TABLA DE CONTENIDO

TERMINOS Y CONDICIONES DE USO DE NUBE ARSAT

CONSIDERACIONES GENERALES

A partir de la firma del contrato de prestación de servicios de Nube ARSAT, el Cliente acepta los Términos y Condiciones de uso del servicio de Nube, el Modelo de Responsabilidad Compartida del servicio de Nube y la Política de Seguridad de la Información del Servicio de Nube. El contenido de dichos documentos se encuentra en el presente apartado y pueden consultarse en: https://nube.arsat.com.ar/

Las PARTES definen y asignan sus responsabilidades relativas a la Seguridad de la Información para el servicio Nube ARSAT sobre el Modelo de Responsabilidad Compartida previamente mencionado. En particular, el Cliente será responsable de: la seguridad en la Nube de sus datos, la plataforma, aplicaciones, identidad y control de acceso, encripción, sistema operativo, redes y configuración de firewall.

En el caso de que dicha información sea actualizada por razones de seguridad y/o con el fin de mejorar los servicios contratados, las nuevas condiciones entrarán en vigencia a partir de su aceptación o a partir de los 30 (treinta) días corridos después de su publicación y podrán consultarse en el mismo enlace.

En caso de no estar de acuerdo, dentro de los 20 (veinte) días corridos a partir de la publicación de la nueva versión el Cliente debe enviar un correo electrónico al ejecutivo designado por ARSAT para proceder a la baja del servicio. De no existir manifestación dentro del plazo estipulado, se entenderá que el Cliente ha aceptado las nuevas condiciones.

TERMINOS Y CONDICIONES DE USO

El Cliente se compromete a:

- No acceder a datos restringidos o intentar violar las barreras de seguridad para llegar a ellos.
- No realizar búsquedas de vulnerabilidades o explotación de las mismas para cualquier fin.
- No divulgar información acerca de la detección de vulnerabilidades encontradas en los servicios contratados.
- Comunicar a ARSAT toda información a la que tenga acceso que pudiera implicar un compromiso a la seguridad de la información o los servicios brindados.
- No proporcionar información personal falsa ni crear cuentas a nombre de terceros.
- No crear otra cuenta sin permiso expreso del usuario administrador, en caso de que este último haya inhabilitado la cuenta original.
- Mantener la información de contacto exacta y actualizada.
- No compartir la contraseña ni permitir que otra persona acceda a su cuenta.
- No llevar a cabo acciones prohibidas, incluyendo, pero no limitándose a:

  - Hostigar, acosar, amenazar, acechar, realizar actos de vandalismo hacia otros Usuarios.
  - Infringir los derechos a la intimidad de otros usuarios del servicio.
  - Solicitar información personal identificable de otros usuarios del servicio con el propósito de hostigar, atacar, explotar, violar la intimidad de los mismos;
  - Publicar de manera intencionada o con conocimiento injurias o calumnias;

- Publicar, con el intento de engañar, contenido que es falso o inexacto;
- Intentar usurpar la identidad de otro Usuario, representando de manera falsa su afiliación con cualquier individuo o entidad, o utilizar el nombre de otro usuario con el propósito de engañar;
- Almacenar, transmitir, promover, defender o mostrar pornografía, obscenidad, o cualquier otro contenido obsceno, inmoral, que incite al odio o la violencia;
- Infringir la Ley N° 25.326 de Protección de Datos Personales;
- Realizar cualquier otra acción contraria a la normativa vigente.

Finalmente, el Cliente declara contar con procedimientos documentados donde se detallan las funciones, atribuciones y responsabilidades en el servicio de Nube. La adecuada utilización de los servicios es, sin excepción, de entera responsabilidad del Cliente.

Obligaciones de Seguridad para las Partes

1. ARSAT pondrá a disposición las características de seguridad que sean configurables, para que el Cliente evalúe cuál/es serán implementadas por él mismo. Se informa que ARSAT parte de una base de configuración de seguridad exigible para el Cliente de acuerdo a estándares de seguridad definidos y alineados con marcos de seguridad reconocidos. Para más información: https://nube.arsat.com.ar/ficha/

2. Las PARTES se comprometen a concientizar, educar y capacitar a los empleados, y solicitar a los contratistas que hagan lo mismo, con respecto al manejo adecuado de los datos del Cliente del servicio en la Nube y de los datos derivados del mismo, así como los riesgos de seguridad de la información relacionados con el servicio y el entorno de Nube.

3. El Cliente manifiesta contar con una Política de Control de Accesos con especificaciones y requisitos para la gestión de los derechos de acceso de los usuarios en el servicio de Nube y con un proceso formal que contempla alta, baja y modificaciones de los registros de los usuarios, su monitoreo y revisión permanente de tales permisos y restricciones conforme dicha política.

4. Con el fin de mitigar los riesgos de Seguridad de la Información vinculados a la gestión de identidades y control de accesos en el servicio de Nube, ARSAT proporcionará al Cliente: a) Funciones y especificaciones para la gestión de los derechos de acceso de los usuarios del Cliente en la Nube; b) Funciones y especificaciones de alta y baja de usuarios; c) Procedimientos para la gestión de la información secreta de autenticación del Cliente y d) Mecanismos que le permitan al Cliente restringir el acceso a sus servicios en la Nube.

5. En relación a la Seguridad Operativa:

   5.1 ARSAT:
   - i) Es responsable de proteger la infraestructura que ejecuta los servicios de Nube la cual está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la misma;
   - ii) Se reserva la facultad de supervisar la capacidad de los recursos contratados con el fin de evitar incidentes de seguridad causados por la falta de los mismos tomando las acciones necesarias;

iii) Resguarda los registros de eventos y alertas recopilados en relación con el uso de servicio de la Nube por parte del Cliente durante 15 y 7 días, respectivamente;
iv) Se compromete a notificar las tareas de mantenimiento preventivo conforme lo acordado en la orden de servicios, y el inicio y finalización de los cambios que puedan afectar negativamente al servicio de la Nube;
v) Utiliza 0.south-america.pool.ntp.org para la sincronización de los relojes de Cloud ARSAT en la cual se basará toda la infraestructura que el Cliente contrate;
vi) Proporciona al Cliente capacidades de supervisión sobre aspectos específicos del funcionamiento de los servicios en la Nube;
vii) Informará cuando existan vulnerabilidades técnicas que afecten servicios contratados por el Cliente para que actúe en consecuencia, en caso de aplicarle.

5.2 El Cliente es responsable de:
i) La administración del sistema operativo huésped (incluidos los parches de seguridad y las actualizaciones), de cualquier utilidad o software de aplicaciones que el Cliente haya instalado en las instancias y de la configuración del firewall provisto por ARSAT;
ii) Administrar sus datos (incluidas las opciones de cifrado), clasificar sus recursos y definir políticas y procedimientos para administrar los recursos en la Nube ARSAT, realizar y recuperar copias de seguridad de sus activos, monitorear y administrar la seguridad del entorno informático en el marco de sus responsabilidades;
iii) Articular los medios necesarios, ya sea por un servicio de *backup* contratado a ARSAT o por mecanismos externos, para la realización de sus copias de seguridad que mantendrán sus datos resguardados en caso de eventualidades;
iv) Realizar las pruebas de recuperación de copias de seguridad; o solicitar a ARSAT una Prueba de Recuperación en caso de tener el servicio contratado, que definirá en conjunto con ARSAT el alcance, costos y periodicidad de las mismas;
v) Definir un proceso a los fines de identificar las vulnerabilidades técnicas que será responsable de gestionar. En caso de que el Cliente identifique una vulnerabilidad técnica deberá adoptar las medidas apropiadas para tratar los riesgos asociados en el marco de sus responsabilidades.

6. El Cliente debe notificar a ARSAT en caso de sospecha de uso indebido de sus cuentas o credenciales, detección de vulnerabilidades existentes, y eventos e incidentes de ciberseguridad.

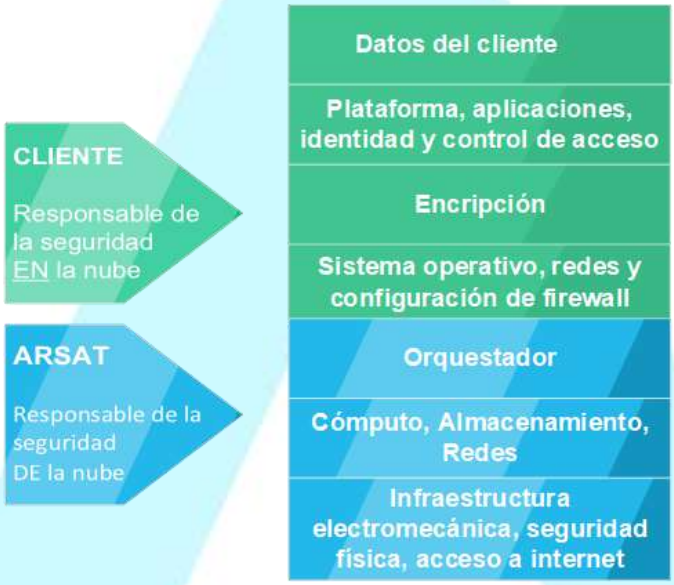
7. Las PARTES, conforme el Modelo de Responsabilidad Compartida, definen procedimientos de gestión de incidentes de seguridad de la información y se comprometen a notificarse cualquier evento y/o incidente de seguridad de la información detectado que pudiere afectarlos, dar seguimiento y utilizar el conocimiento obtenido del análisis y resolución de los mismos para reducir la probabilidad o el impacto en el futuro.

8. Las PARTES cuentan con procesos y procedimientos internos referidos a la continuidad de la gestión de la seguridad de la información en situaciones adversas y han definido controles para verificar periódicamente la validez y eficacia de los mismos.

9. Finalizada la relación contractual, ARSAT efectuará la eliminación segura de todos los recursos contratados (incluidas las copias de seguridad) y se emitirá un informe con las acciones realizados por el operador. La eliminación se hará efectiva en un plazo de 24 (veinticuatro) horas, luego de trascurrido este tiempo no se podrá recuperar la misma.

10. Las PARTES manifiestan tener implementados procedimientos apropiados para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con la normativa atinente a Datos Personales, Propiedad Intelectual y demás regulaciones vinculantes en el servicio de la Nube. Adicionalmente, ARSAT cuenta con auditorias aprobadas y certificaciones internacionales vigentes como ISO/IEC 27001:2013, e ISO 9001:2015 - Avalados por TÜV Rheinland Argentina. Para más información consultar: https://nube.arsat.com.ar/

Esquema - Modelo de Responsabilidad Compartida



Credenciales de acceso

Una vez concluidas todas las gestiones de contratación pertinentes, ARSAT proveerá al Cliente las credenciales de acceso al servicio de Nube para su posterior modificación, debiendo este adoptar las medidas necesarias para evitar el acceso no autorizado. Asimismo, el presente lineamiento se extiende a las tareas realizadas por los empleados del Cliente y/o terceros contratados por el mismo.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO DE NUBE

El Cliente declara conocer y aceptar la Política de Seguridad de la Información de la Nube así como también sus futuras modificaciones luego de ser debidamente comunicada por parte de ARSAT.

Sin perjuicio de las modificaciones que en el futuro pueda tener dicha política, el Cliente acepta que:

1. ARSAT documenta y define las responsabilidades de seguridad de la información para el servicio de Nube y las acuerda con el Cliente, según corresponda.

2. ARSAT no será responsable por la información, datos y/o contenido que transmita, distribuya, acceda y aloje el Cliente en el servicio de Nube. Su propiedad y cualquier daño y/o perjuicio que pudiera generar la misma, responsabilizará de manera exclusiva al Cliente del servicio.

3. Los datos e información almacenada en el servicio de Nube serán tratados como confidenciales. ARSAT no accederá a los contenidos del Cliente, excepto que le sea requerido legal y/o judicialmente.

4. ARSAT no será responsable de proteger y asegurar los datos personales alojados por el Cliente en el servicio de Nube frente a cualquier pérdida, daño o mal uso de los mismos.

5. ARSAT incorpora acuerdos y cláusulas de confidencialidad y no divulgación según las necesidades en todos los convenios/contratos que se suscriban con el Cliente y contratistas.

6. ARSAT incluye en los acuerdos suscriptos con sus proveedores y contratistas obligaciones y aspectos pertinentes a la seguridad de la información con el fin de mitigar los riesgos asociados a los activos de la organización a los cuales tienen acceso.

7. ARSAT prohíbe expresamente utilizar el servicio de Nube para almacenar y/o facilitar la circulación de cualquier contenido ilegal y/o en violación a cualquier regulación vigente en la República Argentina.

8. ARSAT no será responsable por las actividades que realice el Cliente en el servicio de Nube, independientemente de si las actividades fueron realizadas por el Titular del convenio/contrato, un empleado o un tercero.

9. ARSAT implementa controles de acceso y mecanismos de autenticación con el objeto de garantizar que solo el personal autorizado por ARSAT pueda acceder a la infraestructura que ejecuta los servicios de Nube.

10. ARSAT registra y tiene un proceso de revisión periódico del personal operativo que realiza tareas sobre la infraestructura que soporta los servicios de Nube.

11. Los datos almacenados en la infraestructura que ejecuta los servicios de Nube se encuentran cifrados en tránsito mediante algoritmos de encriptación de alta seguridad.

12. ARSAT es el encargado de articular los medios necesarios para resguardar los datos pertenecientes a su infraestructura a fin de brindar los servicios correspondientes de acuerdo a SLA vigente.

13. ARSAT adopta medidas técnicas, organizativas y de seguridad para evitar que el Cliente realice acciones valiéndose de debilidades o vulnerabilidades que afecten y/o pudieren afectar a la infraestructura y/o sistemas asociados al servicio contratado.

14. ARSAT adopta las medidas necesarias para efectuar una adecuada gestión de incidentes que permite prevenir, detectar, contener y erradicar incidentes de seguridad con el objeto de minimizar su impacto en los servicios brindados.

15. ARSAT establece mecanismos de comunicación con el Cliente a través de los canales correspondientes conforme la orden de servicios y/o anexo técnico.

16. ARSAT cuenta con controles preventivos y correctivos para reducir – a niveles aceptables – las posibles interrupciones causadas por fallas significativas, ya sea por desastres naturales o provocadas por el hombre a favor de la continuidad de las operaciones y servicios de Nube brindados.

17. ARSAT cumple con las normas y regulaciones aplicables, incluyendo la normativa de protección de datos personales y aquellas relacionadas con propiedad intelectual e industrial.