



Sistema Centralizado de Logs y Monitoreo

Manual de Usuario

Versión 1.0

Septiembre de 2023



RESUMEN

El presente documento sirve como guía para el manejo del sistema centralizado de logs y monitoreo y que estará publicado en la sección de “Manual” de dicho sistema. En las diferentes secciones del documento se encuentra explicadas las funcionalidades del sistema y como usarlas, las funciones principales del sistema se pueden usar solicitando los permisos necesarios al OSI.

Revisiones del Documento

Historial de Cambios

Fecha	Autor	Versión	Cambios realizados
02/Sep/2023	jacarrion1	1.0	



Contenido

Sistema Centralizado de Logs y Monitoreo	1
RESUMEN	2
Revisiones del Documento.....	2
Historial de Cambios	2
Manual de Usuario.....	4
Ingreso al Sistema	4
Recuperar Contraseña	6
Home.....	7
Menú de Opciones	8
Monitoreo de Logs.....	8
Abrir nueva conexión	8
Conexiones Temporales.....	9
Conexiones Almacenadas	10
Conectarse a MongoDB	10
Logs de Mongo.....	12
Logs de Texto	14
Seguimiento de transacciones	15

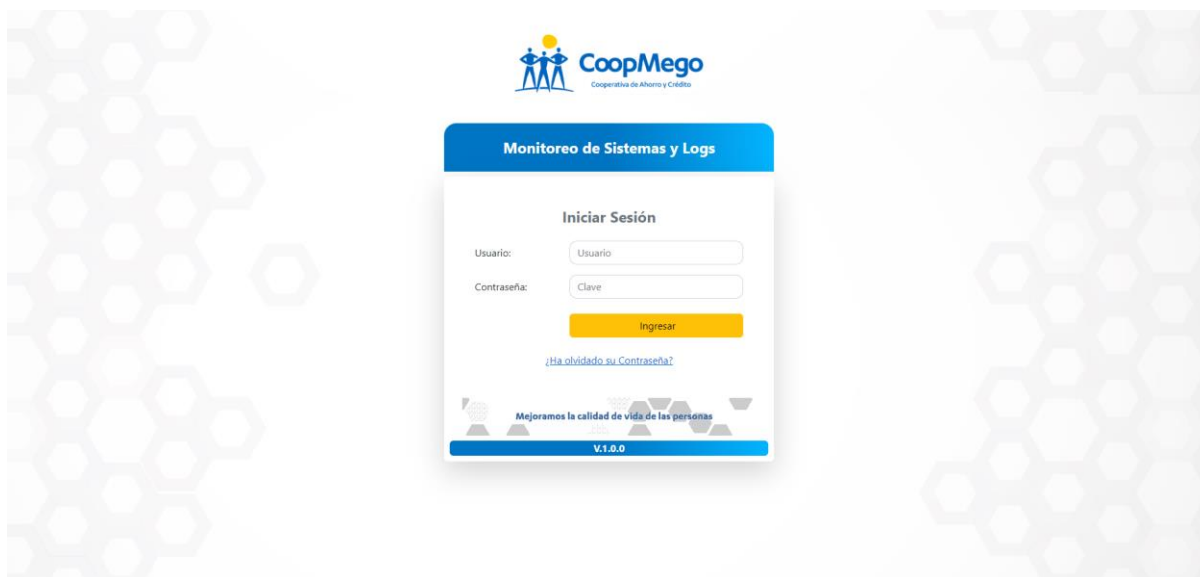
Manual de Usuario

Ingreso al Sistema

Para acceder al sistema desde cualquier navegador Web, se debe ingresar a la siguiente dirección:

// aquí poner la url del sistema

Una vez que se haya cargado el sistema se presentará la pagina de ingreso de usuarios, Login, donde, usando credenciales, se puede acceder al sistema.

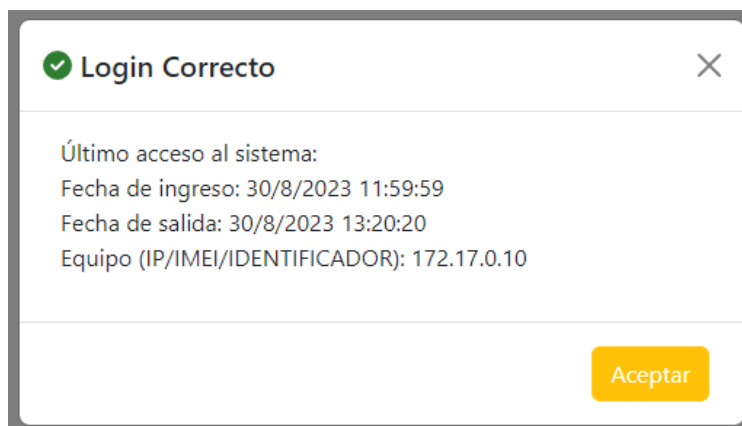


Para ingresar al sistema se debe escribir el usuario y la contraseña que usa para los sistemas internos de la cooperativa, si aún no ha ingresado a otro sistema interno debe usar los datos entregados por el Departamento de Seguridad de la Información cuando solicito la creación de su usuario. Una vez ingresados los datos debe presionar el botón de **Ingresar**.

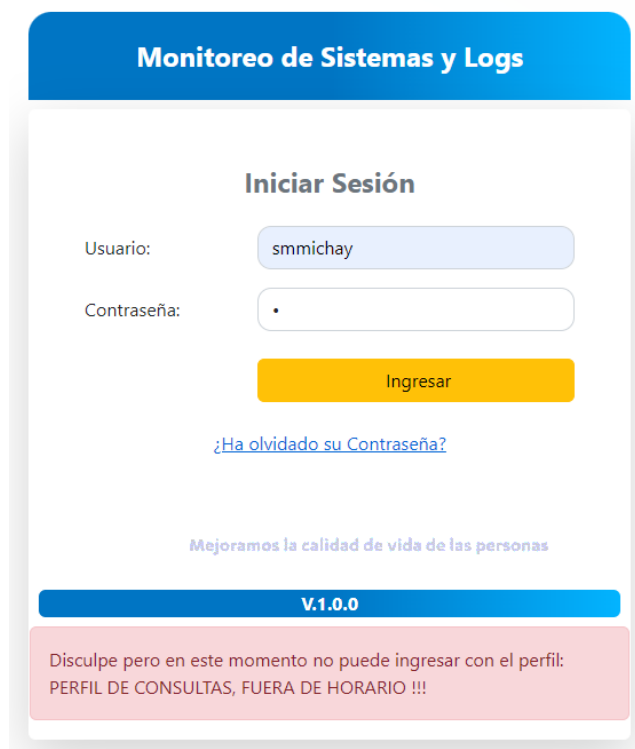




El sistema valida que la información ingresada sea correcta y si su rol de usuario tiene acceso al sistema le mostrara un mensaje con la información de su ultima conexión.



De lo contrario se mostrará un mensaje indicado el motivo por el que no se puede acceder al sistema.



Los usuarios deben cambiar su contraseña cada cierto tiempo, si no se realiza este cambio, el sistema lo solicita antes de ingresar.



Cambiar Password ✕

Clave Anterior:

Clave Nueva:

Confirmar Clave:

Guardar

Cancelar

Al cambiar la clave se deberá volver a ingresar al sistema con los nuevos datos.

Si es la primera vez que ingresa a algún sistema interno, se solicitará el cambio de la clave temporal y el ingreso de las preguntas de seguridad para la recuperación de la clave si se llega a olvidar.

Cambiar Password Primera Vez ✕

Clave Anterior:

Clave Nueva:

Confirmar Clave:

Pregunta

Respuesta

Seleccione...

Seleccione...

Guardar

Cancelar

Recuperar Contraseña

Si ha olvidado la clave de acceso al sistema, se la puede recuperar accediendo a la opción “¿Ha olvidado su Contraseña?”, donde se solicitará el ingreso del usuario y las preguntas de seguridad para luego pedir el ingreso de una nueva contraseña de acceso.

Recuperar Password ✕

Usuario:

Verificar

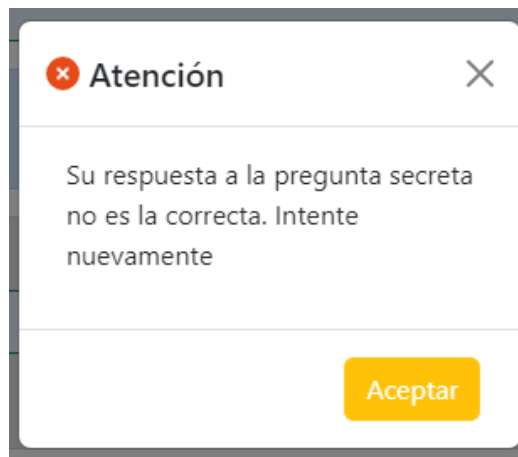
Ingrese la respuesta a la pregunta secreta:

COLOR PREFERIDO:

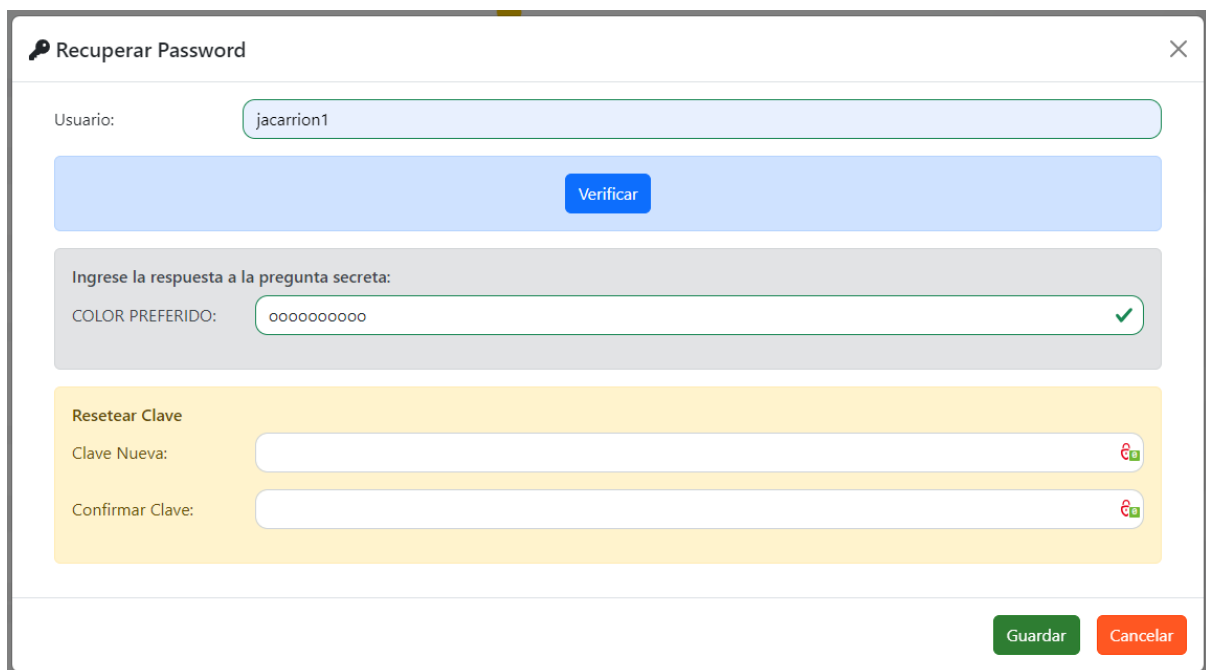
Validar

Cancelar

Si ingresa datos incorrectos se mostrará una alerta indicando el error.



Si los datos son correctos se mostrarán los campos de ingreso de una nueva clave de acceso.

El formulario "Recuperar Password" tiene un título con un icono de llave y una X en la esquina superior derecha. El campo "Usuario:" contiene el texto "jacarrion1". Debajo hay un botón azul "Verificar". El siguiente grupo de campos está titulado "Ingrese la respuesta a la pregunta secreta:" y contiene el campo "COLOR PREFERIDO:" con el valor "oooooooo" y un icono de checkmark verde. Abajo, en un fondo amarillo, se encuentra la sección "Resetear Clave" con campos para "Clave Nueva:" y "Confirmar Clave:", cada uno con un icono de ojo y un checkmark verde. En la parte inferior derecha hay dos botones: "Guardar" (verde) y "Cancelar" (rojo).

Home

Si las el acceso al sistema se ha autorizado se presenta la pantalla principal donde se encuentra la información del sistema; se puede leer el nombre del sistema, la versión, la fecha de la última actualización y la lista de las mejoras realizadas en dicha actualización.

La pantalla principal "Monitoreo de Logs" tiene un encabezado azul con el logo de CoopMego y el título "Monitoreo de Logs". Debajo del encabezado hay una barra de navegación con los enlaces: Home, Logs, Manual, Cambiar Password, Cambiar Preguntas, Salir. En el centro, se muestra la fecha y hora: "Miércoles 13 de Septiembre del 2023, 10:08:20" y el "PERFIL DE CONSULTAS: CARRION PIEDRA JHON ALEXANDER". El título principal es "CoopMego - MONITOREO LOGS", seguido de "Versión: V.1.0.0" y "Fecha Actualización: JULY 29, 2023". En la sección "Mejoras:", hay una lista de puntos: "Registrar conexiones a MongoDB.", "Obtener lista de bases de datos (se obtienen las bases asignadas a las credenciales de conexión).", "Obtener logs de Mongo y de Texto (se puede descargar).", "Realizar seguimiento de transacciones."



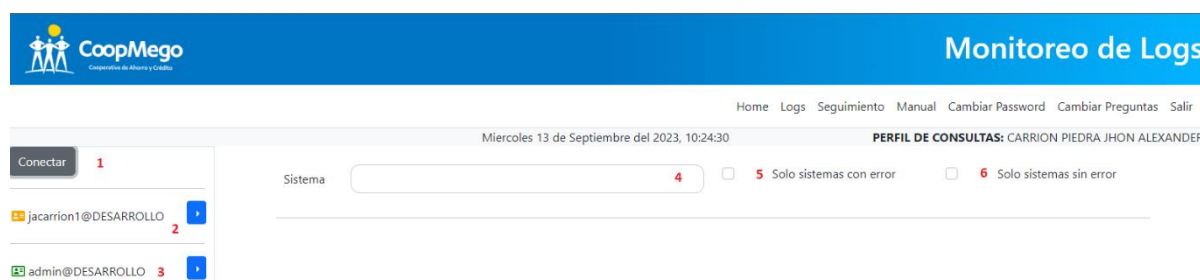
Menú de Opciones

Home 1 Logs 2 Manual 3 Cambiar Password 4 Cambiar Preguntas 5 Salir 6

1. Acceder a la página principal del sistema (Home).
2. Acceder a la sección de monitoreo de logs.
3. Ver el manual de usuario.
4. Cambiar la contraseña de acceso al sistema.
5. Cambiar las preguntas de seguridad para recuperar la clave de acceso al sistema.
6. Cerrar sesión (Salir del sistema).

Monitoreo de Logs

En esta sección se puede visualizar las conexiones y al acceder a cada conexión se puede visualizar el contenido de MongoDB al que el usuario tiene acceso.



1. Botón para poder abrir una nueva conexión.
2. Conexiones temporales, estas conexiones se almacenan en el Local Storage del navegador.
3. Conexiones almacenadas, estas conexiones se almacenan en una colección de MongoDB y están disponibles, para el usuario, desde cualquier navegador.
4. Filtrar lista de logs por el nombre del sistema.
5. Mostrar solo los sistemas que hayan registrado logs de error.
6. Mostrar solo los sistemas que no hayan registrado logs de error.

Abrir nueva conexión

Para abrir una nueva conexión se debe dar clic al botón de “**Conectar**” esto mostrara un dialogo con los campos necesarios para establecer una conexión con MongoDB.

Existen dos tipos de conexiones: temporales y almacenadas; las **conexiones temporales** se almacenan en el Local Storage del Navegador, y por esta razón son temporales, ya que si se borran los datos de navegación o se ingresa desde otro navegador u otro ordenador, estas conexiones no estarán disponibles. Las **conexiones almacenadas** son conexiones que se registran en MongoDB y que se recuperan desde la base de datos cuando el usuario ingresa al sistema, desde cualquier navegador u ordenador.

Para abrir una nueva conexión se necesita tener un usuario y una contraseña en MongoDB que tenga habilitados los permisos de acceso a las bases de datos, si no se cuenta con las credenciales, o con los permisos se mostrara un error indicando que no se pueden obtener datos.



Nueva Conexión

Usuario
jacarrion1 1

Clave
Clave de MongoDB 2

Servidor
Seleccione... 3

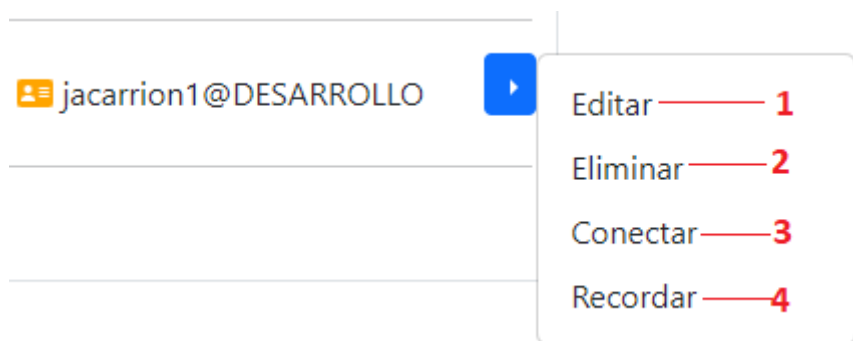
☐ Recordar Conexión 4

5 **Guardar y Conectar** **Cancelar**

1. Usuario de MongoDB
2. Clave de acceso a MongoDB
3. Servidor al que se desea conectar:
 - a. DESARROLLO
 - b. PRODUCCION
4. Opción de almacenar la conexión en MongoDB; si no se selecciona, la conexión se creará como **temporal**.
5. Abrir una conexión con los datos ingresados.

Conexiones Temporales

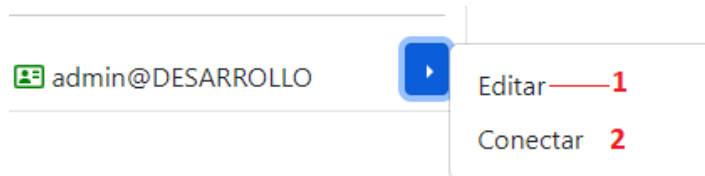
Estas conexiones permanecen almacenadas en la memoria del navegador, por lo que son susceptibles a desaparecer si se llega a borrar los datos de navegación; estas conexiones no estarán disponibles en otro navegador ni en otro ordenador. Se puede realizar las siguientes acciones con ellas:



1. Modificar los datos de conexión: Usuario, Clave y Servidor.
2. Eliminar del Local Storage la conexión.
3. Conectarse a MongoDB usando los datos de la conexión. Para conectarse a MongoDB se puede, también, dar clic sobre la conexión.
4. Almacenar la conexión en MongoDB para que este disponible en cualquier comento.

Conexiones Almacenadas

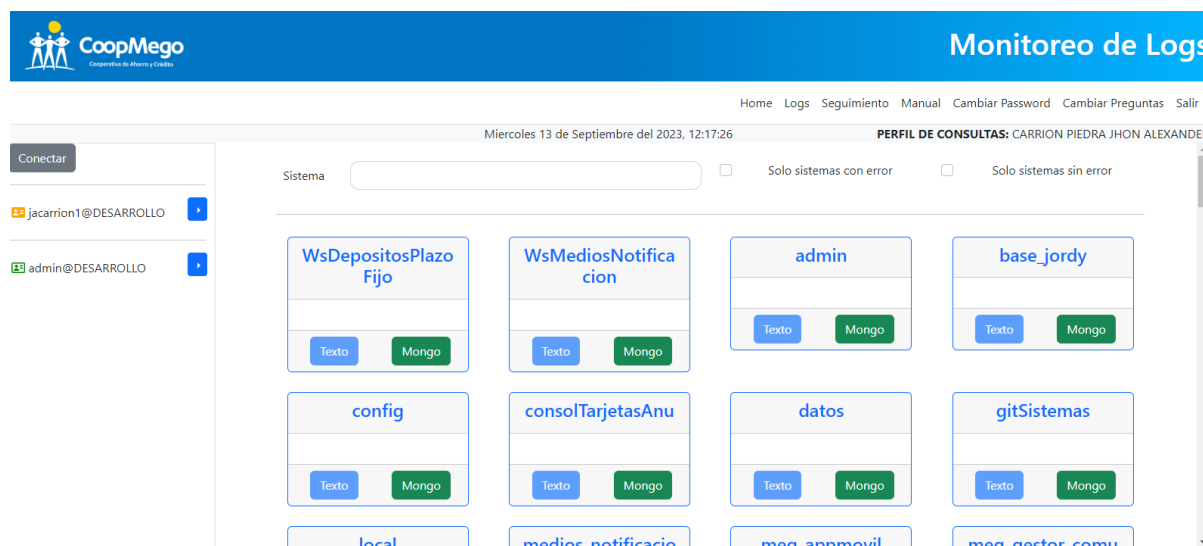
Estas conexiones se recuperan, desde la base de datos de MongoDB, cuando el usuario ingresa al sistema y están disponibles, para el usuario, desde cualquier navegador u ordenador. Las acciones que se puede realizar con ellas son:



1. Modificar los datos de conexión: Usuario, Clave y Servidor.
2. Conectarse a MongoDB usando los datos de la conexión. Para conectarse a MongoDB se puede, también, dar clic sobre la conexión.

Conectarse a MongoDB

Para conectarse a MongoDB y obtener los logs registrados por los sistemas de la Cooperativa se puede hacer clic sobre una conexión o usar la opción de **“Conectar”** en el menú de opciones de cada conexión. Una vez que se establece la conexión se obtiene el listado de todos los registros de logs a los cuales tenga acceso el usuario.



Existen tres tipos de registros:

1. Sistemas que registran logs en MongoDB pero que no usan el servicio wsLogs y, por lo tanto, no cuentan con registros de logs de texto en el sistema de monitoreo de logs y no se ha verificado el seguimiento del estándar ISO 20022. Se representan de color azul, se puede acceder a sus registros en MongoDB, pero no se cuenta con registros de logs de texto, por lo tanto esta opción está deshabilitada.

WsDepositosPlazo Fijo	
Texto	Mongo

2. Sistemas que registran logs a través del servicio wsLogs y que han registrado errores en MongoDB, esto sistemas cuentan tanto con logs de texto como los registros de MongoDB, cada sistema decide si el wsLogs registra logs en archivos de texto (.txt) o no.

wsRegistroCivil	
172.18.0.9 c1dcff67c7a5	
Texto	Mongo

3. Sistemas que registran logs a través del servicio wsLogs y que no han registrado errores en MongoDB, esto sistemas cuentan tanto con logs de texto como los registros de MongoDB, cada sistema decide si el wsLogs registra logs en archivos de texto (.txt) o no.

wsNotificadorSms	
172.18.0.10 280675ab8b66	
Texto	Mongo

Nota: Los sistemas que si usan el servicio wsLogs muestran información del servidor, IP e Id del Contenedor o Host, con la finalidad de ubicar rápidamente donde se encuentra publicado dicho servicio y poder realizar las acciones correspondientes para dar soporte a dichos sistemas.

En algunas tarjetas mostradas en el grid se muestra la leyenda “Posible error de estándar ISO - 2002”, esto quiere decir que el sistema, donde se muestra este texto, ha registrado Logs que no siguen el estándar ISO 2022, ya sea en las peticiones o en las respuestas, esto se debe reportar para su corrección inmediata. Cabe recalcar que esta leyenda puede mostrarse tanto en tarjetas de color verde como en

tarjetas de color rojo, ya que el color de la tarjeta alerta si se ha registrado un error en las peticiones, más no un error de estándar.

Sistema sin errores



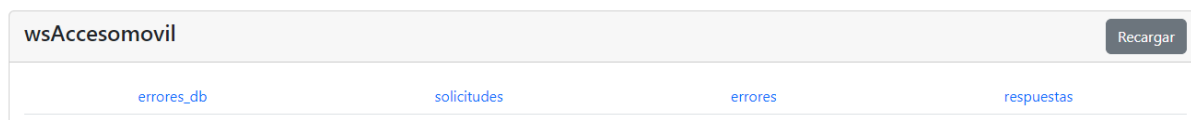
Sistema con errores



Nota: La leyenda del error de ISO 20022 dice “Posible”, ya que si el color de la tarjeta es rojo, es posible que el sistema haya registrado un error y no siga el estándar ISO 20022 o que únicamente haya registrado un error.

Logs de Mongo

Para acceder a los registros de logs en MongoDB se debe hacer clic en el botón “Mongo” en la tarjeta con el nombre del sistema que se desea revisar, esto solicitará la lista de colecciones, a MongoDB, que pertenezcan al sistema seleccionado.



Para mostrar los logs de cada colección basta con hacer clic sobre alguna de ellas, se puede visualizar en dos presentaciones, tipo JSON y en forma de Tabla



wsAccesomovilRecargar

errores_db **solicitudes** errores respuestas

JSON **Tabla** Buscar Recargar

```
"root": [ 10 items
  0: { 34 items
    "_id": string "6501e7ada55ef1904c500fc"
    "str_id_transaccion": string "c788249ae1904ef6be3bd079a5b9d74e"
    "str_ente": string "142672"
    "str_nemonico_canal": string "CANBMO"
    "str_id_sistema": string "79"
    "str_app": string "MEGOMOVIL"
    "str_id_servicio": string "REQ_GET_CONTRATOS"
    "str_version_servicio": string "2.4.0"
    "str_id_usuario": string "0"
```

wsAccesomovilRecargar

errores_db **solicitudes** errores respuestas

JSON **Tabla** Buscar Recargar

0	_id	str_id_transaccion	str_ente	str_nemonico_canal	str_id_sistema	str_app	str_id_servicio	str_version_servicio	str_id_usuario	str_mac_dispositivo	str_id_usuario
	"6501e7ada55ef1904c500fc"	"c788249ae1904ef6be3bd079a5b9d74e"	"142672"	"CANBMO"	"79"	"MEGOMOVIL"	"REQ_GET_CONTRATOS"	"2.4.0"	"0"	"DESCONOCIDO"	"157"
1	_id	str_password	str_token_dispositivo	str_id_transaccion	str_ente	str_nemonico_canal	str_id_sistema	str_app	str_id_servicio	str_version_servicio	str_id_usuario
	"6501d883a55ef1904c5000c"	"*****"	"eUzaCEzhR2aw1GE3s5a1EEAPa91bHhPatTsoH1YSLv1B1NgzTmUs-2L1nCrOG6FDschvoNPK2_JNTOoNk5RMPjOw0-8nqZu8VD--gmiU7FdoUcZzmUBPh-C6-MW8oQ0mc3nH0V9Ru/QS2we1Lum1H9G5On9uA5F"	"5143d9f2d91418a8878048b4cad8076"	"20826"	"CANBMO"	"79"				
2	_id	str_password	str_token_dispositivo	str_id_transaccion	str_ente	str_nemonico_canal	str_id_sistema	str_app	str_id_servicio	str_version_servicio	str_id_usuario
	"6501cd8ea55ef1904c50064"	"*****"	"*6380oYtHWSHWj1bdZ5S-APa91bETkIqrmv4dMmV2ABvFP- YTum3pbUEapHjCwxtCPBjyqW9hMh49ccwdf_18292yg5C32CNGYK9IKTDdMNe4qkoN83V45vs5zhSKVGBLm2a1Pk93YCaUH98IP1deah-	"fd7cce0e68a4dc5a7736ebdbb95c6f5"	"267626"	"CANBMO"					
3	_id	str_password	str_token_dispositivo	str_id_transaccion	str_ente	str_nemonico_canal	str_id_sistema	str_app	str_id_servicio	str_version_servicio	str_id_usuario
			"*6380oYtHWSHWj1bdZ5S-APa91bETkIqrmv4dMmV2ABvFP-								

El botón **“Buscar”** muestra las opciones para aplicar filtros a los resultados obtenidos.

Seleccione...▼

+1

Buscar Limpiar

Los criterios de búsqueda están tomados de los registros obtenidos, es decir, se puede usar cualquier campo de los registros para realizar la búsqueda. Se permite aplicar varios filtros a la vez; usando el botón **“+1”** se puede agregar otro filtro.

str_res_codigo▼000

str_ente▼1456

Seleccione...▼

+1

Buscar Limpiar

Por defecto se cargan paginas de 10 registros cada una, pero esto se puede configurar en la parte inferior de la página, donde, también, se muestra el número total de registros.



El botón **“Cargar más!”** obtendrá los siguientes n registros, para cambiar el numero de registros se debe editar el campo que tiene por defecto **“10”**. Cabe recalcar que mientras mayor sea el numero de registros solicitados, mayor será el tiempo de espera de la respuesta de MongoDB, es decir la respuesta se ralentiza.

Nota: Los botones de **“Recargar”** sirven para recargar la lista de Colecciones y de Registros respectivamente, ya que si se recarga la página, se pierde el identificador del sistema seleccionado y se regresará al usuario a la página donde se lista los sistemas.

Logs de Texto

Los logs de texto son archivos con extinción .txt que contienen información sobre las transacciones realizadas por los sistemas, en estos archivos se encuentra la misma información de los logs de mongo pero organizada de forma que se encuentra tanto peticiones como respuestas en el mismo archivo. Se crea un archivo por día, por lo que se puede encontrar las transacciones están organizadas según su fecha. Cada sistema decide si se registran sus logs en archivos de texto, por lo que no todos los sistemas tendrán registros en esta lista.

wsAccesomovil

Recargar

Archivos de Logs de wsAccesomovil

#	Archivo	Ultima Actualización	Acciones	
1	20230601.txt	2023-JUN-01 17:50:33	Ver	Descargar
2	20230731.txt	2023-JUL-31 17:54:20	Ver	Descargar
3	20230801.txt	2023-AGO-01 17:54:37	Ver	Descargar
4	20230802.txt	2023-AGO-02 18:09:17	Ver	Descargar
5	20230803.txt	2023-AGO-03 17:06:51	Ver	Descargar
6	20230804.txt	2023-AGO-04 18:07:05	Ver	Descargar
7	20230807.txt	2023-AGO-07 17:31:03	Ver	Descargar

Se ofrece la opción de **“Ver”** el contenido de los archivos y también la opción de **“Descargar”** el archivo completo, Se debe tener en cuenta que algunos archivos tienen un tamaño considerable por lo que su descarga podría demorar, si se desea únicamente revisar ciertas transacciones es aconsejable usar la opción Ver.

Dentro de la opción Ver, se muestra el contenido del archivo seleccionado, obteniendo los registros en páginas de 50 registros cada una.



wsAccesomovil

Recargar

Contenido del archivo 20230912.txt

```
23111511 r:{"str_id_transaccion":"be0d18f011e241b5827d71f38f09e9fb","dt_fecha":"2023-09-12T18:11:15","str_tipo":"s\u0003C","str_websevice":"wsAccesomovil","str_clase":"Application.GetContratos.GetContratosHandler","str_metodo":"Handle","str_operacion":"GET_CONTRATO_TC","obj_objeto":{"datos_tc":{"file_bytes":"b1228b58-4a04-46b5-a999-5b9516359a40","file_bytes_pd":"","str_num_documento":"0100027846","str_canal":"Megom\u000F3vil","str_titulo_gen":"","str_descip_gen":"","str_check_url_tc":"https://coopmego.com/bmovil/contratos/Terminos_condiciones_megomovil_v1.5.htm","str_check_url_pd":"https://coopmego.com/bmovil/contratos/Tratamiento_datos_personales_v1.1.htm","str_msj_btn_gen":"","int_tipo_documento":153},"lst_archivos":[{"str_tipo":"TC","str_nombre":"Tu00E9rminos y condiciones","str_data":"Acepto los[Tu00E9rminos y Condiciones] (https://coopmego.com/bmovil/contratos/Terminos_condiciones_megomovil_v1.5.htm)","str_titulo":"Tu00E9rminos y Condiciones","str_descipcion":"En CoopMego nos enfocamos en brindarte un gran servicio y que disfrutes de una mejor experiencia al utilizar Megom\u000F3vil","str_mensaje_boton":"\u000A1Alerta! \n\nPor tu seguridad, sin la aceptaci\u000F3n de [Tu00E9rminos y Condiciones] (https://coopmego.com/bmovil/contratos/Terminos_condiciones_megomovil_v1.5.htm) no podr\u000E1s ingresar a Megom\u000F3vil."},"str_res_original_id_msj":"230912231139477","str_res_original_id_servicio":"REQ_GET_CONTRATOS","dt_fecha_msj_crea":"2023-09-12T23:11:39","str_res_estado_transaccion":"OK","str_res_codigo":"000","str_res_id_servidor":"","str_res_info_adicional":"","str_res_token":"","str_id_transaccion":"be0d18f011e241b5827d71f38f09e9fb","str_ente":"142672","str_r_nemonico_canal":"CANBMO","str_id_sistema":"79","str_app":"MEGOMOVIL","str_id_servicio":"RES_GET_CONTRATOS","str_version_servicio":"2.4.0","str_id_usuario":"0","str_mac_dispositivo":"DESCONOCIDO","str_ip_dispositivo":"157.100.180.228","str_remitente":"COOPMEGO","str_receptor":"Google-sdk_gphone64_x86_64","str_tipo_petition":"REQ","str_id_msj":"230912231139477","dt_fecha_operacion":"2023-09-12T18:11:15.0741694-05:00","bl_posible_duplicado":"false","str_prioridad":"","str_login":"","str_latitud":"-3.99986","str_longitud":"-79.20179333333333","str_firma_digital":"","str_num_sim":"10.0.2.15","str_clave_secreta":"","str_pais":"EC","str_sesion":"","str_id_oficina":"1","str_id_perfil":"1","str_id_identificador":"","str_tipo_error":"","str_error":""}}

23111508 s:{"str_id_transaccion":"be0d18f011e241b5827d71f38f09e9fb","dt_fecha":"2023-09-12T18:11:15","str_tipo":"s\u0003E","str_websevice":"wsAccesomovil","str_clase":"Application.GetContratos.GetContratosHandler","str_metodo":"Handle","str_operacion":"GET_CONTRATO_TC","obj_objeto":{"str_id_transaccion":"be0d18f011e241b5827d71f38f09e9fb","str_ente":"142672","str_nemonico_canal":"CANBMO","str_id_sistema":"79","str_app":"MEGOMOVIL","str_id_servicio":"REQ_GET_CONTRATOS","str_version_servicio":"2.4.0","str_id_usuario":"0","str_mac_dispositivo":"DESCONOCIDO","str_ip_dispositivo":"157.100.180.228","str_remitente":"COOPMEGO","str_receptor":"Google-sdk_gphone64_x86_64","str_tipo_petition":"REQ","str_id_msj":"230912231139477","dt_fecha_operacion":"2023-09-12T18:11:15.0741694-05:00","bl_posible_duplicado":"false","str_prioridad":"","str_login":"","str_latitud":"-3.99986","str_longitud":"-79.20179333333333","str_firma_digital":"","str_num_sim":"10.0.2.15","str_clave_secreta":"","str_pais":"EC","str_sesion":"","str_id_oficina":"1","str_id_perfil":"1","str_id_identificador":"","str_tipo_error":"","str_error":""}}
```

Cada registro de transacción esta codificado con la hora en la que se realizó usando el siguiente formato: HHmmssff, Ejemplo. 23111511, que se traduce en 23 horas, 11 minutos, 15 segundos, 11 milisegundos; para reconocer entre solicitudes, respuestas y errores, después de código de tiempo se encuentra los caracteres de:

- Solicitud -> s:
- Respuesta -> r:<
- Error -> e:<

Para aumentar el número de registros mostrados se debe hacer scroll hasta el final de la pagina y en el paginador cambiar el parámetro de registros, aquí también se puede navegar entre páginas.

Registros: 50

Mostrando 1 - 50 de 32

Nota: Los botones de “Recargar” sirven para recargar la lista de archivos y el contenido del archivo respectivamente, ya que si se recarga la página, se pierde el identificador del sistema seleccionado y se regresará al usuario a la página donde se lista los sistemas.

Seguimiento de transacciones

Esta opción se puede utilizar únicamente cuando se haya establecido conexión correctamente con MongoDB. Al establecer la conexión, en el menú de opciones se aumenta un ítem, de la siguiente manera:

Home Logs **Seguimiento** Manual Cambiar Password Cambiar Preguntas Salir

Dentro de esta opción se encuentra un formulario donde se solicita el ingreso de un “str_id_transaccion”, este dato es el que identifica cada transacción realizada por un usuario, se lo encuentra en los registros de logs, mongo y texto.



Seguimiento de Transacciones

Network

JSON

Tabla

Buscar



Usando este identificador, el sistema rastrea todas las apariciones de esa transacción en los logs de los sistemas y genera un reporte visual donde se observa, tanto los sistemas como los registros, solicitudes y respuestas o errores:

Seguimiento de Transacciones

Network

JSON

Tabla

35e35519ba3c4ea1b0e0e0f6b0734094

Buscar



Al igual que los logs de mongo, se puede visualizar el resultado tanto en formato JSON como en tabla. En la vista grafica se puede acceder al contenido de las peticiones haciendo clic en los óvalos de colores.