ANEXO TÉCNICO Nro. 1 / 2026

A continuación, describimos algunas recomendaciones y aclaraciones para tener en cuenta en la propuesta y posterior Contrato de Soporte Técnico y Actualizaciones de la Plataforma Ariesnet para 2026:

1. SEGURIDAD

Por temas de seguridad en su servidor y demás equipos, Sistemas Aries proporcionará soporte técnico únicamente desde la dirección IP pública que les definiremos a través de las herramientas RustDesk, TeamViewer o Anydesk.

Por parte de Sistemas Aries se asegurará que todas las conexiones de soporte se realicen exclusivamente desde la dirección IP pública que les definiremos y a través de RustDesk, TeamViewer o Anydesk, reforzando así nuestro compromiso con la seguridad. Sin embargo, la responsabilidad final recae sobre la entidad contratante, quien debe garantizar que el acceso remoto esté restringido de manera efectiva, manteniendo un entorno seguro y controlado para la operación del sistema.

Aries Remoto es una herramienta de acceso remoto propiedad de SISTEMAS ARIES S.A.S., desarrollada a partir del software de código abierto RustDesk y adaptada para la prestación de servicios de atención y soporte al cliente. Esta aplicación permite la conexión remota únicamente con asesores debidamente autorizados de SISTEMAS ARIES S.A.S. y no está habilitada para conexiones con terceros externos a la empresa. Al usarlo, la entidad contratante autoriza expresamente el acceso remoto a sus equipos con fines exclusivos de soporte, asistencia y atención al cliente, bajo los lineamientos de seguridad, confidencialidad y protección de la información definidos por SISTEMAS ARIES S.A.S.

Es responsabilidad de la entidad contratante implementar y gestionar las medidas de control necesarias para restringir el acceso remoto al servidor, asegurando un control adecuado del perímetro de seguridad. Esto incluye la configuración de reglas en los firewalls, la limitación de accesos remotos únicamente a conexiones autorizadas, y la reducción de la superficie de ataque para minimizar los riesgos de intrusiones o accesos no autorizados.

2. LIMITACIÓN DE RESPONSABILIDAD:

- ✓ Sistemas Aries S.A.S. no será responsable por interrupciones en la prestación de los servicios contratados que sean consecuencia de factores externos a su control directo, incluyendo pero no limitándose a: fallos en la infraestructura tecnológica o de red del Contratante, problemas de conectividad a internet, mantenimiento no programado del sistema operativo o hardware del Contratante, errores de configuración realizados por personal no autorizado de Sistemas Aries S.A.S., o cualquier otra circunstancia ajena a la gestión y operación directa de Sistemas Aries S.A.S.

- ✓ Fuerza Mayor y Casos Fortuitos: Asimismo, Sistemas Aries S.A.S. no será responsable por interrupciones derivadas de eventos de fuerza mayor o caso fortuito, tales como desastres naturales, actos de terceros, ataques informáticos, virus, malware, ransomware, cortes de energía no gestionados por el Contratante, conflictos laborales, o cualquier otro evento que escape al control razonable de las partes.

- ✓ Obligaciones del Contratante: El Contratante se compromete a mantener su infraestructura tecnológica en condiciones operativas óptimas, incluyendo la actualización y correcto mantenimiento de hardware, software, y medidas de seguridad pertinentes, para asegurar la adecuada recepción y funcionamiento de los servicios prestados por Sistemas Aries S.A.S. En caso de interrupciones atribuibles a deficiencias en la infraestructura del Contratante, Sistemas Aries S.A.S. podrá ofrecer soporte bajo los términos y condiciones acordados, pero no será responsable por la resolución de dichas deficiencias ni por los impactos derivados de las mismas.

- ✓ Procedimiento en Caso de Interrupciones: En el caso de interrupciones en los servicios, Sistemas Aries S.A.S. se compromete a realizar esfuerzos razonables para diagnosticar y, en su caso, sugerir medidas correctivas al Contratante. Sin embargo, la responsabilidad de implementar dichas medidas recaerá exclusivamente en el Contratante, especialmente cuando las causas de la interrupción no sean atribuibles a Sistemas Aries S.A.S.

3. DATOS PERSONALES:

- ✓ Cumplimiento de Normativas: Sistemas Aries S.A.S. se compromete a realizar todas las actividades de soporte, mantenimiento, y manejo de

datos en estricto cumplimiento con las normativas vigentes en Colombia, incluyendo, pero no limitado, a la Ley 1581 de 2012 sobre Protección de Datos Personales, el Decreto 1377 de 2013, y las regulaciones emitidas por la Dirección de Impuestos y Aduanas Nacionales (DIAN) relacionadas con la recepción y manejo de facturación electrónica, así como cualquier normativa aplicable a la contratación pública.

- ✓ Protección de Datos Personales: Sistemas Aries S.A.S. implementará todas las medidas técnicas, administrativas, y de seguridad necesarias para garantizar la confidencialidad, integridad, y disponibilidad de los datos personales tratados en el marco del presente contrato, asegurando que dichos datos sean utilizados únicamente para los fines autorizados y en conformidad con las políticas de protección de datos establecidas por la ley.

- ✓ Responsabilidad del Contratante: El Contratante es responsable de garantizar que la recolección, tratamiento y uso de los datos personales proporcionados a Sistemas Aries S.A.S. cumplan con las leyes aplicables, incluyendo la obtención del consentimiento informado de los titulares de los datos, cuando sea necesario. El Contratante se compromete a proporcionar a Sistemas Aries S.A.S. únicamente aquellos datos necesarios y pertinentes para la ejecución del servicio.

- ✓ Reporte de Incidentes de Seguridad: En caso de cualquier incidente de seguridad que afecte la confidencialidad, integridad o disponibilidad de los datos tratados bajo este contrato, Sistemas Aries S.A.S. notificará al Contratante de manera inmediata y tomará las acciones correctivas necesarias para mitigar los impactos y prevenir futuros incidentes, en conformidad con las regulaciones aplicables sobre gestión de incidentes de seguridad.

4. CONFIDENCIALIDAD:

- ✓ Obligación de Confidencialidad: Sistemas Aries S.A.S. se compromete a mantener la confidencialidad de toda la información sensible, técnica, comercial, financiera, y de cualquier otra naturaleza, que sea proporcionada por el Contratante en el marco de la ejecución del presente contrato. Dicha información será considerada como confidencial y no será divulgada, compartida o utilizada para fines distintos a los específicamente establecidos en este contrato, salvo que exista consentimiento previo y por escrito del Contratante.

- ✓ Excepciones a la Confidencialidad: La obligación de confidencialidad no será aplicable a la información que: (a) sea de dominio público sin que ello se deba a una violación de esta cláusula; (b) haya sido obtenida de manera legítima por Sistemas Aries S.A.S. de un tercero que no esté sujeto a una obligación de confidencialidad; o (c) deba ser divulgada en cumplimiento de una orden judicial o requerimiento legal de una autoridad competente, en cuyo caso Sistemas Aries S.A.S. notificará al Contratante de dicha obligación, salvo que esté legalmente prohibido hacerlo.

- ✓ Devolución o Destrucción de Información Confidencial: A la terminación del presente contrato, y previa solicitud escrita del Contratante, Sistemas Aries S.A.S. devolverá o destruirá, según sea solicitado, toda la información confidencial en su posesión, incluyendo copias, registros o cualquier otro medio que contenga dicha información, certificando al Contratante la completa devolución o destrucción de la misma, salvo que se requiera retenerla por disposiciones legales o regulaciones aplicables.

5. PLAN DE RESPUESTA A INCIDENTES POR CIBERSEGURIDAD:

- ✓ Propuesta de Implementación: Con el fin de fortalecer la seguridad y resiliencia de los sistemas informáticos del Contratante, se recomienda la implementación de un Plan de Respuesta a Incidentes de Ciberseguridad. Este plan deberá incluir procedimientos detallados para la identificación, contención, erradicación, y recuperación ante incidentes de seguridad, tales como ataques de ransomware, accesos no autorizados, o cualquier otra amenaza que pueda comprometer la integridad, confidencialidad, o disponibilidad de los datos y servicios de la plataforma Ariesnet.

- ✓ Medidas Preventivas y Correctivas: Se sugiere al contratante la inclusión de medidas preventivas en el plan, como la capacitación regular del personal del Contratante en buenas prácticas de ciberseguridad, la realización de simulacros de respuesta a incidentes, y la evaluación periódica de la infraestructura tecnológica para identificar y corregir vulnerabilidades potenciales. Asimismo, el plan debe contemplar medidas correctivas para restaurar la normalidad operativa en el menor tiempo posible, minimizando la interrupción del servicio.

6. PROPUESTA DE PROTOCOLOS DE COMUNICACIÓN:

- ✓ Objetivo de los Protocolos de Comunicación: Para garantizar una interacción eficiente y efectiva entre los equipos de soporte de Sistemas Aries S.A.S. y los representantes del Contratante, se propone la implementación de protocolos de comunicación claros. Estos protocolos establecerán los horarios de atención, canales de comunicación preferidos, y procedimientos de escalamiento de problemas, con el objetivo de optimizar la coordinación y resolución de incidentes.

- ✓ Horarios de Atención:

  Horario Regular: El equipo de soporte de Sistemas Aries S.A.S. estará disponible para la atención de solicitudes de lunes a viernes, de 8:00 a.m. a 11:00 a.m. y de 2:00 p.m. a 5:00 p.m.

  Soporte Fuera de Horario: Cualquier solicitud de soporte fuera del horario regular será atendida en el siguiente horario hábil, a menos que se establezca un acuerdo específico para soporte extendido o de emergencia.

  Canales de Comunicación Preferidos:

  Bot de WhatsApp (Sistema llamado "Carito"), se dispondrá de una línea de WhatsApp (+57 300 492 99 06) para el soporte asistido por IA, recepción inicial de solicitudes y la coordinación preliminar de atención.

  Mesa de Ayuda: Las solicitudes de soporte deben ser registradas a través de la plataforma de Mesa de Ayuda (www.sistemasaries.com.co/mesadeayuda), lo cual permitirá una trazabilidad y seguimiento adecuados de cada incidente.

  Soporte Remoto: Para consultas rápidas o intervenciones menores, se utilizarán herramientas de soporte remoto como RustDesk, TeamViewer o Anydesk, previa coordinación y autorización del Contratante.

- ✓ Coordinación con el Líder Técnico del Contratante:

  Punto de Contacto Principal: El Contratante designará un líder técnico o administrador de la plataforma como punto de contacto principal para la coordinación de las actividades de soporte. Este líder será el exclusivo

responsable de la comunicación con Sistemas Aries S.A.S., priorización de solicitudes, y coordinación interna con los equipos del Contratante.

- ✓ Registro y Documentación de Comunicaciones:

  Todas las comunicaciones, incluyendo llamadas y sesiones de soporte remoto, serán registradas y documentadas en el sistema de Mesa de Ayuda, buscando la trazabilidad y el acceso a los historiales de incidentes por parte del Contratante.

7. PROPUESTA PARA LA IMPLEMENTACIÓN DE MEDIDAS DE REDUNDANCIA Y RESILIENCIA:

- ✓ Objetivo de la Propuesta: Con el fin de asegurar la continuidad operativa y minimizar la dependencia de un solo punto de fallo en la infraestructura tecnológica del Contratante, se recomienda la implementación de medidas de redundancia y resiliencia. Estas medidas están diseñadas para incrementar la disponibilidad de los servicios y proteger la operación frente a interrupciones no planificadas, garantizando un nivel óptimo de desempeño y seguridad.

- ✓ Redundancia de Infraestructura:

  Servidores de Respaldo: Se recomienda la instalación de servidores de respaldo que puedan asumir la carga operativa en caso de fallo del servidor principal. Estos servidores deben estar configurados con sincronización en tiempo real o con una frecuencia de sincronización que minimice la pérdida de datos en caso de un incidente.

  Almacenamiento Redundante: Implementar soluciones de almacenamiento redundante, como RAID (Redundant Array of Independent Disks) y sistemas de almacenamiento SAN/NAS con replicación de datos, para asegurar la disponibilidad de la información crítica y mitigar riesgos de pérdida de datos por fallos de hardware.

- ✓ Resiliencia en la Alimentación Eléctrica:

  Sistemas de Alimentación Ininterrumpida (UPS): Instalar sistemas UPS para proteger los equipos críticos de fallos eléctricos, picos de voltaje y cortes de energía, proporcionando tiempo suficiente para una transición segura a una fuente de energía alternativa o para el apagado controlado de los sistemas.

Generadores de Respaldo: Para asegurar la continuidad en caso de fallas eléctricas prolongadas, se recomienda la instalación de generadores de respaldo que puedan suministrar energía durante cortes extendidos y mantener la operatividad de la infraestructura esencial.

Atentamente,



MÓNICA MARÍA RAMÍREZ SEPÚLVEDA
Coordinadora Administrativa y de Recursos Humanos

Sistemas ARIES S.A.S.
Somos conocimiento que acerca el estado al ciudadano