



Procesos de Soporte al cliente



Niveles de escalación CallMyWay

Primer Nivel

Ingreso a nuestro **Centro De Atención Telefónica CallMyWay**. Este centro está disponible para atender consultas de Lunes a Viernes de 6 am a 9 pm. Sábados y Domingos de 7 am a 5 pm.

Segundo Nivel

En caso de requerir ayuda especializada, nuestro **Centro De Atención Telefónica CallMyWay** escalará el caso a alguno de los técnicos de **Nivel 2** que serán asignados a la cuenta para temas específicos.

Tercer Nivel

En caso de requerir un soporte avanzado, nuestro **Nivel 2** escalará el caso a nuestro equipo de **Soporte Avanzado**.

Procesos, personas y tecnología que apoyan el servicio, bajo normas ITIL

Gestión de servicio

Para gestionar servicios y soporte de incidentes tenemos disponibles los siguientes canales:

- **Central Telefónica:**
 - México +5255 4170 8422
 - Chile +56 227609072
 - Colombia +57 15189663
 - Miami +1-305-644-5335
 - Canadá +1 6134168671
 - Perú +51 16409850
 - Panamá +507 8366060
 - Guatemala + 502 (2) 3750299
 - El Salvador +503 (211) 30412
 - Costa Rica +506 40004000
 - Rep. Dominicana +1 (829) 9466346

- **Otros Canales:**
 - **Click2Call** desde nuestra página web: www.callmyway.com
 - **Chat** en nuestro sitio web: www.callmyway.com
 - **Mensajería por medio de WhatsApp** al número: +50640004000
 - **Correo electrónico:** sophorte@callmyway.com

El personal de Soporte CallMyWay brinda apoyo en todo momento gracias a las características de nuestra plataforma telefónica.

Registro de incidencias

Todo incidente debe quedar registrado de forma individual e incluir la mayor cantidad de información posible, para así disponer de datos que faciliten su resolución. En este sentido, se agradecerá el apoyo del cliente con la documentación correspondiente.

Al realizar el reporte por correo electrónico se generará un número de seguimiento automático del caso. El registro debe contener información de vital importancia sobre la incidencia como lo es la hora y la fecha en que se produjo, la persona que registró la incidencia, los datos del usuario y descripción del problema.

Recurso humano

El Recurso Humanos es el principal activo de nuestra empresa. Somos un conjunto de conocimientos, experiencias, motivaciones, habilidades, capacidades, competencias y técnicas. Todo esto con el fin de garantizar un servicio acorde con las expectativas de nuestros clientes.

Procesos y niveles de escalamiento

- **Diagnóstico inicial:**

Esto ocurre cuando el usuario describe su problema y responde preguntas que nos permiten ayudar a encontrar la solución. La mayoría de los incidentes son resueltos por el personal de soporte de primer nivel. Caso contrario se procederá escalar al siguiente nivel.

- **Escalada de incidentes:**

Algunas veces las incidencias no pueden ser resueltas por el equipo de soporte de primer nivel que realiza el contacto inicial, por lo que es necesario que redirijan la misma a una persona o grupo concreto.

Se detalla los niveles de escalamiento:

S1- Crítica El equipo no es operativo y el trabajo está afectado de manera importante a la Compañía. No hay alternativa disponible.

S2 – Alta El equipo está afectado de manera importante.

S3 – Normal Las operaciones del equipo están afectadas, pero se puede continuar trabajando. El equipo no funciona de acuerdo con la documentación del producto.

S4 – Baja Impacto mínimo – el problema no afecta las operaciones normales. Peticiones de funcionalidad, consultas, etc.

Esto se basará en la cantidad de usuarios afectados y el nivel de interrupción que está causando dicha incidencia. En este sentido, la gravedad de los incidentes —es decir, que sus consecuencias negativas (impacto) sean mayores o menores— permite priorizarlos a lo hora de acometer su resolución.

- **Investigación y diagnóstico:**

Estos procesos tienen lugar durante la resolución de problemas cuando la hipótesis del incidente inicial se confirma como correcta. Una vez que se diagnostica el incidente, el personal puede aplicar una solución y solicita algunas pruebas que nos lleven a la resolución del incidente.

- **Resolución y recuperación:**

Una vez encontrada la solución para la incidencia debe ser aplicada, realizando las pruebas necesarias para asegurar que dicha solución sea óptima y queda resuelta. En este paso se confirma que el servicio del usuario se ha restaurado al nivel de SLA requerido.

- **Cierre del incidente:**

En este punto es necesario asegurarse de que el cierre se ha categorizado y que los registros contienen todos los datos relacionados con la incidencia.

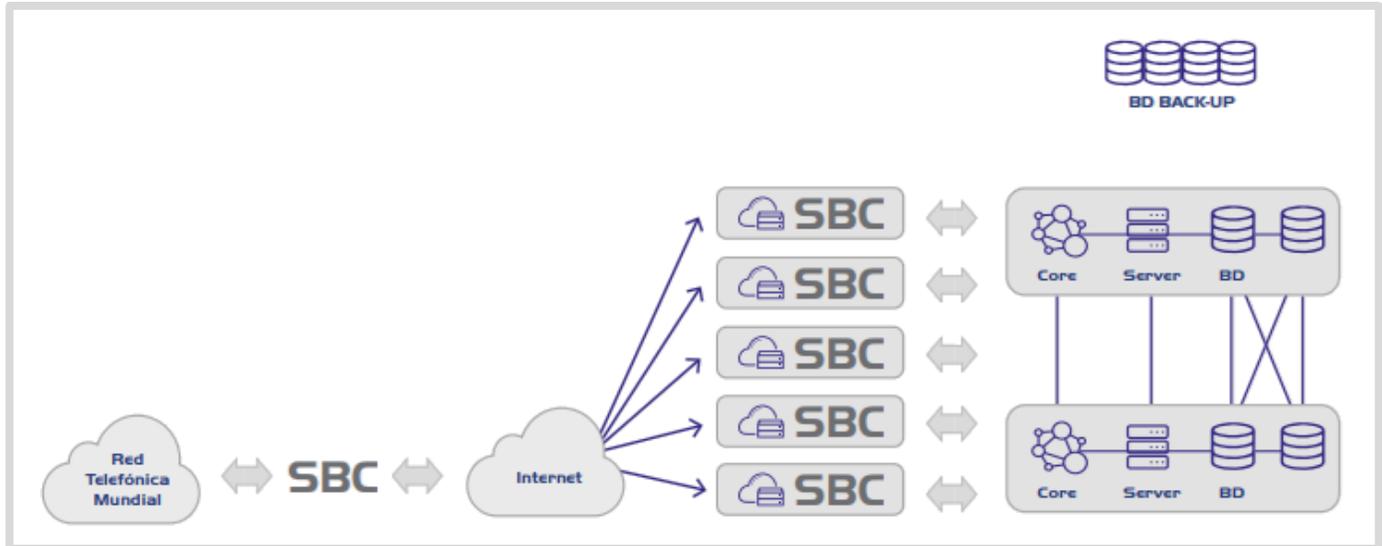
Estrategia de CallMyWay para garantizar la disponibilidad, capacidad, continuidad y seguridad de los servicios.

- Red Robusta

SoftSwitch Distribuido: Nuestro SoftSwitch está concebido de la siguiente manera:

- Dos instancias –CORE- simultáneas: Pueden operar dos instancias de servicio semejantes y simultáneas que se comunican entre sí de manera que si alguna falla como un todo, la otra al estar operativa y operando sustituye a la primera de manera automática.
- Componentes independientes: Los componentes de cada instancia pueden operar y operan en servidores independientes, de manera que si un servidor o su conexión a Internet falla únicamente fallará este componente.
- Componentes simultáneos: Una instancia puede a su vez contar con varios servidores que brindan el mismo servicio.
- Capacidad de soportar ataque DDOS masivo: Dada la configuración de nuestro softswitch nos permite ante un ataque DDOS masivo desconectar los componentes atacados, continuar con los que no lo están y si es necesario levantar componentes nuevos.
- Conexión mediante Intranet de nuestros servidores: Aún en el caso que algún servidor sea atacado o tenga problema en su conexión a Internet, los mismos se conectan mediante una Intranet de manera que normalmente no se pierde acceso a los mismos.

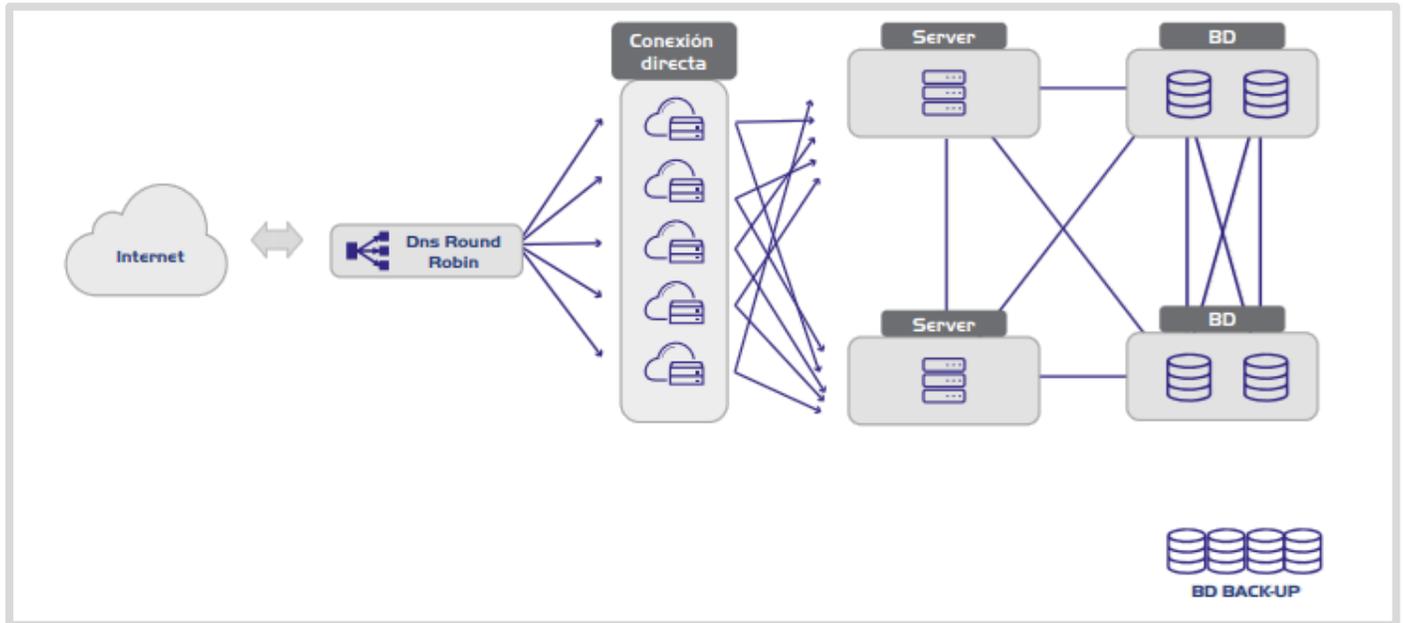
- Topología de la red:



Topología general servidores CallMyWay

- El núcleo o «core» de CallMyWay opera en modo de redundancia activa con dos núcleos operativos.
- El núcleo no es visible desde el Internet
- El núcleo se conecta a las bases de datos para efectos de registro, autenticación y cobro, las bases de datos no son visibles desde el Internet
- A cada núcleo se pueden conectar una cantidad ilimitada de SIPProxys/SBCs. Estos conectan a un núcleo primario y otro de respaldo.
- En caso de un ataque DDOS los elementos de la red atacados son los SIP Proxy/SBCs que son visibles desde el Internet y estos al ser atacados salen de servicio sin afectar el Núcleo.
- En caso de una falla en un sector de Internet de la misma manera el SIPProxy/SBC deja de ser visible para el o los clientes afectados.
- Para ambos casos los equipos se redireccionan a las IPS de otros SIPProxys/SBCs operativos. Para los equipos que toleran cuando menos dos IPS a las cuales registrarse la avería pueden ser imperceptible.
- En el caso que todos los SIPProxy/SBC sean afectados, se pueden levantar nuevos servicios en corto tiempo.

Topología de la Red HTTPS:



Topología general servidores CallMyWay

- El sitio HTTPS opera con múltiples servidores.
- La carga en los servidores se distribuye mediante el protocolo de consulta DNS Round Robin.
- Las bases de datos operan con redundancia y respaldos.
- Las bases de datos nunca son expuestas al Internet de Manera directa.
- Dado que las vulnerabilidades en los sitios, protocolos, servidores, aplicaciones y sistemas operativos son cambiantes, se utiliza el sitio <https://www.ssllabs.com/> para conocer en tiempo real el estado de seguridad del sitio.
- Cuando se detecta una vulnerabilidad todos los sitios que la utilizan, bajan su estado de seguridad, esto se mantiene así hasta que se desarrolla la solución y se implementa en el sitio o el componente correspondiente.

NOC y Control de servicios

- NOC: Contamos con un Centro de Operaciones moderno que nos permite controlar y monitorear en tiempo real el estado de nuestra red y servicios
- Métricas: Contamos con un sistema de monitoreo permanente con miles de parámetros dentro de nuestra red y servicios, lo que nos permite generar y evaluar nuestras métricas.
- Generación de alarmas: Gracias al sistema de métricas y los criterios operativos con que contamos, es posible establecer umbrales de alarma para ciertos parámetros o equipos, permitiéndonos generalmente, actuar de manera proactiva ante posibles fallos o comportamientos atípicos de nuestros servicios o equipos.
- Forense: Debido a que nuestra red y servicios están constantemente monitoreados mediante aplicaciones informáticas que almacenan un histórico de datos de todos los parámetros monitoreados, es posible, en la mayoría de los casos, establecer las causas o síntomas relacionados o correlacionados a cualquier evento que se presente.

Bases de datos

- Conectividad: Nuestras bases de datos no cuentan con conexión a Internet, para accederlas lo hacemos de manera indirecta.
- Redundancia: Operativamente contamos con varias bases de datos que operan simultáneamente de manera replicada, para efectos de consulta y operación.
- Respaldo: Respaldamos nuestras bases de datos varias veces al día y dichos respaldos se almacenan fuera de línea (off-line), de manera que ante una pérdida masiva de datos o secuestro de bases de datos, podemos volver a operar con una pérdida imperceptible o mínima de información.

Tiempos de atención y solución diferenciados por niveles de criticidad (baja, normal, alta, muy alta)

A continuación, se presentan los niveles de servicio:

DESCRIPCION	TIEMPO DE ATENCION	TIEMPO DE SOLUCION
S1- Crítica: El equipo no es operativo y el trabajo está afectado de manera importante a la Compañía. No hay alternativa disponible.	1 hora	3 horas
S2 – Alta: El equipo está afectado de manera importante.	1.5 horas	4 horas
S3 – Normal: Las operaciones del equipo están afectadas, pero se puede continuar trabajando. El equipo no funciona de acuerdo con la documentación del producto.	2 horas	4 horas
S4 – Baja Impacto mínimo – el problema no afecta las operaciones normales. Peticiones de funcionalidad, consultas, etc.	2 horas	4 horas

11. Esquema de penalización de servicio, basado en acuerdos de nivel de servicio (SLA), los cuales deberán ser directamente proporcionales a los tiempos de atención y solución de tres niveles (el cual deberá quedar establecido en el SOW y contrato final) y disponibilidad del sistema 7x24x365 99.99%.

Las penalizaciones se llevarán a cabo basadas en:

- 1.- El porcentaje de cumplimiento de los niveles de servicio acordados (SLA) cada mes, deberá ser mínimo un 98% y el incumplimiento se descontará a la factura general.
- 2.- Los incidentes y requerimientos, no atendidos en tiempo y forma se descontarán a la factura del sitio afectado.
- 3.- Incumplimiento en las actividades pactadas en el documento SOW (nuevos requerimientos, gestión administrativa, reportes, entrega de nuevo equipamiento, controles de cambios, mantenimientos preventivos, etc.). El cálculo de las penalizaciones deberá ser llevado a cabo y pactado por ambas partes.