloca a la escuela frente a la demanda de desarrollar en sus alumnos la alfabetización digital necesaria para la utilización competente de las herramientas tecnológicas. Los entornos virtuales de aprendizaje resultan un escenario óptimo para promover dicha alfabetización, ya que permiten abordar la formación de las tres dimensiones básicas que la conforman: el conocimiento y uso instrumental de aplicaciones informáticas, la adquisición de habilidades cognitivas para el manejo de información hipertextual y multimedia y el desarrollo de una actitud crítica y reflexiva para valorar tanto la información, como las herramientas tecnológicas disponibles, expresa la autora del artículo. Debido a esto, resulta necesario que

los docentes conozcan las funcionalidades técnicas y las potencialidades didácticas de los entornos virtuales, como paso previo para su integración significativa en las propuestas curriculares.

María I. Salinas, explica los objetivos de su informe consisten en:

- Describir las características técnicas y uso didáctico de los entornos virtuales de aprendizaje utilizables en la escuela.
- Puntualizar las razones socio-culturales y educativas que justifican su integración curricular.
- Analizar las características de un modelo de enseñanza-aprendizaje para la virtualidad.
- Proponer diversas técnicas de enseñanza en la red.
- Brindar orientaciones prácticas para iniciar el camino de la docencia virtual.

4.2 Tipos

El EVA tiene usos más extendidos a nivel educacional y se dividen en cuatro tipos de plataformas, estas se distinguen por sus áreas tecnológicas y por las áreas educativas que ofrece, al ser el soporte educacional a distancia.

Salinas M., distingue y describe estas 4 plataformas, de la siguiente manera:

➤ Plataformas de *e-learning*

También conocido como "*Learning Management System*" (LMS) o Sistema de Gestión de Aprendizaje. Son aplicaciones creadas con fines educativos para ser utilizado como propuestas de enseñanza y aprendizaje, durante la década de los 90'. Es un entorno complejo en cuanto a cantidad y variedad de herramientas ya que están conformadas por módulos de *software* con diferentes funcionalidades (por ejemplo, en una plataforma podemos encontrar un módulo de foro, uno de chat o de videoconferencia, de agendas de tareas, pruebas, etc.).

Existen diversas Plataformas *e-learning* tanto gratuitas como de pagos. Como podemos observar las gratuitas son: Moodle, Dokeos, Claroline e Sakai y las de pago o comercializadas son: E-ducativa y Blackboard. Estas plataformas deben ser instaladas en servidores, de manera que un docente no trabaja con este

enteramente sino que en la gran mayoría de los casos es parte de una entidad institucional.

Sin embargo, Salinas explica que el requisito de instalación en un servidor posee una ventaja importante: otorga al administrador mayor control sobre su funcionamiento o en términos más generales, sobre lo que pueda suceder con la aplicación. En cambio la instalación y administración de este tipo de entorno requiere de conocimientos informáticos no tan avanzado pero si superiores a los del usuario promedio.

➤ **Blogs**

Técnicamente los blogs son páginas web compuestos por dos elementos: entradas y comentarios. En estos micro-contenidos solo pueden ser editados o incluso suprimidos por su propio autor. Esta opción les otorga un carácter conversacional o dialogo que infunde las características más típicas de los blogs y los hace ideales para generar interacción entre alumnos en relación a un tema o tarea y lograr la construcción compartida de conocimiento sobre una cuestión determinada.

Los blogs de contenidos específicamente educativos se denominan *edublog* donde son parte de los servicio de las páginas web *Blogger* y *Wordpress* que también son gratuitas.

➤ **Wikis**

La plataforma Wiki se define como una página web que se edita en forma colaborativa, es decir con la participación de varios usuarios, lo cual constituye su esencia. El ejemplo más representativo de wiki es la página web Wikipedia, enciclopedia en línea cuyos artículos puede ser editado por cualquier usuario de la red. En las plataformas de estilo wiki cada usuario no solo puede introducir nuevos contenidos, como en un blog sino que también puede ampliar, modificar o incluso suprimir aquellos creados por otros. De manera que los participantes van co-creando juntos un contenido más exacto. También esto los convierte en co-autores de una información.

El *software* permite identificar al creador de cada contribución, lo cual, en el ámbito educativo, facilita el seguimiento y la evaluación de la actividad por el docente.

Estos tipos de aplicaciones son ideales para el planteo de propuestas de aprendizaje colaborativo, en las cuales se tenga que lograr la creación de un producto final común, a partir de la integración de los aportes de distintos miembros de un grupo. Las wikis de contenidos educativos se denominan *eduwikis*. Este tipo de servicio se puede encontrar en *Wikispaces*, *PBWorks* y *Wetpaint*.

➤ **Redes Sociales**

Se puede definir como una página web orientadas a la interacción de personas con intereses comunes, con el fin de compartir contenidos e intercambiar información. Incluyen herramientas que permiten la publicación de materiales y la comunicación entre los miembros del grupo, como foro, chat y correo electrónico interno.

Su principal utilidad en el terreno educativo es permitir la creación de grupos, ya sea el grupo de una materia determinada o los grupos de alumnos. En el primer caso, el docente puede usar el grupo para: publicar recursos, noticias o avisos sobre la asignatura y consignas para la realización de trabajos, responder consultas, disponer la entrega de trabajos por los alumnos, entre otros. Los grupos de alumnos pueden utilizarse para que resuelvan en equipo una tarea determinada, recopilen allí materiales, intercambien opiniones, etc. Las redes sociales de contenido específicamente educativo se denominan *edured*. Podemos crear gratuitamente una con servicios como *SocialGo*, *Grouply*, *Grou.ps* y *Wall.fm*.

4.3 Ventajas

En la "Revista científica electrónica de educación y comunicación en la sociedad del conocimiento" se presentan las ventajas principales en la utilización del EVA, como son:

- El acceso al contenido es más flexible y no se restringe a las paredes de un aula.
- Posibilidad de acceder a la información desde cualquier lugar que posea conexión a internet.

- Combina distintos recursos para mejorar el proceso de enseñanza aprendizaje.
- Facilitan el aprendizaje colaborativo y cooperativo
- Las aportaciones mejoran en cuanto a calidad se refiere, gracias a la flexibilidad temporal de la que nos dota el uso de estos sistemas, haciendo más simple establecer una evaluación continuada y disminuyendo considerablemente el tiempo de diseño, desarrollo y distribución
- Existe retroalimentación, no sólo con el profesor, sino con el resto de compañeros.
- Aumenta la motivación y participación de los alumnos, posibilitando un seguimiento individual, como la evaluación de conocimientos y habilidades.
- Los sujetos son conscientes y partícipes de su propio aprendizaje.

4.4 Desventajas

El EVA podría no tener limitantes como plataforma, pero posee desventajas en aspectos económicos, técnicos y tecnológicos, que pueden impedir la igualdad de acceso de la población, tales como:

- Fallas de accesibilidad y conectividad.
- Costos de licencias.
- Costos de equipos y actualizaciones.
- Velocidad de conexión.

4.5 Aplicación web Moodle

4.5.1 Conceptualización

En el documento "Moodle, la plataforma para la enseñanza y organización escolar", se presenta la plataforma como como una aplicación web de tipo Ambiente Educativo Virtual, un sistema de gestión de cursos, de distribución libre, que ayuda a los educadores a crear comunidades de aprendizaje en línea. Este tipo de plataformas tecnológicas también se conoce como LCMS (*Learning Content Management System*). La versión más reciente es la 2.8.

Fruto de la Tesis de Martin Dougiamas de la Universidad de Perth, en Australia Occidental surgiría en el 2002 "Moodle". Este profesor universitario quería una herramienta que facilitara el constructivismo social y el aprendizaje cooperativo. Su nombre proviene del acrónimo de "*Modular Object Oriented Dynamic Learning Enviromennt*" (Entorno Modular de Aprendizaje Dinámico Orientado a Objetos), aunque otras fuentes mencionan que proviene del verbo inglés Moodle que describiría el Proceso de deambular perezosamente a través de algo, y hacer cosas cuando se antoja hacerlas. Según las palabras del autor, quería: "Un programa que sea fácil de usar y lo más intuitivo posible". Dominar Moodle es sencillo, apenas es necesario controlar una iconografía compuesta por unos 15 símbolos plenamente significativos.

Martinez de Lahidalga explica que la definición del nombre de Moodle, este se refiere a "objetos de aprendizaje", normalmente de tamaño pequeño y diseñado para distribuirse en internet posibilitando el acceso simultáneo a la información por parte de múltiples usuarios. Este hecho es fundamental ya que a partir de ahora no nos basaremos en la mera lectura de unos apuntes sino en la creación de estos "objetos de aprendizaje", plenos de significado, que siguen secuencias didácticas en las que el profesor guía a los alumnos posibilitando su auto aprendizaje. Facilitamos así el aprendizaje individual y la colaboración entre los participantes. El objetivo sería crear unidades didácticas que responderían a las diferentes capacidades a desarrollar en la asignatura.

En la Universidad Virtual para Cursos en Línea y Educación a Distancia de Univer Colima, presentan a Moodle como parte del grupo de los Gestores de Contenidos Educativos (LMS), conocidos como Entornos Virtuales de Aprendizajes (EVA), un subgrupo de los Gestores de Contenidos (*Content Management Systems* (CMS)). De manera coloquial, podemos definir a Moodle como un paquete de *software* para la creación de cursos y sitios web basados en internet, o sea, una aplicación para crear y gestionar plataformas educativas, donde un centro educativo, institución o empresa, gestiona recursos educativos proporcionados por los docentes y organiza el acceso a esos recursos por los estudiantes, y además permite la comunicación entre todos los alumnos y docentes.

4.5.2 Estructura

Moodle.net, describe como trabaja su plataforma, donde la portada sería la página a la que entra en su navegador de Internet, donde usualmente incluye información acerca del sitio mismo y puede ser **altamente** personalizada. (Tome nota de también es posible bloquear la página para que lo único que vea un usuario al elegir la URL de un sitio Moodle sea la pantalla para ingresar).

La autenticación depende del sitio, pueden ser:

- Habiendo proporcionado cuentas con anterioridad.
- Inscribirse el usuario mismo.
- Ser autenticados automáticamente desde otro sistema.

De acuerdo al site oficial de Moodle, explica que su estructura básica está organizada alrededor de cursos.

- Estos son básicamente, páginas o áreas dentro de Moodle en donde los profesores pueden presentar sus recursos y actividades a los estudiantes.
- Éstas pueden tener diferentes disposiciones, pero usualmente incluyen un número de secciones centrales en donde se muestran los materiales y en donde hay bloques laterales que ofrecen información o características extras.
- Los cursos pueden tener contenido para un año de estudios, para una sesión única o para cualquier variante, dependiendo del establecimiento o el maestro. Pueden ser usados por un maestro o por un grupo de maestros.
- El cómo los estudiantes se inscriben en los cursos depende del establecimiento; por ejemplo, pueden tener auto-inscripción, ser inscritos de forma manual por su maestro o automáticamente por el administrador.
- Los cursos están organizados en categorías. Por ejemplo, en la categoría de Ciencias podrían estar los cursos de Física, Química y Biología.

4.5.3 Interfaz de programación de aplicaciones (API)

En el libro Programación de aplicaciones web, define la interfaz de programación de aplicaciones como un conjunto de constantes, funciones y protocolos que permiten programar aplicaciones.

Una Interfaz de programación de aplicaciones (API) no es más que crear el enlace de la comunicación entre componentes de *software*. Su principal propósito consiste en proporcionar un grupo de funciones.

Entre las principales API que usa la plataforma Web Moodle se encuentran:

- **API de acceso:** La API de acceso le da funciones para que pueda determinar qué se permite que el usuario actual que hacer, y que permite a los módulos para extender Moodle con nuevas capacidades.
- **API de manipulación de datos (DML):** La API de la manipulación de datos le permite leer / escribir a bases de datos de una manera consistente y segura.
- **API de archivos:** La API de archivos controla el almacenamiento de archivos en relación a varios *plugins*.
- **API Form (formulario):** La API Formulario define y maneja los datos del usuario a través de los formularios web.
- **API de registro (log):** La API Evento 2 le permite registrar eventos en Moodle, mientras *logging 2* describe cómo se almacenan y se recuperan los registros.
- **API de navegación:** La API de navegación le permite manipular el árbol de navegación para añadir y eliminar elementos como desee.
- **API de Página:** La API de página se utiliza para configurar la página actual, añadir JavaScript y configurar cómo se mostrarán las cosas al usuario.
- **API Output (salida):** La API de salida se utiliza para representar el código HTML para todas partes de la página.

- **API *String* (cadena):** La API de cuerdas es la forma de obtener las cadenas de texto el lenguaje a utilizar en la interfaz de usuario. Maneja las traducciones que podrían estar disponibles.
- **API de actualización (*upgrade*):** La API de actualización es como su módulo de instalaciones y actualizaciones en sí, no perdiendo de vista su propia versión.
- **API *Moodlelib* (núcleo):** La API *Moodlelib* es el archivo de la biblioteca central de varias funciones de Moodle de propósito general. Funciones puede sobre el manejo de los parámetros de la petición, configuraciones, preferencias del usuario, tiempo, inicio de sesión, *mnet*, *plugins*, cuerdas y otros.
- **Ajustes de administrador (*admin*):** Las ofertas de configuración de administrador de la API con proporcionar opciones de configuración para cada *plugin* y núcleo de Moodle.
- **Disponibilidad:** Los controles disponibilidad API acceso a las actividades y secciones.
- **API de copia de seguridad (*back-up*):** Define exactamente cómo convertir los datos del curso en XML para fines de respaldo y la restauración de API describe cómo convertir de nuevo a la inversa.
- **API de caché:** El Universal Cache Moodle (MUC) es la estructura para el almacenamiento de datos de la caché dentro de Moodle. *Cache_API* explica algo de lo que se necesita para utilizar una memoria caché en el código.
- **API *Calendar* (calendario):** La API de Calendario le permite añadir y modificar los eventos en el calendario para el usuario, grupos, cursos, o todo el sitio.
- **Comentario API:** La API comentario le permite guardar y recuperar los comentarios de los usuarios, de modo que usted puede agregar fácilmente comentando a cualquiera de su código.

- **API definición de datos (DDL):** La API de definición de datos es lo que se utiliza para crear, modificar y eliminar tablas y campos en la base de datos durante las actualizaciones.
- **API de matriculación (inscribirse):** La API de inscripción se ocupa de los participantes del curso.
- **Eventos API (evento):** El Evento 2 permite definir "eventos" con datos de carga útil para ser despedidos cuando quiera, y también le permite definir manejadores de reaccionar ante estos eventos cuando se producen. Esta es la forma recomendada de la comunicación *inter-plugin*. Esto también constituye la base para iniciar sesión en Moodle.
- **Funciones API externa:** Las funciones de la API externa le permiten crear métodos totalmente parametrizado que se puede acceder mediante programas externos (como los servicios Web).
- **API Lock (bloqueo):** La API de bloqueo le permite sincronizar el procesamiento entre múltiples peticiones, incluso para nodos separados en un clúster.
- **API Mensaje:** La API de mensajes le permite enviar mensajes a los usuarios. Ellos deciden cómo quieren recibirlos.
- **Media API (medios de comunicación):** La incorporación de estos medios se pueden utilizar para insertar elementos multimedia como audio, vídeo y Flash.
- **Mi perfil API:** El perfil de la API Mi se utiliza para añadir cosas a la página de perfil.
- **API preferencia:** La API de Preferencia es una forma sencilla para almacenar y recuperar las preferencias para los usuarios individuales.
- **API cartera:** La API de Cartera le permite añadir interfaces de cartera en sus páginas, y permite a los usuarios para empaquetar los datos para enviar a sus carteras.
- **API valoración:** La API de clasificación le permite crear interfaces de calificación AJAX para que los usuarios puedan evaluar artículos en su

- plugin*. En un módulo de actividad, usted puede optar por agregar clasificaciones para formar grados.
- **API RSS (rss):** La API de RSS le permite crear canales RSS seguras de datos en su módulo.
 - **API Tag (etiqueta):** La API *Tag* le permite almacenar las etiquetas (y una nube de etiquetas) a los artículos en su módulo.
 - **API de tareas:** La API de tareas le permite ejecutar trabajos en segundo plano. O bien, una vez fuera, o en un horario regular.
 - **API Time (tiempo):** La API de tiempo se encarga de traducir y mostrar veces entre los usuarios en el sitio.
 - **API de pruebas (test):** La API de prueba contiene la API de prueba Unidad (*PHPUnit*) y la API de pruebas de aceptación (Pruebas de aceptación). Lo ideal sería que todo nuevo código debe tener pruebas unitarias escritas PRIMERO.
 - **API relacionadas por el usuario (el usuario):** Se trata de una agrupación bastante informal de APIs relacionadas usuarios diversos relacionados con la clasificación y la búsqueda de listas de usuarios.
 - **API de servicios Web (servicio web):** La API de servicios Web permite exponer funciones particulares (generalmente funciones externas) como servicios web.
 - **API del módulo Actividad:** Módulos de actividad son el complemento más importante en Moodle. Existen varias APIs básicas que el servicio sólo módulos de actividad.
 - **API finalización actividad (finalización):** El API finalización Actividad es para indicar al sistema cómo se han completado actividades.
 - **API de clasificación avanzada (clasificación):** La API avanzada de clasificación le permite añadir interfaces de clasificación más avanzados (como rúbricas) que pueden producir grados simples para el libro de calificaciones.
 - **Grupos API (grupo):** La API de Grupos le permite comprobar el modo de grupo de actividad actual y establecer el grupo actual.

- **API del libro de calificaciones (grado):** La API del libro de calificaciones le permite leer y escribir desde el libro de calificaciones. También le permite proporcionar una interfaz para obtener información detallada de calificaciones.
- **API plagio:** La API de plagio permite a su módulo de actividad para enviar archivos y datos a los servicios externos para que se verifiquen por plagio.
- **API pregunta:** La API pregunta (que se puede dividir en la API de banco de preguntas y la API del motor pregunta), puede ser utilizado por las actividades que desean utilizar las preguntas del banco de preguntas.

4.5.4 Competencias

El objetivo principal de las plataformas de *e-learning* o LCMS (Learning Content Management Systems) es permitir gestión y creación de cursos de enseñanza virtuales, donde alumnos y formadores puedan interactuar en el proceso de formación.

Espacios de aprendizaje pueden ser de tres aulas de una escuela, en enseñanza en el aula; Sitios de Internet, en el no-cara, virtual o *e-learning* educación; o una combinación de ambos, la coeducación o *b-learning*. Entre las diferentes plataformas que se encuentran actualmente con los conceptos de plataformas de aprendizaje en línea con sistemas libres son:

- | | | |
|-------------|----------|------------------|
| • ATutor | • Dokeos | • Proyecto Sakai |
| • Chamilo | • ILIAS | • SWAD |
| • Claroline | • Moodle | • Sensei LMS |

4.6 Tendencias presentes y futuras de los Entornos Virtuales de Aprendizajes

4.6.1 Panorama actual

“Actualmente existen en el mundo cerca de 330.000 cursos registrados de 196 países y en 70 lenguas diferentes. La *Open University* del Reino Unido cuenta con 180.000 alumnos registrados.” (Martinez de Lahidalga, 2008)

Teniendo en cuenta los grandes desafíos por venir en el mundo de la educación, es necesario tener herramientas interactivas para expandir los horizontes de la enseñanza, permitiendo el crecimiento de las organizaciones y personas. Este ambiente genera un sinnúmero de ventajas para capacitación sin fronteras.

4.6.2 Usuarios y casos de éxitos

En el documento publicado por María Salinas, "Entornos virtuales de aprendizaje en la escuela: tipos, modelo didáctico y rol del docente", se encuentran recomendaciones para las mejores prácticas, apoyando casos exitosos de implementación, como son:

- a. *La primera sugerencia, antes de cualquier consideración de la didáctica, es tener una actitud positiva hacia la tecnología.* Esto significa: perder el miedo: como inmigrantes digitales, los profesores a menudo se acercan a la tecnología de miedo. Hay que atreverse a experimentar y aprender por ensayo y error. Creemos que todos somos capaces de utilizar con éxito. Recién nacido con herramientas web 2.0 se caracterizan precisamente por su facilidad de uso y animar a todos a trabajar con ellos. La confianza en su poder para mejorar las prácticas y emocionada por ello. Usted tiene que engañar a estas herramientas permiten alcanzar des esfuerzos educativos más eficaces y asegurar que los estudiantes aprenden mejor.
- b. *Con referencia específicamente a temas educativos:* Seleccione el contenido que se les enseñe teniendo en cuenta cómo su aprendizaje puede ser enriquecida por la intervención de la tecnología. El uso del entorno virtual tendrá verdadero sentido si permite facilitar y/o mejorar la comprensión de la materia, con respecto a las propuestas tradicionales de la clase física. Centrarse en los objetivos de aprendizaje que deben alcanzarse, teniendo en cuenta que incluyen la práctica de habilidades de pensamiento de alto nivel y las habilidades sociales, aspectos necesarios para promover el entendimiento. Por otra parte, y en relación con los objetivos, no debe caer en la trampa de centrar la atención en las herramientas, el aprendizaje y el olvido. En este sentido, hay que tener en

cuenta que la tecnología está al servicio del aprendizaje, y no al revés. - Hacer una metodología activa, para garantizar la participación de todos los estudiantes en la situación de enseñanza. Es aconsejable también aumentar los casos de interacción y colaboración en grupo. Elegir las herramientas adecuadas para el desarrollo de contenidos, la consecución de los objetivos y la ejecución de las actividades previstas. El profesor tiene que examinar el potencial educativo de las distintas herramientas disponibles y determinar cuál o cuáles son los más adecuados para el logro de un aprendizaje específico.

- c. *Trabajo en equipo*: es esencial para el intercambio de ideas y experiencias con sus colegas, planificar proyectos interdisciplinarios que involucran profesores de diferentes áreas o materias, teniendo el asesoramiento de otros profesores en nuestras prácticas, etc.
- d. *No te rindas los éxitos analógicos*: la implantación de un EVA no tiene que conducir a las buenas prácticas de relegar analógica, es decir, aquellos que son eficaces sin la ayuda de la tecnología. En cualquier caso, se puede pensar en cómo enriquecer su través. Cuando un proyecto de introducción de los entornos virtuales en curso desarrolla, es importante no experimentarla como un choque entre lo tradicional y lo virtual, sino como dos maneras de integrar de una mejor educación.

4.6.3 Productos y Servicios

Entre los productos y servicios disponibles en Latinoamérica son *Edoome*, *Moodle*, *Dokeos* y *Claroline*.

Para aquellos que deseen ofrecer el *e-learning* son muchos EVA de código abierto o de propiedad disponible para su uso inmediato. Servicios de aprendizaje electrónico a petición o bajo demanda son también una opción popular, ya que se pueden implementar en minutos y no requieren instructores o instituciones para implementar sistemas en sus propios servidores.

Muchos EVA está instalado en un servidor, un entorno virtual típico contiene uno o más programas o proporcionar instrucciones para la interfaz de usuario

(profesor-alumno) que interactúa con la base de datos. Por ejemplo, un EVA puede usar PHP como su idioma / programa como administrador de la base de datos MySQL.

Los EVA son lugares cada vez más de la aplicación. Estos incluyen las nuevas tecnologías emergentes y áreas especializadas. Un EVA se puede implementar como un cliente USB, de vez en cuando la sincronización con el servidor a través de la web. EVA se puede utilizar en algo tan genérico como capacitación para el trabajo o algo tan especializado como para cumplir con los requisitos de la certificación ISO 9000.

RESUMEN

El Entorno Virtual de Aprendizaje (EVA) es una herramienta virtual que ofrece un espacio con accesos restringido, pensado y diseñado para un entorno educativo (enseñanza - aprendizaje) donde las personas acceden en el para desarrollar cursos virtuales, donde se desarrollan foros, chats /mensajería, exámenes, se comparten materiales didácticos, videos, entre otros. Facilitando la educación a distancia desde cualquier lugar con acceso al internet.

Lo que más destaca del Entorno Virtual de Aprendizaje (EVA) es su entorno de clase virtual, ya que permite que se impartan uno o varias asignaturas didácticas al mismo tiempo, de manera interactiva y en cualquier lugar que te encuentres, creando así una capacitación sin fronteras.

Resumen gráfico, Capítulo IV.

Entornos Virtuales de Aprendizaje (EVA)

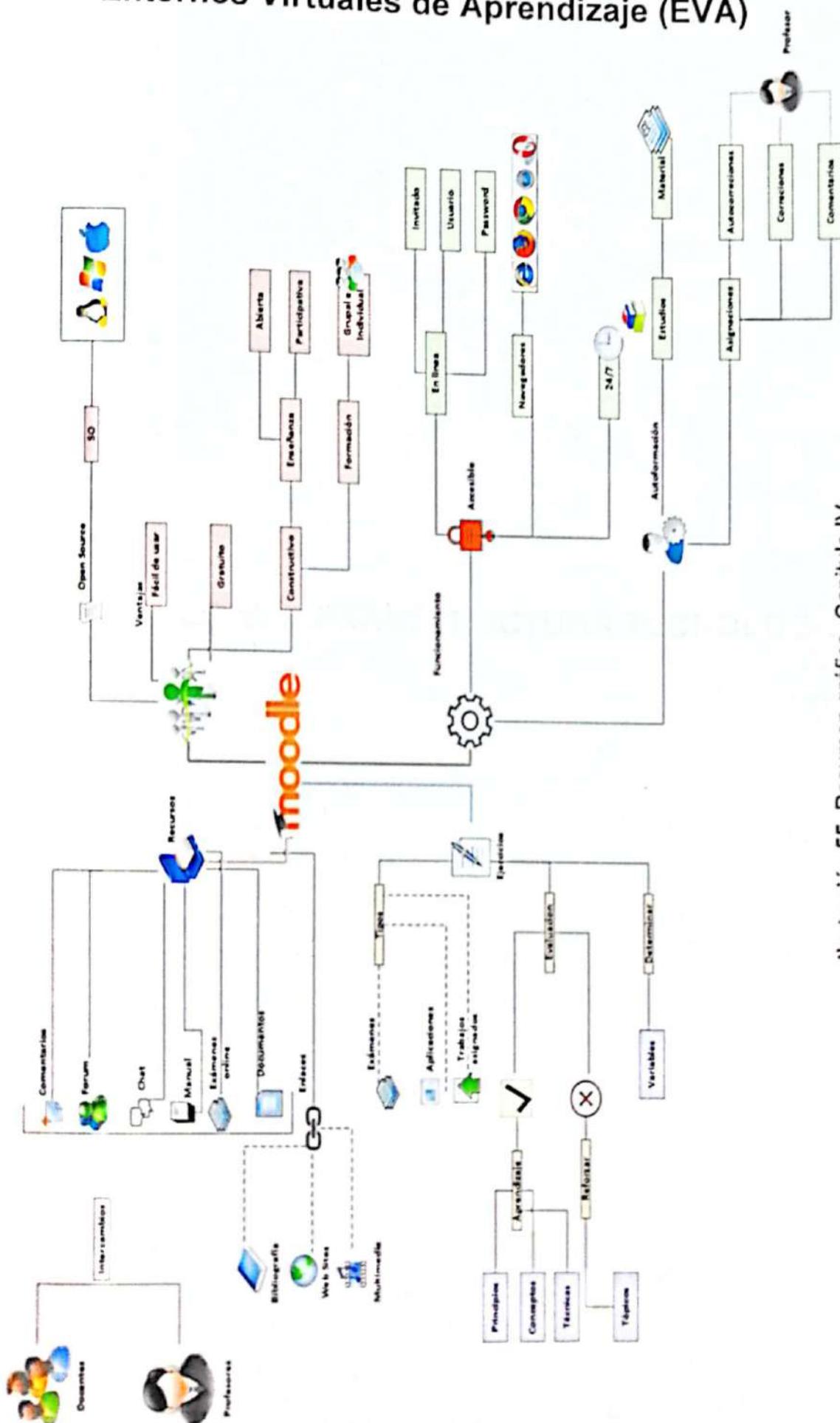


Ilustración 55. Resumen gráfico, Capítulo IV.
Fuente: Imagen propia.

CAPITULO V. INFRAESTRUCTURA TECNOLOGICA

CAPITULO V. Infraestructura tecnológica

El conjunto de *hardware* y *software* donde se encuentran los distintos servicios que la Universidad necesita tener en marcha para poder llevar a cabo toda su actividad se denomina infraestructura tecnológica.

La Infraestructura tecnológica de la Universidad APEC está dotada con equipos de alto rendimiento, sistemas gestores de datos, servidores centralizados para la organización de usuarios, aplicación de políticas de seguridad por departamentos y servicios de aplicaciones para maquinas clientes. También poseen los últimos estándares, certificados, sistemas y equipos de seguridad ayudando a comprometer la integridad de la organización, de sus docentes y estudiantes. Como en toda organización debe haber una alternativa para mantener el flujo de electricidad continua, UNAPEC tiene implementado sistemas de energía eléctrica ininterrumpida, de esta forma, en caso de que ocurra un apagón eléctrico, la continuidad de los servicios eléctricos podrán continuar en los equipos sin preocuparse por este tipo de inconvenientes.

Sin embargo, hay que alabar la excelente infraestructura tecnológica que cuenta la plataforma EVA para el desenvolvimiento del mismo.

5.1 Conectividad

Vivimos en un mundo conectado donde el desarrollo actual viene marcado por el Internet. La dependencia para el uso del mismo está sujeta al número de actividades y procesos que se realizan por ese medio. La conectividad se ha transformado en la pieza importante para optimizar los procesos productivos de la organización.

El Data Center donde se encuentra la plataforma EVA trabaja con dos conexiones fibra óptica ofrecido por el Proveedor de Servicios de Internet (ISP) Claro, con una velocidad de 90 Megabits por segundo. Los enlaces redundantes que posee aumentan la disponibilidad en la red, de esta manera, en caso de que exista alguna falla en uno de sus enlaces, el servicio seguirá brindándose a docentes y estudiantes por medio del otro enlace de reserva. La fibra óptica son cables que contienen fibras de vidrio en el interior de una armazón aislante. Estos cables

están diseñados para transmitir datos a larga distancia y con un gran ancho de banda (velocidad de hasta gigabit por segundo) para comunicaciones de red.

Las señales que envían estos cables son señales de comunicación usando pulsaciones de luz. Los cables de fibra óptica son más caro, pero, son mayormente usados en empresas y organizaciones que requieren una mayor demanda en el uso de la red.

5.2 Seguridad y autenticación de usuario

La seguridad es un elemento muy importante a tomar en cuenta para conservar la integridad de la información y proteger el valor del mismo. La plataforma EVA mantiene una seguridad robusta a la hora de acceder a nuestras cuentas de usuarios registrados en la base de datos, consultar archivos, envío de mensajes instantáneos privados y realizar actividades asignadas por el docente.

El departamento de tecnología de la universidad APEC, tiene en ejecución el certificado AlphaSSL, con 256 bits de seguridad manejable desde la raíz, protegiendo todo lo que sea *.unapec.edu.do*, de esta forma protege la página web del EVA (www.eva.unapec.edu.do) que se encuentra dentro de ese mismo certificado.

La autenticación, que dicho sea de orden se encuentra estrechamente relacionada con la seguridad, decide que usuarios tienen el privilegio de acceder a los recursos de la plataforma y quiénes no. APEC utiliza el certificado de autenticación AlphaSSL CA para validar el acceso de usuarios al EVA de manera segura y privada. SSL ayuda a proteger las transacciones y las comunicaciones al sitio web del EVA. Esto protege las tarjetas de crédito de los clientes, contraseñas y datos confidenciales. El certificados SSL activa la construcción en SSL/TLS con funcionalidades de seguridad de los servidores web, navegadores y aplicaciones. Esta tecnología cifra las comunicaciones de navegador a servidor sobre HTTPS, como las transacciones de tarjetas de crédito, nombres de usuario, correo web y bases de datos a comunicaciones de base de datos. Este certificado brinda confianza y seguridad en páginas web donde se maneja muchas informaciones de gran importancia.

5.2.1 Autenticación con Base de Datos Externa

Moodle está configurada con una Base de Datos MySQL, la misma se encuentra en un servidor fuera del de apache dentro del *data center* de la Universidad. Moodle utiliza el plugin de Autenticación con Base de Datos externa para comprobar que el nombre de usuario y el password sean válidas. Si son válidas, el usuario tendrá acceso al EVA, de ser caso contrario, el usuario deberá de ponerse en contacto con el administrador de la plataforma para crear un usuario y un password en la base de datos y darle entrada al mismo. La aplicación web posee una sincronización automática para agregar usuarios a la base de datos cuando realizan un inicio de sesión a la plataforma, sin embargo, al ser un método no muy seguro, el departamento de tecnología de la Universidad APEC lo tiene deshabilitado para evitar ataques y llevar un control más organizado de sus estudiantes.

5.2.2 Autenticación IMAP

Recordamos que la plataforma EVA tiene servicios de correo electrónico Outlook para aquellos usuarios que se encuentran registrados en la base de datos. Para estos servicios, la autenticación IMAP realiza el trabajo de revisar las cuentas de usuarios. Esto permite integraciones directas con tecnologías con servidores de correo, como Microsoft Exchange.

Una vez se autentifica el ID y password del usuario, la aplicación web Moodle, en su base de datos, provee que permisos tiene cada cual, si como docente o como estudiante para disposición de los recursos del EVA. Protocolo LDAP Durante el proceso, se validan los directorios de los usuarios con el protocolo LDAP. Estos directorios contienen información personal de los docentes y estudiantes suministradas por los mismos y, posteriormente, las informaciones son presentadas en la página del EVA para que el usuario tenga constancia de que sus informaciones se encuentran actualizadas en la plataforma. La seguridad del protocolo es de "aplaudir", ya que se la transferencia de datos está cifrada, de igual forma la sesión entre el cliente y el servidor LDAP para proteger los datos de LDAP transmitidos.

5.2.3 Planificación de modelo de seguridad

La aplicación web Moodle también ofrece Servicios de Autenticaciones Centrales (CAS) como protocolo de inicio de sesión único (SSO) instalados en un servidor externo. Este servicio ofrece la ventaja de interactuar con diferentes aplicaciones web instaladas en Moodle con el inicio de sesión en la cuenta del usuario una sola vez, de esta forma, se simplifica tener que autenticar la cuenta del usuario cada vez que utilice un recurso web externo a la aplicación Moodle.

La tecnología de módulos de autenticación conectables (PAM) de Moodle permite al EVA usar la misma Base de Datos de usuarios para distintos ingresos de usuarios. Este método utiliza PAM para acceder a los nombres de usuario nativos del servidor.

El servicio de autenticación POP3 de la aplicación Moodle utiliza dicho proceso para acceder a los recursos de correo electrónico POP3 del servidor de la plataforma EVA.

Una vez los protocolos, módulos y tecnologías de la aplicación Moodle finalicen con el proceso de verificación y autenticación de cuentas de usuarios, el usuario estará disponible para utilizar los servicios web que le brinda dicha aplicación.

Pero ¿Cómo puedo sentirme seguro y confiado de que mis datos estarán íntegros y a salvo de algún pirata informático?

El departamento tecnológico de la universidad APEC tiene implementado las últimas tecnologías en cuanto a seguridad se refiere para el cuidado de ataques informáticos hacia la plataforma EVA. Para proteger aquellas conexiones entrantes y salientes, un *firewall* Fortinet realiza un monitoreo y luego ejecuta acciones permisivas o denegadas para el cuidado de la plataforma.

Nota: El EVA de UNAPEC no utiliza un servidor RADIUS para la autenticación.

5.3 Infraestructura

En cuanto a infraestructura tecnológica se refiere, la plataforma EVA está desarrollada para cumplir con los requerimientos mínimos y recomendados para que funcione correctamente y sin ningún problema. Dentro de la infraestructura física, el EVA cuenta con un servidor físico con Microsoft SQL Server para la administración de base de datos.

5.3.1 Infraestructura Virtual

En lo que concierne a la infraestructura virtual por la que trabaja el EVA, está conformada por dos servidores virtuales: Un servidor Web, donde se ejecuta la aplicación web Moodle directamente, con una capacidad de 8 Gb de RAM y 4 núcleos de procesador, la hace bastante potente para soportar acceso a la misma en horas picos. El otro servidor está dedicado para Base de Datos, con 12 Gb de RAM y 8 núcleos de procesador.

5.3.2 Infraestructura de Servidores

En cuanto a los servidores, el servidor web que aloja Moodle tiene instalado Apache, con un sistema operativo Red Hat de Linux, donde su procesador es un Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz, con 12 GB de memoria RAM y 8 núcleos. Moodle ocupa un mínimo de 5 Gb de almacenamiento para la instalación base de todos los paquetes incluyendo GNOME y KDE. Provee una arquitectura de 64 bits. Un mínimo de 2 núcleos de CPU, con una recomendación de 4 núcleos de procesador y un mínimo de 8 GB de RAM.

Por otra parte, la Base de Datos MySQL de la plataforma EVA cuenta con un servidor bajo el sistema operativo de Debian, distribución como *software* libre, donde su procesador Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz, con 24 GB de memoria RAM y 8 núcleos. Dicho sistema ocupa 4 Gb de Disco duro y requiere un mínimo de 128 Megabytes de memoria RAM. Como mínimo, se recomienda un Pentium II de 300 MHz. El perfil de este servidor incluye servicios de Web, DNS, FTP, POP y NIS, con 100 MB de espacio en disco sería "*relativamente*"

suficiente, siendo necesario añadir espacio adicional para los datos que pueda ofrecer. Provee una arquitectura de 64 bits.

5.3.3 Bases de Datos

La Base de Datos de la plataforma EVA es aplicada como un modelo in-house, es decir, es creada y administrada por el departamento de tecnología de la universidad APEC, a diferencia del modelo *outsourced*, donde se realiza el mantenimiento y el pago por parte de terceros. Su modelo de base de datos es relacional, permitiendo establecer relaciones entre datos que se encuentran guardados en tablas, a partir de ahí, realiza las conexiones correspondientes para relacionar los datos de varias tablas. Según la variación de sus datos, EVA es dinámica, pues realizan actualizaciones, borrado y ediciones en sus datos cuando se refleja un valor no deseado.

El gestor que utiliza es MySQL. La base de datos del EVA está compuesto a su vez, por diferentes bases de datos de acuerdo a las herramientas que la aplicación Moodle ofrece, de estas incluyen una para Chat/Mensajería, otra base de datos para Foros, otra para documentos, una para exámenes llamada Mdb_Quiz y otra para el almacenamiento de toda esa información que se sube al EVA llamada Moodle Data.

El módulo de base de datos de la aplicación web Moodle permite a los profesores y estudiantes crear, publicar y buscar en un banco de datos sobre un tópico en particular. Dentro del módulo de la base de datos, podemos elegir los parámetros necesarios para el registro o entrada que queremos crear y/o modificar. Los bloques desplegados dentro de la base de datos se encuentran:

- **Propiedades generales:** Dentro de este bloque, es posible crear el nombre del link o enlace por el cual los usuarios accederán a la actividad de la base de datos. También tiene un campo de introducción para explicar brevemente una descripción de la base de datos creada.

General

Nombre* Base de datos CI2

Introducción*

Fuente Tamaño Párrafo

B *I* U ABC x₂ x²

Esta base de datos contiene entradas relacionadas con el curso de las CI2

Ruta: p

Formato HTML

Las demás opciones dentro de las propiedades generales sirven para configurar el tiempo de activación de la base de datos, los datos que se visualizarán de la misma, las entradas requeridas, donde se especificará un número de entradas a introducir para que se dé como finalizada la actividad. En caso contrario, se visualizará un mensaje alertando de que no ha cumplido con las entradas correspondientes. Otra opción son las entradas requeridas antes de verse, que tiene como condición poder visualizar las entradas de los demás estudiantes solo si hemos cumplido con el número de entradas especificadas. En el número máximo de entradas define un valor límite que el estudiante pueda enviar antes de ser bloqueado, evitando a usuarios sobrecargar la base de datos.

La opción de comentarios está disponible en caso de que se requiera o no en dichas entradas. En caso de que se requiera aprobación, el docente podrá visualizar la entrada de los alumnos y decidir si está permitida o no para que otros usuarios puedan verla.

En caso contrario, los usuarios pueden enviar entradas sin necesidad de una aprobación futura. 'Esta opción es importante para moderar aquellas informaciones que puedan resultar ofensivas o inadecuadas. Por último, están los

artículos RSS que indican un número de entradas para publicar Sindicaciones Realmente Simples (RSS) en la base de datos.

Disponible desde Habilitar
 Disponible a Habilitar
 Solo lectura desde Habilitar
 Solo lectura para Habilitar
 Entradas requeridas Habilitar
 Entradas requeridas antes de verse Habilitar
 No. máximo de entradas Habilitar
 Comentarios Habilitar
 ¿Se requiere aprobación? Habilitar
 Artículos RSS Habilitar

Una vez configurado, se visualizan los enlaces de la base de datos de la siguiente manera:

Administración

- Administración del curso
- Calificaciones

Ajustes de mi perfil

Actividades

- Recursos
- Tareas

Eventos próximos

Tarea: El Principio de Intercambio de Lazard
viernes, 29 mayo, 11:00

Ver calendario...
Nuevo evento...

Calendario

mayo 2015

Dom	Lun	Mar	Mie	Jue	Vie	Sáb
2	4	5	6	7	8	9
10	11	12	13	14	16	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Clave de eventos

- Ocultar eventos globales
- Ocultar eventos de curso

Página Principal > Mis cursos > UNAFEC - GRADO > ISC404-43111-001-5962

ISC-404 - Computación Forense



ISC-404 - Programa de Clases

5 de mayo - 11 de mayo

12 de mayo - 18 de mayo

Conceptos Generales

19 de mayo - 25 de mayo

The screenshot shows a Moodle course page. At the top, the browser address bar displays 'eva.unapex.edu.do/moodle/course/view.php?id=211054'. The page title is 'Métodos débiles de educación de requisitos de software'. On the left sidebar, there are sections for 'No hay mensajes en espera' and 'Usuarios en línea' with '13 usuario(s) en línea'. The main content area is titled '14 de mayo - 25 de mayo' and 'SEMANA 03'. It contains a list of topics:

- Técnicas de Educación de Requisitos
- Selección de las Mejores Técnica
- Qué es un requisito o requerimiento?
- Caso Practico de las Técnicas de Educación de Requisitos
- Evaluación de los Requisitos (Checklist and Matriz de Iteración)

Below the list, there are several activity icons and titles:

- Técnicas de Educación de Requisitos
- Material sobre las Técnicas de Educación de Requisitos.
- Ensayo sobre técnicas de Educación de Requisitos
- Hoy que preparar un ensayo de unos 10 paginas de contenido sobre las técnicas de educación de Requisitos que existen actualmente para identificar los requisitos de un sistema Software. Hoy que agregar Bibliografía segun APA de las fuentes referenciadas.
- Cuestionario - 1 Virtualizacion
- Iná - subida de cuestionario
- Métodos débiles del Analisis
- Discusion de los Métodos débiles del Analisis

La calificación se agrupa dentro de categorías. Dicha categoría, tiene su propia calificación que calcula dependiendo de sus elementos. Se puede crear un nombre para dicha categoría, y luego se podrá editar al gusto del docente, como por ejemplo la forma de calificación de los estudiantes de la universidad APEC, 20 puntos para primer parcial y 15 de prácticas para un total de 35 el primer periodo, mismo método para el segundo periodo y un final que contemplara un examen de 30 puntos para un total de 100. Otras opciones como mantener en la categoría solamente las notas sobresalientes y otras para aquellas que están bajas, entre otras opciones.

Grade category

Category name* * Hide Advanced

Aggregation ? Mean of grades

Aggregate only non-empty grades* ?

Aggregate including subcategories ?

Keep the highest* ? None

Drop the lowest* ? None

Parent category

Grade category Moodle Tests

My report preferences

Aggregation view (Default: Full view)* ? Default * Hide Advanced

Save changes Cancel

There are required fields in this form marked*.

También existe un módulo de base de datos para calificaciones, capaz de elegir roles con permisos para calificar cuando se haya creado la base de datos, el tipo de consolidación (por promedio, número, máxima o mínima y suma de calificaciones), entre otras.

Calificaciones

Roles con permiso para calificar ? La comprobación de privilegios no está disponible hasta que se guarde la actividad

Tipo de consolidación ? No hay calificaciones

Escala Escala UA

Limitar las calificaciones a los elementos con fechas en este rango:

Desde 22 febrero 2012 11 20

Hasta 22 febrero 2012 11 20

- **Ajustes comunes del módulo:** Se indica si se manejan grupos en la base de datos, el agrupamiento para realizar distintas tareas a cada estudiante,

la visibilidad de la base de datos, mostrando u ocultando la misma para los alumnos y el número de ID que identifica una actividad en las calificaciones.

Ajustes comunes del módulo

Modo de grupo ? No hay grupos ▾

Agrupamiento* ? Ninguno ▾

Visible Mostrar ▾

Número ID ?

Es posible crear campos que estarán integrados en la base de datos, tales como archivo para la subida de archivos por parte de los estudiantes, botones de radio para seleccionar entre varias opciones, la caja de selección para colocar varios botones de radios, dibujo para subir imágenes, área de texto para que los estudiantes puedan escribir libremente, entre otras opciones.

Crear un nuevo campo

Selección por defecto Elegir...

- Elegir
- Archivo
- Botones de radio
- Caja de selección
- Dibujo
- Fecha
- Latitud/logitud
- Menú
- Menú (selección múltiple)
- Número
- Texto
- Url
- Área de texto

5.4 Alimentación energética

En cuanto a alimentación energética, el Data Center de la universidad APEC se encuentra debidamente preparado para cualquier tipo de interrupción o falla eléctrica que se pueda presentar. El Data Center cuenta con dos Unidades de Distribución de Poder (PDU), o mejor dicho, dos regletas de gran tamaño. Los dos PDU entran en energía constante, se va uno y el otro se encuentra con energía para seguir enviándola. Esas regletas llevan conectadas un UPS, siendo un total de dos UPS. En dado caso que falle una de los UPS, entra el otro UPS conectado a la otra regleta. También se tiene una planta única y exclusivamente para el Data Center, con una durabilidad para entrar de máximo 3 minutos. La capacidad que tiene la planta para durar activa es de alrededor de 1 hora y entra automáticamente cuando detecta pérdida de la energía principal de EDESUR.

RESUMEN

La conectividad que ofrece las fibras ópticas conectada a los Data Center de UNAPEC ofrecen mayor tasa de transferencia de data hacia los servidores.

La seguridad se encuentra completamente robusta al tener asegurado todo el dominio *unapec.edu.do* y certificados de seguridad para el acceso del mismo. Sus infraestructuras van desde físicas hasta virtuales, contando con potentes servidores y un almacenamiento con diferentes backup de discos.

Las bases de datos del EVA se encuentran externas, pero trabajan en conjunto con las de Moodle para ofrecer mayor centralización y sincronización de los datos. La alimentación energética de UNAPEC se encuentra debidamente redundante, ofreciendo un TIER de nivel 4 para el Data Center del mismo.

Resumen gráfico, Capítulo V. Infraestructura tecnológica

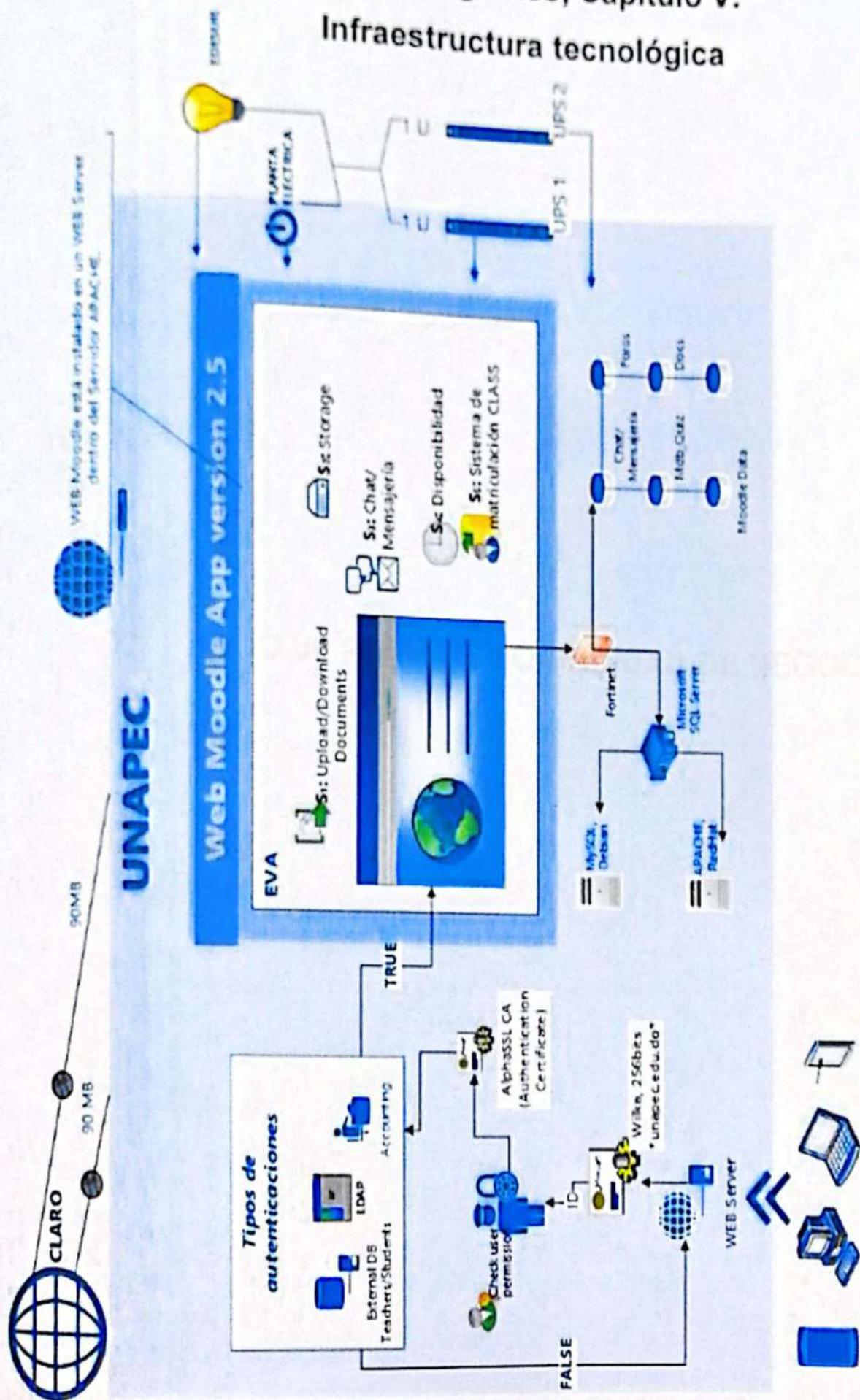


Ilustración 56. Esquematación de la plataforma EVA, UNAPEC.

Fuente: Imagen propia.

CAPITULO VI. PLAN DE CONINUIDAD DE NEGOCIO

FASE I: Análisis y evaluación de riesgos

6.1 Evaluación de riesgo

En esta evaluación de riesgo se han de reconocer las situaciones que podrían afectar perjudicialmente el *data center* de la Universidad Pro-Educación y Cultura (UNAPEC), esto comprende:

- Potenciales daños que podrían causar estos eventos.
- La cantidad de tiempo necesaria para recuperar o restaurar las operaciones.
- Medidas preventivas o controles que deben mitigar la posibilidad de que estos acontecimientos ocurran.

Las siguientes tablas han sido completadas con una puntuación de medidas escalables, valorando el impacto y la probabilidad de los acontecimientos.⁷

Leyenda:

PROBABILIDAD		IMPACTO	
PUNTUACION	NIVEL	PUNTUACION	NIVEL
1	Muy alto	1	Terminal
2	Alto	2	Devastador
3	Medio	3	Critico
4	Bajo	4	Controlable
5	Muy bajo	5	Irritante

6.1.1 Desastres ambientales

Los desastres ambientales pueden provocar fallas y daños graves a la infraestructura del edificio donde está alojado el *data center* y los equipos que mantienen la plataforma funcionando y disponible.

En la siguiente tabla se muestran las probabilidades e impacto que pueden tener estas catástrofes naturales.

⁷ Información válida Santo Domingo, República Dominicana.

Desastre potencial	Probabilidad	Impacto	Consecuencias
Terremoto	2	2	Daño total de los equipos. Desplome de la edificación.
Inundación	5	5	Daño total de los equipos.
Huracán	2	2	Inundaciones, deslizamiento de tierra y fuertes vientos, provocando fallas energéticas.
Tsunami	4	3	Inundación total del área provocando daño total de los equipos.
Tormenta Eléctrica	3	3	Fallas en el sistema eléctrico provocando la entrada temporal de energías alternas.

6.1.2 Interrupciones organizadas o deliberadas

El sistema puede verse fuera de servicio debido a una serie de mantenimientos, estos deben de hacerse periódicamente para asegurar un óptimo funcionamiento y evitar errores o situaciones que puedan decrecer el funcionamiento de la red.

En la siguiente tabla indica el impacto que podría provocar una interrupción deliberada y la probabilidad de que tan frecuente ha de hacerse esta actividad:

Desastre potencial	Probabilidad	Impacto	Consecuencias
Mantenimiento base de datos	1	1	No tiene acceso a la información.
Mantenimiento servidores	1	1	No hay sistema.
Mantenimiento UPS	3	3	Un apagón. Una falla eléctrica donde los demás servicios de soporte no entren para alimentar el sistema.
Mantenimiento equipos de red	1	1	Pérdida de la conexión al exterior.
Mantenimiento cableado	3	3	Pérdida de la conexión total.
Mantenimiento sistema eléctrico	1	1	Un apagón. Una falla eléctrica donde el UPS o la planta eléctrica pasen a ser la alimentación principal por un tiempo limitado.
Mantenimiento Firewall	2	3	Equipo de conexión bidireccional fuera de servicio.

Desastre potencial	Probabilidad	Impacto	Consecuencias
Mantenimiento sistemas	2	2	Servicios suspendidos.

6.1.3 Fallas en servicios públicos

La falta de un servicio público puede afectar directamente los recursos informáticos, debido a que el *data center* depende totalmente de estos servicios para un perfecto funcionamiento.

Una falla en el internet es considerado terminal debido a que UNAPEC cuenta con un solo proveedor de internet, teniendo una alta vulnerabilidad en el caso de que la telefónica tenga un problema de conectividad.

Por otro lado, la electricidad puede ser "manejable" porque la institución posee un TIER 4, en lo que al diagrama eléctrico se refiere.

Desastre potencial	Probabilidad	Impacto	Consecuencias
Internet	1	1	Pérdida de la conexión al exterior.
Electricidad	1	3	Una falla eléctrica donde el UPS o la planta eléctrica pasen a ser la alimentación principal por un tiempo limitado.

6.1.4 Fallas en los equipos o sistemas

El *software*, *hardware*, la electricidad y la planta física pueden tener fallas, donde la falta de uno trae consecuencias críticas para el buen funcionamiento de la plataforma EVA.

Los recursos informáticos que conforman la plataforma tienen una probabilidad de fallo y cada componente con un mal funcionamiento acarrea un impacto.

Desastre potencial		Probabilidad	Impacto	Consecuencias
Software	Database (modo relacional)	2	1	No tiene acceso a la información.
	SQL Server	3	1	No válida la información.
	MySQL	4	4	No tiene acceso a la información.
	Debian	4	2	No hay sistema.
	Apache (Web service)	4	1	No hay servicio web.
	Red Hat	4	1	No tiene acceso a la información.
	LDAP (Protocolo Ligerero/ Simplificado de Acceso a Directorios)	4	1	No hay acceso a los directorios, de manera que no permite ningún tipo de autenticación.
	Autenticación con base de datos	4	1	No tiene acceso a la información.
	Autenticación IMAP (correo electrónico)	3	1	No hay recursos de correo electrónico.
	Fortinet	5	1	Equipo de conexión bidireccional fuera de servicio
	Certificado AlphaSSL CA	5	1	No hay encriptación.
	Virtualizador	3	2	Perdida de conexión con ambos servidores.
	Hardware	Servidores	5	1
SSD SAN Storage		3	1	Perdida de datos.
Convertor de medios (Fibra óptica - Ethernet)		4	1	Pérdida de la conexión hacia al exterior.
Switch		5	1	Pérdida de la conexión total.
Router		5	1	Pérdida de la conexión total.
Wireless Access point		4	3	No hay red inalámbrica.
Racks		5	2	Daño físico de los equipos que soportan.
Gabinete		5	2	Daño físico de los equipos que soportan.
Dispositivos de acceso biométricos		3	3	No hay control de acceso o no hay acceso.
KVM Console Servers		5	4	No hay interfaz gráfica ni entrada del teclado.
Cableado en cobre	2	1	Pérdida de la conexión a la red local.	

Desastre potencial		Probabilidad	Impacto	Consecuencias
	Cableado en fibra	2	1	Pérdida de la conexión hacia el exterior.
	Sensor de vibración	5	3	No se perciben anomalías de acceso o movimientos de la edificación.
	Sensor de humedad	5	3	Humedad excesiva puede producir condensación y a su vez un cortocircuito.
	Sensor de temperatura	5	2	Descontrol de la climatización.
	Cámaras de vigilancia	4	4	No hay visión dentro ni fuera del <i>data center</i> .
	Sistema automático contra incendio	5	3	En caso de una emergencia, pérdida total por falta de alarma a tiempo.
Electricidad	Línea de la Corporación energética	3	3	Entrada inminente del transformador. (Segunda línea eléctrica)
	Transformador	3	3	Entrada inminente de la planta eléctrica.
	Planta eléctrica	3	3	Entrada inminente de los UPS.
	UPS	3	1	Se apagan bruscamente todos los equipos.
Planta física	Iluminación	4	4	Ninguna visibilidad.
	Aire de alta precisión	4	1	Falla en la climatización.
	Climatización (Pasillos encapsulados)	4	1	Sobrecalentamiento de los dispositivos.

6.1.5 Incidentes serios de seguridad

Un incidente de seguridad es un hecho o amenaza que atenta contra la confidencialidad, integridad o disponibilidad de un sistema de seguridad de información. (AGESIC, n.d.)

En la siguiente tabla se encuentran los principales desastres potenciales que podrían enfrentar un *data center*.

Desastre potencial	Probabilidad	Impacto	Consecuencias
Violación perimetral	2	1	Desconexión, hurto, mala manipulación de los equipos causando fallas graves.
Acceso no autorizado al sistema	3	1	Copia de información sensible, desconexión y daños a los sistemas que mantienen la plataforma funcionando.
Personal de servicio	3	3	En el tiempo de espera para que el personal se presente todo el <i>data center</i> pueden haber colapsado sus sistemas como también la estructura física.

6.1.6 Otras situaciones de emergencia

Un incendio, es una situación de emergencia que se puede presentar en un *data center* con consecuencias irreparables y para minimizar el riesgo de que este desastre ocurra, existen estándares para prevenir incendios dentro del cuarto, como son: NFPA 75, EN 50085-1 y EN 61386. Además, otras situaciones que podrían darse son: el colapso de la infraestructura, debido a que fue construido alrededor de 1964 y el departamento de tecnología de Universidad APEC solo cuenta con una puerta de acceso para la entrada y salida del personal.

Desastre potencial	Probabilidad	Impacto	Consecuencias
Incendio	5	1	Pérdida total de los equipos y de la estructura.
Colapso de infraestructura	2	1	Pérdida total de los equipos.
Puerta de acceso al <i>data center</i>	1	1	En caso de alguna emergencia, donde la única puerta de acceso está bloqueada el personal corre el riesgo de muerte.

6.2 Análisis de impacto del negocio

El reto es asignar estratégicamente los recursos para "equipo de seguridad y bienes" que intervengan en el rendimiento del negocio, basándose en el impacto potencial del negocio, respecto a los diversos incidentes que se deben resolver. (Ferro Veiga)

En las siguientes tablas se detallan los procesos claves del de la plataforma EVA, los períodos de tiempo de recuperación (RTO), evaluación impacto financiero y operacional, entre otras.

6.2.1 Procesos de negocio clave

La plataforma EVA cuenta con una serie de procesos indispensables para su correcto funcionamiento, donde cada una dependencia principal.

Área clave para el negocio	Descripción del proceso	Dependencias principales
Sistemas Eléctrico	Reciben la energía eléctrica de EDESUR y la distribuyen al Data Center de UNAPEC.	Suministros de Energía
Sistemas Emergentes	Suministran energía eléctrica por tiempo limitado.	Batería y Combustibles
Autenticación	Verificación de credenciales (matrícula y contraseña) para acceder a los recursos.	Base de Datos
Seguridad	Cifrado y protección de información y equipos informáticos.	Sistemas actualizados
Sistemas de Manejo de Gestión de Base de Datos	Maneja y gestiona las bases de datos del modelo relacional.	Base de Datos
Base de Datos	Almacenan datos en un banco de informaciones para posteriormente ser gestionados.	Microsoft SQL Server
Servicios Web	Ofrecen los recursos web de la aplicación Moodle mediante protocolos y estándares.	Microsoft SQL Server
Base de Datos Relacionales	Almacenan los datos de aquellos servicios web de Moodle.	Microsoft SQL Server, MySQL
Servidores	Centralizan los datos y dan servicios a host clientes	Requerimientos físicos y lógicos

6.2.2 Definición de períodos de tiempo objetivos de

recuperación / RTO

En la siguiente tabla se muestra el porcentaje de la disponibilidad de la data, el volumen de datos en riesgo tolerable, el tiempo máximo de recuperación y el

tiempo de respaldo de la data. Todo dependiendo de qué nivel de impacto tenga el tipo de información del sistema.

Data value class	Data availability	RPO (Data Loss Risk)	RTO (Maximum Recovery Time)	DPW (Copy Data Time)
Operaciones no importantes	85%	2 horas	3 horas	2 horas
Importante para productividad	95%	30 min	1 hora	1 hora
Información importante para el negocio	90%	40 min	1 hora	1 hora
Información vital para el negocio	99%	1 min	5 min	30 minutos
Información crítica para el negocio	99%	5 min	10 min	30 minutos

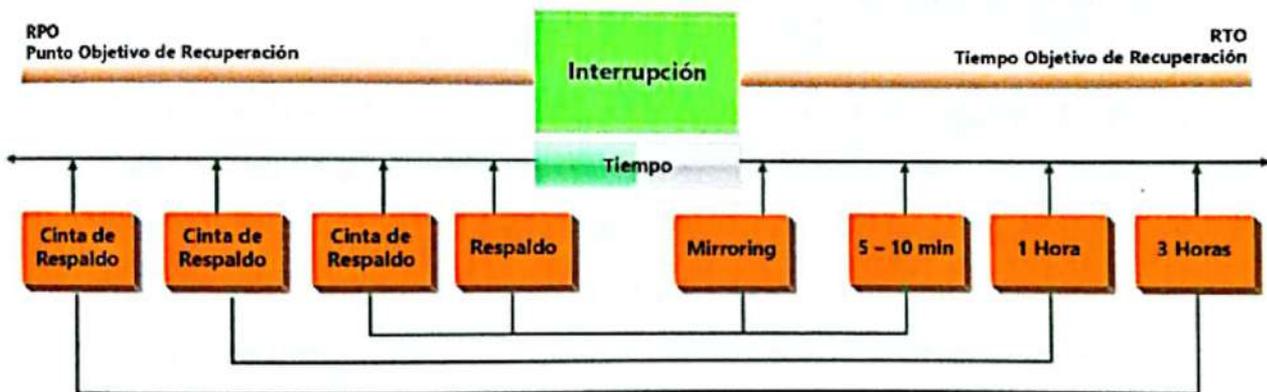


Ilustración 57. Diagrama de RPO y RTO.

Fuente: Imagen propia basada en ORACLE.

6.2.2.1 Parámetros imprescindibles

Los **parámetros imprescindibles** para establecer las estrategias de recuperación, son:

- **Ventana de interrupción:** Tiempo que una empresa puede esperar en el momento una falla hasta su completa restauración.

- **Objetivos de prestación de servicios:** son los servicios alternos utilizados hasta el restablecimiento por completo de los sistemas.
- **Cortes máximos tolerables:** Tiempo tope del modo alterno, es decir, cuando este modo no soporta procesar más tiempo los servicios.

6.2.2.2 Alternativas de recuperación

Una de las principales alternativas de recuperación para situaciones muy críticas es tener un sitio alterno (offsite), donde se encuentren las instalaciones de respaldo de *hardware*. Estas instalaciones se clasifican en:

- **Hot sites:** Son instalaciones listas para operar en varias horas, los equipos y sistemas tienen que ser compatibles con la instalación principal. Este site puede soportar las operaciones de emergencia sin problema pero durante un tiempo limitado y no prolongado.
Las necesidades adicionales tipo de instalación son: personal, programas, archivos de datos y documentación.
- **Warm sites:** Configurados parcialmente, con equipos periféricos seleccionados y conexiones de red.
- **Acuerdo entre organizaciones:** Es un acuerdo con otra organización de manera recíproca, es poco común y en este las partes deben mutuamente proveerse tiempos en los equipos cuando se dé la emergencia.
- **Sincronización *cloud*:** El entorno puede ser compartido o privado, todo depende de los requerimientos y el enfoque de la institución.

6.2.3 Impacto financiero y operacional

El conjunto de consecuencias que pueden ser provocadas por una situación que altere el funcionamiento normal de la plataforma EVA, es considerado como un impacto operacional, este se mide en tiempos de recuperación, los mismos pueden traducirse en pérdidas monetarias.

6.2.3.1 Evaluación del impacto operacional

El impacto operacional va a depender de los tiempos de recuperación para cada proceso de la plataforma.

En la siguiente tabla se muestra un el modelo de evaluación del impacto operacional en diferentes "procesos", cada uno con sus tiempos tope de recuperación.

Procesos	Tiempo de recuperación				
	1	2	3	4	5
Suministro de energía eléctrica de EDESUR al Data Center de UNAPEC.	24 minutos	48 minutos	72 minutos	96 minutos	120 minutos
Suministro energía eléctrica por tiempo limitado.	48 minutos	96 minutos	144 minutos	192 minutos	240 minutos
Verificación de credenciales (matrícula y contraseña) para acceder a los recursos.	1 minutos	2 minutos	3 minutos	4 minutos	5 minutos
Cifrado y protección de información y equipos informáticos.	1 minutos	2 minutos	3 minutos	4 minutos	5 minutos
Manejo y gestión de las base de datos del modelo relacional.	3 minutos	6 minutos	9 minutos	12 minutos	15 minutos
Almacenamiento de datos en un banco de informaciones para posteriormente ser gestionados.	4 minutos	8 minutos	12 minutos	16 minutos	20 minutos
Ofrecer recursos web de la aplicación Moodle mediante protocolos y estándares.	4 minutos	8 minutos	12 minutos	16 minutos	20 minutos
Almacenamiento de datos de servicios web de Moodle.	2 minutos	4 minutos	6 minutos	8 minutos	10 minutos

6.2.3.2 Evaluación del impacto financiero

El impacto financiero va a depender del incremento duradero de los tiempos de recuperación para cada proceso y cuanto se vean afectados cada uno para el correcto desenvolvimiento de la plataforma. En la siguiente tabla se muestra un el modelo de evaluación del impacto financiero en diferentes "procesos", cada uno con sus tiempos tope de recuperación.

Procesos	Tiempo de recuperación				
	1	2	3	4	5
Recibimiento energía eléctrica de EDESUR al Data Center de UNAPEC.	48 minutos	72 minutos	96 minutos	120 minutos	144 minutos
Suministro energía eléctrica por tiempo limitado.	96 minutos	144 minutos	192 minutos	240 minutos	288 minutos
Verificación de credenciales (matricula y password) para acceder a los recursos.	2 minutos	4 minutos	6 minutos	8 minutos	10 minutos
Cifrado y protección de información y equipos informáticos.	2 minutos	4 minutos	6 minutos	8 minutos	10 minutos
Manejo y gestionamiento de las base de datos del modelo relacional.	6 minutos	9 minutos	12 minutos	15 minutos	18 minutos
Almacenamiento de datos en un banco de informaciones para posteriormente ser gestionados.	8 minutos	12 minutos	16 minutos	20 minutos	24 minutos
Ofrecimiento de recursos web de la aplicación Moodle mediante protocolos y estándares.	8 minutos	12 minutos	16 minutos	20 minutos	24 minutos
Almacenamiento de datos de servicios web de Moodle.	4 minutos	6 minutos	8 minutos	10 minutos	12 minutos
Centralizan los datos y dan servicios a host clientes	4 minutos	6 minutos	8 minutos	10 minutos	12 minutos

6.2.3.3.1 Análisis de costo

Conociendo que la Universidad APEC cuenta con más de 8000 estudiantes activos, y que cada cuatrimestre incrementa, se calculará el importe bruto mínimo por un cuatrimestre.

Asumiendo que un estudiante promedio de nacionalidad dominicana toma un mínimo de 12 créditos (alrededor de 4 materias) por cuatrimestre, ¿Cuánto sería el **importe bruto** de la universidad si calculamos los 8000 estudiantes con el "promedio" de 12 créditos?

Conociendo que los montos fijos de un estudiante, son:

Montos fijos ⁸	
Crédito	RD\$ 980.00
Estudiantes	RD\$ 8,000.00
Recursos tecnológicos	RD\$ 1,200.00
Laboratorio	RD\$ 750.00
Inscripción	RD\$ 7,500.00

Un estudiante promedio pagaría:

$$\begin{aligned} \text{Un estudiante pagaría} &= \text{Inscripción} + \text{Recursos tecnológicos} + (\text{Laboratorio } (x_1^9)) \\ &+ (\text{Crédito } (x_2^{10})) \\ &= \text{RD\$ } (7,500.00 + 1,200.00 + (750.00 (1)) + (980.00 (12))) \end{aligned}$$

$$\text{Total a pagar por un estudiante} = \text{RD\$ } 21, 210.00$$

Entonces, por 8000 estudiantes sería:

$$\begin{aligned} \text{Importe bruto} &= \text{Total a pagar por un estudiante} * 8,000 \\ &= \text{RD\$ } (21,210.00 * 8,000) \end{aligned}$$

$$\text{Importe bruto} = \text{RD\$ } 169, 680, 000.00$$

Conociendo un posible valor del importe bruto de la Universidad APEC, ¿Cuánto perderán cuando durante los tiempos picos de un cuatrimestre (semana de parciales) la plataforma tienen que ponerla fuera de servicio por un mantenimiento de emergencia, acontece un evento (falla), congestión del sistema y se hace

⁸ Precios reales.

⁹ "X₁" es una variable. Su valor va a depender de la cantidad de materias que conllevan laboratorios.

¹⁰ "X₂" es una variable. Su valor va a depender de la cantidad de créditos que el estudiante adquiera.

imposible utilizarla en el horario pautado para los exámenes o no se pueden subir las asignaciones?

Si vuelvo a elegir los 8,000 estudiantes, cada uno con 4 materias, con un total de 12 créditos, donde 2 de esas materias tienen 1 hora virtual cada una y un cuatrimestre dura alrededor de 17 semanas, entonces: ¿Cuánto sería el costo de un crédito semanal?

$$3 \text{ créditos} = \text{RD\$ } 2,940.00$$

$$3 \text{ créditos por semana} = \text{RD\$ } 2,940.00 / 17 \text{ semanas} = \text{RD\$ } 172.94$$

Por lo tanto:

$$\text{Un crédito semanal} = \text{RD\$ } 172.94 / 3 \text{ horas semanales}$$

$$\text{Una crédito semanal} = \text{RD\$ } 57.65$$

Entonces, si un crédito cuesta RD\$ 57.65 por semana y durante las 17 semanas del cuatrimestre la Plataforma EVA no está disponible durante 3 horas, ¿Cuánto pierde la Universidad?

$$\text{Fuera de servicio por 3 horas} = \text{RD\$ } 172.94$$

$$\text{Cantidad de estudiantes matriculados} = 8,000$$

$$\text{Pérdidas} = \text{RD\$ } (172.94 * 8,000)$$

$$\text{Pérdidas} = \text{RD\$ } 1, 383, 529.41$$

6.3 Comunicaciones e IT

Cuando se consideran los riesgos del negocio, el impacto en los servicios de las comunicaciones, trae consigo una cadena de dependencias que podrían ser afectadas. A continuación, se sugieren consideraciones a tener en cuenta en el manejo de las comunicaciones e IT.

6.3.1 Especificaciones de IT y telecomunicaciones

En los siguientes recuadros están las especificaciones detalladas (características) de los principales recursos del departamento de IT y de red de la Universidad APEC.

6.3.1.1 Hardware

Tipo	CPU / Modelo	Procesador	RAM	Disco	Vendedor	Sistemas operativos
Servidor	DELL	8 y 4 núcleos	12 y 8 GB	40 GB	DELL Inc.	Debian y Red Hat
Router	CISCO	4 núcleos	2 GB	2 GB	Cisco Ent.	Cisco IOS 15.0
Wireless Access point	Cisco Aironet	2 núcleos	32 MB	20	Cisco Ent.	Versión 2.0
Racks	TL	Ninguno	Ninguno	Ninguno	Quest Int. S.A.	Ninguno
Gabinete	TL	Ninguno	Ninguno	Ninguno	Quest Int. S.A.	Ninguno
Dispositivos de acceso biométricos	X7	Ninguno	Ninguno	Ninguno	Honeywell	Ninguno
KVM Console Servers	Switch G2	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
Cableado	Cobre, Fibra	Ninguno	Ninguno	Ninguno	Spektra	Ninguno
Sensor de vibración	FAG Smart Check	Ninguno	Ninguno	Ninguno	SCHAEFFLER	Ninguno
Sensor de humedad	HCT01	Ninguno	Ninguno	Ninguno	Elektronik	Ninguno
Sensor de temperatura	E5CC	Ninguno	Ninguno	Ninguno	Omron	Ninguno
Cámaras de vigilancia	TL	Ninguno	Ninguno	Ninguno	TP-LINK	Ninguno
Sistema automático	Safe Guard16	Ninguno	Ninguno	Ninguno	Emerson Process	Ninguno

Tipo	CPU / Modelo	Procesador	RAM	Disco	Vendedor	Sistemas operativos
contra incendio	Channel Modbus				Management	

6.3.1.2 Software

Sistemas	Versión	Vendedor / Soporte	Plataforma	Características principales
SQL Server	12.0	Microsoft	Windows	Soporte de transacciones y procedimientos almacenados. Posee un entorno gráfico de administración, donde permite comandos DDL y DML gráficamente. Se puede trabajar cliente-servidor, donde la información y datos se alojan en el servidor y clientes solo acceden a la información.
MySQL	5.6.25	MySQL AB	GNU/Linux	Disponibilidad en gran cantidad de plataformas y sistemas. Conectividad segura. Replicación. Posibilidad de selección de mecanismos de almacenamiento.
Debian	8.0	Comunidad developer	GNU/Linux	Compatible con dos núcleos: Linux y kfreebsd. Ofrece imágenes de DVD y CD para la instalación. El archivo opcionalmente instala el entorno de escritorio, la configuración para portátiles, diversos servidores, base de datos SQL y el cargador de arranque GRUB.
APACHE (Web service)	2.4.9	Robert McCool		Altamente configurable. Bases de datos de autenticación.

Sistemas	Versión	Vendedor / Soporte	Plataforma	Características principales
Red Hat	9.0	Red Hat Inc.	Linux	Es instalado en Anaconda, una ambiente gráfico. Contiene una herramienta para configurar los <i>firewalls</i> , llamada Lokkit. Desde la versión 8.0 incluye un entorno de escritorio gráfico, conocido como Bluecurve.
LDAP (Protocolo Ligero de Acceso a Directorios)	LDAPv3	Internet Engineering Task Force	GNU/Linux	Soporta la capa de autenticación y seguridad (SASL), la seguridad de la capa de transporte (TLS) y la capa de conexión segura (SSL).
Fortinet	Fortigate 100D	Fortinet	FortiManager-200D	Contiene servidor VPN IPSEC y SSL, control de aplicaciones, prevención de intrusiones, antivirus, antimalware, antispam, Seguridad P2P y web filtering.
Certificado AlphaSSL CA	1.1	AlphaSSL	--	Cifra todas las transacciones de comercio electrónico y los datos del cliente permanecerán cifrados.

6.3.2 Sistemas y procesos de información

En la siguiente tabla se listan las fases más críticas de IT mostrando que sistemas pueden significar una "baja" grave durante una interrupción.

Sistema	Proveedor	Versión	Plataforma / Sistemas operativos
SQL Server 2012	Microsoft	11.0	Windows Server 2012
MySQL	Oracle	5.6.25	Debian
Debian	Organización sin fines de lucro (Debian)	8.0	GNU/Linux
Apache (Web service)	Apache Software Foundation	2.2.15	Red Hat
Red Hat	Red Hat Inc.	7.0	Linux

Sistema	Proveedor	Versión	Plataforma / Sistemas operativos
Autenticación AlphaSSL CA	GlobalSign	SHA256 - G2	Linux
Firewall (FortiGate)	Fortinet	5.2	FortiOS
Moodle (Base de Datos relacionales)	Moodle	2.5	Red Hat

6.3.3 Personal interno y lista de contactos de emergencia

La siguiente tabla es una lista del personal interno para casos de emergencia para garantizar que la persona responsable del backup y recuperación pueda contactarse fácilmente.

Nombre del Sistema	Nombre del personal clave ¹¹	Detalle de contacto normal	Detalle de contacto en emergencias ¹²
Fortinet	Arturo Silva	Administrador de seguridad	809-222-0042
Microsoft SQL Server	Alfredo Jiménez	Analista de base de datos	809-222-0065
APACHE	Juan Pérez / Pedro Mateo	Auxiliar de Administración de servidores	809-222-0063 / 809-222-0064
Red Hat			
MySQL	Alfredo Jiménez	Analista de base de datos	809-222-0065
Bases de datos			
Autenticación AlphaSSL CA	Arturo Silva	Administrador de seguridad	809-222-0042

¹¹ Los nombres proporcionados en este documento son modelos para mantener la confidencialidad.

¹² Los números telefónicos proporcionados en este documento son modelos de "flota" para mantener la confidencialidad.

6.3.4 Ingenieros de mantenimiento y personal clave de los proveedores

Lista de contactos principales de telecomunicaciones y los proveedores que pueden ser contactados en el momento de una emergencia y obtener el nivel de servicio acordado.

Nombre del Sistema	Proveedor mantenimiento	Tiempo mínimo contratado	Detalle del contacto normal ¹³	Detalle del contacto de emergencia ¹⁴
Fortinet	Fortinet	1 año	Arturo S. - Administrador de seguridad	809-222-0042
Microsoft SQL Server	Microsoft	1 año	Alfredo J. - Analista de base de datos	809-222-0065
APACHE	Apache Software Foundation	1 año	Juan / Pedro - Auxiliares de Administración de servidores	809-222-0063 / 809-222-0064
Red Hat	Red Hat Inc.	1 año		
MySQL	Oracle	1 año	Alfredo J. - Analista de base de datos	809-222-0065
Bases de datos	Personal interno	1 año		
Autenticación AlphaSSL CA	GlobalSign	1 año	Arturo S. - Administrador de seguridad	809-222-0042

¹³ Los nombres proporcionados en este documento son modelos para mantener la confidencialidad.

¹⁴ Los números telefónicos proporcionados en este documento son modelos de "flota" para mantener la confidencialidad.

FASE II: Selección de estrategias

6.4 Diseño de estrategias de continuidad

Una vez presentado y documentada la primera fase del plan de continuidad de negocio (Análisis y evaluación del negocio), hay que tomar medidas para minimizar los efectos de una potencial emergencia.

En esta nueva fase (Selección de estrategias) se incluyen las estrategias claves para mitigar los efectos de los eventos.

6.4.1 Estrategia de manejo del sitio alternativo

Todas las organizaciones deberían prepararse para posibles situaciones de emergencia, el tipo de back-up va acorde con los requerimientos y actividades del sistema. Para cada proceso clave se ha escogido un tipo de back-up.

Proceso clave	Estrategia de Back-up acordada
Alimentación de la energía eléctrica de EDESUR	Implementación de planta generadora de energía independiente.
Suministran energía eléctrica por tiempo limitado.	Implementación de sistemas de UPS en equipos críticos.
Verificación de credenciales (matricula y contraseña) para acceder a los recursos.	Implementar sistema emergente de autenticación.
Cifrado y protección de información y equipos informáticos.	Implementar sistema emergente de autenticación.
Maneja y gestiona las bases de datos del modelo relacional.	Implementar el Sistema de Disco Duro SAN y el servicio <i>cloud</i> .
Almacenan datos en un banco de informaciones para posteriormente ser gestionados.	Implementar el Sistema de Disco Duro SAN y el servicio <i>cloud</i> .
Ofrecen los recursos web de la aplicación Moodle mediante protocolos y estándares.	Implementar el acceso de la aplicación web moodle en la memoria de cache.
Almacenan los datos de aquellos servicios web de Moodle.	Implementar el Sistema de Disco Duro SAN y el servicio <i>cloud</i> .
Centralizan los datos y dan servicios a host clientes.	Implementar servidor virtualizado emergente.

6.4.2

Respaldo y recuperación para sistemas IT

De los aspectos más importantes para el respaldo y recuperación de los sistemas, está la selección de una estrategia apropiada para el back-up y recuperación de los sistemas basados en IT.

En la siguiente tabla se muestran los sistemas y servicios vitales que ameritan una estrategia de back-up.

Sistema	Proceso clave soportado	RTO acordado	Estrategia de back-up acordada
SQL Server	Maneja y gestiona las bases de datos del modelo relacional.	15 minutos	Tener un servidor SQL virtualizado emergente.
MySQL	Almacena datos en un banco de informaciones para posteriormente ser gestionados.	20 minutos	Tener una imagen idéntica a la base de datos actualizada.
Debian	Aloja la base de datos de la plataforma EVA.	5 minutos	Tener un servidor GNU/Linux Virtualizado emergente
Apache (Web service)	Ofrece los recursos web de la aplicación Moodle mediante protocolos y estándares.	5 minutos	Tener el acceso de la aplicación web moodle en la memoria de cache.
Red Hat	Aloja la aplicación de web moodle.	5 minutos	Tener otro sistema operativo GNU / Linux virtualizado emergente.
LDAP (Protocolo Ligero de Acceso a Directorios)	Aloja cuentas de usuario, las políticas, los permisos, atributos y autenticaciones de usuario.	3 minutos	Hacer la copia en caliente de la partición donde reside el OS y los demás volúmenes donde reside los archivos de datos de Active Directory.
Certificado de Autenticación AlphaSSL CA	Verificación de credenciales (matricula y password) para acceder a los recursos.	5 minutos	Tener sistema emergente de autenticación.
Firewall	Cifrado y protección de información y equipos informáticos.	5 minutos	Tener sistema emergente de corta fuegos.

6.4.3

Respaldo y recuperación para sitios y equipos

esenciales

Los imprevistos pueden dañar los equipos vitales que mantienen la continuidad de los sistemas. El plan de back-up y las estrategias de recuperación se han realizado acorde con los requerimientos necesarios.

En las siguientes tablas se establecerán los costos estimados por equipo por unidad en dólares, se recomienda que el lugar alternativo para el *data center* sea uno de los campus de la Universidad APEC, ya sea el Fernando Arturo Meriño (Campus II) o el Miñeta Roque (Campus III), se estableció el respaldo y recuperación para servicios al cliente.

6.4.3.1 Sitios

Nombre del sitio	Back-up acordado y estrategia de recuperación	Costo estimado ¹⁵
Racks	Tener Racks emergentes. Para recuperación, es necesario adquirir un nuevo rack o repararlo según el daño recibido	\$ 274.99
Gabinete	Tener Gabinetes emergentes. Para recuperación, es necesario adquirir un nuevo gabinete o repararlo según el daño recibido	\$ 759.47
SSD SAN Storage ¹⁶	Tener Caja de disco duro SAN emergentes. Para recuperación, es necesario adquirir uno nuevo o repararlo según el daño recibido	\$ 2,789.99
Patch Panel	Tener Path Panel emergentes. Para recuperación, es necesario adquirir uno nuevo o repararlo según el daño recibido	\$ 45.99

6.4.3.2 Equipos esenciales

Nombre del equipo	Back-up acordado y estrategia de recuperación	Costo estimado ¹²
Servidores Virtuales	Tener un Servidor Virtualizado Emergente. Para recuperación es necesario adquirir un nuevo servidor o repararlo según el daño.	GRATIS
Routers	Tener un Router Emergente. Para recuperación es necesario adquirir un nuevo Router o repararlo según el daño.	\$ 951.99

¹⁵ Costo estimado en dólares americanos (US\$).

¹⁶ SSD SAN Storage (Solid State Drive SAN Storage): almacenamiento no volátil basado en la memoria flash. Este tipo de almacenamiento se utiliza en las unidades de estado sólido. (Rouse, WhatIs.com, 2015)

Nombre del equipo	Back-up acordado y estrategia de recuperación	Costo estimado ¹²
Switches	Tener un <i>Switch</i> Emergente. Para recuperación es necesario adquirir un nuevo <i>Switch</i> o repararlo según el daño.	\$ 807.60
UPS	Tener un UPS emergente. Para recuperación es necesario adquirir un nuevo UPS o repararlo según el daño.	\$ 1,864.00
Fortigate	Tener un <i>Firewall</i> emergente. Para recuperación es necesario activar un nuevo <i>Firewall</i> o repararlo según el daño.	\$ 1,129.00
Wireless Access point	Tener un Wireless Access point emergente. Para recuperación es necesario adquirir un nuevo Wireless Access point o repararlo según el daño.	\$ 427.98
Discos de Almacenamiento	Tener un Servicio de Nube Emergente. Para recuperación es necesario adquirir un nuevo Disco de Almacenamiento tipo SAN o vía Nube.	\$ 209.99

6.4.4 Respaldo y recuperación para servicios al cliente

Es imprescindible que los servicios de la plataforma EVA tengan una disponibilidad mínima de por lo menos un 97% durante los períodos de clases, los impactos potenciales de una interrupción pueden variar dependiendo el servicio no esté disponible en el momento.

En la siguiente tabla se muestran las actividades de la plataforma, back-up acordado y el potencial impacto en caso de una interrupción.

Actividades de servicio al cliente	Back-up acordado y estrategia de recuperación	Potencial impacto de una interrupción previa
Chat / Mensajería	Almacenar datos en un banco de información para posteriormente ser gestionados.	Suspensión de los servicios de chat / mensajería. Impacto: Crítico.
Documentos	Almacenar datos en un banco de información para posteriormente ser gestionados.	Suspensión de los servicios. Impacto: Devastador.
Exámenes online	Almacenar datos en un banco de información para posteriormente ser gestionados.	Suspensión de los servicios. Impacto: Devastador.
Interfaz para solicitar servicios	Hacer un back-up completo.	Suspensión de los servicios. Impacto: Crítico.
Agenda académica (Calendario)	Almacenar datos en un banco de información para posteriormente ser gestionados.	Suspensión de los servicios. Impacto: Crítico.

Actividades de servicio al cliente	Back-up acordado y estrategia de recuperación	Potencial impacto de una interrupción previa
Soporte en línea	Realizar un back-up diferencial.	Suspensión de los servicios. Impacto: Devastador.
Manuales y tutoriales	Almacenar datos en un banco de información para posteriormente ser gestionados.	Suspensión de los servicios. Impacto: Crítico.
Filtro (búsqueda) de cursos	Realizar un back-up espejo.	Suspensión de los servicios. Impacto: Controlable.
Noticias	Almacenar datos en un banco de información para posteriormente ser gestionados.	Suspensión de los servicios. Impacto: Controlable.
Perfil del estudiante	Realizar un back-up completo.	Suspensión de los servicios. Impacto: Controlable.
Enlaces para ingresar a otras plataformas relacionadas	Realizar un back-up completo.	Suspensión de los servicios. Impacto: Devastador.
Calificaciones	Realizar un back-up completo.	Suspensión de los servicios. Impacto: Crítico.
Participantes (Compañeros de curso)	Realizar un back-up completo.	Suspensión de los servicios. Impacto: Controlable.

6.4.5 Respaldo y recuperación para información y

documentación

Es indispensable reconocer la dependencia de la información que la plataforma EVA tiene y desarrollar estrategias de acuerdo a los requisitos que las partes críticas ameritan.

Nombre del documento, datos o información	Sistema o localización donde se mantiene normalmente	Interrupción potencial	Impacto potencial	Método de back-up y recuperación
Mdb_Quiz	Base de datos	4	2	Tumbar el servicio y copiar los data files.
Moodle_data	Base de datos	4	1	Tumbar el servicio y copiar los data files.
Chat / Mensajería	Base de datos	4	3	Tumbar el servicio y copiar los data files.

Nombre del documento, datos o información	Sistema o localización donde se mantiene normalmente	Interrupción potencial	Impacto potencial	Método de back-up y recuperación
Foros	Base de datos	4	4	Tumbar el servicio y copiar los data files.
Datos cuentas de usuario	Base de datos externa (Profesores / Estudiantes)	5	1	Tumbar el servicio y copiar los data files.

6.4.6 Cubrimiento de seguros

Una estrategia imprescindible a tener lista es mantener vigente seguros que cubran los accidentes donde los equipos puedan terminar siendo "pérdidas totales".

Póliza	Tipo de cubrimiento	Periodo de cobertura	Cantidad del cubrimiento	Persona responsable por mantener la póliza	Próxima fecha de renovación
MAPFRE BHD	Seguros Equipos Electrónicos	1 año	Básico / Adicional	Encargado de Control de Calidad	Anual
CISCO	Seguros Dispositivos de Redes	1 año	Avanzado	Encargado de Control de Calidad	Anual
Fortinet	<i>Firewall</i>	1 año	<i>Hardware y iOS</i>	Encargado de Control de Calidad	Anual
Microsoft	Sistemas Operativos	1 año	Full	Encargado de Control de Calidad	Anual
Oracle	Gestor de Datos	1 año	Full	Encargado de Control de Calidad	Anual
MAPFRE BHD	Seguros Equipos Electrónicos	1 año	Básico / Adicional	Encargado de Control de Calidad	Anual
CLARO Dominicana	Convertor, modem y servicios de Internet	1 año	Full	Encargado de Control de Calidad	Anual

6.5 Personal y proveedores claves

Los empleados son los activos más importantes. Durante una emergencia la universidad debe confiar en su personal, que será capaz de recuperar el sistema y volver todo a la normalidad lo antes posible.

6.5.1 Organigrama funcional

Nombre ¹⁷	Cargo	Departamento o unidad
Paula Rosario	Gerente del departamento de IT	Unidad administrativa
Aldo Mejía	Encargado de desarrollo de Software	Unidad operativa de desarrollo
Joham Sem	Analista y diseñador de sistemas	
Eulises Mesa	Desarrollador SENIOR	
Vantroy / Víctor Pérez	Desarrollador JUNIOR	
Chris Rodríguez	Diseñador / Programador Web	
Gabriel Tolentino	Encargado de Redes y Comunicaciones	Unidad operativa de <i>Hardware</i>
Aníbal Olivo	Técnico de redes	
Arturo Silva	Administrador de seguridad	
Elvin Víctor	Auxiliar de soporte técnico	
Pogen Fung	Auxiliar de soporte técnico en sitio	
Elvis Garrido	Encargado de Administración de Servidores	Unidad operativa del <i>Data center</i>
Leorge A.	Administrador de Base de Datos	
Juan P. / Pedro	Auxiliar Administrador de Servidores	
Alfredo Jiménez	Analista de base de datos	Unidad operativa del <i>Data center</i>
Víctor Reyes	Encargado Control de Calidad	
José Cuevas	Auxiliar de Infraestructura	
Nehemías Herrera	Auxiliar de Logística	

¹⁷ Los nombres proporcionados en este documento son modelos para mantener la confidencialidad.

6.5.2

Coordinador y delegado para cada área funcional

Cada unidad debe de tener un coordinador y un coordinador delegado del proyecto, este personal es el responsable de mantener el vínculo con el equipo de trabajo del Plan de Continuidad del Negocio.

Área funcional	Coordinador		Coordinador delegado	
	Nombre	Posición	Nombre	Posición
Unidad Operativa de desarrollo	Aldo Mejía	Encargado de desarrollo de <i>Software</i>	Eulises Mesa	Desarrollador SENIOR
Unidad Operativa de <i>Hardware</i>	Joham Sem	Analista y Diseñador de Sistemas	Chris Rodríguez	Diseñador Web
	Gabriel Tolentino	Encargado de Redes y Comunicaciones	Aníbal Olivo	Técnico de redes
Unidad Operativa del <i>Data center</i>	Elvis Garrido	Encargado Administración de Servidores	Juan P. / Pedro M.	Auxiliar administrador de servidores
	Leorge A.	Administrador de Bases de datos	Alfredo Jiménez	Analista de bases de datos
	Víctor Reyes	Encargado Control de Calidad	Nehemías Herrera	Auxiliar de Logística

6.5.3

Personal clave e información de contactos de emergencia

Posición	Área funcional	Procedimiento o sistema por el que son responsables	Detalle de contactos normales
Encargado de desarrollo de <i>Software</i>	Unidad operativa de desarrollo	Entrenar a los otros desarrolladores, y ayudarles a resolver los problemas que puedan enfrentar. Además, asegurarse de que la ejecución sigue de cerca al diseño planteado, y no se dé lugar a lo que se denomina "invasión de características" durante el desarrollo.	809-222-0020

Posición	Área funcional	Procedimiento o sistema por el que son responsables	Detalle de contactos normales
Analista y diseñador de sistemas		Planificar y organizar todos los elementos que intervienen en el proyecto. Controlar el trabajo del equipo de diseño. Escoger y utilizar los métodos, técnicas y herramientas más adecuadas para el desarrollo del trabajo colectivo. Diseñar el nuevo sistema. Representar algorítmicamente los procesos que se realizan en cada tarea funcional.	809-222-0021
Encargado de Redes y Comunicaciones	Unidad operativa de Hardware	Conexión interna y externa.	809-222-0040
Administrador de seguridad		El <i>firewall</i> y los certificados de encriptación.	809-222-0042
Encargado de Administración de Servidores	Unidad operativa de <i>Data center</i>	Establecer y mantener los sistemas en perfecto funcionamiento.	809-222-0061
Administrador de Base de Datos		Administrar la estructura de la base de datos, el sistema manejador de la misma, la actividad de los datos, establecer el diccionario de datos, asegurar la confiabilidad de la base de datos, confirmar la seguridad de la base de datos.	809-222-0060
Encargado Control de Calidad		Comprobar que la calidad de los servicios esté a la altura necesaria para implantar de manera masiva.	809-222-0062

6.5.4 Proveedores claves e información de contactos de emergencia

Los proveedores de servicios públicos forman parte clave en la transmisión de la información y la disponibilidad de la plataforma. En la siguiente tabla se encuentran los proveedores de servicio primordiales.

6.5.4.1

Proveedores normales

Nombre del proveedor	Productos o servicios claves que provee	Detalle de contacto normal
Claro Dominicana	Internet	809-220-1212
EDESUR	Electricidad	809-683-9393

FASE III: Desarrollo del Plan de Continuidad

6.5.5 Los comités

Se han establecido diferentes tipos de comité para jerarquizar las operaciones, dividiendo las responsabilidades y las tareas a implementar para garantizar una recuperación de la plataforma EVA.

En la siguiente imagen se muestran los comités y su distribución jerárquica.

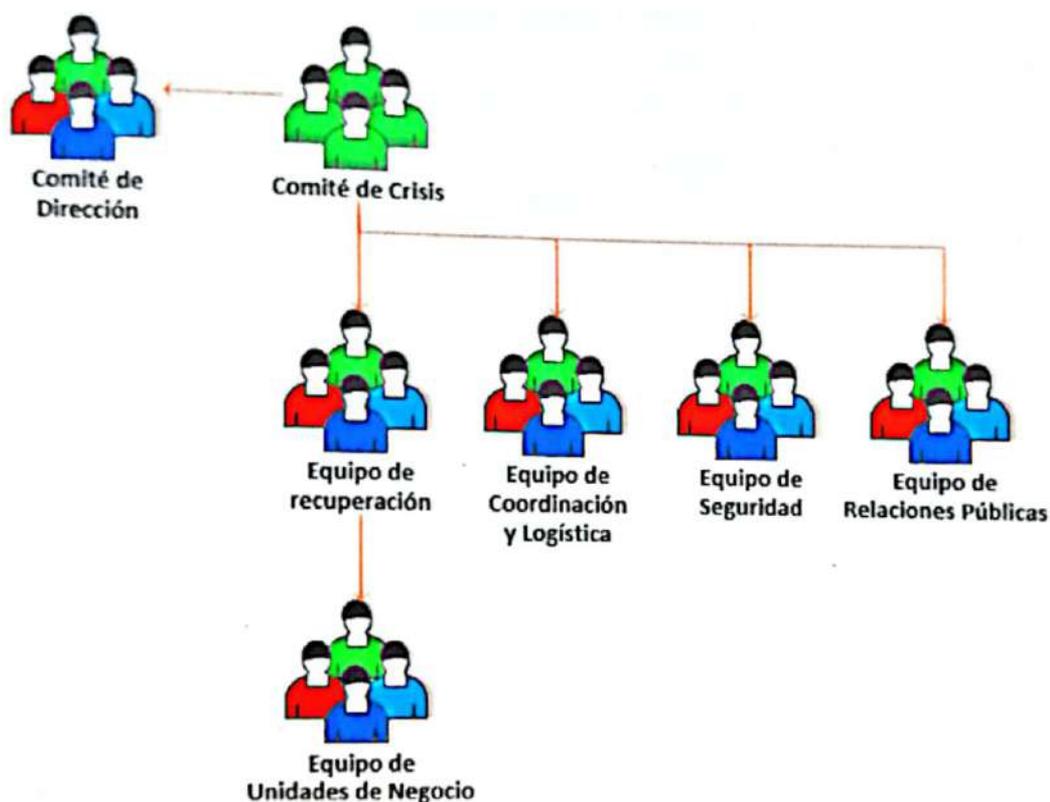


Ilustración 58. Distribución jerárquica de los comités.

Fuente: Imagen propia.

6.5.5.1 Establecer el equipo de recuperación de desastres (DRT)

El equipo de recuperación de desastres (DRT) es responsable de trabajar con los servicios de emergencia para despejar la situación inicial de una crisis. El DRT solo será capaz de iniciar sus propias actividades de recuperación una vez que los servicios de emergencias (Comité de Dirección) han dado el permiso para que estos deberes empiecen. (YourWindow.to, n.d.)

Cargo	Departamento dentro de la organización	Comité al que pertenece
Encargado de Administración de Servidores	Tecnología	Comité de Recuperación
Auxiliar Administrador de Servidores		
Auxiliar Administrador de Servidores		

6.5.5.2 Movilizar el equipo de recuperación del negocio (BRT)

Cargo	Departamento dentro de la organización	Comité al que pertenece
Técnico de Recursos Humanos	Recursos Humanos	Equipo de Unidades de Negocio
Representante	Atención al Cliente	
Encargado Control de Calidad	Tecnología	

6.6 Documentos y procedimientos claves

Todas las entidades cuentan con políticas de seguridad, bitácoras, manuales e instructivos de registros o procedimientos que se llevan a cabo dentro del departamento, siendo considerados parte fundamental de la institución y de cada una de las operaciones que llevan a cabo.

En la siguiente tabla se listan los tipos de documentos o registros que debe de contar el departamento de tecnología de la Universidad APEC.

6.6.1 Documentación y registros vitales para el negocio

Nombre del documento / registro	Breve descripción	Ubicación Mantenido	Persona Responsable	
			Nombre	Contacto No.
Inventario de activos electrónicos	Equipos actuales y futuros para el departamento.	Disco Duro, USB, <i>Cloud</i>	Analista de Base de datos	(809) 222-0065
Políticas de seguridad	Plan para defender los activos del Data Center.	Disco Duro, USB, <i>Cloud</i>	Administrador de Seguridad	(809) 222-0042
Manuales y Guías	Documentos que contienen configuraciones y procedimientos para la instalación y uso de los equipos.	Disco Duro, USB, <i>Cloud</i>	Encargado Control de Calidad	(809) 222-0062

Nombre del documento / registro	Breve descripción	Ubicación Mantenido	Persona Responsable	
			Nombre	Contacto No.
Bitácoras de logs	Directorios para la búsqueda de registros	Disco Duro, USB, <i>Cloud</i>	Administrador de Base de datos	(809) 222-0060
Licencias de sistemas	Convenio entre el licenciante y el licenciario	Disco Duro, USB, <i>Cloud</i>	Administrador de Base de datos	(809) 222-0060
Documentación	Documentos que indican como se encuentran el Data Center	Disco Duro, USB, <i>Cloud</i>	Encargado de Redes y Comunicaciones	(809) 222-0040

6.6.2 Almacenamiento en sitio alterno

El almacenamiento en un sitio alterno resguarda asegura más la información (Off-Site Storage), tener instalaciones de respaldo de *hardware* garantiza los respaldos y los sistemas por un tiempo prudente (no prolongado) para reestablecer el *data center* principal.

Alternativas	Ventajas	Inconvenientes	Empresa
Otro Data Center alojado en una extensión de UNAPEC.	Asegura a la compañía unas instalaciones.	En caso que ocurra una catástrofe en el territorio nacional, ambas extensiones se verán fuertemente afectadas.	UNAPEC
	Disponible durante cualquier desastre.		
	Se pueden hacer pruebas a bajo costos.		
	Están guardados los <i>back-ups</i> de los dispositivos intermediarios (<i>switches</i> , <i>routers</i> , <i>access point</i> , etc.).		
	Solo se requiere personal con experiencia dentro de la compañía.		
Alianza de ayuda mutua.	El almacenamiento de backups en otras empresas mediante el acuerdo de un contrato presenta una solución a bajo coste ante una situación crítica.	Es fiable solo si existe un acuerdo legal.	UNAPEC, Microsoft

Alternativas	Ventajas	Inconvenientes	Empresa
	Soluciona la centralización de equipos y archivos importantes en una misma compañía.	Los archivos importantes y esenciales se encuentran expuestos en la institución o compañía acordada.	
	Refuerza las estrategias de backups de ambas compañías.		
Acuerdos con proveedores de equipos.	Tanto más alto y completo sea el nivel de acuerdo que se solicite más fiable será el servicio proporcionado por el proveedor.	No muchos proveedores se comprometen por escrito abastecer backup lo mejor posible.	DELL, CISCO, Fortinet.
	Los proveedores están obligados atender la necesidad de la universidad las 24 horas y los 7 días de la semana.	El <i>hardware</i> puede cambiar con el tiempo llegando a no ser compatible con algunos dispositivos. Necesidad de garantía en la infraestructura de comunicaciones.	
Empresas de servicios	Es una solución más profesional junto con la anterior.	Necesidad de garantía en caso de una concurrencia.	EDESUR, CLARO Dominicana, Orange.
	Soporte técnico de sus servicios basados en <i>hardware</i> y <i>software</i> .	Necesidad de garantía de seguridad.	
	Disponibilidad inmediata por un tiempo limitado.	Tiempo de proceso limitado	
	Realización de pruebas.	No siempre se consigue la configuración de <i>hardware/software</i> necesario.	
	Solución a la medida y costes conocidas.		

6.6.3 Suministros de oficina

En la situación de que los equipos de oficina sean destruidos, se listan en las siguientes tablas a continuación proveedores para suplir equipos de emergencia y aquellos que pueden entregar los recursos de forma definitiva.

6.6.3.1 Suministros de oficina mantenidos en sitio alterno

Ítem	Nombre Ubicación	Dirección o localización	Contacto No.
Equipos Electrónicos (PC, Laptops, Servidores, UPS)	MAPFRE BHD	Ave. Abraham Lincoln #952 Esq. José A. Soler, Piantini. Distrito Nacional, Rep. Dominicana.	(809) 549-7424
Router, Switches y Access Point	Cisco Rep. Dominicana	Torre Piantini, Piso 5, Local 50A, Ensanche Piantini, Santo Domingo, República Dominicana.	(809) 623-1212
Base de Datos	Oracle "Latinoamérica"	Oracle Caribbean, 250 Muñoz Rivera Avenue - Edificio UBS Suite 300, American International Plaza, Hato Rey, Puerto Rico 00918.	+1 (888) 900-6500
Fortigate (Fortinet)	Multicomputos	Av. Abraham Lincoln 1007, Santo Domingo, República Dominicana.	(809) 540-2846
Sistemas Operativos	Microsoft Dominicana, S.A.	Av. A. Lincoln Edf. Progressus Suite-3a, Distrito Nacional, Santo Domingo, La Española, República Dominicana.	(809) 567-4049
Convertor de medios, modem	CLARO Dominicana	Av. John F. Kennedy #51, Serallés. Frente a Americana Departamentos, Distrito Nacional, Rep. Dominicana.	(809) 220-1212

6.6.3.2 Recursos de oficina que pueden ser ordenados y atendidos al día siguiente de los proveedores normales

Ítem	Nombre del proveedor habitual	Persona Contacto	Contacto No.
Equipos Electrónicos (PC, Laptops, Servidores, UPS)	MAPFRE BHD	Representante de ventas	(809) 549-7424
Router, Switches y Access Point	CISCO	Representante de ventas	+1 (888) 156-1464 Ext. 6214
Base de Datos	Oracle	Representante de ventas	+1 (888) 900-6500
Fortigate	Fortinet	Representante de ventas	809-540-2846
Sistemas Operativos	Microsoft	Representante de ventas	(809) 334-5333
Convertor de medios, modem	CLARO Dominicana	Representante de ventas	(809) 220-1212

6.6.4 Procedimientos de manejo de los medios

El comité de Relaciones Públicas está conformado por el personal capacitado y autorizado para distribuir información y hacer conferencias de prensa.

Posición dentro de la organización	Departamento al que pertenece	Número de contacto	Comité
Representante	Atención al Cliente	809-222-1111	Equipo de Relaciones Públicas
Diseñador Web	Tecnología	809-222-0023	
Técnico Comercial	Relaciones Públicas	809-222-2111	

6.6.5 Procedimientos de autorización en emergencia

Los procedimientos de autorización serán implantados durante una situación de emergencia, cuando se requiera otra autorización diferente a las existentes.

En la siguiente tabla se listan los procesos necesarios y la persona con autorización para gestionar dichas actividades en situaciones normales, pero al momento de la toma de decisión, el responsable es alguien mejor posicionado jerárquicamente.

Nombre del Proceso o actividad	Persona Autorizada en condiciones normales	Persona Autorizada en situaciones de emergencia	
		Cargo	Detalle de contacto
Manejar y gestionar las base de datos del modelo relacional.	Analista de base de datos	Administrador de base de datos	809-222-0060
Almacenar datos en un banco de informaciones para ser posteriormente gestionados.	Analista de base de datos		
Cargar la data de la base de datos	Analista de base de datos		
Cargar los recursos de la página Web.	Auxiliar de Administración de Servidores	Encargado Administración de Servidores	809-222-0061
Autenticación de cuentas de usuario, las políticas, los permisos, atributos y autenticaciones de usuario.	Administrador de Seguridad	Encargado de Redes y Comunicaciones	809-222-0040
Cifrado y protección de información y equipos informáticos.	Administrador de Seguridad		

6.6.6 Presupuesto para back-up y recuperación

Backup o estrategia de recuperación	Costo estimado ¹⁸	¿Costo incluido del proceso en el presupuesto general?
Tener un servidor SQL virtualizado emergente.	\$ 14,256.00	SI
Tener una imagen idéntica a la base de datos actualizada.	€ 4,344.00 ¹⁹	SI
Tener un servidor GNU/Linux Virtualizado emergente.	GRATIS	NO
Tener el acceso de la aplicación web moodle en la memoria de cache.	GRATIS	NO
Tener otro sistema operativo GNU/Linux virtualizado emergente.	GRATIS	NO

¹⁸ Costo estimado en dólares Americanos (US\$).

¹⁹ Costo estimado en Euros (€ \$).

Backup o estrategia de recuperación	Costo estimado ¹⁸	¿Costo incluido del proceso en el presupuesto general?
Hacer la copia en caliente de la partición donde reside el OS y los demás volúmenes donde reside los archivos de datos de Active Directory.	\$ 2,789.99	NO
Tener certificado emergente de seguridad	\$ 366.00	NO
Tener sistema emergente de autenticación.	\$ 120.00	NO
Tener sistema emergente de corta fuegos.	\$ 1,129.00	SI

6.7 Procedimientos de recuperación

Los procedimientos de recuperación necesitan, por lo general, más tiempo para ser puestos en marcha y son a menudo más costosos y complicados de implantar. Por ejemplo, la reconstrucción de los registros perdidos y los ordenadores personales dañados puede llevar días o semanas y requiere mayor dedicación.

Considerando que se debe seleccionar una estrategia de recuperación de negocio que asegure la continuidad de los procesos que hemos considerado críticos en el Análisis de Impacto.

Es particularmente importante tener procedimientos de recuperación que estén cuidadosamente meditados y ensayados para los incidentes más graves, particularmente para los que pueden producir daños físicos y pérdida de información.

6.7.1 Coordinar la preparación del lugar de recuperación

Para coordinar el mejor lugar y establecer la recuperación de los procesos primordiales o totales del EVA, hay que tomar en cuenta ciertas medidas, antes de aplicar las alternativas de respaldo existentes en sitios alternos. Estas medidas son:

1. Informar la situación al Comité de Crisis, donde evaluarán la situación con toda la información detallada del incidente, se decidirá si se activa o no el plan de continuidad de negocio.

2. Planificar el espacio geográfico de trabajo, tomando en cuenta los aspectos críticos del negocio.
3. Establecer la seguridad de los *backups* para realizar el respaldo de los sistemas, sabiendo que los sitios alternos son:
 - a. Un *data center* emergente alojado en una extensión de UNAPEC
4. Poner en marcha al Comité de Recuperación para desarrollar el programa de instalación de equipos y mobiliario dentro del *data center*.
5. Comprobar que el correo electrónico haya sido reestablecido en lugares alternativos.
6. Comprobar la recepción de informaciones importantes para procesos vitales de recuperación. De igual forma, es importante coordinar con los demás departamentos, si es necesario, personal o mobiliarios de los mismos.

6.7.2 Traslado al centro de respaldo

1. Dar a conocer la dirección del *data center* alternativo a los empleados que lo ameriten.

6.7.3 Procedimiento de recuperación del Sistema Operativo

Los sistemas operativos deben de ser recuperados por orden de importancia, priorizando los más críticos.

1. Microsoft SQL Server
2. Debian (MySQL)
3. Red Hat (APACHE)

FASE IV: Pruebas y Mantenimiento

6.8 Pruebas y entrenamiento del plan

La buena documentación de manuales y guías no garantiza que el Plan de Continuidad de Negocios (BCP) será todo un éxito. Los programas de entrenamiento y pruebas periódicas son valiosas para lograr que un BCP logre una recuperación eficaz.

El programa de pruebas y entrenamiento debe constar como mínimo de 3 elementos:

1. Revisiones periódicas
2. Ejercicios de entrenamiento
3. Pruebas técnicas

Anualmente, se deben implementar estos 3 ejercicios para garantizar la viabilidad del plan. Luego de cada ejercicio se deben actualizar los componentes del plan.

6.8.1 Revisiones periódicas

De acuerdo a Gaspar Martínez²⁰, las revisiones deben comprobar los siguientes puntos:

- ¿Siguen siendo válidas las premisas de partida sobre las que se construyó el plan?
- ¿Se han transformado en críticas, funciones de negocio que antes no lo eran?
- ¿Están todavía disponibles los recursos de recuperación, incluyendo las copias de seguridad actualizadas en el almacenamiento externo?
- ¿Son todavía apropiados, en cantidades y umbrales de recuperación, que ahora la haga esencial para la recuperación?
- ¿Ha habido algún cambio en la criticidad de alguna información, que ahora la haga esencial para la recuperación?

²⁰ Doctor Ingeniero Superior de Telecomunicación por la E.T.S.I. de Telecomunicaciones de Madrid. Socio Director de InfoSafe S.L., Ex-Director de la División Synstar Business Continuity de Synstar International en España.

- ¿Son todavía apropiados los umbrales de recuperación de las funciones de negocio identificadas como críticas?

6.8.2 Ejercicios de entrenamiento

Los ejercicios deben realizarse anualmente, de manera parecida a la revisión de operaciones de respuesta y recuperación realizada durante el desarrollo del BCP.

A estas reuniones deben de participar los componentes de cada equipo de recuperación, incluso los equipos alternos. Estas reuniones o sesiones tienen como propósito familiarizarse nuevamente con las estrategias y procedimientos previstos en el plan.

6.8.3 Pruebas técnicas

En el libro "Plan de Continuidad del Negocio" plantea que una buena parte del funcionamiento del plan se basa en el buen funcionamiento de la tecnología. Algunos elementos requieren pruebas reales para asegurarse de que todo funcionará según lo planeado.

Al igual que los 2 elementos anteriores, las pruebas técnicas deben realizarse anualmente para determinados elementos logísticos y lógicos.

Además, Gaspar Martínez lista que las pruebas técnicas deben incluir:

1. Restaurar todos los back-up de PCs y LANs.
2. Conmutar las telecomunicaciones de voz y datos al centro alternativo.
3. Comprobar la idoneidad de los back-ups existentes en el almacenamiento externo y su posibilidad de lectura. Igualmente con toda la información almacenada en otros soportes.
4. Verificar la disponibilidad de los proveedores de recursos críticos.
5. Recuperar los elementos custodiados en el almacenamiento externo utilizando la logística descrita en el plan.
6. Efectuar algunas transacciones y procesos reales utilizando los recursos y registros identificados en el plan.

6.8.3 Mantenimiento

Además del Plan de Continuidad de Negocio, cada unidad del departamento de IT, debe tener su propio plan de Recuperación (sencillo y metódico), donde se presente como establecer su simplemente su área de trabajo de manera rápida y sencilla.

Gaspar Martínez explica que el BCP es válido según la información que contenga. Para asegurarse de que el plan puede ser utilizado con efectividad en una emergencia, debe ser preciso y completo. Debido a esto, tiene que ser revisado y actualizado periódicamente. Cada encargado de equipo es responsable de la identificación de todas las modificaciones y mejoras que puedan ser necesarias para reflejar de forma continua y precisa los procedimientos y responsabilidades de recuperación del negocio de su equipo de recuperación.

Cuando amerite realizar cambios en el BCP, cada unidad a de incorporar los cambios factibles en sus planes correspondientes. Después, cada unidad debe enviar una copia de su modificación al coordinador del BCP.

De acuerdo al libro "Plan de Continuidad del Negocio", el coordinador es responsable de:

- Revisar los cambios propuestos y verificar que se ha recibido la correspondiente aprobación de la Dirección para el cambio propuesto. Si el cambio es de naturaleza técnica, refleja un cambio en la logística de recuperación del negocio, o afecta a diferentes equipos de recuperación, el coordinador del plan debe enviar las revisiones propuestas a todos los equipos afectados para su conocimiento y aprobación, si tal aprobación es necesaria.
- Distribuir las copias necesarias de las secciones actualizadas a todos los equipos afectados.
- Luego de emitir y que el coordinador de cada equipo/unidad recibió los cambios realizados, cada coordinador de unidad debe reemplazar todas las copias de su sección con el plan actualizado.

RECOMENDACIONES

Basado en los avances de la tecnología actual y en la profunda investigación de este trabajo, toda empresa que ofrece servicio con cierta magnitud a un conglomerado, se debe considerar un proveedor de servicios de internet adicional para suplir cualquier eventualidad de conectividad o falla al *Data Center* por parte del ISP contratado. De igual forma, tener una Base de Datos de respaldo en caso de mantenimiento o falla reduce las posibilidades de tener un error de acceso al EVA, haciendo posible la realización de exámenes online en tiempo real y la carga de trabajos digitales al EVA sin interrupción alguna.

Para reducir gastos de mantenimientos a la plataforma EVA, la migración a la nube es una opción que muchas empresas están realizando. Correr la aplicación web Moodle en la nube permite fácil administración para el encargado de sistemas y acceso a todas horas para demás usuarios. La carga de trabajo se vuelve menos pesada al tener el EVA en la nube, pues los proveedores de servicios cuentan con una capacidad bastante amplia en sus servidores y en las transferencias de sus datos al ser una empresa escalable.

Sin el servicio web capaz de presentar la aplicación web Moodle, no tendríamos ninguna opción de interactuar con el EVA. Tener un segundo servidor web es una solución idónea para que los usuarios no se vean afectados por la realización de actividades en el EVA y reservaciones de recursos tecnológicos.

Por último y no menos importante, nuestras recomendaciones están basadas en la correcta realización de un plan de continuidad de negocios (BCP), el cual permite la disponibilidad del servicio de la plataforma y recuperación de tiempos perdidos en servicios y en términos económicos.

CONCLUSIÓN

En la actualidad, la tecnología sigue evolucionando de manera significativa, buscando facilitar el diario vivir y tratando de conservar la seguridad en los procesos claves de las organizaciones. Como observamos, en el ámbito educativo ya existen las herramientas necesarias para tener una formación continua desde cualquier con conectividad a internet. Vimos que la Tecnología de *cloud computing* ha estado en constante evolución y que será la base para las próximas plataformas tecnológicas, debido a que la tendencia de web posee un crecimiento exponencial y la mayoría de los Sistemas de Contenidos de Aprendizaje (LCMS) están migrando a esta tecnología para un mayor desempeño en el servicio a los usuarios.

Todos los recursos tecnológicos se encuentran en el *data center*, el cual constituye la matriz de los sistemas de la empresa, por esta razón se debe definir un nivel de TIER para el centro de datos, que permita la continuidad de los sistemas informáticos operando ininterrumpidamente.

La seguridad de la tecnología en las nubes juega un papel importante para este tipo de plataforma debido a que evitar amenazas y riesgos que pueda incurrir en los sistemas.

Actualmente, existen alrededor de 3 mil millones de usuarios activos en Internet donde el 53% de los usuarios usarán los servicios de la computación en la nube para el 2018, de acuerdo a datos revelados por la compañía de telecomunicaciones, CISCO.

Para las empresas y los proveedores de servicios, estos indicadores representan un activo importante y útil, pues las informaciones de los usuarios viajarán a través de una red pública que está abierta a nuevos ataques constantemente. Por ende, el estándar ISO / IEC 27018 está orientado para mantener la seguridad en la nube, definiendo los controles principales que permiten proteger la privacidad, rige las

directrices fundamentales y los objetivos de control para la protección de la información de identificación personal (PII).

La aplicación web Moodle es un sistema LCMS capaz de crear actividades y asignaciones para el estudiantado, desde la realización de trabajos digitales hasta la creación y evaluación de exámenes virtuales. Moodle se encuentra instalada en la gran mayoría de las universidades del país, siendo la plataforma de aprendizaje preferida por la mayoría de las instituciones académicas.

El departamento de TI de UNAPEC cuenta con altos niveles de tecnologías en su infraestructura física y virtual, donde la conectividad *data center*, el cual está protegido con cables de fibra óptica. La plataforma EVA está protegida por KERBEROS y TLS, además de certificados de seguridad como AlphaSSL para la encriptación hacia el exterior y un *firewall* Fortinet para el filtrado de conexiones entrantes y salientes. La base de datos está orientada por el gestor MySQL para la creación de usuarios de la plataforma EVA. El centro de datos tiene una alta redundancia de sistemas eléctricos.

La elaboración de un plan de continuidad de negocios conlleva al análisis, preparación, documentación y recolección de informaciones sobre el tiempo y el punto de recuperación ante desastres. Este plan debe estar diseñado y orientado para mantener la disponibilidad del sistema durante posibles eventos. Como todo Plan de Continuidad conlleva costos y beneficios, se demostró que son factible y necesarias las mejoras de la implementación del plan para lograr la recuperación de las posibles pérdidas producidas por desastres.

BIBLIOGRAFÍA

Libros:

- Dixit, J., & Yadav, A. (2010). *Electrical Power Quality*. Nueva Delhi: University Science Press.
- Administración y gestión de una red de área local. (s.f.). En A. Abad, *CEO - Redes de área local* (pág. 222). McGraw-Hill.
- Aguilera López, P. (2010). *Seguridad informática*. Editex.
- Arregoces, M., & Portolani, M. (2003). *Data Center Fundamentals*. Indianapolis: Cisco Press.
- Atelin, P., & Dordoigne, J. (2007). *TCP/IP y protocolos de Internet*. Barcelona: ENI.
- Bhuvaneshwari, N., & Sujatha, S. (2011). *Integrating Soa and Web Services*. Dinamarca: River Publishers.
- Blahut, R. (2014). *Cryptography and Secure Communication*. Reino Unido: Cambridge University Press.
- Bobillier, S. (2013). *Linux: Administración del sistema y explotación de los servicios de red* (Segunda Edición ed.). Ediciones ENI.
- Roebuck, K. (2012). *OAuth: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. Emereo Publishing.
- Roebuck, K. (2012). *XBRL (eXtensible Business Reporting Language): High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. Emereo Publishing.
- Schulz, G. (2009). *The Green and Virtual Data Center*. Boca Ratón: CRC Press.
- Torres Viñals, J. (2011). *Ventajas y retos del Cloud Computing*. (L. Rubió, Ed.) Barcelona.

- Whitman, M., & Mattord, H. (2011). *Principles of Information Security*. Boston: Cengage Learning.
- Winkler, V. (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Elsevier
- Curtis, P. (2011). *Maintaining Mission Critical Systems in a 24/7 Environment*. New Jersey: John Wiley & Sons.
- Desongles Corrales, J., & Moya Arribas, M. (2006). *Conocimientos Basicos de Informatica*. Sevilla: MAD.
- Eck, M. (2001). *La Internet: por dentro y por fuera*. New York: Rosen Publishing Group.
- Fernández, M. F. (2008). *Técnicas comunes de Ataque a equipos con sistema operativo Unix o derivados*. Buenos Aires.
- Geng, H. (2014). *Data Center Handbook*. New Jersey and Canadá: John Wiley & Sons.
- Gimian, J., & Boyc, B. (2008). *Las reglas de la victoria: Cómo transformar el caos y el conflicto*. España: Edaf.
- Hashem Sherif, M. (2010). *Handbook of Enterprise Integration*. Boca Ratón, Florida: Auerbach Publications.
- Hausman, K. K., Gunderloy, M., & Tittel, E. (2003). *Developing and Implementing Windows-based Applications with Visual Basic .NET and Visual Studio .NET*. USA: Que Certification.
- Herrera Pérez, E. (2003). *Tecnologías y redes de transmisión de datos*. México: Limusa.
- Hordeski, M. (2005). *Emergency and Backup Power Sources: Preparing for Blackouts and Brownouts*. Estados Unidos de América: The Fairmont Press, Inc.

- Javvin Technologies Inc. (2005). *Network Protocols Handbook* (Segunda Edición ed.). California.
- Menken, I. (2014). *Cloud Computing: Software as a Service (SaaS)*. Emereo Publishing.
- Pérez, M. (2009). *Windows Server 2008: instalación, configuración y administración*. RC Libros.
- Dix, P. (2011). *Service-Oriented Design with Ruby and Rails*. Massachusetts: Pearson Education, Inc.
- Instituto Tecnológico Metalmecánico (AIMME). (2012). *Análisis de la oferta y la demanda de los servicios Cloud Computing*. Valencia.
- Morimoto, R., Noel, M., Droubi, O., Mistry, R., & Amaris, C. (2010). *Windows Server 2008 R2*. Indiana: Pearson Education, Inc.
- Noel, M. (2007). *Microsoft ISA Server 2006*. Estados Unidos de América: SAMS.
- Reis, D. (2013). *Seguridad para la nube y virtualización para DUMMIES*. Trend Micro by John Wiley & Sons, Inc.
- Tanenbaum, A. (s.f.). *Redes de computadoras* (Tercera Edición ed.). México: Pearson.
- Pitt Turner IV, W., Seader, J., Renaud, V., & Bill, K. (2008). *TIER Classifications Define Site Infrastructure Performance*. Santa Fe: Uptime Institute.

Artículos:

- Council, C. S. (s.f.). Security for Cloud Computing 10 Steps to Ensure Success. *Cloud Standards Customer Council*, 5-7.

Reportes:

- Comisión Federal de Mejora Regulatoria. (2014). *Parámetros de Autorregulación en Materia de Protección de Datos Personales*. Distrito Federal: Secretaría de Economía. Obtenido de

http://207.248.177.30/mir/formatos/MIR_ImpactoModeradoViewAIC.aspx?SubmitID=408291

Fundación de la Innovación Bankinter. (2010). *Cloud Computing. La tercera ola de las Tecnologías.*

Ipsos. (2013). *Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General.* Distrito Federal: Ipsos Public Affairs. Obtenido de <http://inicio.ifai.org.mx/EncuestaNacionaldeProtecciondeDatosPersonales2012/02ReporteEmpresas.pdf>

Web sites:

Laird, P. (29 de Mayo de 2008). *Blogspot.* Obtenido de Laird Ondemand: <http://peterlaird.blogspot.com/2008/05/saas-soup-navigating-a-service-acronyms.html>

Cruz, E. (15 de Agosto de 2014). *IHS Technology.* Obtenido de <https://technology.ihs.com/508877/ihs-finds-infrastructure-as-a-service-market-to-have-surpassed-4-billion-in-revenues-in-2013>

Cruz, E. (7 de Octubre de 2014). *IHS Technology.* Obtenido de IHS Technology. Information, analytics, expertise: <https://technology.ihs.com/512609/the-data-centers-of-infrastructure-as-a-service-iaas-providers>

Fabian, F. (7 de Octubre de 2008). *Wordpress.* Obtenido de <https://ffabian.files.wordpress.com/2008/10/dibujo14.jpg>

IBM. (29 de Julio de 2009). Obtenido de IBM developerWorks: http://www.ibm.com/developerworks/websphere/downloads/xs_rest_service.html

ITU: Committed to connecting the world. (Octubre de 2012). *Sector de Normalización de las Telecomunicaciones de la UIT.* Obtenido de <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509>

Martinez de Lahidalga, I. R. (29 de Julio de 2008). *Moodle, la plataforma para la enseñanza y organización escolar*. Obtenido de Universidad del País Vasco: http://www.ehu.eus/ikastorratza/2_alea/moodle.pdf

ORACLE. (Junio de 2012). ORACLE. Obtenido de ONC+ Developer's Guide: http://docs.oracle.com/cd/E23824_01/html/821-1671/rpcintro-47601.html

Passeri, P. (21 de Junio de 2012). *HACKMAGEDDON*. Obtenido de <http://www.hackmageddon.com>

Salinas, M. I. (4 de Julio de 2011). *Entornos virtuales de aprendizaje en la escuela: tipos, modelo didáctico y rol del docente*. Obtenido de Pontificia Universidad Católica Argentina: http://www.uca.edu.ar/uca/common/grupo82/files/educacion-EVA-en-la-escuela_web-Depto.pdf

TREND MICRO. (s.f.). *Seguridad cibernética: protección frente a los ciberataques*. Obtenido de TREND MICRO: <http://www.trendmicro.es/tecnologia-innovacion/seguridad-cibernetica/>

International Organization for Standardization. (8 de Mayo de 2015).

Obtenido de: <http://www.iso.org/iso/home.html>

Conferencias:

Musser, J. (2011). Open APIs: State of the Market. *Glue Conference 2011* (pág. 12). Glue Conferenc. Obtenido de <http://www.slideshare.net/jmusser/open-apis-state-of-the-market-2011>

STAMFORD. (19 de Noviembre de 2012). *Gartner*. Obtenido de <http://www.gartner.com/newsroom/id/2242415>

ANEXOS

Anexos, Capítulo I.

**Anteproyecto de trabajo de grado para optar por el título:
Ingeniero en Sistemas**

Anexos, Capítulo III.



UNAPPEC
UNIVERSIDAD APEC

Decanato de Ingenierías e Informática

Escuela de Informática

Tema:

Elaboración de un plan de continuidad de negocios para la disponibilidad en la plataforma web Moodle de la Universidad APEC, Santo Domingo, R. D., 2015.

Sustentantes:

Paula Rosario Ventura	2010 – 1724
Gabriel Antonio Tolentino Rosario	2011 – 0264
Leorge Artajerjes Jiménez Peralta	2009 – 2054

Asesor:

Ing. Santo Rafael Navarro

Anteproyecto de trabajo de grado para optar por el Título de:

Ingeniero en Sistemas

Distrito Nacional, República Dominicana

INDICE

INTRODUCCIÓN.....	5
JUSTIFICACIÓN.....	6
DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA.....	8
OBJETIVOS DE LA INVESTIGACION.....	11
CAPITULO I. MARCO TEÓRICO REFERENCIAL.....	12
1.1 Marco referencial.....	13
1.2 Marco conceptual.....	16
1.3 <i>Cloud Computing</i>	19
1.4 Componentes de la Nube.....	22
1.4.1 Clientes - Usuarios.....	22
1.4.2 Servicios de distribución.....	23
1.4.3 Centro de datos.....	24
1.5 Empresas y Servicios.....	24
1.5.1 <i>Software</i> como un servicio (SaaS).....	27
1.5.2 Plataforma como un servicio (PaaS).....	28
1.5.3 Infraestructura como un servicio (IaaS).....	29
1.5.4 <i>Hardware</i> como un servicio (HaaS).....	30
1.6 Compañía de servicio.....	32
1.7 Aspectos legales.....	33
1.7.1 Leyes.....	38
1.8 Plan de Continuidad de Negocios (BCP).....	38
1.8.1 Plan de contingencia.....	39
1.8.2 Diferencias y Estándares.....	40
1.8.3 Diseño y desarrollo del Plan de Continuidad de Negocios.....	44
CAPITULO II. ASPECTOS METODOLÓGICOS.....	47
2.1 Tipo de investigación.....	48
2.1.1 Descriptivo.....	48
2.1.2 Explicativo.....	49

2.2 Métodos de investigación.....	49
BIBLIOGRAFIA.....	51

INDICE DE ILUSTRACIONES

Ilustración 2. Definición y componentes básicos de Cloud Computing. _____	21
Ilustración 3. Evolución de las arquitecturas de cálculo. _____	21
Ilustración 4. Distribución de Carga 2010 – 2015 _____	27
Ilustración 5. Modelos de servicios incorporados en la nube. _____	32
Ilustración 6. La nube tráfico del centro de datos se representan más de un tercio del total del tráfico del centro de datos para el año 2015 _____	33
Ilustración 7. Trilogía relacional entre proveedores, clientes y contratistas (terceros) entre los aspectos legales del Cloud Computing. _____	37
Ilustración 8. Fases indispensables para la elaboración del BCP. _____	40
Ilustración 9. Ciclo operacional del Plan de Continuidad de Negocios y sus procesos. _____	46

Elaboración de un plan de continuidad de negocios para la disponibilidad en la plataforma web Moodle de la Universidad APEC, Santo Domingo, R. D., 2015.

INTRODUCCIÓN

Durante la investigación se persigue ofrecer las recomendaciones para incorporar mejoras técnicas en los procesos existentes en el Entorno Virtual de Aprendizaje (EVA) de la Universidad APEC, con la finalidad de crear un mejor tiempo de ejecución en los procesos, así como explicar los beneficios de la computación en la nube (*Cloud Computing*), garantizando la continuidad de sus operaciones basado en un Plan de Continuidad de Negocios (BCP) y de los servicios que ofrece, tanto a los estudiantes como a los docentes.

La computación en la nube es un sistema basado en plataformas virtuales por medio del internet y de centros de datos remotos, la cual comprometen la integración de diversos servicios para su correcto funcionamiento. La seguridad de la información y el sistema de continuidad de negocios desempeñan un papel importante al momento de evaluar cualquier proveedor.

Existen factores críticos que son evaluados por las empresas antes de contratar estos servicios, lo primordial es la disponibilidad de los sistemas y la integridad de la información ante cualquier evento o catástrofe.

Los acuerdos de cada nivel de servicios, el dominio y la gestión de la información, las regulaciones y el cumplimiento de políticas, son temas a discutir durante el proceso de la evaluación del contrato de servicios en la nube (*Cloud Computing*).

Bajo este mismo esquema se creará un Plan de Continuidad de Negocios (BCP) que le permitirá al Departamento de Tecnología de la Universidad APEC responder ante cualquier falla, mantenimiento o desastre basado en las mejores

prácticas y normas de la institución. Esto incrementará la capacidad de acceso a los servicios y documentos que ya tiene incluido el Entorno Virtual de Aprendizaje (EVA).

Los planes de recuperación y el análisis de impacto son elementos a tomar en cuenta, al momento de realizar una implementación de continuidad de negocios integrada con la infraestructura actual de la institución.

JUSTIFICACIÓN

La plataforma web Moodle se encuentra en ejecución en varias universidades dominicanas, como son: INTEC, PUCMM, UASD, UNPHU, APEC, y sus características de ser un *software* libre y gratuito ha sido de gran ventaja para estas instituciones.

La aplicación Moodle ha estado activa desde el año 2002, y hasta el día de hoy, con más de 5 versiones realizadas de manera estable, la aplicación sigue siendo de gran utilidad para millones usuarios con materias virtuales en universidades, a causa de sus módulos que presenta un amplio beneficio dinámico de aprendizaje.

La disponibilidad en el acceso a la información va a ser siempre un condicionante para su uso y la creación de un plan de contingencia (para la recuperación y continuidad de la empresa frente a fallas o catástrofes) seguirá siendo una práctica infalible para la satisfacción del usuario en el servicio de la aplicación web Moodle.

Sin embargo, estas condiciones no se ponen de manifiesto por la falta de un plan de continuidad de negocios, trayendo consigo grandes problemas en la disponibilidad de la plataforma EVA. Según el libro "*La calidad en el servicio al cliente*" (Editorial Vértice), se define el nivel de excelencia de un servicio de la siguiente manera: Un servicio alcanza su nivel de excelencia cuando satisface las necesidades o la demanda de un grupo que ha sido seleccionado previamente. El nivel de excelencia de la plataforma EVA, no califica para ingresar entre los altos estándares de servicios, debido a que el 80 % de la población estudiantil, presentan inconvenientes con la plataforma EVA al momento de realizar un mantenimiento de ella, y es un problema tan importante a tomar en cuenta, ya que degradan la disponibilidad a un nivel por debajo de lo que la aplicación web Moodle puede ofrecer.

Otro aspecto a tener en cuenta es el inconveniente de la plataforma web Moodle al momento de tomar exámenes virtuales. Recordamos que cuando existen por lo menos 3 secciones de clases simultáneas tomando examen virtual, toda la red se torna lenta conjuntamente con el servicio, debido a que el tráfico de datos es mayor que la demanda que dicha aplicación puede manejar, provocando un cambio de fecha para los exámenes y una publicación de los exámenes fuera del calendario académico.

DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA

El sistema educativo internacional ha evolucionado enormemente, se ha desarrollado una enseñanza sin fronteras. Hoy en día existen plataformas tecnológicas conocidas como Sistema de Gestión de Contenido de Aprendizaje (LCMS) que permiten la capacitación y certificación a distancia. Moodle es una de las plataformas más utilizadas en todo el mundo, traducida a 86 idiomas, con más de 67,000 sitios registrados que brindan más de 5.5 millones de cursos, en los que participan más de 54 millones de usuarios entre estudiantes y docentes. Estas nuevas tecnologías han revolucionado la República Dominicana, provocando que el Plan Decenal del Ministerio de Educación Superior, Ciencia y Tecnología (MESCyT), (2008-2018), se establezca el uso de las tecnologías de la información y la comunicación (TIC), como lo exige la nueva sociedad del conocimiento. Sin embargo, en el Distrito Nacional todas las universidades cuentan con una plataforma de Sistema de Gestión de Contenido de Aprendizaje (LCMS).

En el caso de la Universidad APEC, han implantado un Entorno Virtual de Aprendizaje (EVA), esta tiene como base la aplicación web en PHP "opensource", "Moodle". La misma se utiliza para producir cursos modulares basados en Internet que admiten una pedagogía del construccionismo social moderna, permitiendo al docente llevar a cabo clases virtuales, colocar asignaciones, entre otras herramientas interactivas para un aprendizaje sin fronteras. La universidad está presentando inconvenientes con la disponibilidad en los servicios cuando el tráfico está en su máxima capacidad. Actualmente, el Plan de Continuidad de Negocios

no está implementado en el Entorno Virtual de Aprendizaje (EVA) de la Universidad APEC, pero este sistema podría ayudar al mejoramiento de la plataforma facilitando la administración del sistema, reduciendo los gastos de inversión y mantenimiento del espacio físico.

Los archivos que se suben al EVA son guardados en una caja de Red de Área de Almacenamiento (SAN), se almacenan alrededor de setenta a cien gigabytes por cuatrimestre y se realiza una copia de los datos para sacar la información del sistema. Actualmente, UNAPEC cuenta con 8,202 estudiantes, una universidad con una población estudiantil muy numerosa y que cada cuatrimestre incrementa significativamente. La plataforma EVA no tiene ninguna función de ofrecer almacenamiento, debido a que su principio de creación es la interacción docente-estudiante sin límites. Sin embargo, esto podría ser un desperfecto para aquellas mentes que solamente se mantienen en la función de lo que realiza una aplicación y puede que no vean una nueva funcionalidad para mejorar la plataforma. La aplicación web "Moodle" es adaptable y permite evolucionar, continuar mejorando su desempeño debido a la facilidad que brinda el "opensource", la plataforma EVA ha sido adaptada a las necesidades de la universidad APEC, ¿no se ha vuelto una necesidad mantener los recursos bibliográficos del estudiante?

Al menos un 80 % los de estudiantes por carrera han tenido problemas con la plataforma EVA, con quejas por fallas de accesibilidad durante la semana de parciales. Esta cifra es alarmante, debido a que la Universidad APEC cuenta actualmente con 16 carreras en donde 5 de cada 6 estudiantes se han visto con

dificultades técnicas, es decir, que aproximadamente un 80 % de la población estudiantil de la universidad, ha presentado continuamente tienen problemas con la plataforma, y el porcentaje incrementa cada vez más a causa del auge que ha tenido EVA en los últimos 3 cuatrimestres.

Entre los diversos fallos podemos especificar el acceso al EVA durante el mantenimiento a la base de datos. Es una falla grave debido a que los estudiantes necesitan la plataforma disponible en un 98% aproximadamente, para la realización de sus asignaciones o tomar exámenes. El problema se vuelve aún más crítico cuando se presenta en el tiempo pico (alto tráfico de usuarios), en semana de parciales.

Si este tipo de problema continúa presentándose sin ser transparente para el usuario, el EVA no sería un entorno virtual de aprendizaje eficaz, capaz de brindar buenos servicios. La plataforma no cuenta con un plan de continuidad de negocios sobre este fallo, de acuerdo a lo expresado por el Ing. Ricardo Pérez, Encargado del departamento de Infraestructura. No obstante, cuando están haciendo un mantenimiento a la aplicación Moodle, las materias del estudiante y del docente no se visualizan cuando estos acceden al EVA y por ende, han tenido que trasladarse hasta UNAPEC a reportar el problema de inconformidad con el servicio. Para un profesor, que maneja grandes cantidades de materias, no poder encontrar a tiempo la materia en su entorno virtual para la asignación de una tarea o habilitar un examen, se traduce en pérdidas de tiempo y que a su vez genera pérdidas monetarias.

OBJETIVOS DE LA INVESTIGACION

Objetivo general

Elaborar un plan de contingencia operativa para la recuperación y continuidad de los servicios de la plataforma EVA, mediante el mejoramiento a la accesibilidad de Moodle de la Universidad APEC.

Objetivos específicos

1. Optimizar la disponibilidad de la plataforma EVA de UNAPEC.
2. Crear un plan de contingencia operativa que permita la recuperación y continuidad de la empresa frente a fallas y/o desastres basada en un estándar de recuperación de desastres.
3. Detallar los servicios de la aplicación web Moodle.
4. Identificar los Proveedores de Servicios de Internet (ISP) para el tráfico de red de la Universidad APEC.
5. Definir el sistema del Protocolo Ligero-Simplificado de Acceso a Directorios (LDAP).
6. Cualificar los servicios asociados de los servidores de aplicación.
7. Describir los tipos de base de datos para la producción de la aplicación web Moodle.
8. Identificar la matriz energética del centro de cómputo de la plataforma EVA.
9. Mencionar los sistemas eléctricos emergentes.

CAPITULO I. MARCO TEÓRICO REFERENCIAL

1.1 Marco referencial

Samantha Villareal Torres (2012). Implementación de conferencia web sobre Moodle de la UPIICSA, para el aprendizaje colaborativo. México.

Cabe destacar que en una herramienta eficaz para el aprendizaje y la colaboración, los profesores necesitan saber cómo hacer el mejor uso de sus aulas virtuales. Ruth Colvin Clark (2005), un conocido investigador en el campo de la enseñanza a distancia y multimedia, ha sugerido varias maneras de utilizar las características de estos entornos para apoyar las metas de instrucción en diversos tipos de cursos.

Leiva Garzón Ana Lucía (2008). Desarrollo del plan de continuidad de negocio para el departamento de TI de una empresa farmacéutica.

Se recomienda al mantener el Plan de Continuidad actualizado mediante revisiones cada 6 meses y simulacros anuales, con el fin de mantener vigentes todas sus actividades. Además, utilizar los equipos de recuperación en otros procesos que no sean críticos, cuando no se los utilice en casos de desastre y se recomienda que se utilice una herramienta que ayude a obtener imágenes de servidores como respaldo en caso de que ocurra un desastre.

Tacury Calderón Karla García y Vivar Naula Sara Azucena (2008). Implementación de un plan de continuidad del negocio para el área financiera-tributaria a una empresa industrial dedicada a la producción, comercialización y exportación de madera de balsa. Guayaquil.

Es recomendable que se realice frecuentemente un Análisis de Riesgos del Negocio (BIA) en todas sus áreas, con el objetivo de mantenerse siempre alerta

ante cualquier circunstancia e implementar un Plan de Continuidad de Negocio como medida para estos casos.

Tener en consideración la estrategia que nos brinda el BIA, aunque la contingencia ya se presentó, permanecen con el proceso de impugnación ante el SRI, lo cual involucra a la empresa en una serie de auditorías por partes del ente regulador.

Armando Sandoval Maravilla (2013). Implementación de plataforma educativa Moodle en escuela preparatoria Adolfo Chávez. Michoacán. Editorial: Apatzingan.

En la proyección de la plataforma se requiere claramente de un web master que es la persona encargada de administrar la página y forma la estructuración, desempeño de las actividades a realizar para cada maestro y es que da los roles de los mismos cursos es por ello importante la contratación de un ing. En sistemas o similar. Con la implementación de la plataforma hay cambios tanto educativos como institucionales es por eso que la dirección de la escuela tiene que dar seguimiento a los cursos que estén virtualizados y los maestros tomen el curso correspondiente para el manejo de la plataforma estén al 100% en la proyección de la materia virtual porque es un paso importante entre el alumno y el profesor donde se asignen a las actividades en relación con la plataforma Moodle en cual tiene que existir un portal de comunicación contando con las herramientas modernas adecuadas para cada concepto (en materia virtual). La plataforma educativa es sin duda un herramienta hacia el futuro donde podemos construir un

futuro educativo con bajos costos si ir a la ciudad donde se oferta dicho estudio ya sea de nivel medio superior o superior.

Daniel Díaz Sánchez (2008). Contribuciones a protocolos y mecanismos de análisis y decisión para control de acceso en entornos distribuidos. España. Editorial: PeerReviewed.

Dado el gran número de dispositivos existentes en estos entornos y la gran distribución y replicación de los servicios, los dispositivos personales deben asistir al usuario en los procesos de control de acceso distribuido. Esta tesis define los objetivos y un marco de trabajo orientado a mejorar el control de acceso, respetando la autonomía de todos los actores como dispositivos, elementos de red y servicios, permitiendo que, mediante mecanismos de decisión y selección, se pueda negociar de forma flexible el acceso a los servicios y que, utilizando extensiones a protocolos de seguridad, se facilite el acceso a los mismos. Por otro lado, la tesis se enfocará también en hacer la seguridad más usable y eficaz; capaces de comunicar eficazmente a los humanos la información de seguridad, analizando sistemas de comunicación gráfica con el usuario, que permitan a personas sin conocimientos técnicos entender los riesgos de determinadas acciones.

Audie René Juárez Najarro (2011). Plan de Continuidad TI en la biblioteca central de la Universidad de San Carlos de Guatemala. Guatemala.

En la elaboración de la guía análisis y diseño para la implementación y mantenimiento del plan de continuidad de operaciones, se tomaron en cuenta aspectos tecnológicos, capital intelectual y factores externos que representan

vulnerabilidad sobre la continuidad, basados en el análisis de impacto y análisis de riesgo.

Detalles de los aspectos fundamentales a tomar en cuenta para la elaboración de un plan de continuidad de negocios basado en las tecnologías de la información TI de la empresa u institución.

1.2 Marco conceptual

Computación en la nube (*Cloud computing*): Se utiliza para definir a un sistema informático basado en internet que permite gestionar archivos y aplicaciones sin necesidad de instalarlas en la computadora. Debemos tener en cuenta que el término "nube" al que estamos acostumbrados, se usa como una metáfora.¹ En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan." (Gómez Treviño, 2010)

Almacenamiento en la nube: es la extensión y el desarrollo del concepto de la computación en nube. Sistema de Almacenamiento en la nube es un nuevo tipo de estructura del sistema de almacenamiento nublado. Se compone de varios equipamientos de almacenamiento, utilizando los *clusters* de aplicaciones, sistemas de archivos distribuidos o tecnología de red y otras funciones.²

¹ Virginia Caccurri, 2012 *Computación para Docentes*, Argentina, USERHOP.

² Hsiang-Chuan Liu, et al. Wen-Pei Sung & Welin Yao, 2014, *Computer Intelligent Computing and Education*, CRC Press

Seguridad informática: Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.³

Arquitectura de cliente – servidor: Es un modelo de gestión en el que un equipo (servidor) ofrece un servicio a otros equipos (clientes) que lo necesitan. El cliente y el servidor suelen ejecutarse en distintos sistemas informáticos. Normalmente, el servidor se ejecuta en un sistema más potente donde se realiza la mayor parte del procesamiento y el almacenamiento de datos.⁴

Almacenamiento remoto: El almacenamiento se considera remoto cuando el dispositivo donde vamos a almacenar la información no está en el equipo donde estamos trabajando, es decir, no es un almacenamiento local.⁵

Copia de seguridad: Son duplicados de toda información o parte de ella que se desee conservar y almacenar en algún medio independiente del que se encuentran normalmente, ya sea a través de internet, en otro disco duro o en un medio extraíble.⁶

Servidores Web: La primera aplicación cliente – servidor que cubre todo el planeta es el World Wide Web (WWW), este consiste en clientes que mediante un

³ Purificación Aguilera López, 2010, *Seguridad Informática*, Editex.

⁴ Carlos Valdivia Miranda, 2014, *Sistemas Informáticos y redes locales*, España, Ediciones Paraninfo, SA.

⁵ Alfonso García-Cervigón Hurtado y María Pilar Alegre Ramos, 2011, *Seguridad Informática*, España, Ediciones Paraninfo, SA.

⁶ Purificación Aguilera López, 2010, *Seguridad Informática*, Madrid, Ediciones Editex.

navegador se conectan a los servidores web, este servidor devuelve un documento cuando el cliente pregunta por el nombre del mismo.⁷

Servidores de archivos: Permiten la transferencia de ficheros entre un cliente y un servidor. Para la transferencia de archivos se emplea el protocolo FTP (File Transfer Protocol). La comunicación entre cliente y servidor es independiente del sistema de archivos utilizado en cada sistema informático, de manera que no importa que sus sistemas operativos sean distintos.⁸

Plan de continuidad de negocios (BCP): su propósito es proporcionar procedimientos para sustentar las operaciones esenciales de negocios mientras que el sistema se recupera de un trastorno significativo.⁹

Cluster: grupo de sectores adyacentes que son siempre asignados como una unidad.¹⁰

Disponibilidad: la información ha de estar disponible para los usuarios autorizados siempre que la necesiten.¹¹

⁷ Carlos Valdivia Miranda, 2014, *Sistemas Informáticos y redes locales*, España, Ediciones Paraninfo, SA.

⁸ Carlos Valdivia Miranda, 2014, *Sistemas Informáticos y redes locales*, España, Ediciones Paraninfo, SA.

⁹ Javier Areito, 2008, *Seguridad de la Información, Redes, Informáticas y Sistemas de información*, Madrid, Ediciones Paraninfo.

¹⁰ Andrew Schulman, Ralf Brown, David Maxey Raymond J. Michells y Jim Kyle, 2000, *El DOS no documentado*, Ediciones Díaz de Santos.

¹¹ Purificación Aguilera, 2010, *Seguridad informática*, Madrid, Ediciones Editex.

Virtualización: consiste en la creación, a través de software, de una versión virtual de un recurso tecnológico, ya sea hardware o software.¹²

1.3 Cloud Computing

La tecnología de *cloud computing* empieza con los sistemas operativos Unix, que admitieron la configuración de *clústers*. No son más que un conjunto mezclado de computadoras que han sido construidas mediante el uso de un sinnúmero de *hardware*, las cuales funcionan de tal forma que se comportan como si fuesen una sola computadora. En la actualidad, el *cluster* cumple con un papel muy importante en la solución de problemas de ciencias, ingeniería y comercio moderno. (Pethuru Raj, Ganesh Chandra Deka, 2014). Sin embargo, la tecnología del *cluster* presenta cierta complejidad para utilizarlas en infraestructuras y dificultades de portabilidad entre ellas.

Estas dificultades han sido la causa por la cual nunca se ha podido popularizar en otros ámbitos, fuera de la investigación y lo académico. Los avances tecnológicos hicieron posible incorporar la virtualización como solución a problemas que presentan los *clusters*. Esto ha permitido crear máquinas virtuales que separan los requisitos *hardware-software* y replicar el ambiente del usuario sin necesidad de instalar y configurar todo el *software* de la máquina actual.

¹² José Carlos Gallego Cano, 2014, *Operaciones auxiliares para la configuración y la explotación*, Madrid, Editorial Editex.

Con la nueva tecnología de la virtualización, la puerta del *cloud computing* se abre para poder ofrecer sus servicios vía internet de manera pública o privada, sin la necesidad de tener los dispositivos físicos en algún departamento existente.

De acuerdo con el profesor de la Facultad de Ingeniería Universidad Nacional de Asunción (UNA) de Paraguay, Joyanes Aguilar, establece que: "La nube (*The Cloud*) es el conjunto "infinito" de servidores de información (computadores) desplegados en centros de datos, a lo largo de todo el mundo donde se almacena millones de aplicaciones Web y enormes cantidades de datos (*big data*), a disposición de miles de organizaciones y empresas, y cientos de miles de usuarios que se descargan y ejecutan directamente los programas y aplicaciones de *software* almacenados en dichos servidores tales como Google Maps, Gmail, Facebook, Tuenti o Flickr."

La nube de almacenamiento puede conectar un gran número de diversos tipos de dispositivos de almacenamiento en la red entre sí para proporcionar acceso y servicios de negocios, mediante la aplicación del *software* y ciertas aplicaciones externas comunes o en la interfaz. El almacenamiento en la nube es también un sistema de computación en la nube, cuyo núcleo es el almacenamiento de datos y gestión de datos.

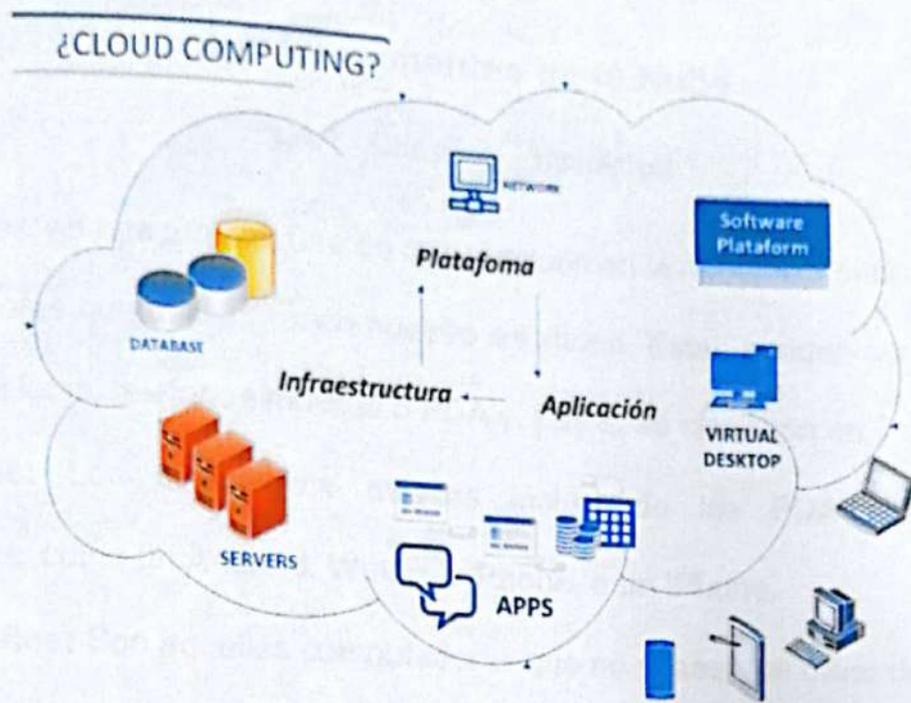


Ilustración 1. Definición y componentes básicos de Cloud Computing.
Fuente: propia.

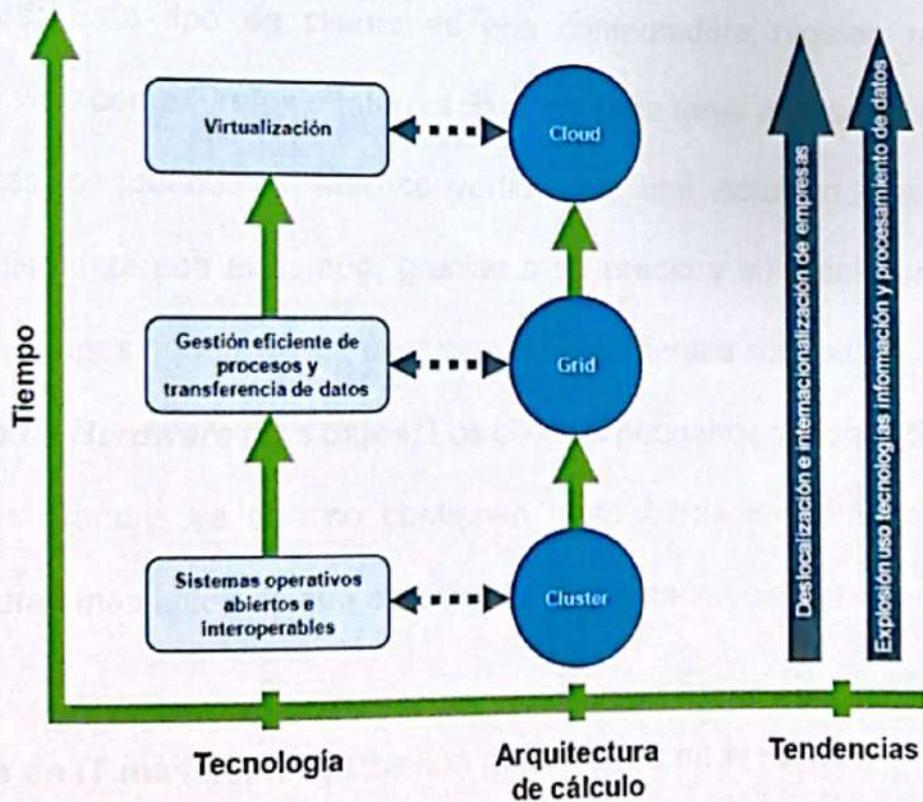


Ilustración 2. Evolución de las arquitecturas de cálculo.
Fuente: (Ureña, Ferrari, Blanco, & Valdecasa, 2012)

1.4 Componentes de la Nube

1.4.1 Clientes - Usuarios

Los clientes, en una arquitectura de computación en la nube, son básicamente las computadoras que utilizamos en nuestro escritorio. Estas pueden ser ordenador portátil, tabletas, teléfonos móviles o PDA's. Estos, se clasifican en 3 categorías:

- **Móviles:** Los dispositivos móviles incluyendo los PDA's o teléfonos inteligentes, como un Android, Windows Phone, o un iPhone.
- **Pequeños:** Son aquellas computadoras que no poseen un disco duro interno, más bien permiten al servidor hacer todo el trabajo para luego mostrar la información.
- **Grandes:** Este tipo de cliente es una computadora regular, usando un navegador web como Firefox o Internet Explorer para tener acceso a la nube.

Los clientes pequeños se han convertido en una solución que aumenta considerablemente con el tiempo, gracias a su precio y su efecto en el medio ambiente. Algunos beneficios de usar este tipo de clientes son los siguientes:

- **Costos de Hardware más bajos:** Los clientes pequeños son más baratos que los clientes grandes ya que no contienen tanto *hardware* como estos. Ellos también duran más antes de que se necesite actualizarlos o que se conviertan en obsoletos.
- **Costos de IT más bajos:** Estos son gestionados en el servidor y hay menos puntos de falla en el sistema.
- **Seguridad:** Ya que el procesamiento toma lugar en el servidor y allí no hay disco duro, hay menos posibilidades de que un malware invada el servicio.

- **Seguridad de datos:** Ya que la data es almacenada en el servidor, hay menos posibilidades de que la data se pierda si el cliente se daña o es robado.
- **Menos consumo de energía:** Los clientes pequeños consumen menos energía que los grandes.
- **Fáciles de reparar o reemplazar:** Si un cliente pequeño se daña, es fácil reemplazarlo, se remueve la caja que lo protege y el escritorio del usuario regresa exactamente como estaba antes de la falla.
- **Menos ruidosos:** Sin un disco duro que gire, hay menos ruido. (Parga, 2011)

1.4.2 Servicios de distribución

No todos los servidores están en el mismo sitio, por el contrario, estos se encuentran separados geográficamente en distintas localidades. Para el usuario, suscriptor de la nube, esos servidores actúan como si estuvieran uno al lado del otro.

Esto le da al proveedor de servicio más flexibilidad en opciones y seguridad. Por ejemplo, Amazon tiene su nube de solución en servidores ubicados por todo el mundo. Si algo le pasara a uno de esos servidores, causando una falla, el servicio sería aun accesible a través de otro sitio. También, si la nube necesita más *hardware*, no necesitan eliminar servidores, ellos pueden añadirlos a otro sitio y simplemente convertirlos en parte de la nube. (Giulio E. Lancioni, Jeff Sigafos, Mark F. O'Reilly, Nirbhay N. Singh, 2012)

1.4.3 Centro de datos

El *data center*, o centro de datos, es una colección de servidores donde las aplicaciones a la que el cliente es suscrito, son almacenadas. Podría ser una habitación enorme en la base de un edificio o incluso un cuarto lleno de servidores del otro lado del mundo al cual se accede por medio de internet.

Gracias a ellos, el *software* puede ser instalado, permitiendo a múltiples servidores virtuales ser utilizados. En este sentido, es posible tener media docena de servidores virtuales funcionando en un servidor físico.

Cabe destacar que el número de servidores virtuales que pueden estar contenidos en un servidor físico depende del tamaño y la velocidad del antes mencionado, así como también las aplicaciones que se estén ejecutando en el servidor virtual.

(Venkata Josyula, Malcolm Orr, Greg Page, 2012)

1.5 Empresas y Servicios

El "Almacenamiento en la Nube" es un importante servicio de la computación en la nube, permitiendo a los propietarios de datos (dueños) para albergar los datos de sus sistemas informáticos locales a la nube. Almacenamiento en la nube es un modelo de almacenamiento conectado en red en línea, donde los datos se almacenan grupos de almacenamiento que se alojan generalmente por terceros (por ejemplo, los proveedores de servicios de almacenamiento).

Los proveedores de servicios operan grandes centros de datos, y la capacidad de almacenamiento de arrendamiento de datos de ellos en una modalidad de pago

según el modelo de negocio. Los proveedores de servicios, en el fondo, virtualizan los recursos de acuerdo con los requerimientos de los clientes y los exponen como grupos de almacenamiento que los clientes pueden utilizar ellos mismos para almacenar archivos u objetos de datos. Físicamente, el recurso puede extenderse a lo largo de varios servidores. (Kan Yang, Xiaohua Jia, 2013).

En los últimos tiempos, las necesidades que requieren los centros de cómputos en grandes empresas y organizaciones han crecido a un ritmo constante y acelerado, las demandas son aún más exigentes. De esta forma, para integrar las carencias de aquellos sistemas más rigurosos, se ha originado la evolución de las arquitecturas de tecnologías en la nube, basada principalmente en la realización simultánea de procesos en múltiples equipos informáticos.

Podemos encontrar diversos recursos bibliográficos sobre la computación en la nube, desde un punto de vista tecnológico, aunque las ventajas del *cloud* van más allá, cuenta con características esenciales para un mejor desenvolvimiento y desempeño de funciones empresariales.

Desde un enfoque de negocios, puede tener un enorme impacto empresarial por las facilidades que ofrece en este sector, como son:

“Permite a las empresas escalar rápidamente, en función de sus necesidades, sin tener que añadir equipamiento, *software* ni personal. A través de la “nube” (una red pública, generalmente Internet), los clientes pueden acceder bajo demanda (siguiendo el modelo de pago por uso) a un gran número de recursos informáticos asignados dinámicamente, dotándose así de una enorme capacidad de procesamiento y

almacenamiento sin necesidad de instalar máquinas localmente, lo que se traduce en considerables ahorros de todo tipo, incluso de consumo energético." (Lastras Hernansanz, Lázaro Requejo, & Mirón García, 2009)

Debido a la continua demanda de recursos tecnológicos, es necesario conocer técnicas que permitan la escalabilidad de las tecnologías implementadas.

Conociendo de qué modo el *cloud computing* puede contribuir a mejorar el funcionamiento de su empresa, siendo de enorme utilidad mostrar a los empresarios en que consiste y de qué manera les puede ayudar a mejorar la cadena de valor de sus productos y servicios, o inclusive a diseñar, mejorar e implantar su modelo de negocio.

Un análisis realizado por la compañía CISCO, empresa líder en las telecomunicaciones, muestra que actualmente el 57 % de los *data center* tradicionales han sido migrados a plataformas *Cloud*. Estas estadísticas

demuestran un claro aumento durante los últimos 5 años en la migración de equipos y aplicaciones a la nube.

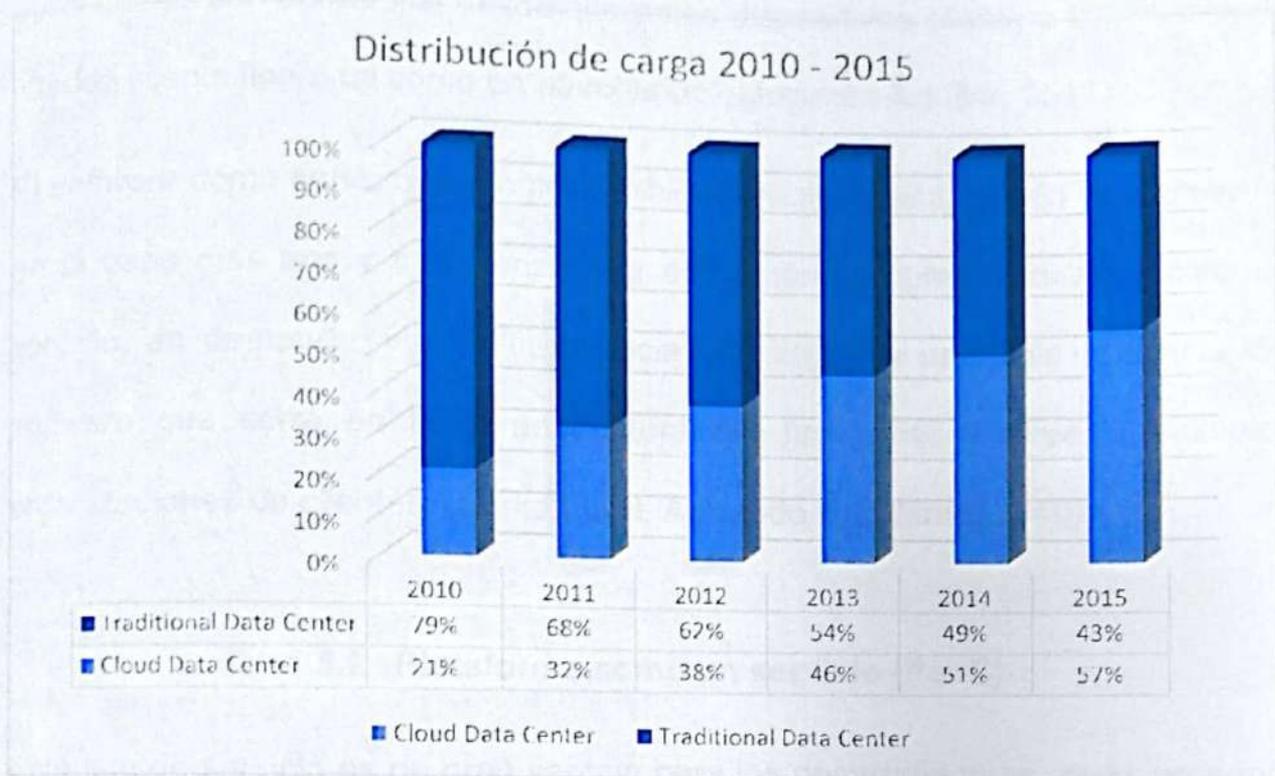


Ilustración 3. Distribución de Carga 2010 – 2015
Fuente: (CISCO, 2011)

Las empresas pueden exigir cualquier tipo de servicio, *cloud computing* es capaz de proporcionar diferentes modelos de servicios, como son:

1.5.1 Software como un servicio (SaaS)

Se ofrece aplicaciones de todo tipo a través de la nube y por ende, es importante tener conectividad a Internet para acceder a este *software*. "El término *software* como servicio se refiere esencialmente al *software* residente (instalado) en la nube, aunque no todos los sistemas SaaS son sistemas instalados en la nube, si

son la mayoría. **SaaS** es un modelo de *software* basado en la Web que proporciona el *software* totalmente disponible a través de un navegador web. Las aplicaciones son accesibles desde diferentes dispositivos cliente a través de una interfaz cliente ligera tal como un navegador." (Joyanes Aguilar, 2011)

El *software* como servicio (en inglés *Software as a Service*, SaaS) se encuentra en la capa más alta y caracteriza una aplicación completa ofrecida como un servicio, en demanda, vía multitendencia que significa una sola instancia del *software* que corre en la infraestructura del proveedor y sirve a múltiples organizaciones de clientes. (Borko Furht, Armando Escalante, 2010).

1.5.2 Plataforma como un servicio (PaaS)

Este tipo de servicio es de gran ventaja para los desarrolladores, pues presenta una plataforma de programación para X lenguaje, permitiendo así crear y compilar programas desde la nube. "Proporciona un entorno de lenguaje de programación para los desarrolladores de aplicaciones para y en la propia nube. El entorno de *software* también ofrece un conjunto de interfaces de programación de aplicaciones bien definidas (API) para utilizar servicios en la nube e interactuar con otras aplicaciones en el *cloud*. Esta capa permite a las empresas desarrollar sus propias soluciones informáticas, que posteriormente, generalmente, se ejecutarán en la capa SaaS." (Fons Gómez, 2014)

Aunque, existen dos grandes obstáculos en el desarrollo de PaaS. Porque los proveedores utilizan los servicios de propiedad o desarrollo de lenguajes, algunos desarrolladores temen ser limitados para un solo proveedor. El proveedor puede

permitir que la aplicación sea traída al sistema por otro proveedor, sin embargo, el costo incrementa en comparación con mover la aplicación entre sistemas de alojamiento convencionales. (Nate Stammer, Scott Wilson, 2014).

1.5.3 Infraestructura como un servicio (IaaS)

Muestra un modelo de servicio orientado a las infraestructuras (máquinas virtuales, almacenamiento, *hardware*, etc.) necesarias para ejecutar una aplicación donde requiera recursos aún más exigentes de la que podría comprar la compañía. "El consumidor no gestiona ni controla la infraestructura fundamental de la nube, pero tiene el control sobre sistemas operativos, almacenamiento y aplicaciones desplegadas y es posible un control limitado de componentes seleccionados de red y correos, p.e. *firewalls*, hospedajes alojados. En la práctica el cliente IaaS "alquila" (paga por uso y prestaciones) recursos informáticos en su propio centro de datos, en lugar de comprarlos e instalarlos." (Joyanes Aguilar, 2011)

Este modelo de servicio puede dividirse en otros servicios que se le ofrecen indirectamente:

1. **Almacenamiento de datos como un servicio (DaaS):** Facilita recursos de almacenamiento de datos.

"El DaaS permite a los usuarios obtener el servicio de almacenamiento flexible en discos remotos que se pueden acceder desde cualquier lugar.

Este servicio, también debe cumplir con una serie de requisitos básicos:

alta disponibilidad, fiabilidad, rendimiento, replicación y la consistencia de los datos." (Fons Gómez, 2014)

2. **Comunicación como un servicio (CaaS):** Entrega servicios de aplicaciones de Voz sobre IP (VoIP), videoconferencia, etc. Es sumamente necesaria esta capa de servicio pues sirve para comunicar los demás módulos de servicios.

"El servicio debe cumplir algunos requisitos de calidad de servicio que incluirán temas como: la seguridad de red, disponibilidad, ancho de banda dedicado y supervisión de la red." (Fons Gómez, 2014)

1.5.4 *Hardware* como un servicio (HaaS)

"El extremo inferior del modelo de capas de la computación en nube es el *hardware* físico real, que forma la columna vertebral de cualquier oferta de servicios *cloud computing*." (Fons Gómez, 2014)

HaaS envuelve varios aspectos:

- **Niveles de acuerdo de servicio.** Este es un acuerdo entre el proveedor y el cliente, garantizando cierto nivel de rendimiento del sistema.
- ***Hardware* de la computadora.** Estos son los componentes cuyos recursos se alquilan. Los proveedores de servicios a menudo tienen esto arreglado como una red, para más fácil escalabilidad.
- **Red.** Esto incluye *hardware* para servicio de seguridad, *routers*, balance de carga, entre otros.

- **Conectividad a internet.** Esto permite al cliente acceder al *hardware* desde su propia organización.
- **Plataforma de entorno de Virtualización.** Esto permite al cliente ejecutar la máquina virtual que él quiera.

Utilidad de la informática de facturación. Usualmente la facturación del cliente está basado en cuántos recursos del sistema está utilizando. (Borko Furht, Armando Escalante, 2010)

HaaS ofrece servicios de *hardware*, se refiere a la composición de máquinas virtuales trabajando en la nube.

En el artículo de *Cloudtech* se define un nuevo tipo de servicio llamado **Todo como un servicio (XaaS)**, como:

"Yo cuestiono que XaaS es un término legítimo, y que es útil para describir un nuevo tipo de servicios en la nube - aquellos que hacen uso de IaaS, PaaS y SaaS todas bien entregadas en un solo paquete. Estos paquetes están diseñados para desplazar completamente la entrega de un servicio de TI de los productos básicos." (Dixon, 2014)

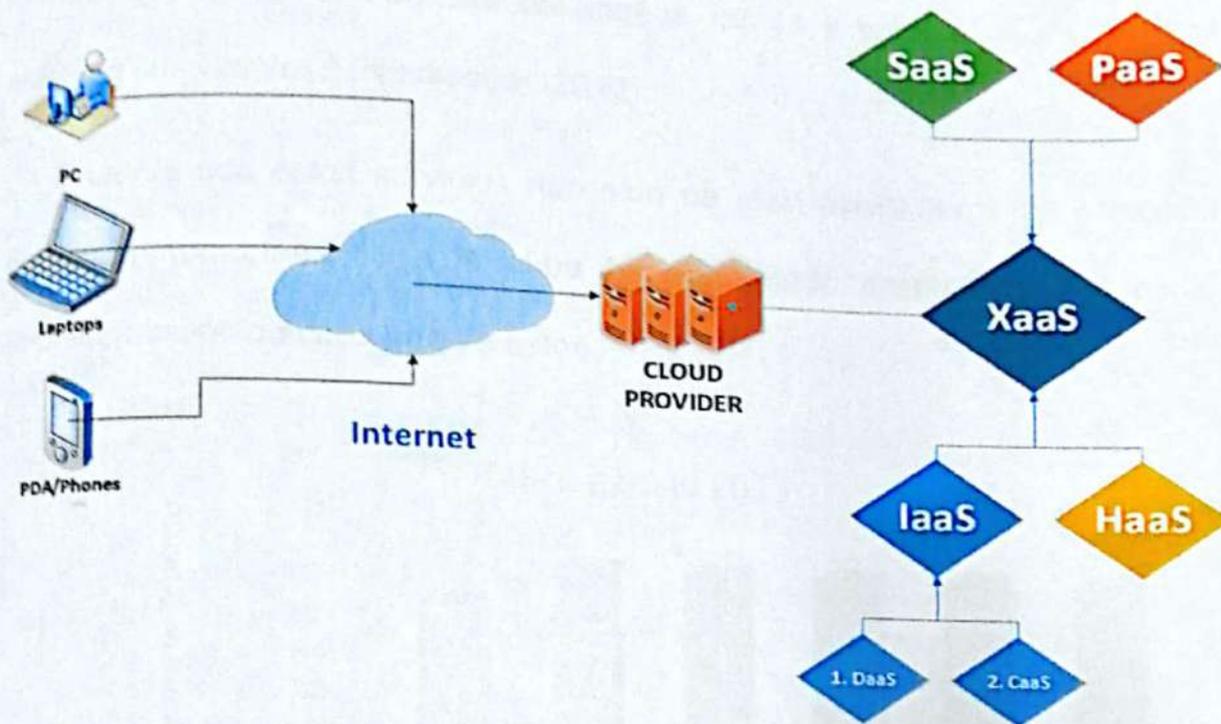


Ilustración 4. Modelos de servicios incorporados en la nube.
Fuente propia.

1.6 Compañía de servicio

La compañía de servicio en la nube "Windows Azure", ofrece servicios de *software*, plataformas e infraestructuras, todos juntos en la nube de una compañía, como si pudiéramos adquirir el paquete de servicios completo en lugar de adquirirlos individualmente.

Por otro lado, con la incorporación de esta nueva definición llamada XaaS, se crea consigo un nuevo servicio denominado **Negocio como un Servicio (BaaS)**. "Utilizando BaaS, los vendedores no solo albergan la solución de *software* en su infraestructura en nombre de una organización, pero también participan en la gestión del negocio, para asegurar que se cumplan los objetivos. Pone la arquitectura empresarial y las capacidades de planificación en el lugar para

permitir que cualquier empresa de entrega rápida y soluciones de negocio a escala a sus clientes." (Nussbaum, 2012)

Es evidente que estos servicios han sido de gran ayuda para las compañías, debido a que el tráfico a la nube ha aumentado drásticamente, desde la implementación de cada uno de estos.

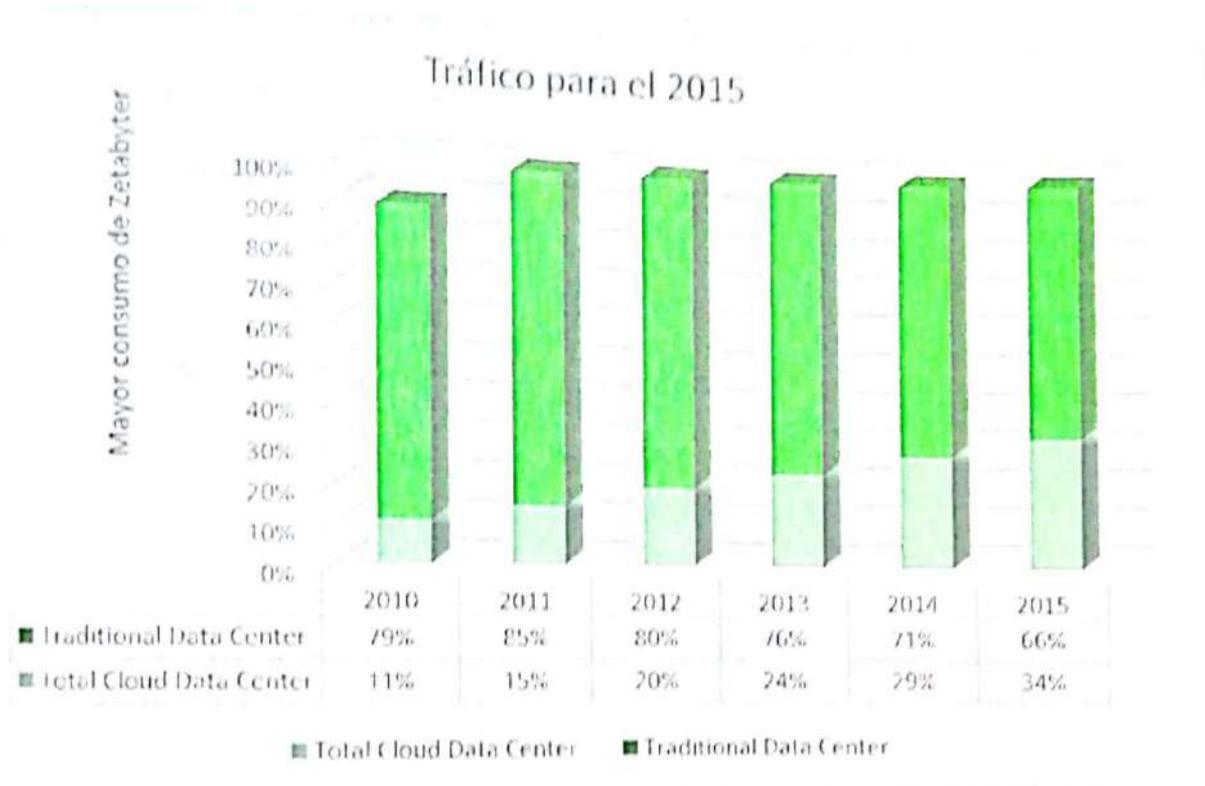


Ilustración 5. La nube tráfico del centro de datos se representan más de un tercio del total del tráfico del centro de datos para el año 2015
Fuente: (CISCO, 2011)

1.7 Aspectos legales

En cuanto se refiere a los aspectos legales, la computación en la nube toma muy serio sus leyes a la hora de presentar cargos o acusaciones contra una compañía o servicio dado. Antes de conocer los aspectos legales que conlleva tener un servicio en la nube, es necesario tener información de los derechos que nos permite la computación en la nube por medio de contratos. La Agencia de

Protección de Datos (2013) ofrece gratuitamente una guía para clientes que contraten servicios de *Cloud Computing*, ofreciendo detalles claros y específicos antes de adquirir un servicio en la nube. Algunas recomendaciones que ofrece la Agencia Española, son las siguientes:

- "Se debe evaluar la tipología de datos que trata en función del nivel de seguridad exigido por la Ley Orgánica de Protección de Datos (LOPD) y decidir para qué datos personales contratará servicios en la nube, cuáles prefiere mantener en sus propios sistemas de información y el tipo de nube que se ira a elegir." (Agencia Española de Protección de datos, 2013)

Este acuerdo es importante pues definirá las finalidades para las que el proveedor puede tratar los datos, ya que debe garantizarse expresamente que no los utilizará para otro propósito que no tenga relación con los servicios contratados.

En el libro (Guía para clientes que contraten servicios de *Cloud Computing*, 2013) se plantean cláusulas imprescindibles a la hora de adquirir servicios de *cloud computing*.

- El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos personales. Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al prestador del servicio. Por el otro lado, quien ofrece la contratación de *cloud computing* es un prestador de servicios.

- El modelo de *cloud computing* hace posible que tanto los proveedores de servicios como los datos almacenados en la nube se encuentren ubicados en cualquier punto del planeta.
- Debe solicitar y obtener información sobre si intervienen o no terceras empresas (subcontratistas) en la prestación de servicios de *cloud computing* y el contrato que se firma ha de incorporar cláusulas contractuales para la protección de los datos personales según se detalla en las siguientes preguntas.
- La localización de los datos tiene importancia porque las garantías exigibles para su protección son distintas según los países en que se encuentren.
- Pregunte al prestador de servicios de *cloud computing* si hay transferencias internacionales de datos y, en caso afirmativo, con qué garantías, del mismo modo, cuando los datos están localizados en terceros países podría suceder que una Autoridad competente pueda solicitar y obtener información sobre los datos personales de los que el cliente es responsable. En este caso el cliente debería ser informado por el proveedor de esta circunstancia (salvo que lo prohíba la ley del país tercero).
- El nivel de seguridad exigible depende de la mayor o menor sensibilidad de los datos personales. Asimismo, el acceso a la información a través de redes de comunicaciones debe contemplar un nivel de medidas de seguridad equivalente al de los accesos en modo local.

- Como cliente debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable. El cliente debe ser informado diligentemente por el proveedor de *cloud* sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse.
- El proveedor del servicio debe comprometerse a garantizar la confidencialidad utilizando los datos solo para los servicios contratados. Asimismo debe comprometerse a dar instrucciones al personal que depende de él para que mantenga la confidencialidad.
- La portabilidad significa que el proveedor ha de obligarse, cuando pueda resolverse el contrato o a la terminación del servicio, a entregar toda la información al cliente en el formato que se acuerde, de forma que este pueda almacenarla en sus propios sistemas o bien optar porque se traslade a los de un nuevo proveedor en un formato que permita su utilización, en el plazo más breve posible, con total garantía de la integridad de la información y sin incurrir en costes adicionales.
- Deben preverse mecanismos que garanticen el borrado seguro de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato. (Un mecanismo apropiado es requerir una certificación de la destrucción emitido por el proveedor de *cloud computing* o por un tercero).

- El cliente de *cloud computing*, como responsable del tratamiento de datos, debe permitir el ejercicio de los derechos ARCO (Derechos de acceso, rectificación, cancelación y oposición) a los ciudadanos, y para ello, el proveedor debe garantizar su cooperación y las herramientas adecuadas.

De acuerdo con el diagrama, muestra los aspectos legales del *cloud computing* donde existe una trilogía entre los proveedores de servicios, los clientes externos, y los terceros (contratistas). Esta relación da lugar a controversias de carácter internacional y el tratamiento de la información derechos de autor:

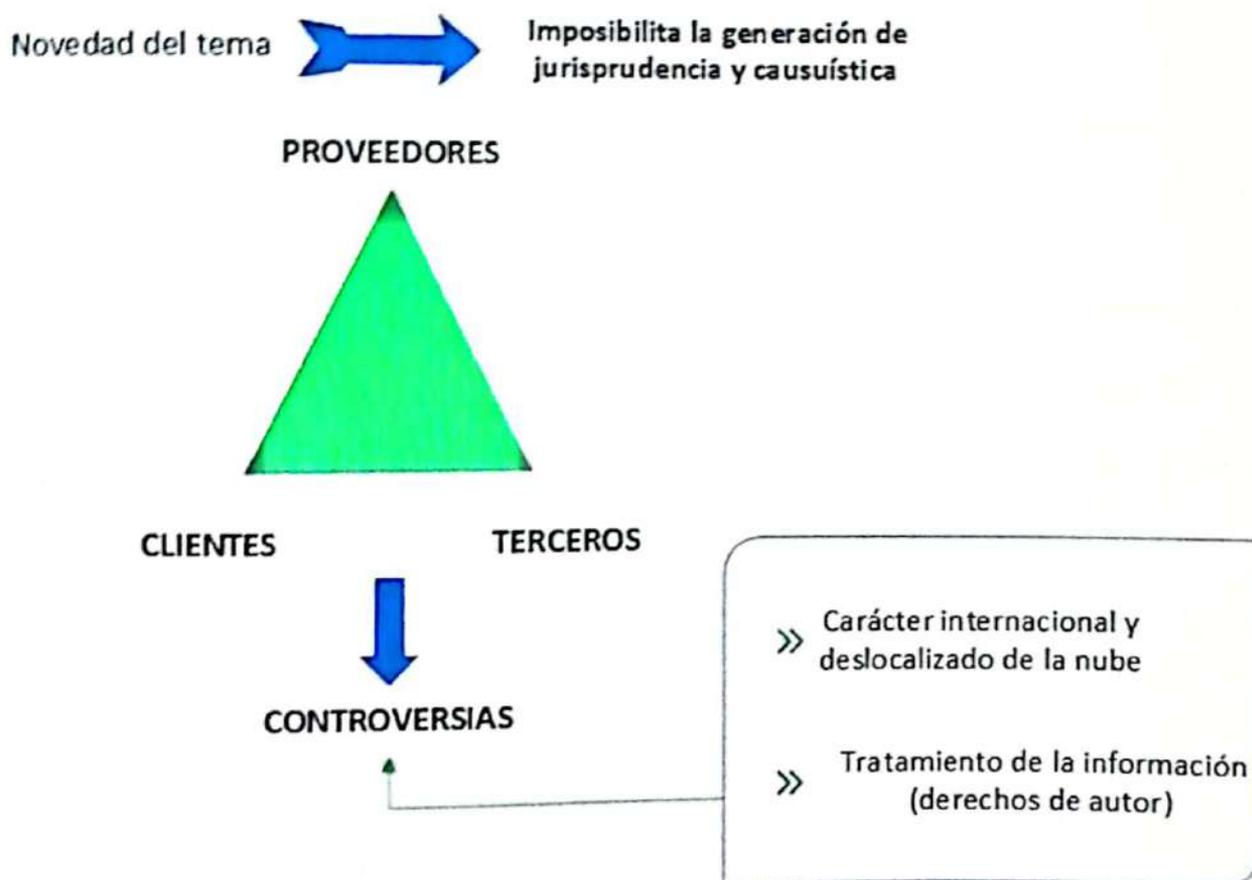


Ilustración 6. Trilogía relacional entre proveedores, clientes y contratistas (terceros) entre los aspectos legales del Cloud Computing.
Fuente: Aspectos legales de la computación en la nube, José A. Gómez

1.7.1 Leyes

Las empresas que contratan servicios en la nube al igual que sus proveedores deben tener en cuenta una serie de leyes aplicables que afectan al tratamiento de la información y la protección de los datos con respecto a ella de acuerdo con el país donde se encuentren asentadas las compañías.

La República Dominicana, cuenta con el Instituto Dominicano de Telecomunicaciones (INDOTEL), quien es el organismo que se encarga de regular y supervisar el desarrollo del mercado de las telecomunicaciones, fue creado por la Ley General de las Telecomunicaciones 153-98.

Específicamente, la ley 126-02 de protección de datos de carácter personal al sujeto regulado, la cual establece:

"La obligación de las Entidades de Certificación de garantizar la protección, confidencialidad y debido uso de la información suministrada por el Suscriptor así como de lo regulado en la letra (c) del artículo 21 del Reglamento de Aplicación que regula la posibilidad de que el INDOTEL regule lo relativo a la protección de los Datos de Carácter Personal de los Suscriptores de Certificados."

1.8 Plan de Continuidad de Negocios (BCP)

Según el autor del libro "Planes de contingencias de la continuidad del negocio en las organizaciones " (Gaspar Martínez, 2004), la tendencia imparable del uso

anglicismos dentro del mundo de las Tecnologías de la Información, el término Continuidad de Negocio (*Business Continuity*) se ha ido extendiendo de manera generalizada frente a los anteriormente utilizados, Recuperación de desastres (*Disaster Recovery*) primero y *Contingency Planning* (Plan de Contingencia) después.

Hoy día, el concepto de Plan de Continuidad de Negocios (BCP) está siendo sustituido por la Gestión de la Continuidad del Negocio (*Business Continuity Management*), es decir, no se limita a la planificación de la continuidad sino a la gestión integral de la misma.

1.8.1 Plan de contingencia

Un plan de continuidad de negocios define la continuidad del servicio como una mezcla de capacidades, tácticas y estrategias pre-aprobadas por la dirección de una empresa o compañía para responder a contratiempos e interrupciones del servicio con el objetivo de continuar con sus operaciones de manera transparente para el usuario.

Un plan de continuidad de negocios se hace de manera robusta y eficiente incluyendo un Plan de Recuperación de Desastres (DRP) y una Evaluación de Impacto de Negocios (BIA).

Dicho plan está planteado no solo para grandes empresas, sino también para las Pymes, ya sean industriales, comerciales o de servicios. De igual manera, el DRP estará enfocado hacia los recursos y servicios de tecnología informática, el BCP

es mucho más amplio y está dirigido hacia las operaciones e instalaciones en general de la empresa.

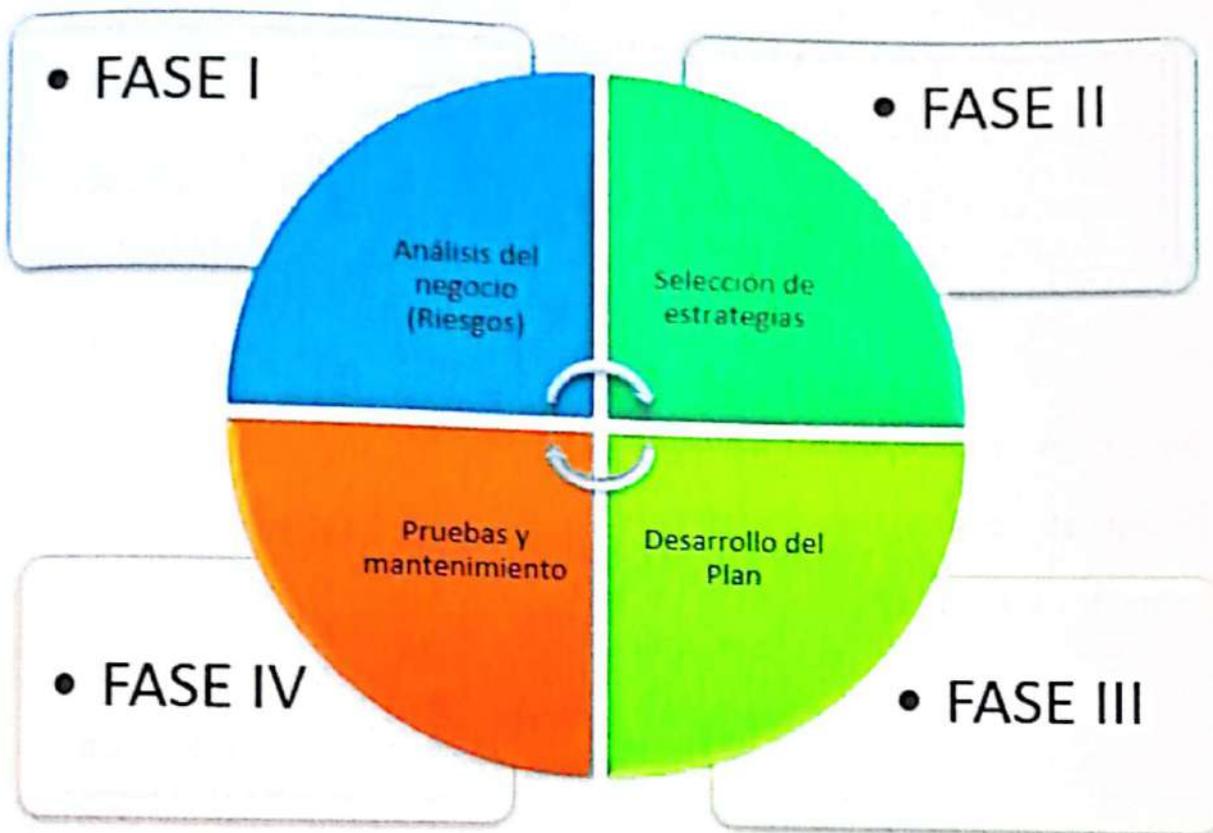


Ilustración 7. Fases indispensables para la elaboración del BCP.
Fuente: propia basada en el libro (Del Pino Jiménez, 2007)

1.8.2 Diferencias y Estándares

La importancia de tener un BCP en las empresas ofrece grandes ventajas en la optimización de sus servicios y en la disponibilidad de las mismas. El hecho de no tenerla representa gran descontento para usuarios que utilizan el servicio, y con ella trae consigo bajo nivel de competencia con otras compañías. "Las estadísticas indican que el 80 % de las organizaciones e Instituciones que se enfrentan a una discontinuidad de negocios importante, y no cuentan con planes

adecuados y suficientes para garantizar la continuidad del negocio, no sobreviven al evento." (Figuerola, 2014)

Una de las normativas principales que se aplica hoy en día y, que de hecho, ha estado vigente desde los inicios del plan de continuidad de negocios, es la BS25999, en ella se define el BCP pero con un enfoque a la disponibilidad de la información. Figuerola (2014), define dos normativas que existen en la actualidad:

- **ISO / IEC 24762:2008:** Directrices para la prestación eficaz de la información y las comunicaciones (TIC) ante la Recuperación de Desastres (DR) de servicios. El asesoramiento y orientación de esta norma es genérico, por lo que es aplicable a cualquiera empresa o proveedor subcontratado de servicios TIC.
- **ISO 22301: 2012:** Seguridad Societaria y Continuidad de Negocio - Sistema de Gestión – Requisitos. Se publicó en mayo de 2012 y sustituye a la norma BS 25999, que se retira en noviembre de 2012. Especifica los requisitos para planificar, establecer, implementar, operar, monitorizar, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de incidentes perturbadores que puedan surgir.

Para fortalecer un plan de continuidad de negocios es necesario tomar en cuenta los siguientes componentes:

1. **Definir la estrategia de continuidad:**

Antes de estructurar cualquier plan es necesario comprender los riesgos que enfrenta la compañía, para luego definir las estrategias necesarias que sirvan de prevención a esos riesgos.

2. **Análisis de Impacto (BIA):**

El análisis de impacto de negocios (BIA) se podría mencionar como el paso crítico para la implementación de un Plan de continuidad de negocios (BCP), ya que el BIA se enfoca en el análisis de los elementos crítico que impacta y afecta a una organización. Se debe establecer las partes críticas de los recursos de información de:

- Sistemas.
- Datos.
- Redes.
- *Software* de sistemas.
- Instalaciones.

De acuerdo a la publicación del Ing. Carlos Ormella Meyer (2008), lo define como "un paso clave en el proceso de la elaboración del BCP (Plan de Continuidad de Negocios)".

Además, explica que esto se debe a que BIA está básicamente relacionado con eventos indeseados que provoquen una interrupción o degradación de las operaciones de una empresa, es decir, afectando la disponibilidad de los recursos críticos para mantener operando adecuadamente los procesos de negocio correspondientes. Incluso en este contexto no se necesita conocer la razón y/o la

probabilidad de tales eventos para poder determinar el impacto de una falla en dichos procesos.

Ventajas del Análisis de Impacto de Negocios (BIA)

- Tener información clara y concisa sobre los puntos críticos del sistema.
- Prevenir los Riesgos que se puedan presentar.
- Evitar Costos innecesarios que se pueda generar por caídas del sistema.
- Encontrar las soluciones de los puntos críticos del sistema.

De acuerdo con el Ing. Ormella Meyer en su publicación (Seguridad de la Información, Redes y Telecomunicaciones, 2008) da a conocer los diferentes factores indispensables para el proceso del Análisis de Impacto de Negocios (BIA) se clasifican en:

- **Crítico:** Estas funciones no pueden realizarse a menos que sean reemplazadas por capacidades idénticas. Las aplicaciones críticas no pueden ser reemplazadas por métodos manuales. La tolerancia a la interrupción es muy baja. Por lo tanto, el costo de interrupción es muy alto.
- **Vital:** Estas funciones pueden realizarse manualmente por solo por un período breve de tiempo. Hay mayor tolerancia a la interrupción que con los sistemas críticos, por lo tanto, los costos de interrupción son un poco más bajo considerando que las funciones son restauradas dentro de un marco de tiempo determinado.
- **Sensible:** Estas funciones se pueden realizar manualmente, a un costo tolerable y por un período prolongado de tiempo. Aun cuando se

pueden realizar manualmente, por lo general es un proceso difícil y requiere de personal adicional para llevarlas a cabo.

- **No Sensible:** Estas funciones pueden ser interrumpidas por un período prolongado de tiempo, a un costo muy pequeño o nulo para la compañía que requiere de poco o ningún esfuerzo para ponerse al día cuando son restauradas.

1.8.3 Diseño y desarrollo del Plan de Continuidad de Negocios

Durante esta fase de desarrollo se toman en cuenta aquellos procesos y/o sistemas importantes que puedan ser vulnerables y que puedan traer grandes pérdidas si no se encuentran disponibles. El diseño y desarrollo para la optimización de los servicios es vital en todo plan de continuidad de negocios.

De acuerdo a Norberto Figuerola (2014), existen 6 pasos generales involucrados para la creación de un plan de continuidad de negocios:

1. Alcance del plan.
2. Identificar las áreas clave del negocio.
3. Identificar las funciones críticas.
4. Identificar las dependencias entre las distintas áreas de negocio y funciones.
5. Determinar el tiempo de inactividad aceptable para cada función crítica.
6. Crear un plan para mantener las operaciones.

Otros aspectos a tomar en cuenta a la hora de desarrollar un BCP conjunto con el BIA, es detallar la lista que incluya la ubicación de las zonas de respaldos de

datos, los proveedores de servicios de respaldos, toda la información necesaria de contactos que manejen esa parte de respaldo dentro del departamento de tecnología, etc. "Una herramienta común de planificación de continuidad del negocio es una lista que incluya suministros y equipo, la ubicación de copias de seguridad de datos y sitios de respaldo, disponibilidad del plan y quien debería tenerlo, información de contacto de los servicios de emergencia, personal clave y los proveedores de sitios de respaldo. El plan de Recuperación de Desastres es parte del Plan de Continuidad del Negocio, así que se debería consultar con el departamento de TI." (Figuerola, 2014)

1.8.3.1 Pruebas y mantenimiento

Se deben realizar pruebas para determinar qué tan viable es el plan desarrollado, si existen debilidades, es necesario rediseñar el plan con la nueva solución a esa falla encontrada, y por supuesto, se deben de realizar mantenimientos a esos sistemas y procesos que intervienen en el BCP para un servicio continuo y óptimo.

1.8.3.2 Necesidad de entrenamiento

Es de vital importancia ofrecer entrenamientos y charlas para la capacitación del personal. En caso de tener una emergencia o un fallo en el sistema, el personal debe de estar debidamente entrenado para la solución de esos errores sin alterar la disponibilidad de los servicios.

1.8.3.3 Mantenimiento y Reevaluación del plan

Es necesario actualizar el plan de continuidad de negocios cada cierto tiempo, los avances tecnológicos surgen y evolucionan con mayor rapidez y se debe estar preparado para cualquier nueva falla que pueda surgir.



Ilustración 8. Ciclo operacional del Plan de Continuidad de Negocios y sus procesos.
Fuente: propia.

CAPITULO II. ASPECTOS METODOLÓGICOS

2.1 Tipo de investigación

Esta investigación será descriptiva y explicativa, debido a que la misma se basa en la descripción exacta de factores, actividades, procesos, objetos y fenómenos, donde se pretende exponer las causas de los eventos o sucesos que se estudian. Los factores a tomar en cuenta serán: la disponibilidad de los servicios y el plan operativo del Departamento de TI de la Universidad APEC con respecto a la Plataforma EVA para la elaboración de un plan logístico que garantice la operatividad de la plataforma durante una falla, mantenimiento o luego de alguna catástrofe.

La detección de dichos problemas permite identificar la vía de mayor eficacia para la obtención de mejores resultados y para mejorar la disponibilidad en Entorno Virtual de Aprendizaje (EVA) de la universidad APEC.

Las informaciones recopiladas son de campo, para su obtención se requerirá de técnicas e instrumentos de investigación aplicadas a usuarios-estudiantes, usuarios-docentes y al personal administrativo del Departamento de TI de la Universidad.

Además, he de medir el posible impacto que tendrían los usuarios con la implementación del plan logístico y mejora de la disponibilidad en una plataforma totalmente virtual.

2.1.1 Descriptivo

Durante de la investigación se describirán los factores que involucran a la falta de disponibilidad de la aplicación web Moodle y la implementación de continuidad de

negocios basado en la nube. Se graficarán diferentes estadísticas y estimados, obtenidos mediante diferentes técnicas ayudando a identificar informaciones relevantes para la investigación.

Su enfoque será cualitativo pues, se recolectaran datos o componentes sobre 0diferentes aspectos de los usuarios (docentes y estudiantes) de la Universidad APEC, de igual forma, se realizará un análisis y medición de los mismos.

2.1.2 Explicativo

Este será utilizado en todo el proceso de la realización del trabajo para predefinir cada problema que pueda surgir, explicando las razones, consecuencias y causas que conlleva detallando los pasos para su resolución de forma clara y precisa, mediante un análisis, síntesis e interpretación de la información recolectada.

2.2 Métodos de investigación

Se utilizará la lógica o razonamiento deductivo debido a que se llegará a conclusiones particulares a partir de premisas generales para determinar cuáles serían las mejoras prácticas a utilizar en el Entorno Virtual de Aprendizaje (EVA). El método inductivo es aquel que partiendo de los elementos particulares se eleva a conocimientos generales. Todas las referencias o informaciones recopiladas a partir de los servidores de redes, virtualización, conectividad y disponibilidad, permitirá observar de manera clara donde radica el principal problema del almacenamiento de datos.

El método estadístico, consiste en una secuencia de procedimientos para el manejo de los datos cualitativos de la investigación. Para realizar un estudio profundo y unas conclusiones basadas en la realidad, estadísticamente se plantearán las cantidades de usuarios que almacenan sus datos en el EVA, la disponibilidad y el tiempo de interrupción, que son datos primordiales para el correcto enfoque de la investigación.

2.3 Técnicas de estudio

En esta etapa del proyecto se elaborará la recolección de datos con un enfoque cualitativo, utilizando dos herramientas vitales, como son: la entrevista y la encuesta, para tener mayor fiabilidad en la información reunida.

- **Encuesta:** El instrumento a utilizar para esta técnica será el cuestionario con preguntas cerradas. Permitirá conocer la tendencia de uso de la plataforma por los usuarios y el crecimiento o disminución que pueda tener el Sistema de Almacenamiento de datos en la nube.
- **Entrevista:** El instrumento a utilizar para esta técnica será el cuestionario con preguntas abiertas al Encargado del Departamento de Infraestructura en el Departamento de TI, para poder dar a una correcta recomendación en base de las informaciones proporcionadas.

BIBLIOGRAFIA

- CISCO. (2011). *Cisco Global Cloud Index: Forecast and Methodology, 2010 - 2015*. San José. Pág. 5, 6
- Del Pino Jiménez, L. (2007). *Guía de desarrollo de un Plan de Continuidad de Negocio*. Madrid. Pág. 7
- Gómez Treviño, J. A. (2010). Aspectos legales de la computación en la nube. *Aspectos legales, información en la nube*.
- Hsiang-Chuan Liu, Wen-Pei Sung & Welin Yao. (2014). *Computer, Intelligent Computing and Education*. Reino Unido : CRC Press. Pág. 1053
- Joyanes Aguilar, L. (2011). *Computación en la nube e innovaciones tecnológicas*. Paraguay. Pág. 1, 5 y 7
- Kan Yang, Xiaohua Jia. (2013). *Security of Cloud Storage Systems*. Hong Kong: Springer Science & Business Media. Pág. 2
- Lastras Hernansanz, J., Lázaro Requejo, J., & Mirón García, J. D. (2009). *Arquitectura de red para servicios en Cloud Computing*. Madrid. Pág. 21
- Gaspar Martínez, J. (2004). *Planes de contingencias de la continuidad del negocio en las organizaciones*. Madrid: Díaz Santos, S.A. Pág. xxv
- Figuerola, N. (2014). *Continuidad del Negocio y Recuperación de Desastres*. Pág. 3 y 7

- Fons Gómez, F. (2014). *Cloud Computing: Caracterización de los impactos positivos obtenidos por la optimización del modelo Cloud Computing por las PYMES, basado en la tipología de modelos de negocio*. Valencia. Pág. 24 y 25
- Borko Furht, Armando Escalante. (2010). *Handbook of Cloud Computing*. United States: Springer Science & Business Media. Pág. 346
- Nate Stammer, Scott Wilson. (2014). *CompTIA Cloud+ Certification Study Guide*. United States : McGraw-Hill.
- Ormella Meyer, C. (21 de Octubre de 2008). *Seguridad de la Información, Redes y Telecomunicaciones*. Pág. 1
- Parga, D. C. (2011). *Cloud Computing: retos y oportunidades*. España: Fundacion IDEAS. Pág. 22 y 23
- Pethuru Raj, Ganesh Chandra Deka. (2014). *Handbook of Research on Cloud Infrastructures for Data Analytics*. United States : IGI Global.
- Ureña, A., Ferrari, A., Blanco, D., & Valdecasa, E. (2012). *Cloud Computing: Retos y Oportunidades*. España. Pág. 14
- Venkata Josyula, Malcolm Orr, Greg Page. (2012). *Cloud Computing: Automating the Virtualized Data Center*. United States : Cisco Press
- Giulio E. Lancioni, Jeff Sigafoos, Mark F. O'Reilly, Nirbhay N. Singh. (2012). *Assistive Technology: Interventions for Individuals with Severe/Profound*

and Multiple Disabilities. United States : Springer Science & Business Media.

Editorial Vértice. (s.f.). *La calidad en el servicio al cliente*. España: Vértice. Pág. 2

Agencia Española de Protección de datos. (2013). *Guía para clientes que contraten servicios de Cloud Computing*. España. Obtenido de <http://www.agpd.es>. Pág. 13 – 18

Areito, J. (2008). *Seguridad de la Información: Redes, informática y sistemas de información*. Madrid: Paraninfo. Obtenido de https://books.google.com.do/books?id=_z2GcBD3deYC&pg=PA260&dq=plan+de+continuidad+de+negocios&hl=es-419&sa=X&ei=Hd_1VPreJYSyggS48oKQCQ&ved=0CDUQ6AEwAw#v=onepage&q=plan%20de%20continuidad%20de%20negocios&f=false

Dixon, J. (2014, Agosto 18). *Cloudtech*. Retrieved from <http://www.cloudcomputing-news.net/news/2014/aug/18/x-as-a-service-xaas-what-the-future-of-cloud-computing-will-bring/>

Ministerio de Educación Superior, Ciencia y Tecnología. (2008-2018). *Plan Decenal del Ministerio de Educación Superior, Ciencia y Tecnología (MESCyT)*. Obtenido de <http://www.mescyt.gob.do/index.php/19-mescyt/viceministerios/153-plan-decenal-de-educacion-superior-2008-2018>

Nussbaum, C. (21 de Junio de 2012). *AtomRain*. Obtenido de <http://www.atomrain.com/it/enterprise-software/business-service-baas-cloud-management-concept>

ESQUEMA PRELIMINAR DE CONTENIDO DEL TRABAJO DE GRADO

AGRADECIMIENTOS

DEDICATORIAS

RESUMEN EJECUTIVO

INTRODUCCION

CAPITULO I. CONCEPTOS GENERALES

1.1 *Cloud Computing*

1.1.1 Ventajas

1.1.2 Desventajas

1.2 Tipos de infraestructura de Nube

1.2.1 Nubes privadas

1.2.2 Nubes públicas

1.2.3 Nubes híbridas

1.2.4 Nubes de comunidad

1.3 La dependencia de la información

CAPITULO II. COMPONENTES DE LA NUBE

2.1 Clientes

2.2 Servicios de distribución

2.3 Internet – Protocolos

2.4 Data center

2.4.1 Niveles de data centers (TIER)

2.4.2 Tipos de UPS

2.6 Seguridad en la nube

2.6.1 Características de la seguridad en la nube

2.6.2 Características de funcionamiento de las nubes

2.6.3 Las nubes utilizando funciones

CAPITULO III. Entorno Virtual de Aprendizaje (EVA)

3.1 Conceptualización

3.2 Tipos

3.3 Ventajas

3.4 Desventajas

3.5 Aplicación web Moodle

3.5.1 Concepto

3.5.2 Estructura

3.5.3 API

3.5.4 Competencias

3.6 Tendencias presentes y futuras de los Entornos Virtuales de Aprendizajes

3.6.1 Panorama actual

3.6.2 Usuarios y casos de éxitos

3.6.3 Productos y Servicios

CAPITULO IV. INFRAESTRUCTURA TECNOLOGICA

4.1 Conectividad

4.2 Seguridad y autenticación de usuario

4.3 Infraestructura

4.3.1 Infraestructura virtual

4.3.2 Infraestructura de servidores

4.3 Bases de datos

4.4 Alimentación energética

CAPITULO V. PLAN DE CONTINUIDAD DE NEGOCIO

5.1 Sistema de Continuidad basado en Servicio

5.2 Sistema de Continuidad basado en aplicaciones

5.3 Sistema de Continuidad basado en la Recuperación de Desastres

5.4 Sistema de Continuidad de Respaldo Basado en la Nube

5.5 Sistema de Continuidad de Respaldo Basado en Almacenamiento

5.6 Análisis financiero en la Continuidad de Negocios

CAPITULO VI. SISTEMA DE CONTINUIDAD BASADO EN LA NUBE

6.1. FASE I: Análisis del negocio

6.1.1 Replicación

6.1.2 Alta disponibilidad

6.1.3 Software como servicio

6.1.4 Seguridad como servicio

6.2. FASE II: Selección de estrategias

6.3 FASE III: Desarrollo del Plan

6.4 FASE IV: Pruebas y mantenimiento

CONCLUSION

RECOMENDACIÓN

BIBLIOGRAFIA

ANEXOS O APENDICES

Anexo 1. Estándares

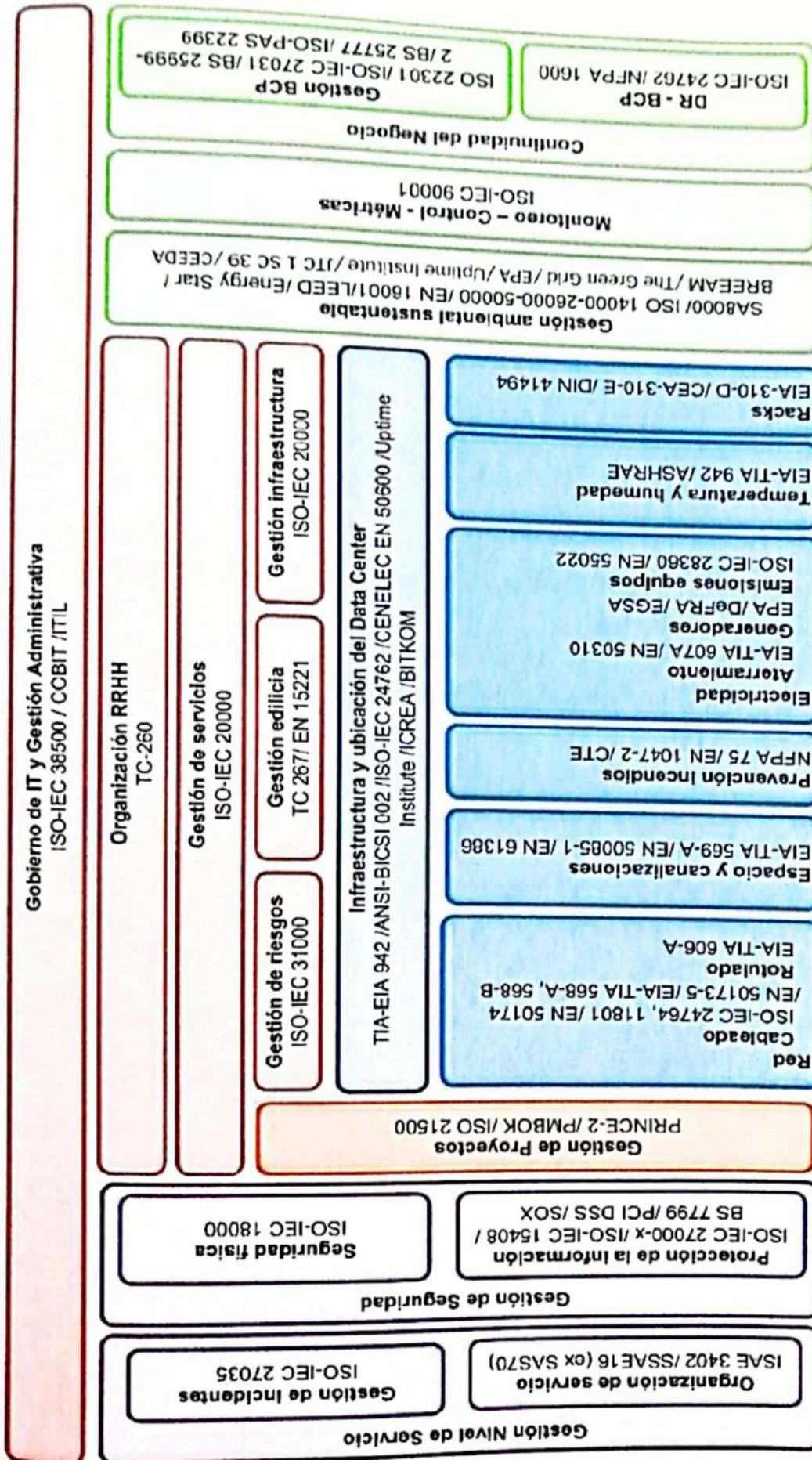


Ilustración 59. Estándares internacionales.

Los gráficos de burbujas representan subdivisiones por módulos agrupadas por color según el área de aplicación.

Fuente: (International Organization for Standardization, 2015)

Anexos Marco Aplicativo, Capítulo VI.

Anexo 2. Modelo de Organigrama

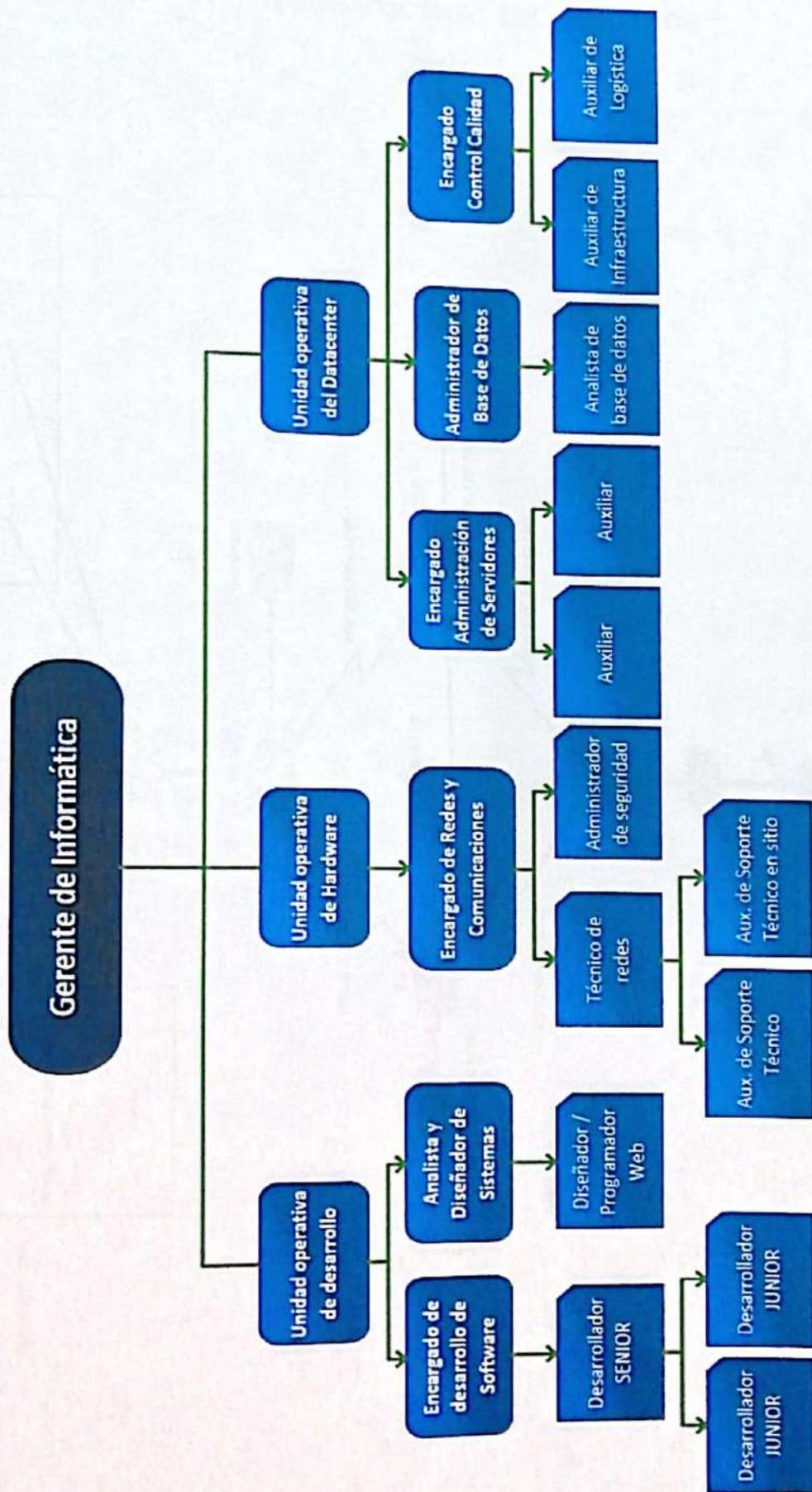


Ilustración 60. Modelo de organigrama

Fuente: Imagen propia

Anexo 3. Infraestructura tecnológica

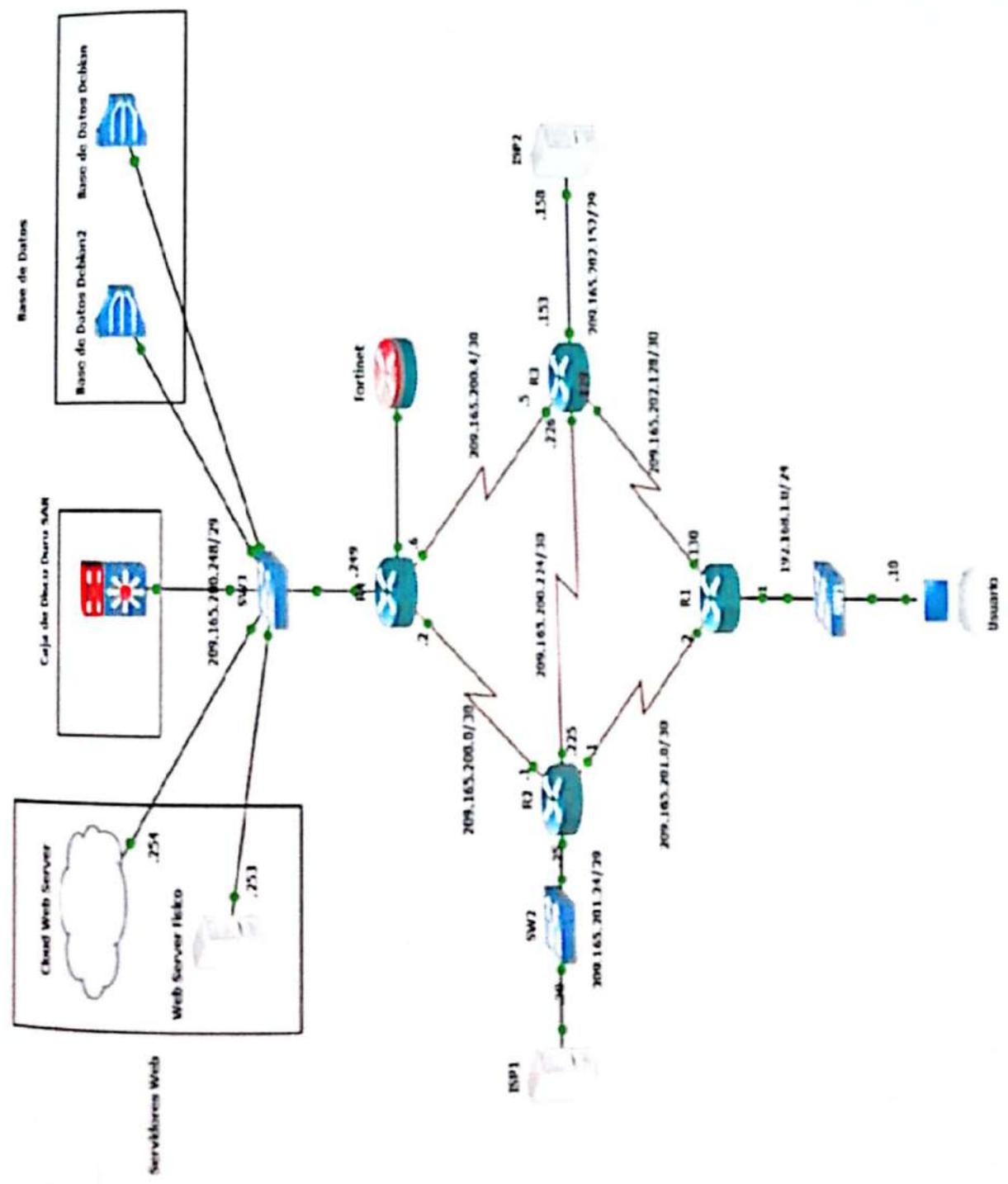


Ilustración 61. Infraestructura tecnológica de UNAPEC, después de la ejecución de un Plan de Continuidad de Negocios.

Fuente: Imagen propia.

Anexo 4. Instalación de Web Moodle

Para la instalación de la aplicación web Moodle se configuraron los siguientes parámetros a la máquina virtual:

- Memoria RAM: 1 GB
- Procesador: 1 procesador con 2 procesador por núcleo
- Disco Duro: 30 GB
- Sistema Operativo: Ubuntu Server 14.04.2
- Arquitectura: 64 bits

Una vez instalado el sistema operativo, accedemos con nuestro usuario root y password al servidor e instalamos el editor *heavyweight* VIM.

```
sudo apt-get install vim
```

Luego, procedemos a actualizar la OPcache del servidor e instalar Apache2, MySQL y PHP.

```
sudo apt-get update
```

```
sudo apt-get install apache2 mysql-client mysql-server php5
```

NOTA: Se recomienda anotar la contraseña del root password para MySQL cuando le pregunte a configurar, ya que más adelante la contraseña será utilizada.

Ahora se instalará módulos adicionales de PHP para la comunicación de los servicios Moodle y una vez instalados, se procede a reiniciar Apache para que los módulos se encuentren debidamente instalados:

```
sudo apt-get install graphviz aspell php5-pspell php5-curl php5-gd php5-intl php5-mysql php5-xmllrpc php5-ldap clamav
```

```
sudo service apache2 restart
```

Ahora instalamos el *Git* para instalar y actualizar las aplicaciones núcleos de Moodle.

```
sudo apt-get install git-core
```

Después de haber instalado el *git*, configuramos la ruta local donde se descargara e instalara Moodle. Para esta ocasión usaremos el */opt*, debido a que cualquier cambio o nueva instalación de *plugin*, solo tendrá que ser descargado en esa carpeta y los cambios serán reflejados directamente en la aplicación.

```
cd /opt
```

Ahora descargamos el código Moodle y el *index* de la página y cuando haya descargado, cambiamos el directorio en la carpeta Moodle descargada.

```
sudo git clone git://git.moodle.org/moodle.git
```

```
cd moodle
```

Ahora reparamos las ramas disponibles y con el comando *git* especificamos que ramas queremos que sea rastreada para ser usada.

```
sudo git branch -a
```

```
sudo git branch --track MOODLE_27_STABLE origin/MOODLE_27_STABLE
```

Para cerciorarnos, chequeamos la versión de Moodle especificada.

```
sudo git checkout MOODLE_27_STABLE
```

Ahora copiamos el directorio local de la carpeta de instalación *opt* al directorio */var/www/html/*, los archivos de Moodle al *webroot* y los cambios que se generen de la instalación de nuevas aplicaciones.

```
sudo cp -R /opt/moodle /var/www/html/
```

```
sudo mkdir /var/moodledata
```

```
sudo chown -R www-data /var/moodledata
```

```
sudo chmod -R 777 /var/moodledata
```

```
sudo chmod -R 0755 /var/www/html/moodle
```

Una vez finalizado el copiado de archivos, empezamos a cambiar el almacenamiento por defecto al *innodb*, para eso accedemos al *my.cnf* de MySQL.

```
sudo vi /etc/mysql/my.cnf
```

Cuando estemos dentro, presionamos la tecla *Insert*, y nos bajamos hasta llegar al apartado de `[mysqld]` y debajo de ella, en la sección configuraciones básicas, colocamos en la última línea el siguiente comando.

```
default-storage-engine = innodb
```

Presionamos *ESC* y guardamos la configuración con `:w` luego con `:q` salimos.

Reiniciamos el servidor MySQL para que los cambios surjan efectos.

```
sudo service mysql restart
```

Ahora crearemos la base de datos Moodle y el Moodle MySQL *User* con los permisos apropiados.

```
mysql -u root -p
```

NOTA: Cuando se pregunte por la contraseña, debemos colocar la contraseña que configuramos más arriba, aquella que fue para el *root* de MySQL.

```
CREATE DATABASE moodle DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;
```

Creamos el usuario y el *password* que se desee. Donde dice 'miusuario' y 'passusuario' es el nombre de la cuenta y el password respectivamente.

```
mysql> create user 'miusuario' IDENTIFIED BY 'passusuario';
```

```
mysql> GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE TEMPORARY TABLES,  
DROP,INDEX,ALTER ON moodle.* TO miusuario IDENTIFIED BY ' passusuario';
```

```
mysql> quit;
```

Ya con nuestro usuario creado en la base de datos, pondremos el *webroot* editable con el siguiente comando.

```
sudo chmod -R 777 /var/www/html/moodle
```

Ahora revertimos los permisos para que no sean editables por otro usuario.

```
sudo chmod -R 0755 /var/www/html/moodle
```

Finalmente, nos dirigimos a nuestro navegador de preferencia y nos iremos a la *ip* donde instalamos Moodle, en este caso <http://209.165.200.254/moodle>.

Cuando entremos, cambiamos la ruta para el Moodle data a `/var/moodledata`. El tipo de base de datos a elegir es `mysql`. Presionamos a siguiente y en las configuraciones de la base de datos debemos seleccionar los parámetros configurados previamente en la base de datos.

Host server: localhost

Database: moodle

User: miusuario

Password: passusuario

Tables Prefix: mdl_

Port: 3306

Presionamos siguiente y veremos el chequeo de todos los parámetros instalados de color verde, en caso de tener uno que no haya cumplido con los requisitos se mostrara de color rojo. Damos siguiente hasta llegar al apartado de crear el administrador de cuentas y del entorno Moodle. Nos saldrá un mensaje diciendo que ya hemos instalado por completo la aplicación web Moodle.

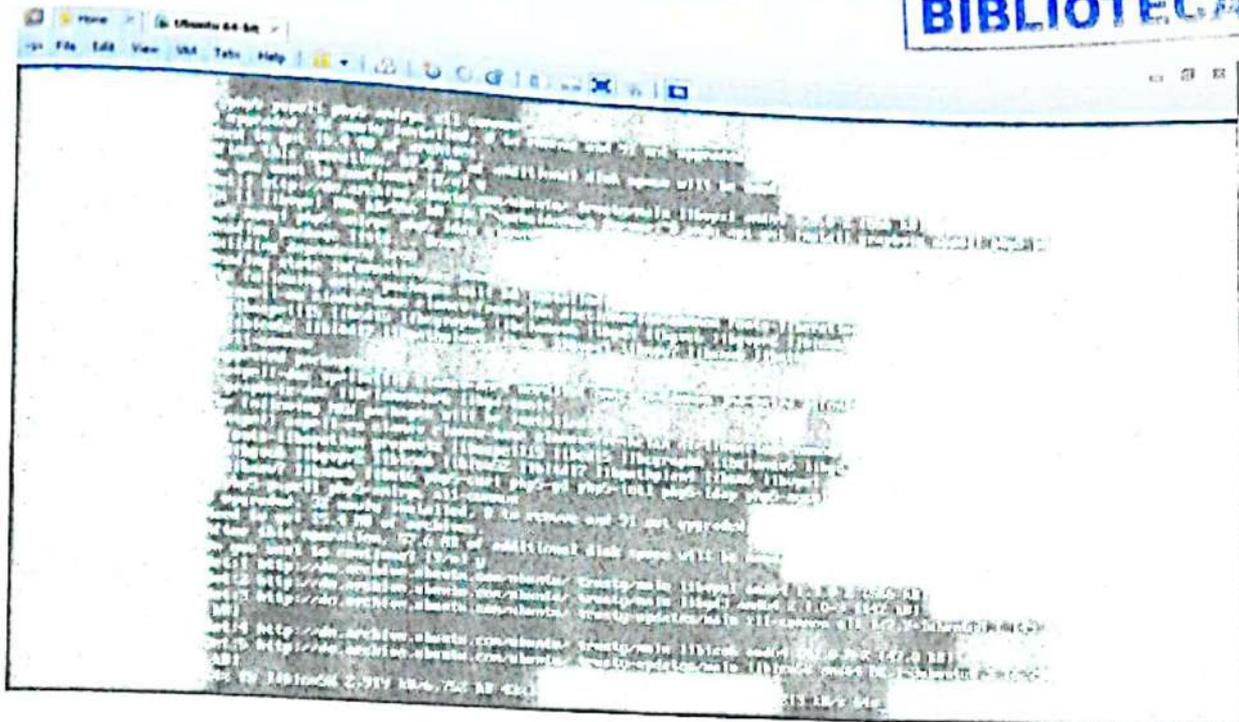


Ilustración 62. Proceso de descarga e instalación de los módulos de comunicación PHP.

Fuente: Imagen propia.

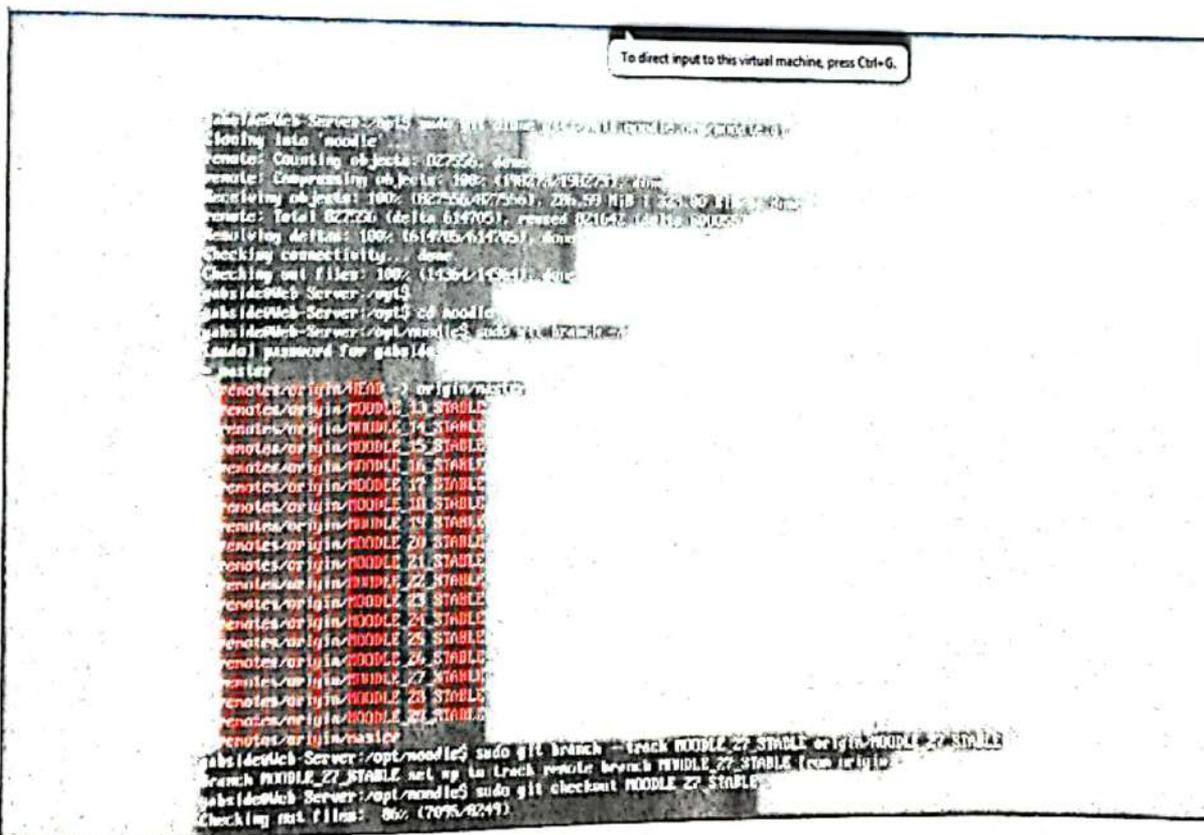


Ilustración 63. Reparación de ramas disponibles, rastreo y chequeo de la versión.

Fuente: Imagen propia.

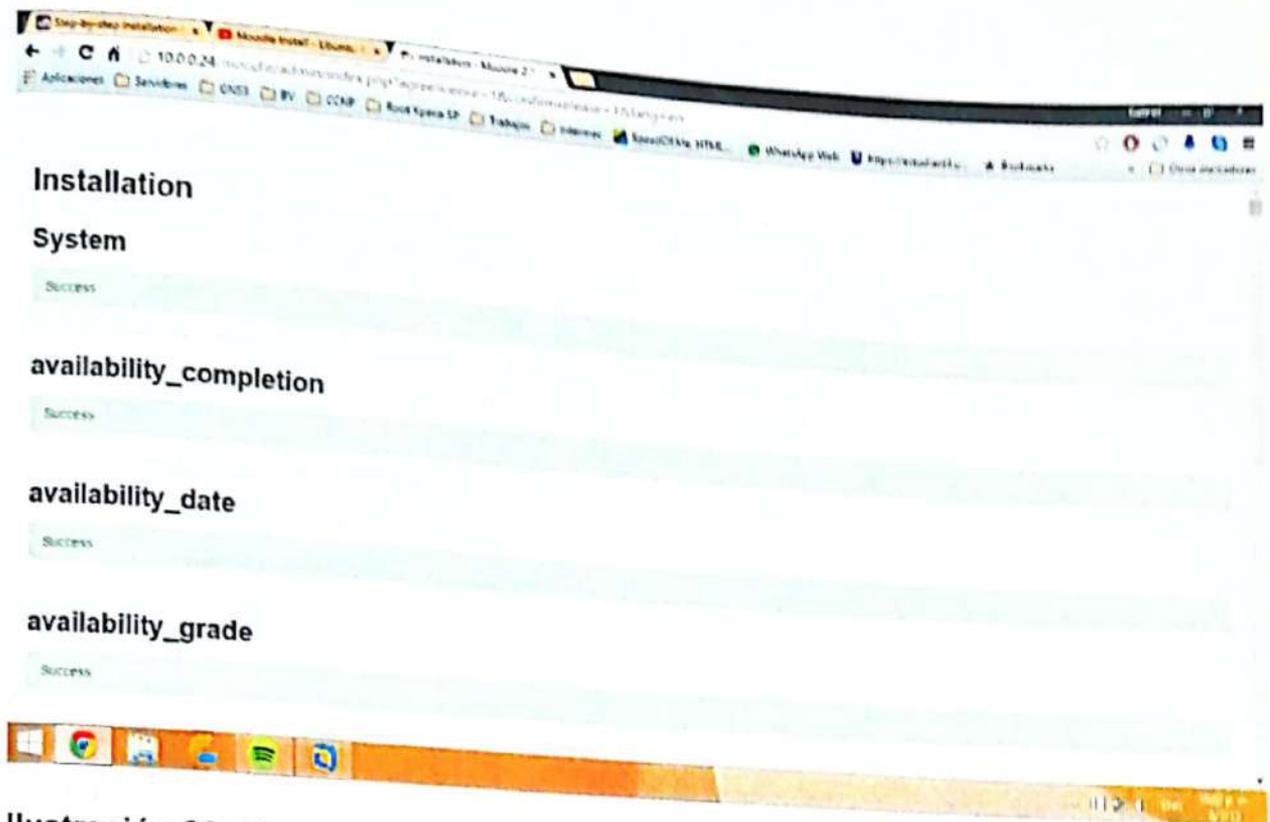


Ilustración 66. Chequeo de parámetros de correcta instalación de Moodle.

Fuente: Imagen propia.

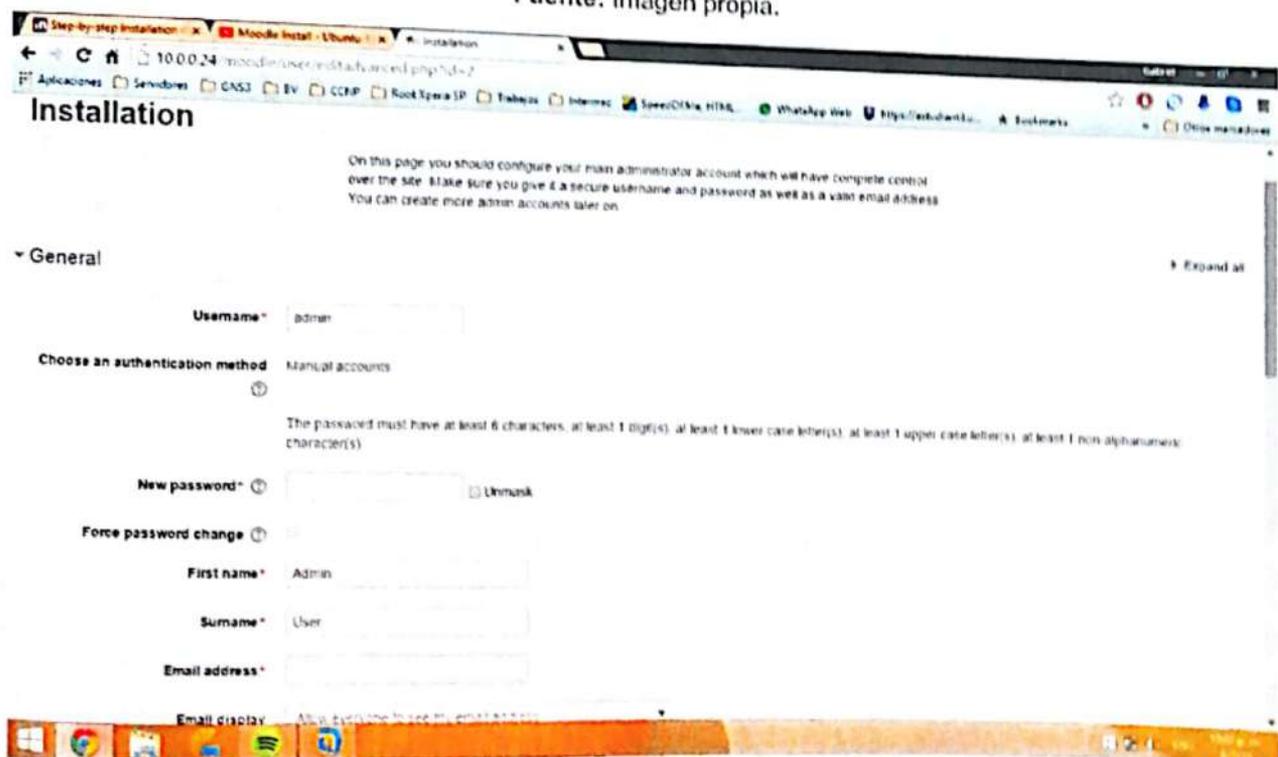


Ilustración 67. Creación de usuarios como administrador de cuentas y del sistema Moodle.

Fuente: Imagen propia.

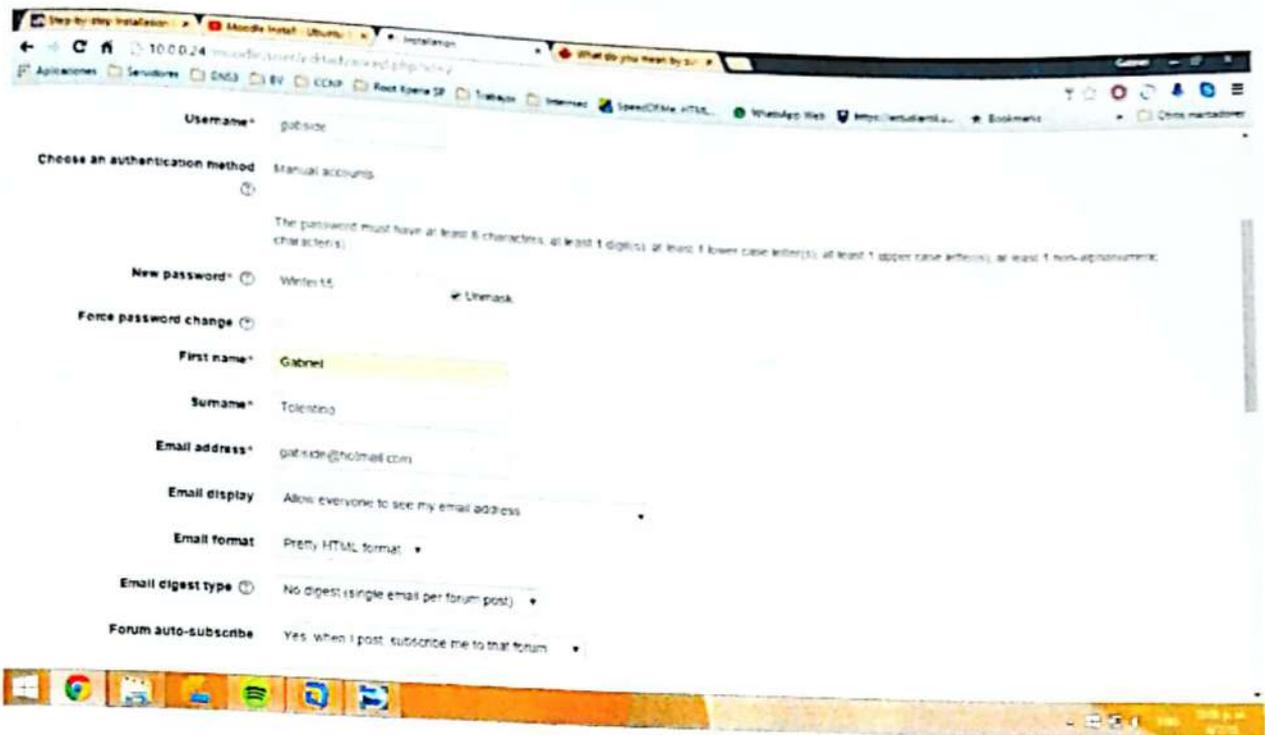


Ilustración 68. Creación de usuarios como administrador de cuentas y del sistema Moodle.

Fuente: Imagen propia.

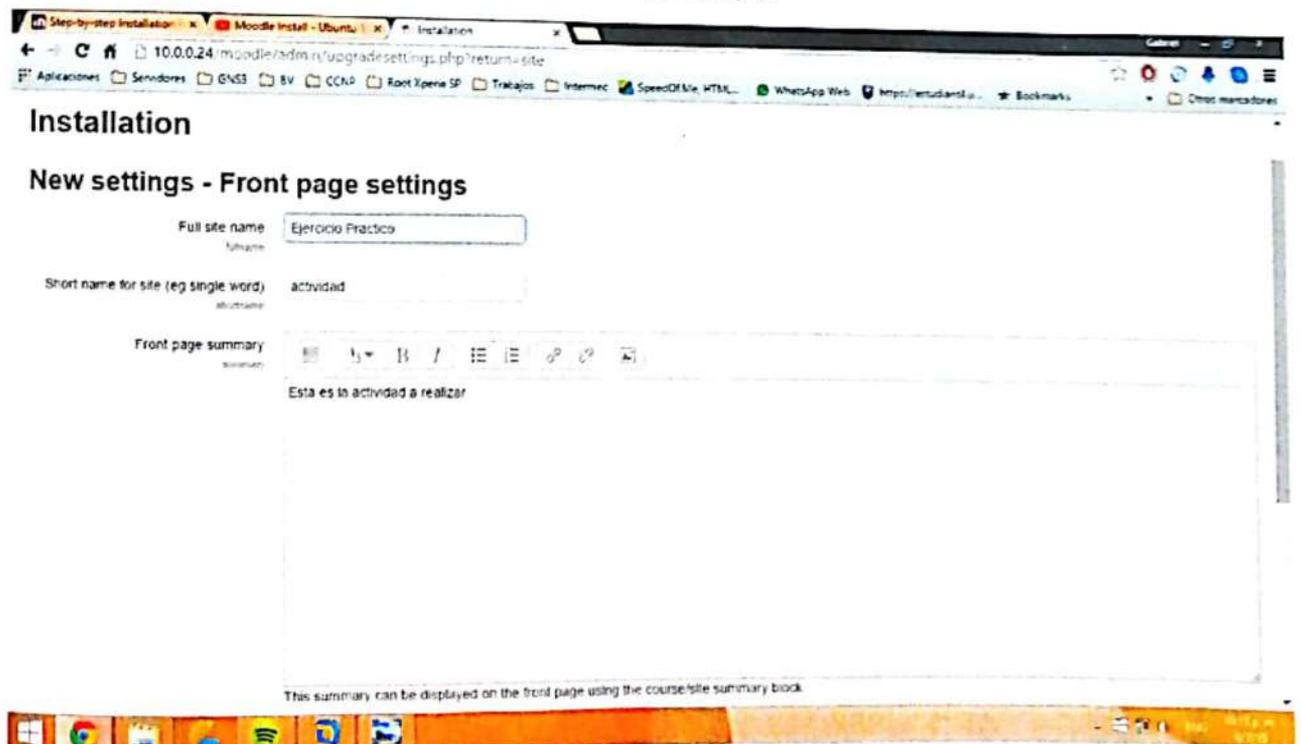


Ilustración 69. Configuración de la página frontal de Moodle. Requieren campos como el nombre completo de sitio, así como un nombre corto del mismo y un pequeño resumen.

Fuente: Imagen propia.

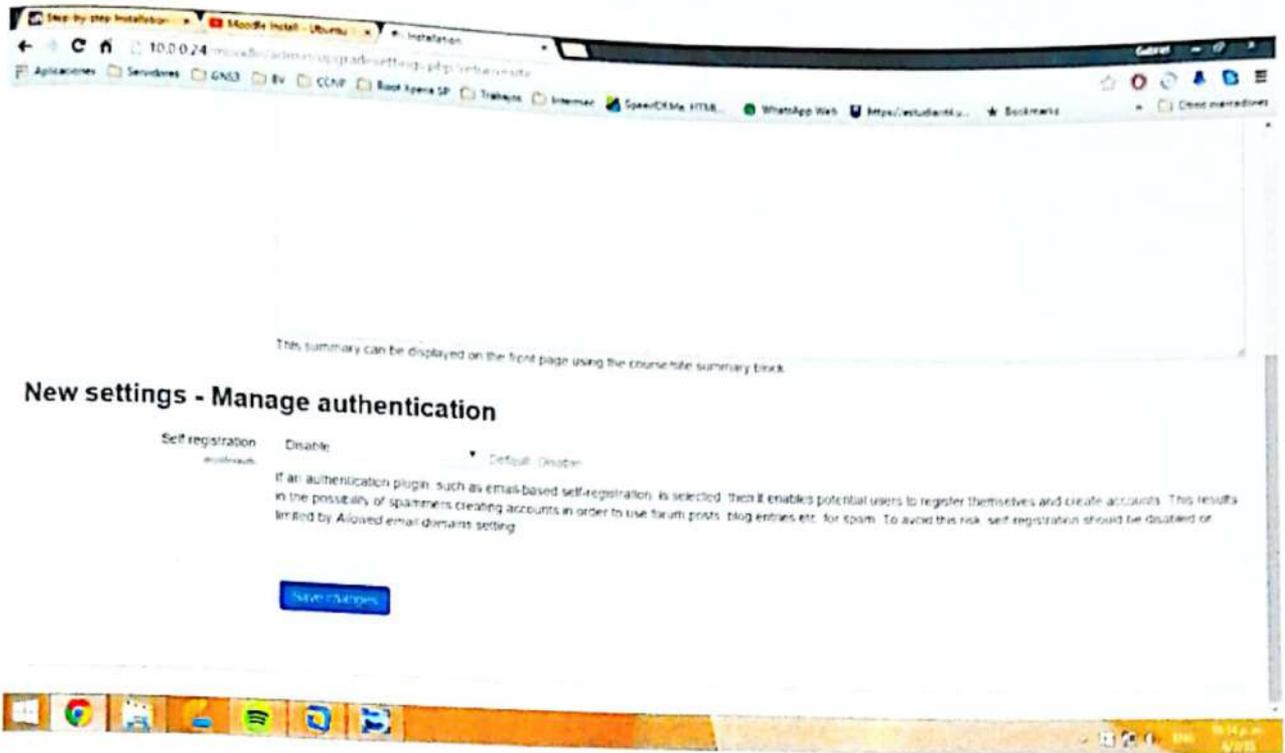


Ilustración 70. La administración de autenticación permite decidir cómo se desea configurar la registración de cuentas, si el usuario por su propia cuenta o si el por parte del administrador.

Fuente: Imagen propia.

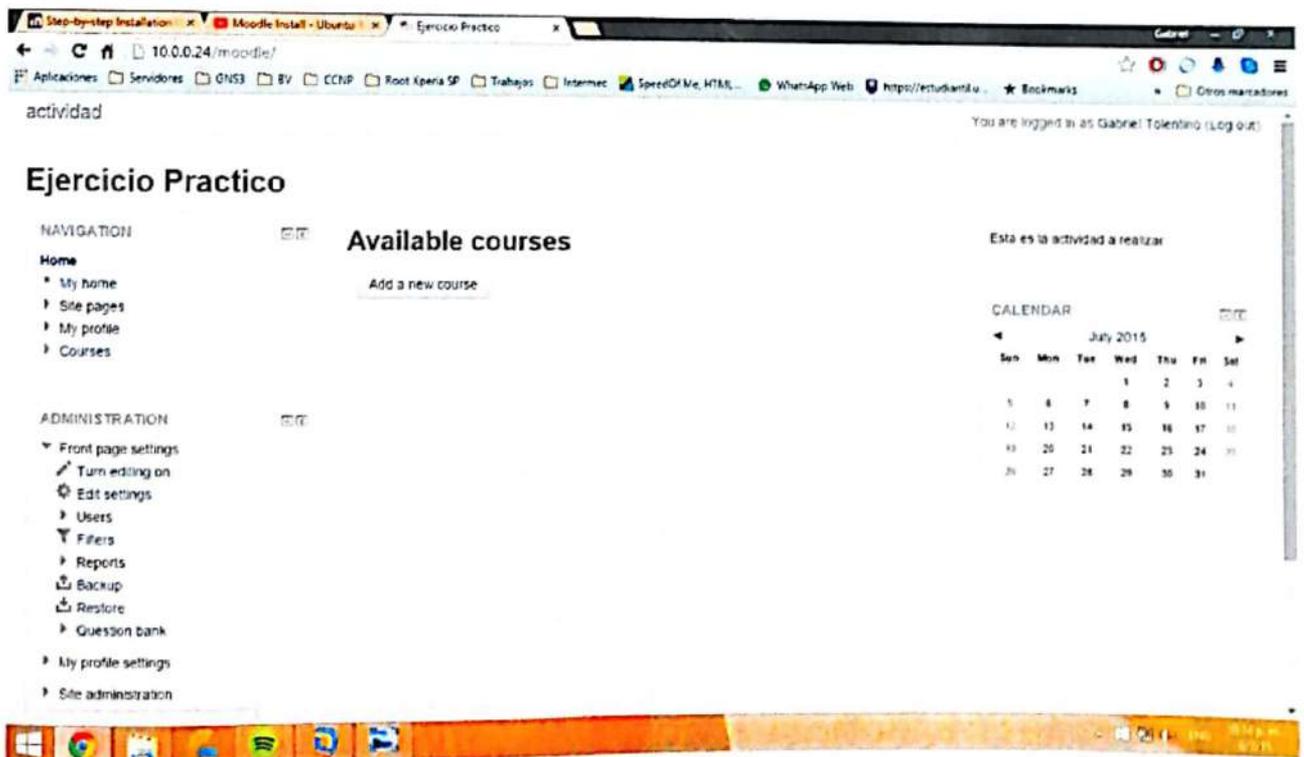


Ilustración 71. Moodle instalado y configurado. Página de inicio de Moodle.

Fuente: Imagen propia.

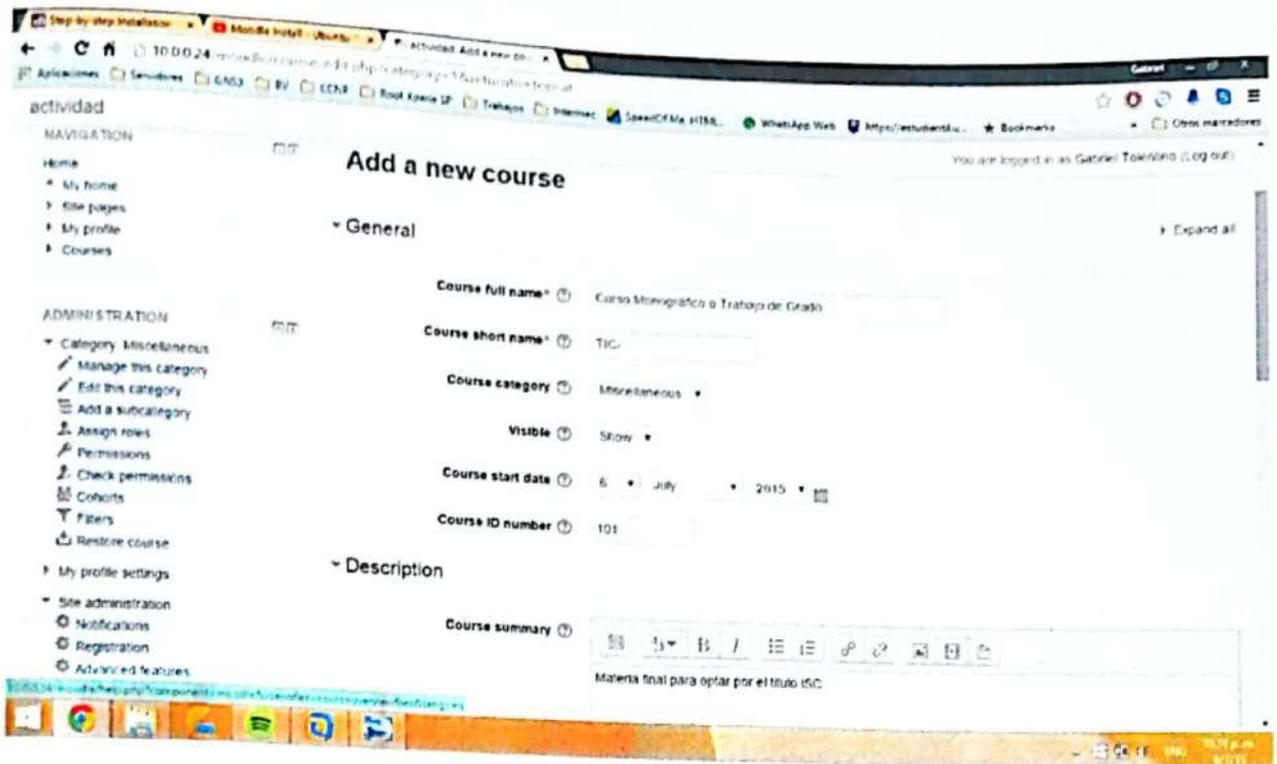


Ilustración 72. Configuración para la creación de un nuevo curso.

Fuente: Imagen propia.

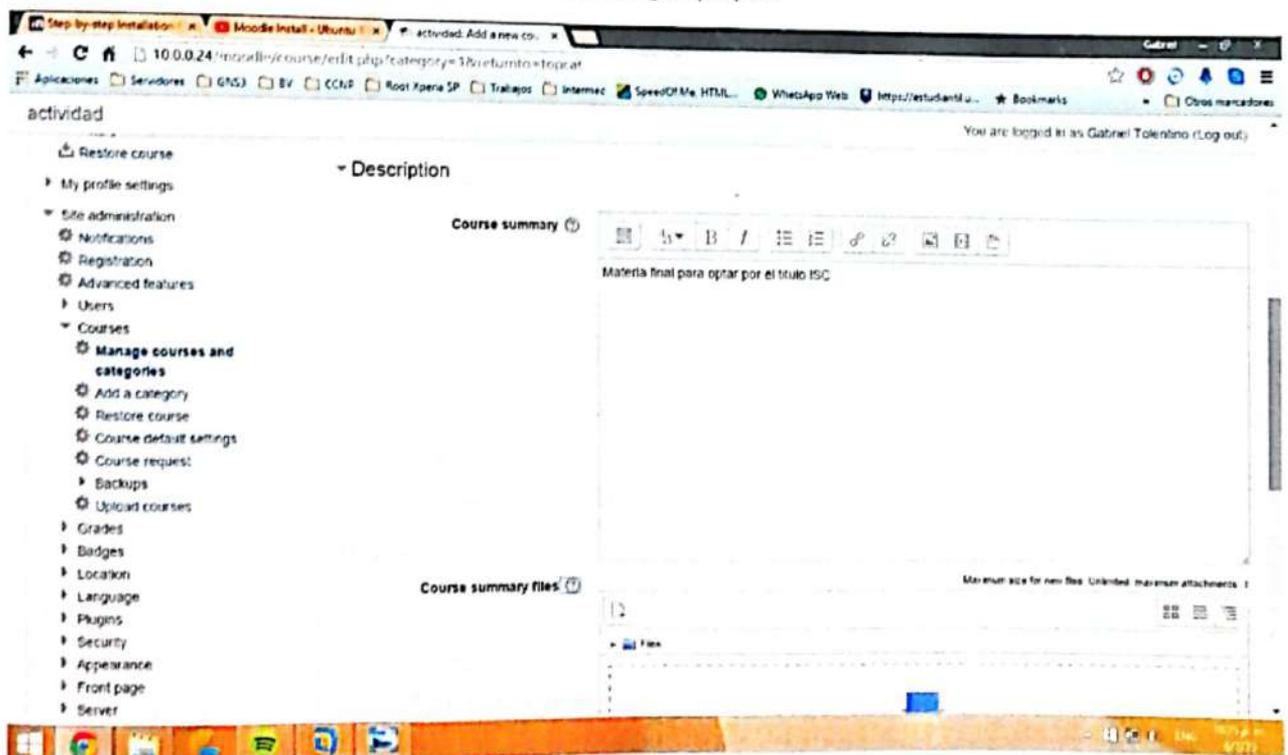


Ilustración 73. Descripción del curso y archivos a subir (PDF, Word, .JPG, etc.)

Fuente: Imagen propia.

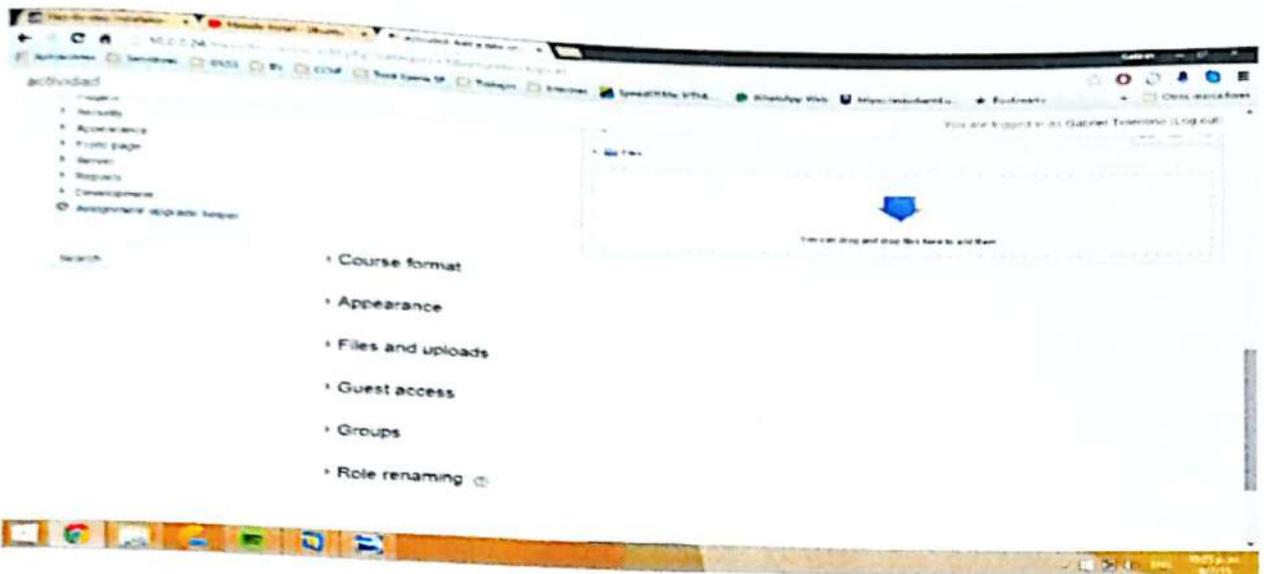


Ilustración 74. Se muestran más configuraciones para el curso a crear, como formato, apariencia, archivos y límites de tamaño de subida, acceso de invitado, grupos y roles asignados para quienes necesitan una descripción del rol de ese usuario.

Fuente: Imagen propia.

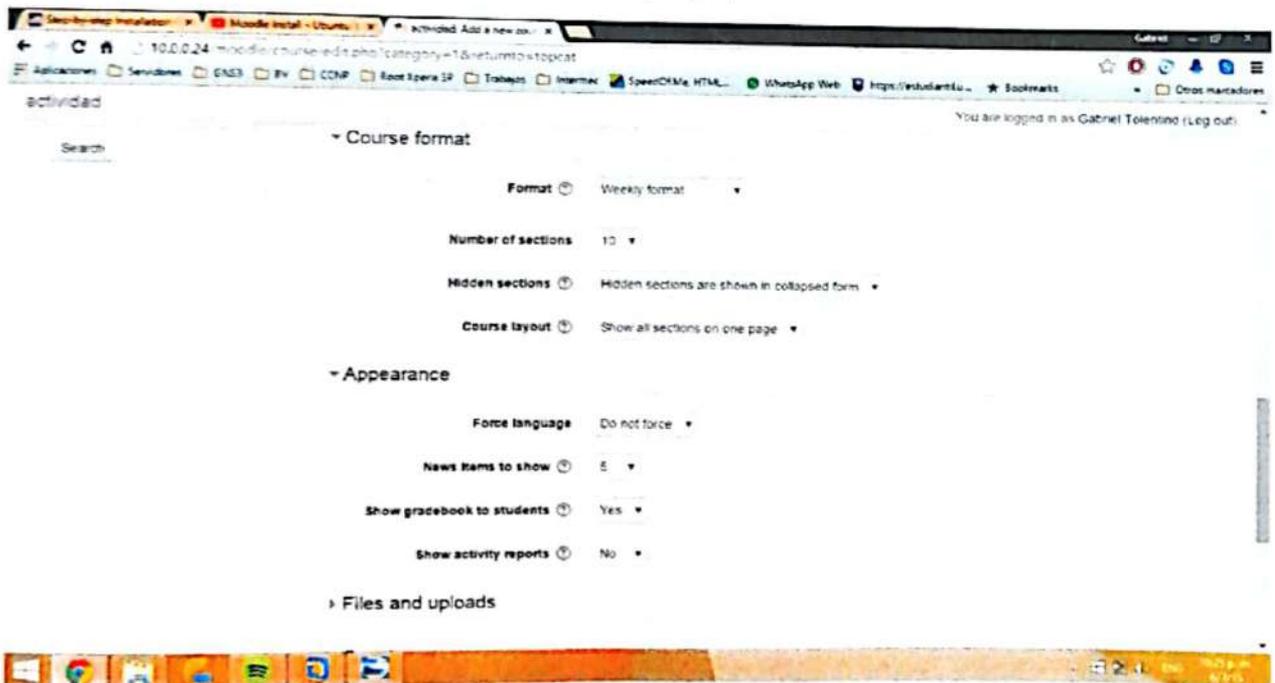


Ilustración 75. La opción para el formato permite especificar si se desea poner el curso como visible o no visible, también se especifica cuantas secciones se permiten a ese curso creado por tiempo definido. La apariencia configura que parámetros desees tener en tu entorno virtual.

Fuente: Imagen propia.



Ilustración 76. En *files and upload* puedo decidir qué tamaño de subida pueden los estudiantes y docentes subir al EVA, también presenta la opción de invitado para aquellos que pueden acceder al EVA temporalmente con o sin contraseña. La opción de grupo permite la interacción y realización de actividades en grupo.

Fuente: Imagen propia.

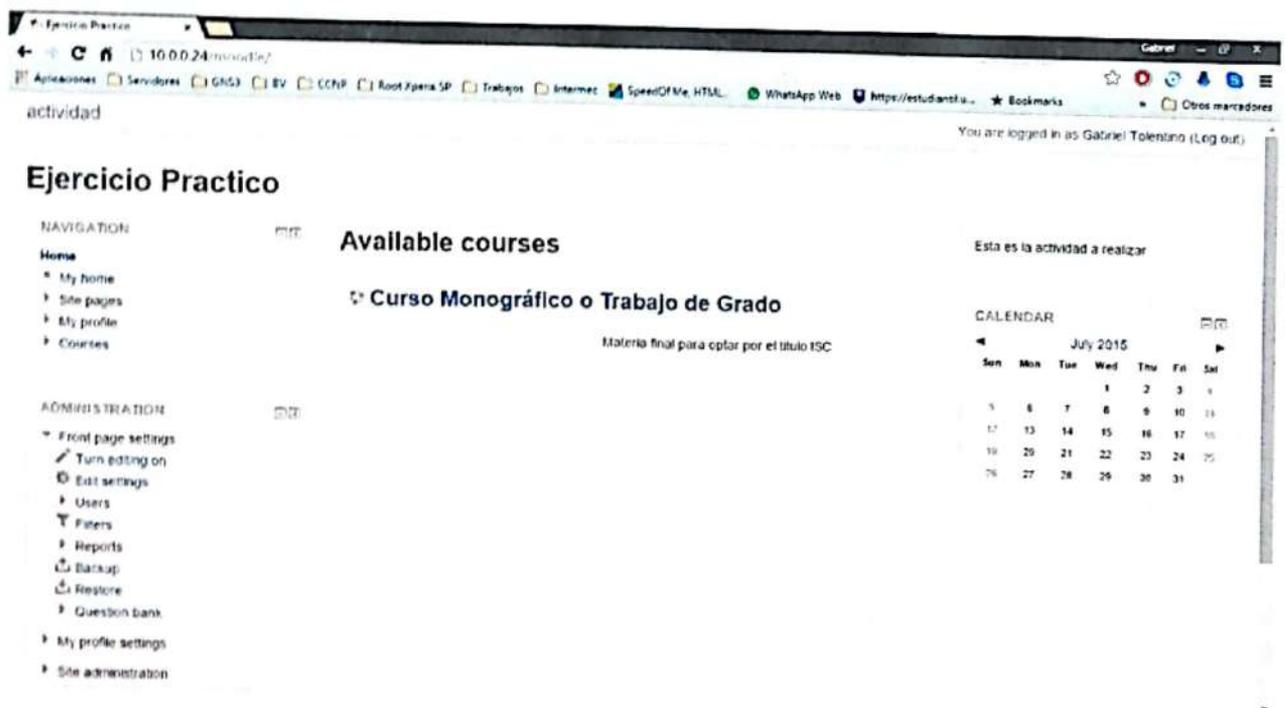


Ilustración 77. Esta es la página con los parámetros del curso creado.

Fuente: Imagen propia.

T180065

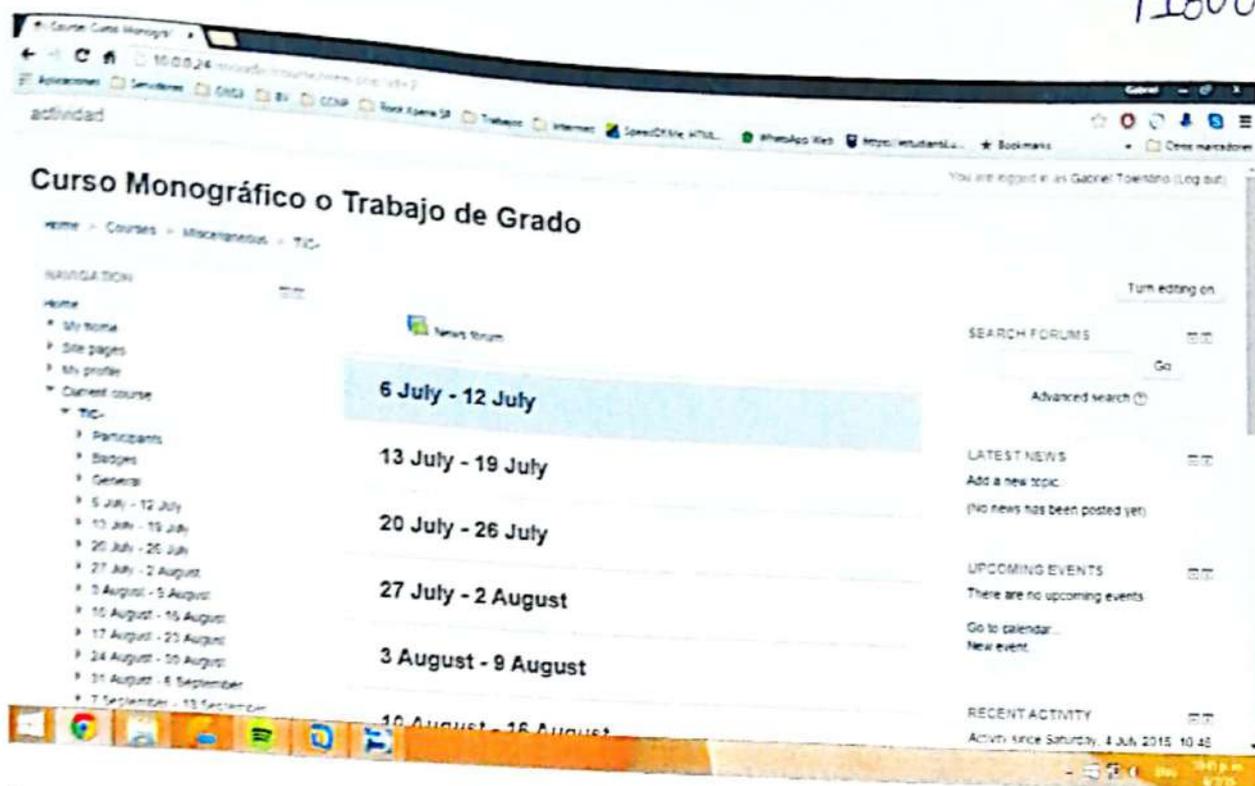


Ilustración 78. Esta es la página cuando accedemos al curso.

Fuente: Imagen propia.