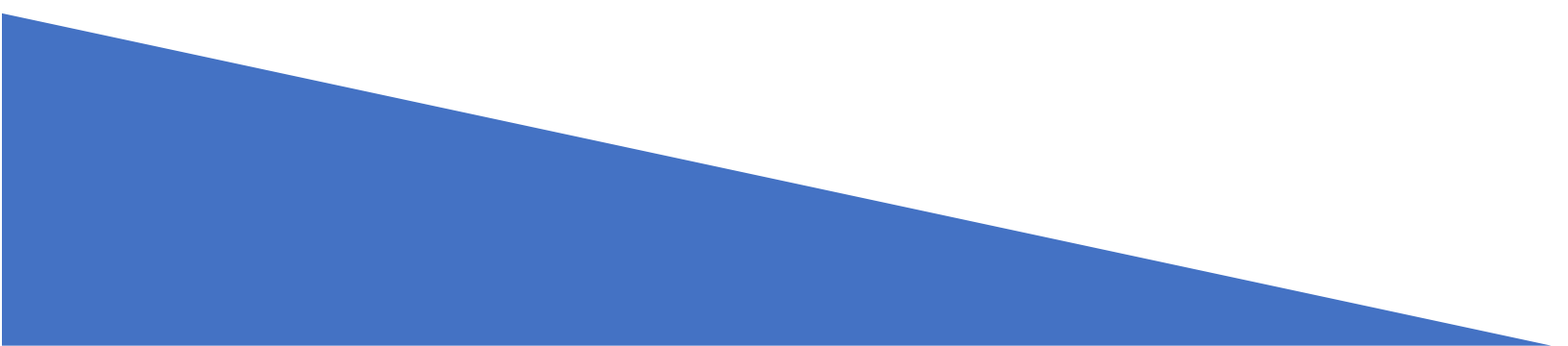


Digital Team

Diseño de Bajo Nivel

23/03/2022

Versión 1.3



Historial de revisiones

Autores:

Darien Miguel Sánchez Arévalo

Angel Alejandro Salinas García

Fernando De Luna Guardiola

Fecha	Versión	Descripción	Autor
18/03/2022	1.0	Elaboración Inicial del Diseño de Bajo Nivel	Darien Miguel Sánchez Arévalo
19/03/2022	1.1	Implementación de diseño y formato	Fernando de Luna Guardiola
21/03/2022	1.2	Elaboración de la instalación del software	Darien Miguel Sánchez Arévalo
22/03/2022	1.3	Últimos añadidos y retoques	Angel Alejandro Salinas García

Índice

1. Introducción	4
2. Objetivo	4
3. Antecedentes	5
4. Requerimientos de diseño	5
Figura 1. Mapa Central	6
Figura 2. Mapa E-R	7
5. Información General del Hardware	8
6. Información General de Software	8
6.1 Instalación de PHP	8
6.2 Instalación de IIS (Internet Information Services)	10
6.3 Configuración de IIS	11
6.4 Instalación de MySQL	12
7. Monitoreo	15
7.1 Monitoreo del Sistema Operativo de Windows	15
7.2 Métrica estándar por monitorear.	15
8. Licenciamiento	15
9. Redes	16
10. Sistema Operativo	17
11. Niveles de Servicio	18
12. Términos y Condiciones	19



1. Introducción

En el presente documento se presentará al cliente un diseño de bajo nivel (LLD) que tiene como propósito mostrar la implementación de dos máquinas virtuales: la página web y la base de datos, cada una adecuándose a los requerimientos pedidos por el mismo cliente.

Como se utilizó Microsoft Azure para montar las máquinas virtuales, ciertas configuraciones e infraestructura de red no las podemos cambiar, ni manipular el hardware físico, dado que accedemos a estas máquinas virtuales desde un servidor remoto.

Se verá las especificaciones de las máquinas virtuales, instalación y configuración de los softwares necesarios para su funcionamiento y también los cambios necesarios en los puertos.

También se contará con las especificaciones de la página web y también del gestor de base de datos que utilizaremos y toda la información referente a estas.

2. Objetivo

Para solucionar la problemática que nos solicitó el cliente, presentaremos las partes esenciales para su funcionamiento.

La página web se trata sobre un videojuego creado por la empresa, el juego consta de tres mapas, en donde cada uno cuenta con diferentes niveles y un jefe final, todos estos mapas el usuario los podrá disfrutar sin ninguna restricción, teniendo también la posibilidad de iniciar una partida con dos jugadores, así mismo, se tendrá toda la información como estadísticas de juego, fechas en las cuales jugaron, entre otras.

Al saber el fin de la página, entendemos la idea base y podemos empezar a trabajar en el diseño de la página web y la base de datos, para poder realizar lo que solicitó el cliente.

3. Antecedentes

Dado que este es el primer trabajo que Digital Team se está encargando en realizar, no está la posibilidad de compararlo con otros trabajos previos. Sin embargo, realizaremos la investigación necesaria para llevar a cabo estos tipos de páginas web y así poder implementar y desarrollar de una manera correcta.

4. Requerimientos de diseño

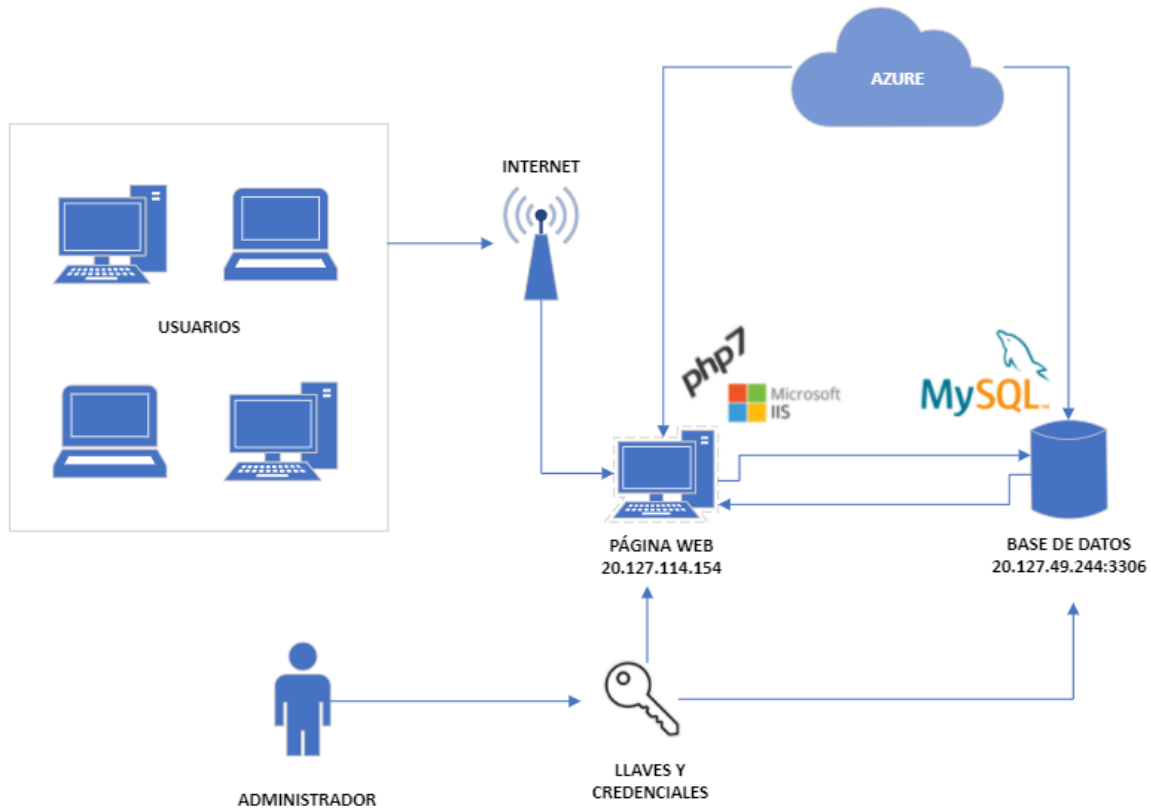
Utilizaremos el servicio de Azure para crear una máquina virtual donde se desarrollará y hospedará la aplicación web. Contará con un sistema operativo de Windows Server 2019 Datacenter, al mismo tiempo, éste tendrá una conexión con una base de datos externa que se hospedará también en los servicios de Azure. Se ha establecido, sin embargo, que se requiere de una división lógica entre 3 partes específicas del producto:

Como se ha mencionado anteriormente, utilizaremos una base de datos para almacenar la información que se genere del sistema, para esto se utilizará una base de datos en MySQL

Por otra parte, el sistema contará con un backend que se encargará de comunicarse con la base de datos y así realizar el intercambio entre la información almacenada.

Finalmente, la interfaz gráfica de usuario, que se encargará de la captura de la información mediante los eventos que el mismo usuario activará.

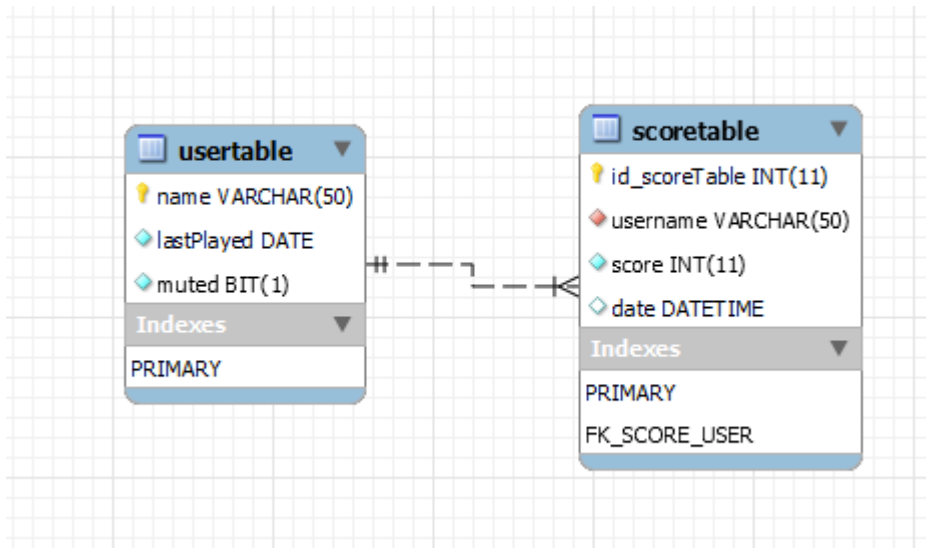
Figura 1. Mapa Central



Dentro de la arquitectura, debe planearse un modelo lógico que permita ingresar y almacenar los datos que se manejarán en nuestra página y que se estarán mostrando al cliente.

Una idea de este modelo se plantea en el siguiente diagrama E-R.

Figura 2. Mapa E-R



Dado que la página es únicamente para jugar, simplificamos la base de datos donde solo hay dos tablas: usuarios y puntuaciones.

5. Información General del Hardware

Máquina Virtual Página Web / Base de Datos	
Procesador	Intel Xeon Platinum
RAM	16 GB
Almacenamiento	127 GB
vCPU	2
Discos de Datos	4

6. Información General de Software

Para Página Web:

Versión PHP	7.4.28, VC15 x86 Non-Thread Safe
Versión IIS	10.0.17763.1

6.1 Instalación de PHP

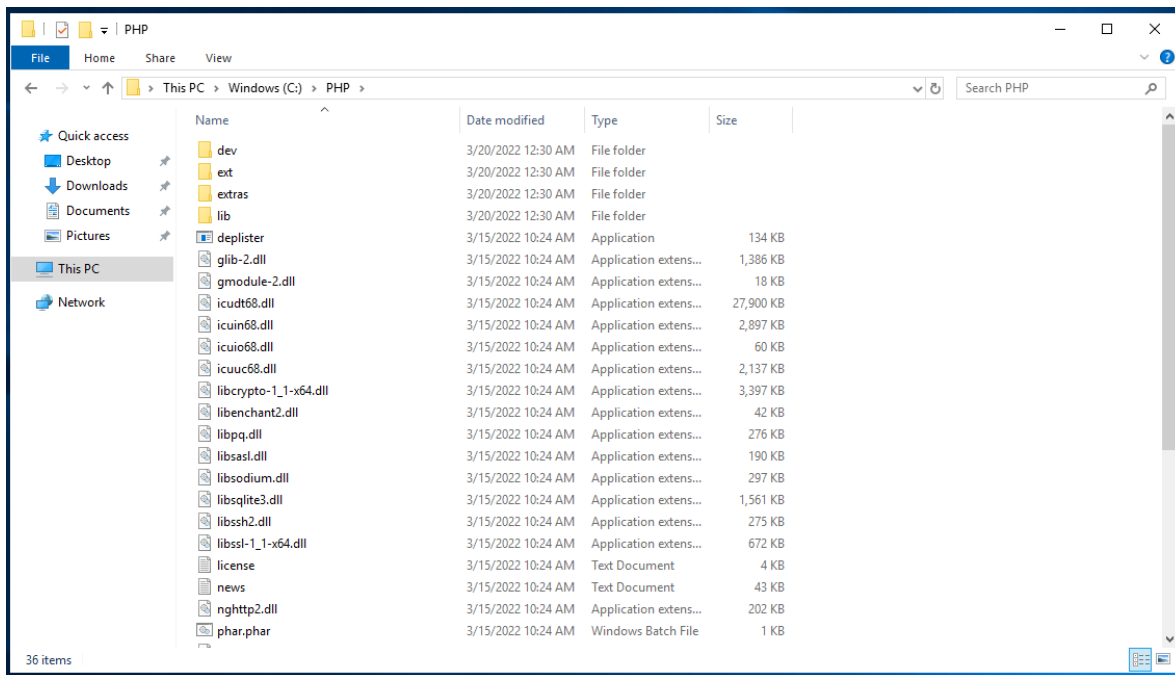
Para instalar *PHP* en la máquina virtual debemos acceder a su [página oficial](#) para descargar los recursos necesarios. En nuestro caso queremos utilizar la versión 7.4.28 y de los que nos presentan, elegiremos este [zip](#).

```
VC15 x86 Non Thread Safe (2022-Feb-24 17:53:21)
  Zip [23.15MB]
  sha256: 3e1721390f0262b5b1c710047f92a60b3668412bdf282a9130eab15ab38c4fca
```

* Si está utilizando *PHP* como *FastCGI* con *IIS*, debe usar las versiones de *PHP Non Thread Safe (NTS)*. *

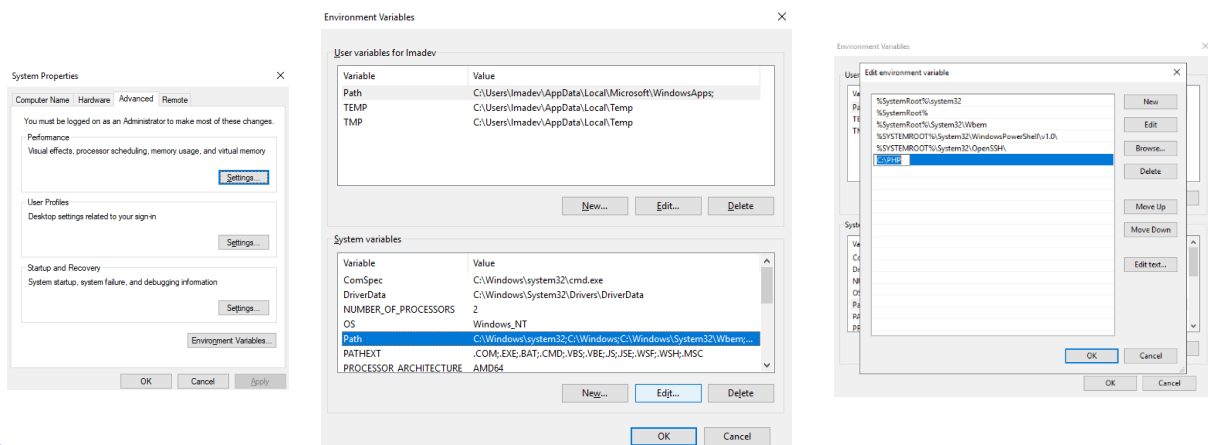
Ahora, necesitamos las librerías para compilar las versiones de *PHP*. Necesitamos la VC15 en x86. [Se descarga aquí](#).

Ahora que ya descargamos lo necesario, creamos una carpeta llamada “*PHP*” localizada en C:\ y extraemos todos los archivos del .zip que descargamos. Debe de verse así:



Lo siguiente que debemos hacer es instalar VC15, ejecutamos el .exe y lo instalamos, no es muy complejo los pasos para la instalación.

Ahora debemos crear la variable de entorno para manejar *PHP*. Abrimos la barra de búsqueda de Windows y escribimos “*Variables*” y seleccionamos la opción “*Edit the system environment variables*”. Se nos abrirá una ventana de “*System Properties*” y clickeamos “*Environment Variables...*”, a continuación, seleccionamos “*Path*” y le damos al botón de “*Edit*” y agregamos la ruta donde instalamos *PHP*, en nuestro caso es: C:\PHP.



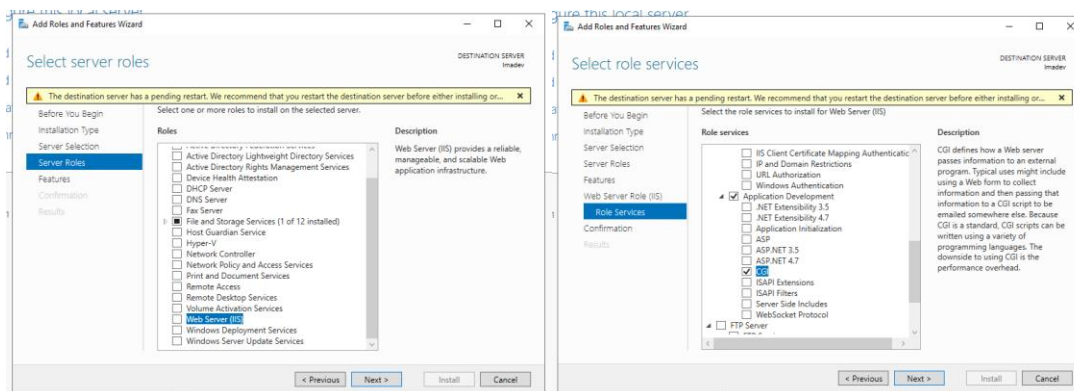
Para finalizar la instalación, vamos a C:\PHP y buscamos el archivo llamado “*php.ini-production*” y lo renombramos como “*php.ini*”. Abrimos el archivo y cambiamos ciertas configuraciones que nos interesan.

```
date.timezone = America/Sao_Paulo
fastcgi.impersonate = 1
cgi.fix_pathinfo=1
cgi.force_redirect = 0
extension_dir = "ext"
extension=bz2
extension=curl
extension=gd2
extension=ldap
extension=mbstring
extension=mysqli
extension=openssl
```

¡Y listo! Hemos terminado de instalar PHP en la máquina virtual.

6.2 Instalación de IIS (Internet Information Services).

Abrimos la aplicación “*Server Manager*” y seleccionamos “*Add roles and features*”. Cuando lleguemos a la parte de “*Server Roles*”, debemos asegurarnos de seleccionar “*Web Server (IIS)*”, ya que nos proporcionará una infraestructura de aplicaciones web confiable, manejable y escalable. En “*Role Services*” de “*Web Server Role (IIS)*” debemos marcar la casilla de “*CGI*”, que define como un servidor web pasa información a un programa externo.

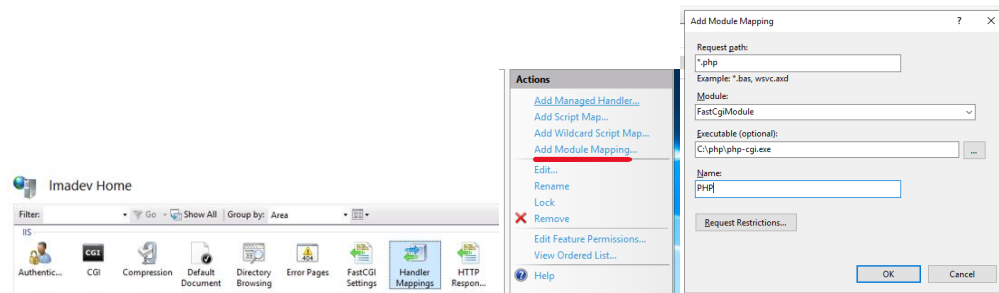


Una vez que estemos asegurados de haber seleccionado los puntos anteriores, continuamos con los pasos hasta terminar la instalación.

6.3 Configuración de IIS.

Una vez instalado, debemos configurar ciertas cosas para poder trabajar con *PHP*.

Abrimos la aplicación de *IIS* y seleccionamos el servidor, en nuestro caso es “*Imadev*” y seleccionamos “*Handler Mappings*” y entonces “*Add Module Mapping*” y lo llenamos con la siguiente información:



Entramos a “*Request Restrictions...*” y en la nueva ventana seleccionamos el Radio Button que dice “*File or folder*” y le damos Ok.

Con esto, ahora podremos ejecutar correctamente código *PHP* en nuestra aplicación web. Una configuración extra es entrar a “*Default Document*” y agregar “*index.php*” para que el archivo llamado “*index.php*” sea lo que se ejecute por defecto al entrar al dominio web.

Por último: la carpeta donde se almacenan los archivos de la página web se encuentran en *C:\inetpub\wwwroot* (Aparece una vez instalado *IIS*). Eliminamos los archivos predeterminados dentro de la carpeta *wwwroot* y movemos los archivos de nuestra página web ahí mismo.

Para Base de Datos:

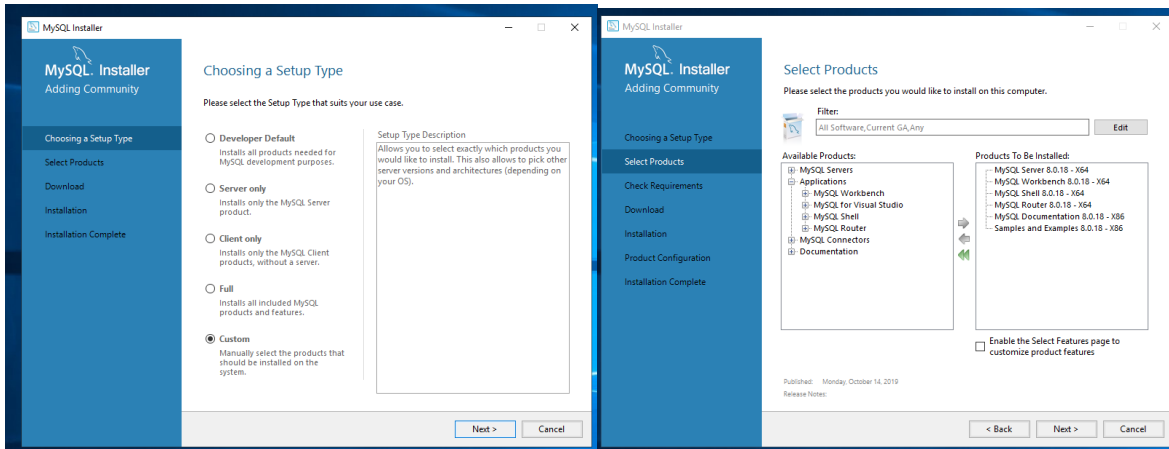
MySQL Server	8.0.18 – x64
MySQL Workbench	8.0.18 – x64
MySQL Shell	8.0.18 – x64
MySQL Router	8.0.18 – x64

6.4 Instalación de MySQL

Primeramente, debemos descargar el instalador de MySQL para Windows, lo podemos [descargar aquí](#).

Una vez abierto el instalador nos mostrará qué tipo de instalación queremos, en nuestro caso elegimos la opción “Custom” para hacer una instalación personalizada y elegir las herramientas que necesitamos.

A continuación se ve los productos que instalaremos en nuestra máquina virtual:



¿Qué hacen esos programas?

MySQL Server es el programa donde habilita todas las funciones de la base de datos y hacer posible la creación de tablas, queries, entre otras cosas.

MySQL Workbench es una herramienta de diseño de bases de datos visuales que integra el desarrollo, la administración, el diseño, la creación y el mantenimiento de bases de datos SQL en un único entorno de desarrollo integrado para el sistema de bases de datos MySQL

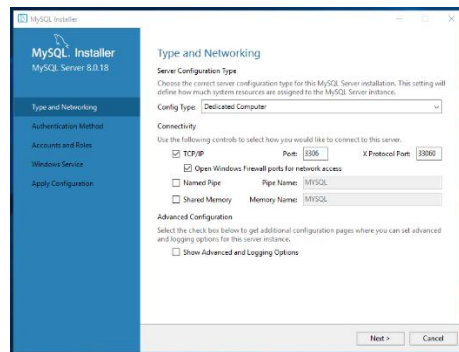
MySQL Shell es un cliente avanzado y editor de código para MySQL. Proporciona capacidades de scripting para JavaScript y Python e incluye API para trabajar con MySQL

MySQL Router es un middleware ligero que proporciona enrutamiento transparente entre su aplicación y cualquier servidor MySQL backend.

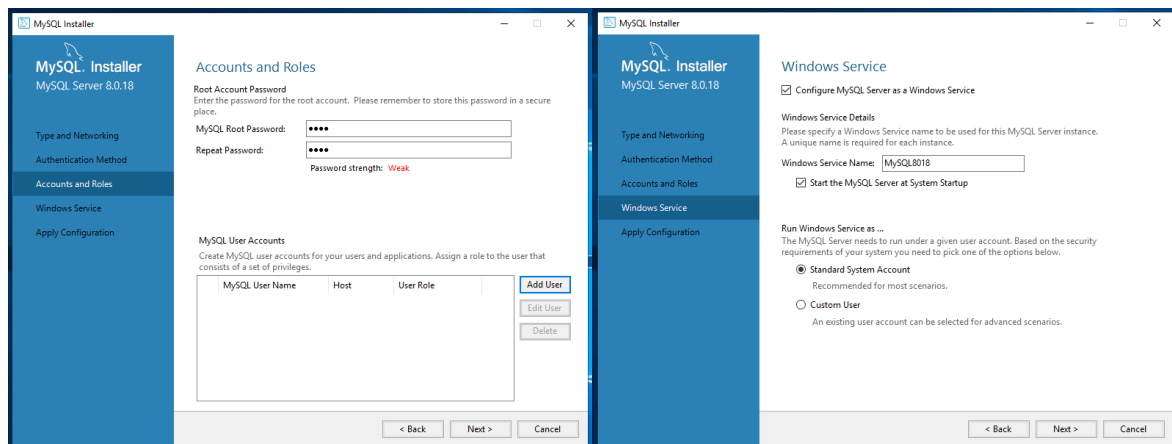
Proseguimos con la instalación, es posible que le pidan instalar programas adicionales (VC16 en nuestro caso) para el correcto funcionamiento de los programas.

En “*Type and Networking*” debemos elegir ciertas configuraciones, en nuestro caso elegimos “*Dedicated Computer*” para que todos los recursos se operen en la base de datos, hay otras opciones por si hay aplicaciones adicionales en la máquina virtual y limitar los recursos que agarra MySQL.

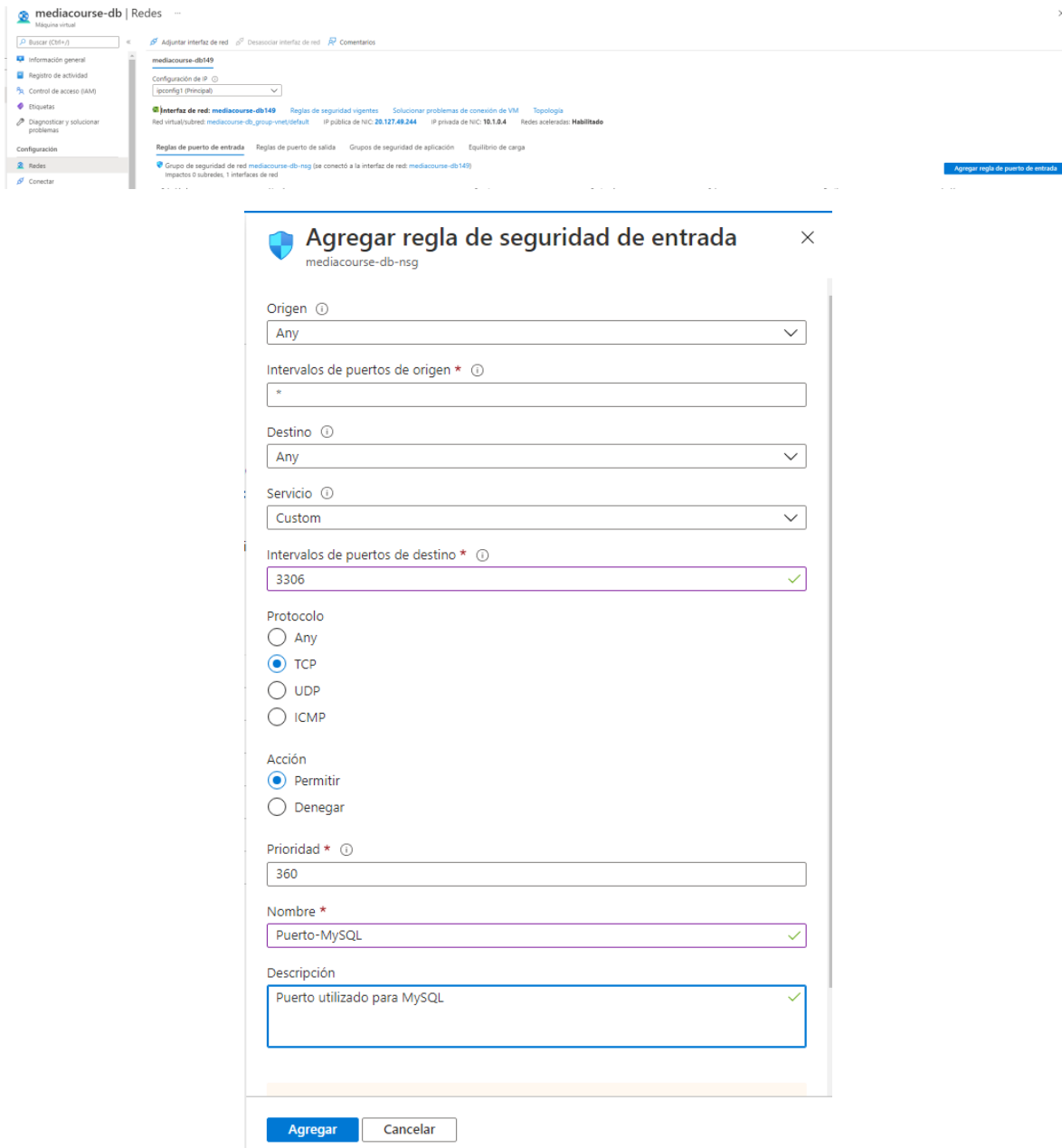
El puerto predeterminado que se suele usar para MySQL es el 3306, nosotros dejamos ese mismo. El protocolo que usa es *TCP/IP* y es importante saber esto.



Elegimos la contraseña con la que nos conectaremos con la cuenta principal (root), determinamos como queremos que se llame el servicio de Windows de MySQL (MySQL 8018) y continuamos con los pasos hasta terminar la instalación.



Por último, necesitamos abrir el puerto 3306 en la máquina virtual, en nuestro caso utilizamos Azure, así que en el *Dashboard* nos vamos a “Redes” y “Agregar regla de puerto de entrada” y lo llenamos con los siguientes datos:



The screenshot shows the Azure portal interface for a virtual machine named 'mediacourse-db'. The 'Redes' (Network) section is active, and the 'Agregar regla de seguridad de entrada' (Add inbound security rule) dialog is open. The dialog contains the following fields and values:

- Origen** (Origin): Any
- Intervalos de puertos de origen** (Intervals of origin ports): *
- Destino** (Destination): Any
- Servicio** (Service): Custom
- Intervalos de puertos de destino** (Intervals of destination ports): 3306
- Protocolo** (Protocol): TCP
- Acción** (Action): Permitir (Allow)
- Prioridad** (Priority): 360
- Nombre** (Name): Puerto-MySQL
- Descripción** (Description): Puerto utilizado para MySQL

The 'Agregar' (Add) button is highlighted in blue, indicating the rule has been successfully added.

Y listo, al agregar el puerto ya se puede conectar a la base de datos.

7. Monitoreo

7.1 Monitoreo del Sistema Operativo de Windows

Al utilizar los servicios que nos ofrece Microsoft Azure, nos ofrece un Dashboard donde podemos ver diferentes métricas y estadísticas para llevar a cabo un correcto monitoreo y mantenimiento de las máquinas virtuales.

7.2 Métrica estándar por monitorear.

Las métricas que más se consideran importantes a monitorear son las siguientes:

- Porcentaje de utilización de la CPU.
- Entrada de red (bytes)
- Salida de red (bytes)
- Lecturas de disco (bytes)
- Escrituras de disco (bytes)

Se necesitará de una cuenta para poder monitorear las máquinas virtuales.

8. Licenciamiento

Al utilizar Microsoft Azure, ya nos otorga la licencia del sistema operativo que se desea utilizar, en nuestro caso es Windows Server 2019 Datacenter.

9. Redes

A continuación, se mostrarán las siguientes direcciones y seguridad agregada a los equipos que se utilizarán. Todas éstas fueron dadas por Microsoft Azure.

Máquina Virtual Página Web

WINDOWS SERVER 2019 DATACENTER	
IPv4 Pública	20.127.114.154
DNS IPv4 Pública	mediacourse.eastus.cloudapp.azure.com
ID Subred	Imadev_group-vnet/default

SEGURIDAD		
Puerto	Nombre	Protocolo
3389	RDP	TCP
80	HTTP	TCP
443	HTTPS	TCP

Máquina Virtual Base de Datos

WINDOWS SERVER 2019 DATACENTER	
IPv4 Pública	20.127.49.244
DNS IPv4 Pública	mediacourse-db.eastus.cloudapp.azure.com
ID Subred	mediacourse-db_group-vnet/default

SEGURIDAD		
Puerto	Nombre	Protocolo
3389	RDP	TCP
80	HTTP	TCP
443	HTTPS	TCP
3306	MYSQL	TCP

10. Sistema Operativo

El Sistema Operativo que utilizaremos será Windows Server, el cuál es una distribución de Microsoft para el uso de servidores. Utilizaremos la versión Windows Server 2019 Datacenter. La edición Datacenter está optimizada para la virtualización a gran escala; su licencia permite que un servidor ejecute un número ilimitado de instancias de Windows Server.

11. Niveles de Servicio

Componentes	Descripción del componente	Compromiso	Unidad	Periodo	Observaciones / Condiciones
Monitoreo	Recolección de información de la máquina virtual.	100%	Minutos	Mensual	Incluye monitoreo del rendimiento del servidor. Los diagnósticos deberán ser monitoreados desde dentro de la máquina
Almacenamiento de Puntuaciones	Tiempo en el que se solicita información de los puntajes y su tiempo de respuesta.	100%	Días	Semanal	Cada que sea posible, se aplicará una optimización, que será aplicada desde dentro de la máquina.
Atención de solicitudes de servicio	Solicitud de cambio que requiera la carga del juego.	90~%	Evento	-----	Los tiempos de atención y solución dependerá del grado de incidente registrado o detectado al centro de atención.
	Solicitud de cambio que requiera el cambio de vista de las puntuaciones.	90~%	Evento		
	Solicitud de cambio que añada los cambios del cliente.	90~%	Evento		

DEFINICIÓN DE TIEMPOS	
Atención	El tiempo mínimo desde que el cliente ha enviado el correo correspondiente y/o generación de una solicitud.
Respuesta	Entre el tiempo mínimo y medio, dependiendo la cantidad de pedidos que se hayan generado anteriormente y que no han sido respondidos aún.
Solución	Entre el tiempo mínimo y medio, dependiendo la urgencia y actividad que el cliente ha solicitado, además de las solicitudes que aún están en cola.

12. Términos y Condiciones

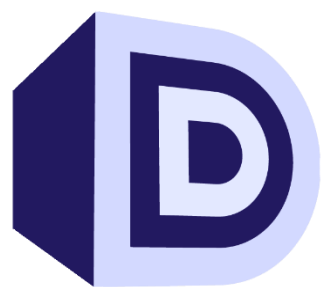
Todas las modificaciones, cambios o mantenimiento que se hicieron durante el desarrollo del trabajo, se realizaron bajo el nombre de Digital Team.

La configuración hasta el fin del desarrollo será decidida y ejecutada por Digital Team, una vez activada será ejecutada por el cliente, con la posibilidad de comunicarse con nosotros.

Para la configuración y monitoreo se debe ejecutar una sesión para ingresar a la cuenta de Microsoft Azure y visualizar el dashboard con los datos a monitorear.

La configuración y gestión de la página web será ejecutada por parte de la empresa, una vez activada será ejecutada por el cliente.

La administración y gestión de la base de datos será ejecutada por parte de la empresa.



Digital Team

Políticas de Seguridad

22/05/2022

Versión 1.0

Historial de revisiones

Autores:

Darien Miguel Sánchez Arévalo

Angel Alejandro Salinas García

Fernando De Luna Guardiola

Fecha	Versión	Descripción	Autor
22/05/2022	1.0	Elaboración Inicial del Documento	Darien Miguel Sánchez Arévalo

1. Introducción.	4
1.1 Objetivo y ámbito de la aplicación.	4
2. Glosario.	5
3. Seguridad Perimetral.	7
4. DRP (Plan de Recuperación de Desastres)	8
4.1 Análisis de riesgos	8
4.2 Análisis de brecha	9
5. BCP (Plan de Continuidad Empresarial)	10
5.1 Ámbito y objetivos.	10
5.2 Operaciones en riesgo.	10
5.3 Estrategia de recuperación	11
5.4 Funciones y responsabilidades	11

1.Introducción.

El presente documento tiene como objetivo ser una guía de apoyo para dar a conocer las reglas de seguridad que se tomarán con los recursos de la plataforma, en caso de que haya algún inconveniente y aclarar como actuaremos en estos casos. También veremos las distintas medidas de seguridad que implementamos.

1.1 Objetivo y ámbito de la aplicación.

El presente apartado del Documento de Seguridad para la Protección de Datos en Videojuegos y Privacidad tiene por objetivo establecer las directrices y actividades para la generación de cada uno de los elementos que conforman el Documento de Seguridad para la protección de los datos personales.

Considerando los siguientes artículos:

Artículo 6. Se refiere que la vida privada y los datos personales serán protegidos con las excepciones que fijen las leyes correspondientes.

Artículo 16. Señala que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición al uso de su información personal, en los términos que dije la ley, la cual establecerá los supuestos de excepción de principios de orden público, seguridad y salud pública o para proteger los derechos de terceros.

Artículo 33. Se establecen las actividades interrelacionadas que deben realizar los responsables para establecer y mantener las medidas de seguridad para la protección de los datos personales.

2. Glosario.

Documento de Seguridad. Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Datos personales. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Seguridad Perimetral. Un perímetro de red es el límite seguro entre el lado privado y administrado localmente de una red, a menudo la intranet de una empresa, y el lado público de una red, a menudo Internet.

Firewall. En informática, un cortafuegos es la parte de un sistema o una red informáticos que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

IPS. Un sistema de prevención de intrusos es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

IDS. Un sistema de detección de intrusiones es un programa de detección de accesos no autorizados a un computador o a una red.

Microsoft Azure. Microsoft Azure es un servicio de computación en la nube creado por Microsoft para construir, probar, desplegar y administrar aplicaciones y servicios mediante el uso de sus centros de datos.

Microsoft. La empresa desarrolla, fabrica, licencia y da soporte a ordenadores personales, servidores, dispositivos electrónicos y servicios.

Azure Firewall. Azure Firewall es un servicio de seguridad de firewall de red inteligente y nativo de la nube que le proporciona la mejor protección contra amenazas para las cargas de trabajo en la nube que se ejecutan en Azure.

DRP. Un plan de recuperación ante desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

Bases de Datos. Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Nube. Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

BCP. Un plan de continuidad del negocio es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

3. Seguridad Perimetral.

Los puntos más importantes que conforman la seguridad perimetral tienen que ver con el **Firewall**, **IPS** (sistema de prevención de intrusiones) e **IDS** (sistema de detección de intrusos).

Dado que nosotros estamos utilizando los servicios de **Microsoft Azure** para alojar las máquinas virtuales: Al establecer las defensas de la nube de Azure, primero debe comprender que un sistema de detección de intrusiones (IDS, Intrusion Detection System) en Azure es fundamentalmente diferente que en entornos locales.

En Azure, no se administra la infraestructura de red subyacente, lo que dificulta el acceso a la información a nivel de paquete mediante la creación de reflejo de puertos, las pulsaciones o los métodos tradicionales basados en la red. **Microsoft** es responsable de proteger su infraestructura, ya que operan bajo el modelo de responsabilidad compartida. Sin embargo, usted sigue siendo responsable de supervisar y proteger las aplicaciones que se ejecutan en Azure.

Pero la manera que tenemos para manejar el IPS e IDS en Microsoft Azure es mediante el Firewall que nos proporciona el mismo servicio. Dado que **Azure Firewall** ofrece IPS/IDS.

4.DRP (Plan de Recuperación de Desastres)

4.1 Análisis de riesgos

Los datos personales a los que los servidores públicos tienen acceso en el ejercicio de sus atribuciones se resguardan de manera física y electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento.

Tanto para la protección de datos personales, como para los datos sensibles, que son determinados junto con su ciclo de vida por las Unidades Administrativas, sin ser discriminados por su valor o ciclo de vida, pues su vulnerabilidad podría traer la divulgación o incluso un daño moral o patrimonial para los titulares de los datos, por lo tanto, el valor de los datos personales en la actualidad cobra cada día mayor relevancia por las implicaciones e información vinculados a ellos.

En este sentido, tanto los sistemas electrónicos como los medios a través de los cuales se resguardan de manera física los datos personales presentan diferentes particularidades debido a las características de cada uno de ellos.

Los datos personales que se guardan de forma física tienen diferentes tipos de riesgos existentes, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción; por ello, se cuenta con un área de soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y con acreditación para su uso.

Por su parte, los datos personales contenidos en un sistema electrónico presentan riesgos por su propia naturaleza como los son el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas, por ello, se cuenta con un área de soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos y previa acreditación de su personalidad a través de medios electrónicos para su uso.

4.2 Análisis de brecha

Las medidas de seguridad existentes y efectivas para la protección de datos personales con las que actualmente se cuenta son:

- **Medidas de seguridad:** La información que contiene datos personales se resguarda en una ubicación que cuenta con diversas medidas de seguridad como cámaras de seguridad, archiveros específicos para su resguardo y uso de cerraduras para su acceso.
- **Medidas de control:** Medidas de carácter administrativo encaminadas a contar con un registro físico de los servidores públicos que tienen acceso a datos personales, así como de los datos personales contenidos en los documentos.
- **Medidas legales:** Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos, se realiza el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.
- **Medidas cibernéticas:** Contamos con atribuciones para establecer normas y lineamientos e implementar esquemas de seguridad para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras.

5.BCP (Plan de Continuidad Empresarial)

5.1 Ámbito y objetivos.

Indica la finalidad del BCP, incluidas las funciones empresariales específicas a las que debe darse prioridad para garantizar la recuperación durante una emergencia.

Este **BCP** se usa para garantizar la continuidad de los servicios de **TI** y las líneas de clientes en el caso de una *interrupción* del suministro eléctrico imprevista y prolongada. La *interrupción* del suministro eléctrico podría estar causada por condiciones meteorológicas de emergencia o el incendio en un edificio. Las áreas funcionales que se priorizan para la recuperación en este BCP son el departamento de atención al cliente y el equipo de finanzas.

5.2 Operaciones en riesgo.

Incluye posibles riesgos con funciones operativas clave que interrumpirían en gran medida el negocio y la continuidad de los clientes.

Operación: Atención al cliente.

Descripción de la operación: el equipo de atención al cliente intenta, después de 24 horas, poner en marcha operaciones globales de chat en directo y llamadas de clientes.

Descripción del impacto: todos los chats en directo se realizan a través del equipo de atención al cliente de Digital Team. El 20 % de las llamadas en directo se dirigen a la oficina de Digital Team. Una interrupción quiere decir que ya no se podrán ofrecer servicios de asistencia mediante chat en directo y que los clientes experimentarán tiempos de espera prolongados en las llamadas, los plazos de los proyectos y los horarios del equipo.

5.3 Estrategia de recuperación

Describe todos los procedimientos relevantes para restablecer las operaciones empresariales después de un incidente o una crisis.

El personal de TI y los comités de BCP deben poner en marcha servidores y programas de reserva alternativos para guardar solicitudes de clientes después de una interrupción del suministro eléctrico. El servicio de atención al cliente debe ser capaz de recibir las solicitudes y responder a los clientes en un plazo de 30 minutos.

5.4 Funciones y responsabilidades

Hace referencia al personal clave y sus tareas asignadas durante o después de un incidente.

Representante: Darien Sánchez

Función: director de operaciones

Datos de contacto: darienmsa@example.com

Descripción de las responsabilidades:

1. Debe garantizar que los BCP se actualicen y debe coordinar los cambios con los responsables de equipo.
2. Ayuda a notificar a las principales partes interesadas en la región de EMEA sobre amenazas en las herramientas y los programas de atención al cliente.