

UNIBROSA WEB GMSC

“Describe la infraestructura optima necesaria para
implementación del Unibrosa Web GMSC”

Abril 2022

Versión 1.3.1



Mercantil Santa Cruz

TABLA DE CONTENIDOS

1.	CONTROL DE VERSIONES	2
2.	REFERENCIAS	3
3.	FIRMAS	4
4.	OBJETIVO	5
5.	ALCANCE	5
6.	ARQUITECTURA	6
6.1.	VISTA LÓGICA	6
6.1.1.	DIAGRAMA CONCEPTUAL	6
6.1.1.1.	FRONT WEB / BACK	6
6.1.1.2.	BD: PORTAL UNIBROSA	7
6.2.	VISTA FÍSICA	8
6.2.1.	DIAGRAMA DE CONEXIONES	8
6.2.1.1.	CLIENTE UNIBROSA – WAF	8
6.2.1.2.	FUNCIONARIO UNIBROSA – WAF	9
6.2.1.3.	WAF – FRONT WEB / BACK	9
6.2.1.4.	FRONT WEB – BD: UNIBROSA WEB	10
6.2.1.5.	FRONT WEB – EXCHANGE	11
6.2.2.	DIAGRAMA DE BLOQUES	12
7.	TABLA DE ILUSTRACIONES	13



1. Control de Versiones

Control de cambios del documento			
Versión	Realizado por	Fecha	Cambios Realizados
0.9.0	Franz Alvarez	15/03/2021	Creación del documento
1.0.0	Franz Alvarez	25/03/2021	Actualización de los diagramas conceptual y de conexión.
1.3.1	Franz Alvarez	21/04/2022	Actualización del diagrama de conexiones y de bloques. Se eliminó el servidor Back, porque el proveedor confirmó que no es posible separar Front de Back. Se aprovisiona el servidor Web que contendrá los componentes Back detrás la DMZ por el riesgo que conlleva alojarla en DMZ con componentes Back. Se reutiliza el servidor de Exchange aprovisionado para el grupo.



2. Referencias

Control de dependencias del documento		
Versión	Nombre	Relación de dependencia
1.1.0	UNIBROSAWEB-ARQDIA-Diagramas.vsdX	Diseño de componentes de la arquitectura

3. Firmas

SHA1 Documento Para Firmas:

Elaborado Por:

Franz Alvarez Analista de Arquitectura Tecnológica		

Revisado Por:

Luis Iturry Analista de Arquitectura de Seg. Inf.		
Nota: Al firmar esta sección da la conformidad de que el documento cumple con los criterios de aceptación de su área.		

Aprobado Por:

Victor Cocarico Subgerente de Tecnología	Erick Calderón Subgerente de Seguridad de Información	Gonzalo Viscarra Subgerente de Analisis y Programación
Proveedor		
Nota: Al firmar esta sección da la conformidad de que el documento cumple con los criterios de aceptación de su área.		

Conocimiento de:

Boris Cazuriaga Gerente de Sistemas	Fernando Quevedo Gerente de Riesgo Operativo	
Nota: Al firmar esta sección da la conformidad de que el documento cumple con los criterios de aceptación de su área.		

4. Objetivo

Este documento detalla la arquitectura tecnológica del Proyecto Unibrosa Web GMSC.

5. Alcance

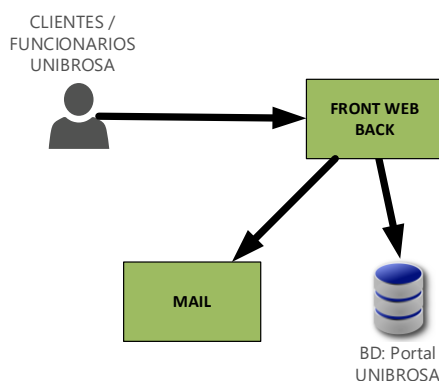
Este documento debe ser utilizado por todos que necesiten informaciones referentes a la arquitectura definida para el Proyecto Unibrosa Web GMSC en la infraestructura del BMSC. Debe cubrir todas las visiones para que sea comprendido por la gerencia, desarrollo, proyectos o demás interesados.

6. Arquitectura

6.1. Vista Lógica

El sistema está compuesto por una aplicación middleware y Base de datos.

6.1.1. Diagrama Conceptual



1 Diagrama Conceptual

6.1.1.1. Front Web / Back

Servidor de aplicaciones web donde reside la aplicación Unibrosa Web.

Criterio	Descripción
Alta Disponibilidad	Proporcionada por la infraestructura VMWare
Sitio Alterno	No se considera la instalación en el sitio alternativo puesto que el servicio no está dentro de los servicios críticos del Banco.
Logs	El equipo cuenta con Logs propios.
Control Acceso	El sistema utiliza la autenticación propia del sistema.
Contingencia	Procedimiento de contingencia manual establecido en BMSC.

6.1.1.2. BD: Portal Unibrosa

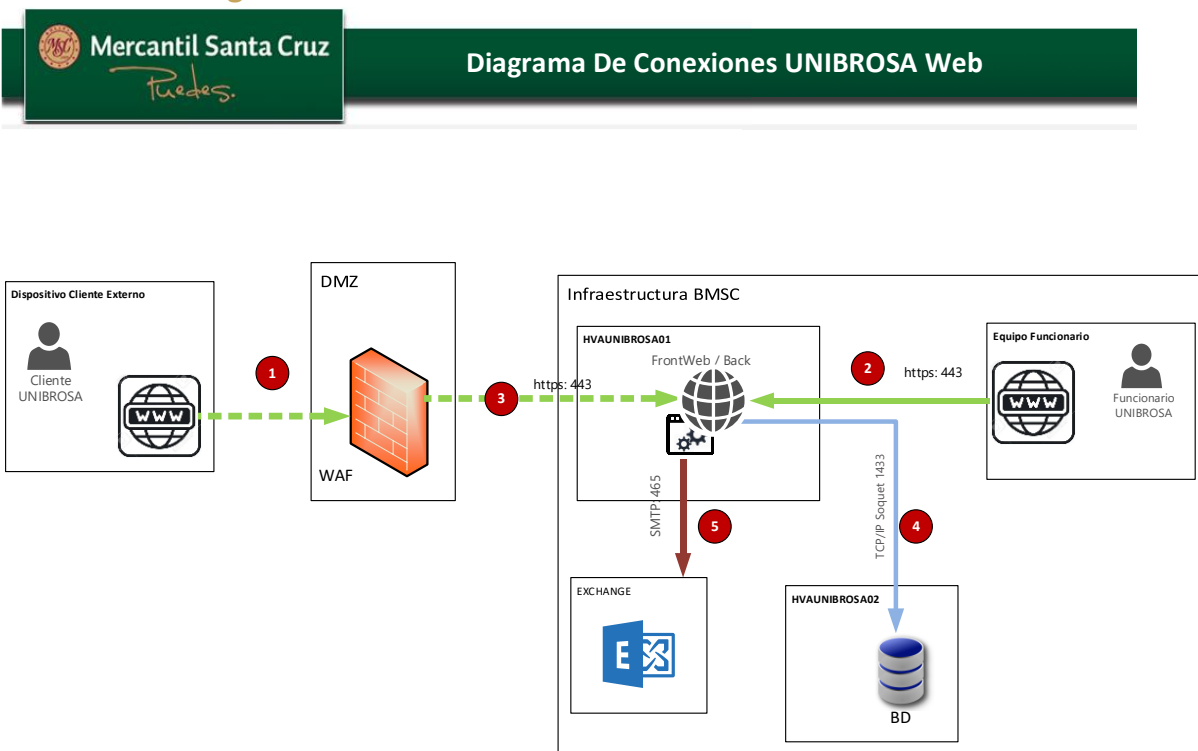
Servidor de Base de datos donde reside el motor de base de datos.

Criterio	Descripción
Alta Disponibilidad	Proporcionada por la infraestructura VMWare
Sitio Alterno	No se considera la instalación en el sitio alerno puesto que el servicio no está dentro de los servicios críticos del Banco.
Logs	El equipo cuenta con Logs propios.
Control Acceso	El sistema utiliza la autenticación propia del sistema.
Contingencia	Procedimiento de contingencia manual establecido en BMSC.

6.2. Vista Física

La estructura física utilizada por esta arquitectura comprende:

6.2.1. Diagrama de Conexiones



2 Diagrama de Conexiones

6.2.1.1. Cliente Unibrosa – WAF

Criterio	Descripción
Cliente	Cliente Unibrosa
Servidor	WAF
Autenticación	Credenciales de Autenticación proporcionadas por el Servidor Web.
Autorización	Para utilizar los recursos en el aplicativo el Usuario deberá contar con un perfil usuario.
Confidencialidad	La conexión utiliza el protocolo HTTPS para evitar que la información sea expuesta a terceros.

Integridad	Se utiliza el protocolo HTTPS que incorpora mecanismos de verificación de los mensajes que se envían.
Protocolo	HTTPS

6.2.1.2. Funcionario Unibrosa – WAF

Criterio	Descripción
Cliente	Funcionario Unibrosa
Servidor	WAF
Autenticación	Credenciales de Autenticación proporcionadas por el Servidor Web.
Autorización	Para utilizar los recursos en el aplicativo el Usuario deberá contar con un perfil usuario.
Confidencialidad	La conexión utiliza el protocolo HTTPS para evitar que la información sea expuesta a terceros.
Integridad	Se utiliza el protocolo HTTPS que incorpora mecanismos de verificación de los mensajes que se envían.
Protocolo	HTTPS

6.2.1.3. WAF – Front Web / Back

Criterio	Descripción
Cliente	WAF
Servidor	Front Web / Back

Autenticación	Credenciales de Autenticación proporcionadas por el Servidor Web.
Autorización	Para utilizar los recursos en el aplicativo el Usuario deberá contar con un perfil usuario.
Confidencialidad	La conexión utiliza el protocolo HTTPS para evitar que la información sea expuesta a terceros.
Integridad	Se utiliza el protocolo HTTPS que incorpora mecanismos de verificación de los mensajes que se envían.
Protocolo	HTTPS

6.2.1.4. Front Web – BD: Unibrosa Web

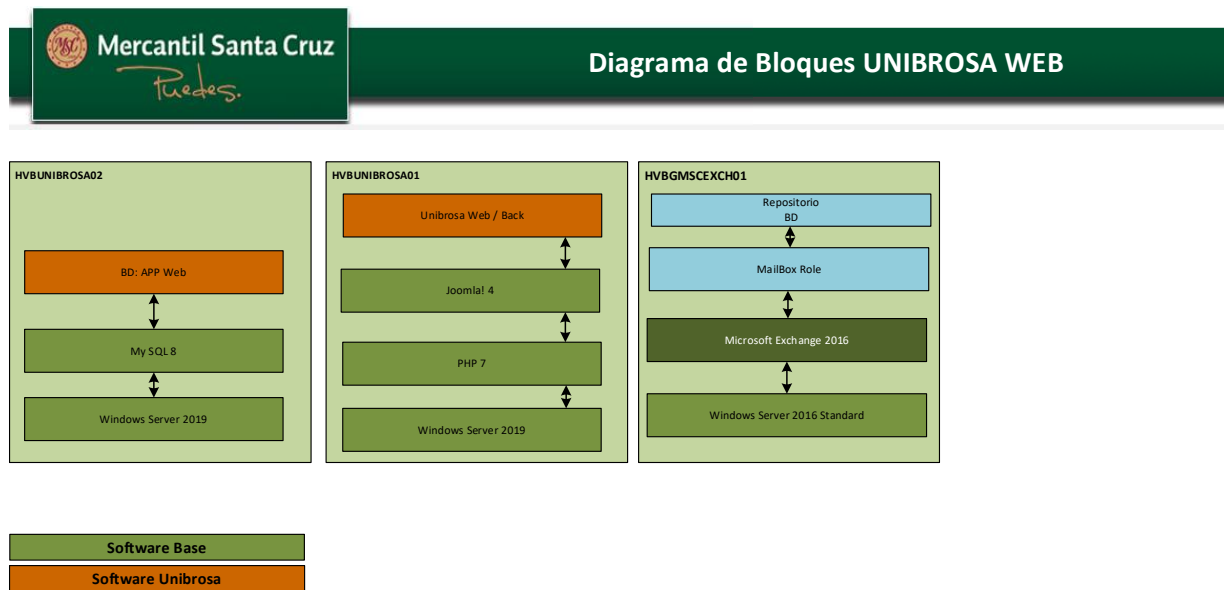
Criterio	Descripción
Cliente	Front Web
Servidor	BD: Unibrosa Web
Autenticación	El componente orquestador tiene un usuario y contraseña de Base de Datos.
Autorización	El usuario de Base de Datos tiene permisos de acceso a todos los objetos que requiere.
Confidencialidad	Garantizada por el protocolo
Integridad	Garantizada por el protocolo
Protocolo	SQL Server

6.2.1.5. Front Web – Exchange

Criterio	Descripción
Cliente	Front Web
Servidor	Servidor SMTP EXCHANGE
Autenticación	No aplica, se utiliza la configuración relay.
Autorización	El servidor SMTP controla que el cliente que solicita tenga permisos para realizar el envío de correos.
Confidencialidad	La conexión se encuentra sobre TCP/IP
Integridad	La conexión se encuentra sobre TCP/IP
Protocolo	Se utiliza el protocolo SMTP



6.2.2. Diagrama de Bloques



3 Diagrama de bloques

7. Tabla de Ilustraciones

1 DIAGRAMA CONCEPTUAL	6
2 DIAGRAMA DE CONEXIONES.....	8
4 DIAGRAMA DE BLOQUES.....	12

