sistemaISIS

QSA

Condiciones del **Servicio SLA**[1].

(Service Level Agreement)

// **Anexo** servicio de Mantenimiento, Actualización y Soporte del Sistema (SLA)

// **Anexo** servicio de Mantenimiento, Actualización y Soporte del Sistema (SLA)

Condiciones del **Servicio SLA**[1].

(Service Level Agreement)

01 Objeto.

Tener activo el SLA tiene como objetivo **establecer los parámetros de operación** relacionados con el Soporte Técnico, Atención de Peticiones, Quejas y Reclamos que, como empresa proveedora de servicios, estamos en capacidad de ofrecer. Así también mantener el funcionamiento de todas las opciones incluidas en la versión de su Sistema Isis®.

02 | Alcance.

02.1 El soporte **por mesa de ayuda** es brindado por medio de Ticket Web, vía telefónica o control remoto, según lo indique el nivel de servicio contratado. Siempre una consulta o solicitud de servicio debe iniciarse a través de un ticket. El mismo hace referencia a cualquier consulta sobre el uso puntual de los componentes del sistema implementado, incidentes, problemas en la operación y modificaciones por requerimientos impositivos en los formularios de Remitos, Facturas (A, B, C, E y M) y Recibos de haberes. Todo lo que se encuentre excluido de lo anteriormente mencionado, será analizado y de ser posible la modificación, se enviará el presupuesto correspondiente.

El servicio **NO incluye** la atención de incidencias sobre aplicativos que no hayan sido desarrollados por QSA, así como tampoco la cobertura de problemas referentes a la red del cliente, funcionamiento de sus sistemas externos, instalaciones, ni horas de capacitación.

02.2 Provisión de todas las nuevas versiones que QSA desarrolle de su Sistema ISIS®, más las actualizaciones que se generen, sean estas legales, impositivas, contables o **mejoras que se incorporen.**

02.3 La disponibilidad de **nuevas versiones y upgrades son informadas** por notificación en el sistema. Este procedimiento es de exclusiva responsabilidad del usuario o el responsable de sistemas del cliente. Si el cliente solicita una instalación personalizada que no está incluida en el SLA, se cotizará por hora de servicio al valor vigente en nuestra lista de precios y estará sujeta a la disponibilidad del personal técnico de QSA.

02.4 El **llamado telefónico y acceso remoto** a la terminal del cliente será solicitado por el operador de mesa de ayuda si lo considera necesario para poder visualizar/analizar el inconveniente, siendo tarea del cliente realizar cualquier paso indicado por el operador para solucionarlo.

Nota importante [1]: El presente SLA solo cubre actividades de soporte una vez que el (los) servicio(s) contratados entran en etapa de producción, lo que se aplica a partir del informe del área de Implementaciones indicando que el cliente cumplió con los requisitos de prácticas correspondiente durante la implementación.

03 | Horario de **soporte.**

El servicio se prestará los días hábiles de **lunes a viernes de 09:00 a 18:00 horas.**

El usuario podrá ingresar tickets de consulta fuera de este horario desde el portal tickets.sistemaisis.com, aunque los mismos serán analizados y asignados por orden de ingreso en el primer día hábil siguiente, cuando el personal de mesa de ayuda **se reintegre a sus tareas.**

04 | Nivel del **servicio (SLA).**

El SLA establece y documenta el nivel de servicio a brindar por QSA para la atención de requerimientos del Cliente en cuanto al exclusivo funcionamiento del sistema.
Los requerimientos se tipifican como se indica a continuación:

01/ Errores o Incidentes del Sistema.
02/ Consultas funcionales.
03/ Mejoras funcionales.
04/ Impacto en el sistema por cambios legales.
05/ Solicitud de servicios adicionales, capacitaciones y/o implementaciones.

04.1 Los requerimientos tipificados como Errores o Incidentes del Sistema se clasifican en los siguientes niveles **según su criticidad:**

04.1.1 NIVEL 1 – CRITICIDAD ALTA

Significa que la funcionalidad del Sistema o procesos críticos no están operando correctamente debido a un error o parada no programada del Sistema y no hay una solución inmediata disponible, impidiendo al cliente realizar las tareas que impliquen la necesidad de utilizar el sistema.

Tiempo de reacción:
1 hora a partir del momento en que se recibe el reclamo.
Tiempo de respuesta:
Se le dará tratamiento con alta prioridad **dentro de las 24 horas hábiles** a partir del momento en que se asigna el ticket a un operador.

04.1.2 NIVEL 2 – CRITICIDAD MEDIA

Significa que la funcionalidad del sistema o procesos no críticos presentan inconvenientes, pudiendo continuar en forma restringida y solo está disponible una solución temporal.

Tiempo de reacción:
2 horas a partir del momento en que se recibe el reclamo.
Tiempo de respuesta:
Se le dará tratamiento **dentro de las 48 horas hábiles** a partir del momento en que se asigna el ticket a un operador.

04.1.3 NIVEL 3 – CRITICIDAD BAJA

Significa que la funcionalidad del sistema o procesos no críticos presentan inconvenientes menores, permitiendo al usuario continuar utilizando el sistema de forma habitual. Se incluyen aquí preguntas generales de uso y requerimientos de customización.

Tiempo de reacción:
4 horas a partir del momento en que se recibe el reclamo.
Tiempo de respuesta:
se le dará tratamiento **dentro de los 7 días hábiles** a partir del momento en que se asigna el ticket a un operador.

Importante.

QSA puede **recategorizar la criticidad** de un ticket si el cliente no describe claramente el problema o no adjunta la documentación correspondiente. En caso de contar con disponibilidad, el ticket puede resolverse en plazos menores, sin importar la criticidad asignada.

QSA **solo brinda soporte** sobre problemas o consultas relacionadas con el software provisto. No se incluyen problemas de equipamiento, redes, sistemas operativos o internet.

Los tiempos de **reacción y respuesta** se contemplan dentro del horario de atención de la mesa de ayuda.

04.2 NIVEL DE ESCALAMIENTO

En caso que el error o incidente **no pueda ser resuelto** por el operador de mesa de ayuda, el requerimiento será escalado al jefe del sector; si no puede ser resuelto por éste, se escalará al gerente de servicios o producto, dentro de los plazos especificados en el nivel de criticidad.

04.3 MEJORAS FUNCIONALES

Se solicitarán en forma fehaciente a QSA quien evaluará el pedido, pudiéndose solicitar una reunión de relevamiento para analizar los mismos. Ante solicitudes de cambios legales particulares o específicos a su actividad, la documentación y reglamentaciones de los mismos deberán **ser suministrados por el Cliente.**

Una vez analizada la solicitud, QSA elevará un informe al cliente con el resultado del análisis de factibilidad.

Todos los desarrollos adicionales para personalizar el sistema, se cotizarán por separado ya que no se encuentran cubiertos por el presente SLA, y tienen impacto en el costo del SLA, debido a que requieren de actualizaciones al igual que el sistema estándar.

04.4 CAMBIOS LEGALES

Es responsabilidad de QSA, mantener actualizados los sistemas por cambios legales y/o impositivos que afecten la operatoria de los sistemas, de tal manera que el Cliente reciba en tiempo y forma las

actualizaciones.

En algunos casos donde los cambios legales y/o impositivos no sean claros en la reglamentación, pueden ocasionar demoras hasta que los consultores internos y externos dictaminen el procedimiento a aplicar y así poder realizar el cambio apropiadamente en los sistemas, y que los mismos estén funcionando correctamente.

Las versiones del sistema ISIS® no actualizadas, pueden no ser compatibles con la legislación contable e impositiva vigente.

05 | Capacitaciones e **implementaciones.**

Todas las horas adicionales que requiera el Cliente en concepto de capacitación, implementación y asistencia personalizada, se cotizarán por separado ya que no se encuentran cubiertas por el presente SLA. **El valor de la hora será el vigente a la fecha de cotización.**

06 | Consultas a la mesa de ayuda **con SLA activo.**

(CLIENTE CON SERVICIO DE MANTENIMIENTO CONTRATADO)

Las consultas a la mesa de ayuda deben ser iniciadas por medio de un ticket ingresado a nuestro portal **tickets.sistemaisis.com,** completando toda la información requerida.

El SLA no contempla la solución de problemas si el usuario no realizó las capacitaciones correspondientes. En ese caso, nuestro operador de mesa de ayuda derivará la consulta al área correspondiente, dando por cerrado el ticket.

06.1 GENERACIÓN DE TICKETS

Deben ser ingresados desde nuestro portal **tickets.sistemaisis.com**

06.1.1 La información solicitada es necesaria para que nuestro asesor de soporte pueda detectar rápidamente su inconveniente. Si se omite parte de la misma, puede derivar en demoras adicionales.

06.1.2 Cuando se adjunta una imagen con un cartel de error, el mismo debe ser enviado en su contexto, evitando el recorte parcial de la imagen que no permita identificar mayores datos del sistema.

06.1.3 Las solicitudes de modificaciones de reportes/formularios deben tener especificado el reporte/formulario en cuestión y el detalle de las modificaciones expresamente detalladas, independientemente de si se envía algún ejemplo.

06.1.4 Debe mantenerse actualizada la información de contacto en nuestro portal para que nuestros asesores puedan comunicarse con el cliente sin inconvenientes.

06.2 CONDICIONES DE LOS TICKETS

Por cada tema o consulta debe subirse un ticket reportándolo con todas las especificaciones descritas en el punto 6.1. No se aceptarán tickets con más de una consulta.

06.2.1 Las consultas que la mesa de ayuda puede resolver son de carácter operativo y puntuales. En el caso que las mismas refieran a operatorias que no se hayan implementado o se desconozca su funcionalidad, serán derivadas al área correspondiente.

06.2.2 El sistema enviará un mensaje por WhatsApp al teléfono del usuario registrado en nuestra web de tickets cuando la consulta sea asignada y otro cuando esté respondida.

06.2.3 El acceso remoto a la terminal del cliente será solicitado por el operador de mesa de ayuda si lo considera necesario para visualizar/analizar el inconveniente. Será tarea del cliente realizar cualquier paso indicado por el operador para solucionarlo. Dicha conexión se llevará a cabo exclusivamente con previo consentimiento.

06.2.4 El personal debe ser tratado con el mismo respeto con el que tratamos a los clientes. No se atenderán llamados telefónicos o tickets que contengan agravios al operador, el servicio o el sistema; directamente serán rechazados.

07 | Consultas a la mesa de ayuda con **el SLA inactivo.**

(CLIENTE NO ABONADO A MANTENIMIENTO)

QSA solo ofrece **soporte y actualizaciones rentados,** para lo cual pone a disposición del cliente opciones de convenios de mantenimiento que cubren distintos alcances, el cliente que no tiene un convenio de SLA activo, no está habilitado para acceder a la mesa de ayuda, ni a recibir actualizaciones de ningún tipo, l sistema no procesará consultas de clientes que no tengan una opción de SLA activa.

sistemaISIS

QSA

Anexo **I.**

// **Al servicio** de Cloud.

Anexo I.

// **Al Servicio** de Cloud.

PRIMERA

El cliente en caso de querer suspender o cancelar el servicio debe informarlo de modo fehaciente a QSA con **al menos 30 días.**

QSA tomará nota del pedido y dará de baja el servicio siempre que el cliente esté al día con los pagos.
En estos casos regirá la política de backups incluida en el Anexo II al presente.

SEGUNDA

QSA informará al cliente los cortes en el servicio programados por mantenimiento y actualización.
Sin embargo, en **aquellos casos de fuerza mayor o caso fortuito** —ajenos a QSA— no será responsable del no servicio por ser ajeno a su control y no haber podido proveerlos. Por supuesto que hará sus máximos esfuerzos para que el servicio se reestablezca a la brevedad.

TERCERA

El **Servicio de mesa de ayuda** tiene las características y el formato descripto en el principal de este contrato.

CUARTA

El cliente deberá:

(i) Actuar en forma responsable, conservando de la mejor forma posible la integridad de los recursos informáticos que son propiedad de QSA y que ella pone a disposición.

(ii) Respetar los derechos de otros usuarios y respetar la integridad de sus sistemas de seguridad, respetar toda licencia y/o acuerdos contractuales que estén relacionados con los sistemas de información o las herramientas informáticas de la organización.

(iii) Actuar de acuerdo a este convenio y Anexos, además de las Leyes y Normas ya previstas, en cuanto al cuidado y responsabilidad de los materiales y recursos aportados por QSA.

QUINTA Seguridad.

El cliente es consciente que ningún sistema de información es completamente seguro, que personas dentro o fuera de la organización pueden encontrar formas de tener acceso a la información considerada confidencial, vital o estratégica.

SEXTA Uso y conservación.

El cliente se obliga a contribuir al cuidado y conservación de las instalaciones y sistemas

SÉPTIMA Uso laboral y uso personal.

El cliente tiene en especial consideración que la utilización de los diferentes sistemas de información de QSA es de uso exclusivo para fines laborales.

El uso personal de cualquier sistema de información para acceder, descargar, transmitir, distribuir o almacenar material obsceno está absolutamente prohibido. El uso de los recursos informáticos (sistemas de información y equipos) que tengan como objetivo cualquier tipo de ganancia económica personal para cualquier cliente está prohibido sin excepción alguna.

Bajo ninguna circunstancia el uso personal de estos sistemas por parte de los clientes debe influir de manera negativa en el desempeño de las tareas y responsabilidades para la organización.

El cliente le asegura a QSA que no utilizará Internet para propósitos que puedan influir negativamente en la imagen de QSA o de sus directivos, y en caso de hacerlo será responsable de esas circunstancias.

OCTAVA

El cliente sabe que el acceso no autorizado a los sistemas de información de QSA está terminantemente prohibido.

De este modo el cliente debe usar la identificación, identidad, firma electrónica, firma digital o contraseña propia sin poder remitirla o permitir que la use otro usuario o cliente.

Así las cosas el cliente asume el compromiso de no informar a terceros su contraseña o identificación, a excepción en casos que deban facilitarse para la reparación o mantenimiento de algún sistema o equipo. En este caso y en forma estrictamente circunstancial, solo deberá hacerlo al personal técnico o informático autorizado, debidamente identificado.

NOVENA Política de Contraseñas.

Es obligación de los clientes respetar la siguiente política de contraseñas:

(i) Seleccionar una contraseña con un largo mínimo de ocho caracteres utilizando letras y números, mayúsculas y caracteres especiales.

(ii) Queda prohibido establecer contraseñas que estén basadas en algún dato de índole personal, como, por ejemplo, fecha de cumpleaños o de nacimiento del cliente, su número de teléfono, etc.

(iii) En caso de sospechar que algún tercero pudo haber tenido acceso a la contraseña, deberá solicitar el cambio sin dilación siendo responsable en caso que eso no ocurra.

(iv) En caso de haber extraviado u olvidado la contraseña el cliente deberá solicitar a QSA que revoque la contraseña actual y le permita asignar una nueva.

DÉCIMA Política de Contraseñas.

El cliente se compromete a no hacer uso del sistema con alguna de las siguientes finalidades:

1. Intentar modificar, reubicar o sustraer, software; información, sin la debida autorización.

2. Modificar, alterar, borrar o inferir cualquier otro daño en las configuraciones de sistemas operativos, o sistemas aplicativos que se encuentren instalados en los distintos equipos, sin las autorizaciones correspondientes.

3. Acceder sin la debida autorización, mediante los equipos y/o software, a sistemas externos y que no pertenezcan a la organización.

4. Interferir sin autorización, el acceso a otros clientes o terceros a los recursos de los sistemas.

5. Transgredir o eludir las verificaciones de identidad u otros sistemas de seguridad.

6. Utilizar los sistemas de información para fines ilegales o no autorizados.

7. Enviar cualquier transmisión de datos en forma fraudulenta.

8. Revelar a terceros contraseñas de acceso o compartirlas con terceros.

9. Realizar cualquier actividad de recreación personal o de promoción de intereses personales

10. Iniciar sesiones de Internet usando recursos de QSA desde ubicaciones remotas, salvo que estén especialmente autorizados para ello.

11. Almacenar archivos personales de cualquier índole

12. Violar cualquier licencia de software o derechos de autor, incluyendo la copia o distribución de software protegido legalmente, sin la autorización escrita del propietario del software.

13. Acceder al código fuente de una obra de software sin autorización del autor con la finalidad de modificarlo superficial o sustancialmente.

14. Realizar conductas semejantes a las descriptas en el punto anterior que puedan tener como resultado el plagio de una obra de software.

15. Efectuar el “downloading” o descarga de archivos, salvo que esta posibilidad no implique vulnerar o infringir los derechos de terceros titulares de derechos de autor.

16. Instalar o procesar sistemas o software no autorizado, con el propósito de la utilización personal de los mismos.

17. Usar cualquier método de correo electrónico o cualquier tipo de comunicación electrónica con el propósito de acosar, amenazar, molestar, entorpecer a terceros.

18. Usar cualquier método de correo electrónico o cualquier tipo de comunicación electrónica con el propósito de revelar información privada de otros clientes,

19 Leer información o archivos de otros clientes,

20. Realizar cualquier actividad contraria a los intereses de QSA, tal como publicar información reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros mediante el mal uso deliberado de recursos comunes.

21. Alterar, falsificar o de alguna otra forma usar de manera fraudulenta los archivos, permisos, documentos de identificación, u otros documentos o propiedades.

22. Usar cualquier método de correo electrónico o cualquier tipo de comunicación electrónica con el propósito de dañar o perjudicar de alguna manera los recursos informáticos.

23. Lanzar cualquier tipo de virus, gusano, o programa de computación cuya intención sea hostil, destructiva, o que impacte directamente en el funcionamiento adecuado de los diferentes sistemas de QSA propios y/o de terceros.

24. Descargar o publicar material ilegal, con derechos de propiedad o material nocivo, a través de los recursos brindados por QSA.

25. Uso personal de cualquier sistema de información, para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno y/o pornográfico o que excedan los límites de los estándares generalmente aceptados de ética y buen gusto.

26. Violar cualquier ley o norma municipal, provincial o nacional, respecto al uso de los sistemas de información, así como también realizar cualquier conducta ilegal contraria a la legislación aplicable de cualquier país al que se pueda tener acceso por la red.

27. La transmisión de publicidad no deseada.

28. Utilización del sistema para juegos recreativos.

29. Queda estrictamente prohibido instalar, ejecutar, operar, “bajar” o copiar cualquier tipo de programa o archivo que no sea laboral.

30. No se puede almacenar pornografía, ni elementos racistas, ni cualquier otra cosa que pueda considerarse ofensiva, o que atenten contra la ley, la moral y las buenas costumbres, en ningún servidor o sistema provisto por QSA.

31. Eliminar, detener o de algún otro modo inutilizar, ya sea en forma temporal o permanente, cualquier dato informático, programa informático o software informático del sistema de QSA.

32. Causar el mal funcionamiento del sistema de QSA sin importar la duración de dicho mal funcionamiento.

33. Alterar o borrar algún dato, programa o software.

sistemaISIS

Stark Cloud®

Anexo **II.**

// **Política** de Respalos.

Anexo I.

// **Política** de Respaldos.

Objetivo.

La información almacenada y procesada es uno de los **activos más importantes de la empresa,** todos los dispositivos o equipos informáticos que albergan esta información pueden verse involucrada en situaciones como robos, virus, borrados accidentales o catástrofes naturales, es por eso por lo que es importante contar con medidas que permitan garantizar o maximizar la disponibilidad de esta con el objetivo de poder acceder a este siempre que se necesite.

Alcance.

Esta política aplica activos, bienes o servicios que **la empresa defina como críticos o clave** en su continuidad operativa, esto sea información contenida en servidores, estaciones de trabajo o correos que contenga datos, configuraciones, aplicaciones, bases de datos y servicios críticos por StarkCloud.

Esto será aplicable a todos los usuarios tanto internos como externos que utilicen recursos de la empresa inclusive empresas que presten servicios a StarkCloud.

Definiciones.

- **Activo de Información:** Recursos del sistema de Información que para la institución es considerada importante o de alta validez que utiliza y son necesarios para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Integridad:** Se entiende como la característica que implica la corrección y completitud de los datos o de la información manejada, contar con todas sus partes y estar completo.
- **Disponibilidad:** Es el aseguramiento de que los usuarios autorizados tienen acceso a la información, sistemas y a los activos cuando es requerido.
- **Confidencialidad:** Es la propiedad de la información, un documento o mensaje que únicamente está autorizado para ser leído o entendido por algunas personas o entidades. Mantiene la cualidad de mantenerse reservada para el conocimiento de una persona o de algunas, pero no debe ser expuesta en forma masiva.
- **Retención:** Periodo por el cual permanece vigente el respaldo, pudiendo ser semanal, mensual, semestral, anual.
- **Periodicidad:** Frecuencia con la que se ejecutará el respaldo de la información.
- **TS:** Componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red, comúnmente se hace referencia a un servidor específico TS.

Roles y **responsabilidades.**

TI / Plataforma Inxap:

- **Debe Definir** el estándar de respaldo de los servidores y equipos de hardware, que contenga activos importantes con respecto a BBDD, aplicaciones, configuraciones de servicios y de los datos en ambiente de producción.
- **Debe Autorizar** las solicitudes de respaldo especiales, Coordinar, ejecutar y velar por la realización de las pruebas y restauración de las copias de respaldo efectuadas utilizando las herramientas pertinentes para tales efectos.
- **Mantener** un inventario de los activos de información sobre los que se realiza copia de seguridad.
- **Mantener** las condiciones ambientales óptimas y de seguridad de acceso a los activos de información que estén bajo su responsabilidad.
- **Cumplir** con lo formalizado en esta Política y así garantizar que los activos de información que se encuentren a su cargo estén protegidos contra el mal uso, robo, falta de disponibilidad o destrucción.
- **Utilizar** los medios de respaldos facilitados de acuerdo con lo establecido en esta política.

Gerente Cloud:

- **Debe controlar** que los administradores de Plataforma controlen el estado diario de los Backup.
- **Supervisar** que el personal a su cargo cumpla la actual política.

Oficial de Seguridad:

- **Velar** por la difusión y cumplimiento de esta política.
- **Monitorear** el correcto funcionamiento y operación respecto a la ejecución de respaldos, tanto de servidores como de BBDD o cualquier otro activo que se estime valioso.
- **Actualizar** la política.

Usuarios TS:

- **Respaldar** datos personales tales como documentos, fotos y cualquier otro material que esté fuera del alcance de los servicios de Plataforma, siendo estos de su propia responsabilidad y no le compete, ni responsabiliza a StarkCloud o QSA.

Directrices **Generales.**

- **Debe existir** personal entrenado y capacitado en los procedimientos definidos y además conocer claramente los roles y responsabilidades que le competen en el marco de la continuidad del negocio.

- **Los procesos o servicios** de StarkCloud o QSA que sean desarrollados por terceras personas deben disponer de planes de continuidad y estos deben ser entregados a personal de Plataforma.

Política.

Toda la **información de los sistemas informáticos críticos** en producción de StarkCloud o QSA deben ser protegidos de posibles fallos por lo que debe ser respaldada con cierta frecuencia, que permita asegurar un adecuado proceso de recuperación, estableciendo para ellos pruebas de manera regular.

El Departamento de Tecnologías o Plataforma, **debe considerar soluciones de respaldo** para servidores, BBDD y aplicaciones (códigos fuentes, bases de datos, archivos de configuración) que se consideren críticos para la empresa así como también garantizar la disponibilidad de infraestructura adecuada de respaldo, con servidores dedicados albergados de manera local o remota a la plataforma productiva, esto con el objetivo de asegurar que estos estén disponibles incluso después de un desastre o la falla de un equipo.

Identificación de **activos críticos.**

Los responsables de las distintas áreas / Plataforma de StarkCloud serán los **encargados de identificar y mantener un registro actualizado** de todos los activos que son relevantes mantener y resguardar debido a que son claves para mantener operativo sus procesos y serían necesarios restaurar en caso de eventuales problemas.

- BBDD Instance SQL
- Directorio Archivos ISIS Cloud (Directorios específicos).
- Aplicaciones y desarrollos específicos.
- Archivos de Licencia.

Plan de **respaldo.**

El equipo de plataforma define los **tipos de respaldos a aplicar** según el tipo de activo a resguardar o servicios específicos contratados por el cliente, cada estándar especifica:

- Frecuencia del respaldo.
- Tipo de contenido y archivos.
- Tiempo de retención y borrado.

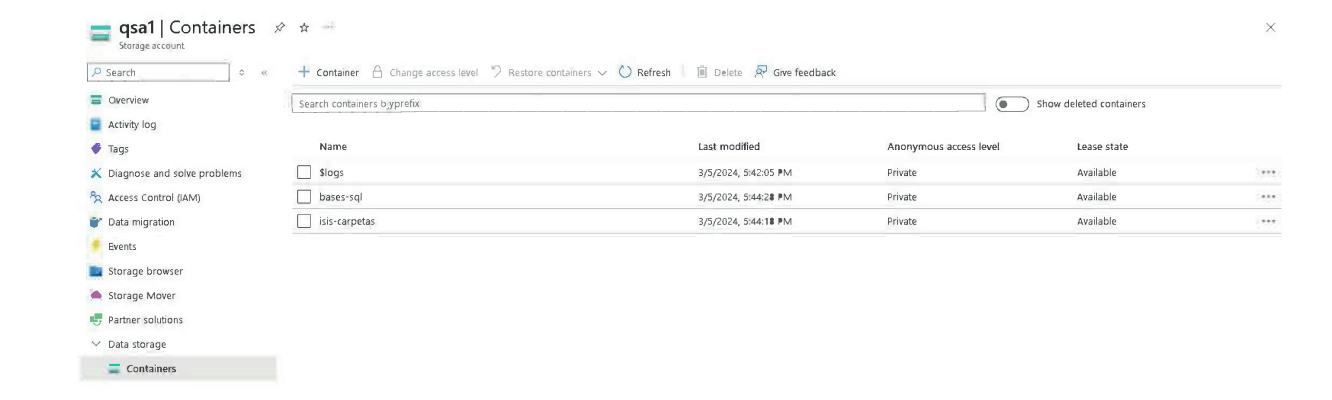
Tabla resumen Frecuencia y **Modalidad de Respaldos.**

Servidor	Frecuencia	Tipo Respaldo	Retención
SQL	Diaria **23:00 PM**	Máquina Virtual **(Incremental)**	**7 días**
Aplicaciones	Diaria **23:00 PM**	Máquina Virtual **(Incremental)**	**7 días**

Respaldo (CBR) almacenado en contenedores Cloud ubicados en Datacenter Huawei Chile AZI.
Revisión diaria gestionada por personal específico de Plataforma StarkCloud.

Existe una **modalidad adicional de respaldo** orientado a resguardar las bases de datos específicas de los clientes, esta modalidad las lleva a una ubicación remota, esto con el objetivo de que en caso de que la plataforma base (Datacenter) se vea afectada por un desastre y se pierda el acceso a estas.

Objeto	Frecuencia	Tipo Respaldo
Logs	Diaria	Respaldo Ubicación Remota **(Azure)**
Bases-sql	Diaria	Respaldo Ubicación Remota **(Azure)**
Datos de Clientes	Diaria	Respaldo Ubicación Remota **(Azure)**



RPO / **RTO**

Concepto	Restauración Instancia 2	Restauración Schema (1 sola)
RTO	horas Aprox.	BD) 1 hora Aprox.
RPO	24 horas Aprox.	24 horas Aprox.

***Los Tiempos de restauración** de Instancia y Schema son estimados debido a que el tiempo de restauración o recuperación de una base de datos o Schema varía según el tamaño y crecimiento que esta va teniendo.

***Hay que considerar que una restauración** por logs de transacciones solo será efectiva en el día en curso y se asocia a la instancia completa, afectando a todas las bases alojadas en el servidor.

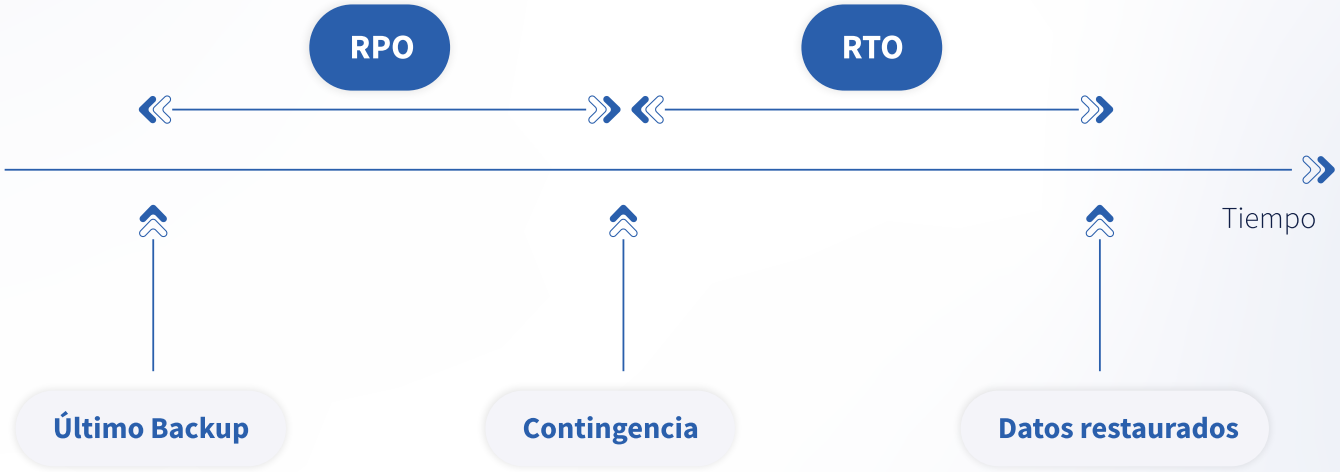
Tiempos **de respuesta.**

RTO (Recovery Time Objective):

El RTO es la **cantidad máxima de tiempo** que debe tomar restaurar la funcionalidad de la aplicación y/o servidor en caso de una pérdida repentina del servicio.

Normalmente se mide este intervalo en segundos, minutos, horas o días. Idealmente se desea un RTO en el extremo más corto del espectro: 60 minutos es un sólido punto de referencia.

La respuesta dependerá de la criticidad de cada aplicación.



Evaluación **y Difusión.**

La configuración y ejecución de respaldos **se debe monitorear y evaluar constantemente** a través de controles de ejecución diario-semanal.

Pruebas semestrales o anuales de recuperación deben ser solicitadas y coordinadas por el cliente y pueden requerir evaluación comercial según el tipo de recuperación a realizar.

Validación configuración **/ Ejecución de respaldos.**

La política actual debe **ser evaluada por el personal de StarkCloud** al menos una vez al año o cuando las circunstancias lo requieran con el fin de asegurar la eficiencia y efectividad de la política.