Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

INFORME TECNICO

La Secretaría de Servicios Digitales, requiere tramitar una contratación de acuerdo al siguiente requerimiento asociado al Servicio: AWS Cloud Resell:

Renglón 1: Servicios Informáticos mensualizado por consumo: Servicio AWS Cloud Resell incluye las siguientes 2 especificaciones técnicas, en enmarcado en las normas ISO 9001-2005.

1.1. Gestionar el Id de cuenta de AWS ante las entidades correspondientes
1.2. Generar un usuario root con la cuenta de correo que el cliente indique y dar soporte para configurar el MFA tal como indican las buenas prácticas de AWS.

Servicio	Cantidad requerida	Precio Unitario	Precio Total 12 meses
Cloud Resell – AWS Según consumo mensual bajo precios oficiales de AWS	**1 Unidad de Créditos de Nube (Equivale a 1 USD en AWS) Se requiere mínimo 12.000 créditos mensuales.**		

Renglón 2: Servicios Informáticos mensualizado por soporte y asistencia tecnica

1.1. Soporte y asistencia técnica mensual.

Servicio	Cantidad requerida	Precio Unitario	Precio Total 12 meses
El Servicio de soporte y mantenimiento	**Según especificaciones 1**		

Especificación 1: ESPECIFICACIONES TECNICAS – SERVICIO DE HOSTEO AGENCIA DE INNOVACION DE PROVINCIA DE TIERRA DEL FUEGO, de acuerdo a lo siguiente:

Las presentes especificaciones tienen por objeto la provisión de los servicios de alojamiento de servidores virtuales en una plataforma de nube sobre los servicios que fueron migrados desde el Datacenter.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

El Oferente deberá cumplir con las disposiciones establecidas en las presentes Especificaciones Técnicas y así como asumir todas las responsabilidades relacionadas:

1. **El siguiente cuadro esquematiza los Servicios y actividades que el Oferente se compromete a brindar:**

1.1. Administración: Gestión y administración remota de la infraestructura virtual, la plataforma de servidores, especificados en Infraestructura a Suministrar, los respaldos, la performance y la replicación de datos.
1.2. Infraestructura virtual: Provisión y gestión de la infraestructura virtual donde se alojarán las máquinas virtuales.
1.3. Plataforma: Provisión y gestión de la plataforma sobre la cual se ejecutarán las máquinas virtuales.
1.4. Performance: Garantía de un rendimiento adecuado de la plataforma para las necesidades de la AITF. La AITF y el adjudicatario deben establecer y acordar métricas de performance y el adjudicatario deberá reportar a LA AITF de forma mensual.
1.5. Respaldos y restauración: El Oferente deberá compromete a realizar respaldos diarios de las configuraciones, datos, aplicaciones y todos los elementos tecnológicos, sean físicos o virtuales, intervinientes en la solución, según lo especificado en el ANEXO II Apéndice C – Copia de respaldo y restauración. Estos respaldos se almacenarán en un lugar seguro y accesible para LA AITF. En caso de cualquier fallo o incidente, el adjudicatario se compromete a restaurar la información, los sistemas y la continuidad del negocio de LA AITF, de acuerdo con los procedimientos establecidos en el ANEXO II Apéndice C – Copia de respaldo y restauración.
1.6. Replicación de datos: Replicación de los datos entre distintas zonas geográficas para garantizar la continuidad operativa ante fallas siguiendo lo indicado en el ANEXO II Apéndice C – Copia de respaldo y restauración.
1.7. Soporte técnico: Prestación de un servicio de soporte técnico y mantenimiento en una modalidad 24/7 para LA AITF y debe estar disponible en español e inglés.
La EMPRESA trabajará en manera conjunta con LA AITF, brindando soporte y administración remota sobre los recursos de hardware descritos en el punto 2.

El Servicio de soporte y mantenimiento a brindar por el Adjudicatario:

- Chequeo del estado de los enlaces de Internet y del funcionamiento general del hardware.
- Envío de alertas real time en el caso de alguna falla en los servicios.
- Reportes internos semanales del estado general del servidor (rutas, upgrades disponibles, etc).
- Reportes internos quincenales de seguridad (accesos, fallas, alertas).
- Detección de intrusos.
- Alertas de espacio disponible en los discos rígidos.
- Detección y corrección de problemas de performance originados por problemas en las consultas y o derivados de código defectuoso.
- Planificación de una política de Backups y contingencias.
- Actualización periódica de los paquetes instalados en el servidor.
- Actualización de las configuraciones y versiones de los servicios implementados en caso de que aparezcan vulnerabilidades que los afecten.
- Monitoreo en tiempo real de todos sus servicios implementados.

1.8. Alta Disponibilidad: El Oferente deberá comprometerse a arbitrar todos los medios necesarios para garantizar la alta disponibilidad de los servicios, tanto en la infraestructura física, de hipervisores y virtual, para asegurar el correcto y óptimo funcionamiento de la solución. Los mismos están especificados en el Apéndice B – Alta Disponibilidad.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

1.9. Cambios Evolutivos y Correctivos: El Oferente se compromete a realizar los cambios evolutivos y correctivos que se consideren necesarios a todo nivel tecnológico y técnico, en acuerdo con la Agencia de Innovación, para asegurar la alta disponibilidad del servicio.

1.10. Comunicación y Coordinación: El Oferente deberá comprometerse a mantener una comunicación y coordinación fluida con la Agencia de Innovación para garantizar que se implementen las medidas necesarias para la alta disponibilidad del servicio.
En estos casos de requerimiento de servicio deberá ser notificado por correo a la una casilla de correo a suministrar por el Oferente y bien a través de un sistema web de tickets, a definir entre la Agencia y el Oferente.

1.11. Cumplimiento de los acuerdos de Nivel de Servicio: El Oferente deberá comprometerse a cumplir y asegurar que todo su Servicio cumplirá con los niveles de calidad y servicio establecido en el Apéndice A – Acuerdo de Niveles de Servicio.

1.12. Cumplimiento de los Acuerdos: El Oferente deberá asegurar que todo su Servicio cumpla con lo suscripto en el ANEXO II– Acuerdo de Cumplimiento y sus Apéndices.

2. De las certificaciones

Certificación del Hito 1 – Proyecto de Migración a la Nube (E-67699-2024)

Encontrándose cumplida y certificada la implementación inicial de AWS Control Tower y la migración de servidores.

Certificación del Hito 2 – Proyecto de Migración a la Nube (E-67699-2024)

Encontrándose cumplida y certificada las actividades se llevaron a cabo dentro de los plazos estipulados, se ha implementado la VPN, migración de servidores y replicación del Active Directory cumpliendo con las especificaciones técnicas.
Encontrándose en proceso los Hitos 3, 4 y 5, siendo necesario dar continuidad **al Servicio AWS** Cloud Resell.

3. Plazo de contratación

Se establece como plazo de contratación 12 meses con la posibilidad de renovar el mismo por periodos iguales. Las partes podrán desistir de la renovación con la notificación formal de cualquiera de las partes con una antelación de 90 días previos al vencimiento de cada periodo.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

ANEXO I

Apéndice A– Acuerdo de Niveles de Servicio.

Definición de Niveles de Servicio (SLAs): Los Niveles de Servicio (en adelante "SLA") se definen como los parámetros y estándares de rendimiento acordados entre el Oferente y la AITF para garantizar la calidad y la disponibilidad de los servicios proporcionados por el Oferente.
Alcance de los Niveles de Servicio: Los SLAs se aplican a los siguientes servicios proporcionados por el Oferente a la AITF.
Parámetros de los Niveles de Servicio:

SLA	Descripción	Condición
SLA de Alta Disponibilidad	El Oferente se compromete a mantener una disponibilidad del servicio anual, excluyendo los tiempos de mantenimiento programado y los casos de fuerza mayor.	99,9% anual Disponibilidad ((365 *24hs) *0,01) = 87hs cantidad de horas de indisponibilidad anual
KPI de respaldo y Restauración	Respaldo: Configuraciones, datos, aplicaciones y todos los elementos tecnológicos, sean físicos o virtuales, intervinientes en la solución. Los respaldos deben ser almacenados en un lugar seguro y accesible para LA AITF	Infraestructura física y virtual: Diario: Backup completo (24 horas). Semanal: Backup completo (complementario al diario). Mensual: Backup completo Expedientes electrónicos y bases de datos: Diario: Backup incremental (2 horas). Semanal: Backup completo (complementario al incremental). Mensual: Backup completo (archivo de referencia).
	Restauración: El Oferente también se comprometerá a restaurar la información, los sistemas y la continuidad del negocio LA AITF en caso de cualquier fallo o incidente, en un plazo máximo de X horas.	Un plazo no superior a _____horas/días_____ desde el momento del fallo o incidente Cobertura 7x24.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

<table>
<tr>
<td>KPI de Atención de Soporte técnico 7x24</td>
<td>Gestión de incidentes y peticiones del servicio. La prestación del servicio puede estar sujeta a incidentes que pueden comprometer el mantenimiento de unos niveles de servicio adecuados. En este sentido y para evitar que estos incidentes impacten en la menor medida posible en la prestación del servicio, se establecen unos criterios de priorización de incidentes que permitan ofrecer unos tiempos de respuesta y resolución correctos.
Estos criterios de priorización quedan recogidos en 3 tipos: Normal, Alta y críticos.
Normales: Incidentes que no implican la detención total del servicio o que no comprometen la seguridad del mismo en cualquiera de sus parámetros.
Críticos: Incidentes que implican la detención total del servicio o que pueden comprometer la seguridad del mismo</td>
<td>
<table>
<tr><th>Nivel de Severidad</th><th>Criterios</th><th>Tiempo de Atención</th><th>Tiempo de Asignación</th><th>Tiempo de Respuesta</th></tr>
<tr><td>Severidad 1 (Crítica)</td><td>Afecta a servicios críticos del negocio, causando una interrupción total o mayor del 80% de las operaciones.</td><td>Inmediato (0 minutos)</td><td>Inmediato (0 minutos)</td><td>30 minutos</td></tr>
<tr><td>Severidad 2 (Alta)</td><td>Afecta a servicios importantes del negocio, causando una interrupción significativa del 20% al 80% de las operaciones.</td><td>15 minutos</td><td>30 minutos</td><td>2 horas</td></tr>
<tr><td>Severidad 3 (Normal)</td><td>Afecta a servicios no críticos del negocio, causando una interrupción leve o menor al 20% de las operaciones.</td><td>4 horas</td><td>8 horas</td><td>24 horas</td></tr>
</table>
</td>
</tr>
<tr>
<td>KPI de Performance</td>
<td>El Oferente se compromete a garantizar que la performance de la plataforma sea la acordada entre LAS PARTES y presentar los reportes de forma mensual</td>
<td>Acordado entre LAS PARTES</td>
</tr>
</table>

Procedimiento de Monitoreo y Reporte: El Oferente será responsable de monitorear continuamente el cumplimiento de los SLAs y proporcionar informes periódicos a la AITF sobre el rendimiento del servicio. Los informes incluirán métricas de rendimiento detalladas y cualquier desviación con respecto a los SLAs acordados.
Procedimiento de Revisión y Mejora: Las partes acuerdan llevar a cabo revisiones periódicas de los SLAs para garantizar su relevancia y eficacia. Cualquier cambio en los SLAs requerirá el consentimiento mutuo por escrito de ambas PARTES.
Resolución de Incumplimientos: En caso de incumplimiento de los SLAs por parte del Oferente, las partes acuerdan negociar de buena fe una solución adecuada. LA AITF tendrá derecho a aplicar penalizaciones o tomar otras medidas correctivas según lo establecido en el CONVENIO.
Penalizaciones por incumplimiento: Todas las desviaciones a la baja en el nivel de cumplimiento del servicio estarán asociadas a una compensación por parte del Oferente a LA AITF.
Para establecer la compensación se definen dos niveles de incumplimiento: leve y grave.

Incumplimiento	Desvío Leve	Desvío Grave
Tiempo de respuesta excedido Incidencia normal	Entre 4 y 6 horas	Más de 6 horas
Tiempo de respuesta excedido Incidencia Críticos	Entre 2 y 4 horas	Más de 4 horas

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

% de disponibilidad inferior al ofrecido	Entre 99,98% y 99,90%	Menor que 99,90%

Siempre que los niveles de servicio no sean cumplidos, el Oferente deberá compensar a LA AITF. Las compensaciones por incumplimiento de los Niveles de Servicio se detallan a continuación:

Incumplimiento	Penalización por incumplimiento leve	Penalización por incumplimiento grave
Tiempo de respuesta excedido Incidencia normal	1% de descuento en la próxima factura. Máximo 10% acumulable	4% de descuento en la próxima factura. Máximo 20% acumulable
Tiempo de respuesta excedido Incidencia Críticos	4% de descuento en la próxima factura. Máximo 20% acumulable	10% de descuento en la próxima factura. Máximo 30% acumulable
% de disponibilidad inferior al ofrecido	4% de descuento en la próxima factura. Máximo 20% acumulable	10% de descuento en la próxima factura. Máximo 30% acumulable
% de disponibilidad inferior al ofrecido – reiteradas (más de 3 en el año)	20% de descuento en la próxima factura.	40% de descuento en la próxima factura.

Vigencia: Entrará en vigor en la misma fecha que el CONVENIO y permanecerá en vigor durante el plazo de duración del mismo, a menos que sea modificado o terminado de conformidad con los términos y condiciones del CONVENIO

Apéndice B – Alta Disponibilidad

Definición de Alta Disponibilidad: Se entiende por alta disponibilidad la capacidad del servicio para estar disponible para su uso durante un período de tiempo determinado, expresado como un porcentaje. El objetivo de la alta disponibilidad es minimizar el tiempo de inactividad del servicio, lo que se traduce en una mayor disponibilidad para los usuarios.
Medios para Garantizar la Alta Disponibilidad: El Oferente deberá comprometerse a implementar las siguientes medidas para garantizar la alta disponibilidad del servicio:

- **Infraestructura redundante:** Implementar una infraestructura redundante con múltiples servidores, dispositivos de almacenamiento y enlaces de red para minimizar el impacto de las fallas.
- **Monitoreo constante:** Monitorear constantemente la infraestructura y el servicio para detectar y solucionar problemas de forma proactiva.
- **Mantenimiento preventivo:** Realizar un mantenimiento preventivo regular para evitar posibles fallos.
- **Pruebas de recuperación ante desastres:** Realizar pruebas de recuperación ante desastres de forma regular para asegurar la capacidad de restaurar el servicio en caso de un fallo grave.

Apéndice C – Gestión de copia de respaldo y restauración

Respaldo Mensual y Diario: El Oferente se compromete a brindar su Servicio cumpliendo con lo establecido por LA AITF en ANEXO II - Apéndice C – Política de Respaldo y Restauración.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

La EMPRESA se compromete a realizar al menos una copia de respaldo al menos por mes de las configuraciones, datos, aplicaciones y todos los elementos tecnológicos, sean físicos o virtuales, intervinientes en la solución.
Además, realizará respaldos diarios de los mismos elementos. Estas copias de respaldo se almacenarán en un lugar seguro y accesible para LA AITF.
La EMPRESA entregará al Cliente una copia de cada respaldo realizado en un plazo no mayor a 5 días hábiles, pudiendo el plazo establecerse en Acta Complementaria.

Replicación de Datos: LA AITF establecerá una política de replicación de datos según en ANEXO II - Apéndice D – Política de Replicación de datos. Esta política incluirá la replicación de datos entre distintas zonas geográficas de forma automática y transparente para LA AITF. Se establecerán los procedimientos y protocolos necesarios para asegurar la integridad y consistencia de los datos replicados. El plazo máximo para la restauración de datos será el establecido en el SLA comprometido por el Oferente.
Periodo de Retención de Respaldos: El Oferente retendrá las copias de respaldo por un período mínimo de 10 años para asegurar la disponibilidad de la información histórica en caso de necesidad, siempre y cuando el Oferente tenga un contrato vigente.
Restauración de Respaldos: En caso de incidente o fallo, El Oferente se compromete a restaurar la información, los sistemas y la continuidad del negocio de LA AITF a partir de las copias de respaldo. Este proceso se llevará a cabo dentro del plazo máximo establecido en el SLA comprometido por El Oferente para minimizar el impacto en las operaciones.

ANEXO II

El Oferente debe ponderar la importancia de proteger los intereses de LA AITF y se compromete a llevar a cabo todas las acciones necesarias para garantizar el cumplimiento de los compromisos que surjan de este proceso, este Acuerdo de Cumplimiento (en adelante “Acuerdo”) y de todas las políticas que la AITF informe, leyes, normas, reglamentos y directivas y directrices gubernamentales aplicables en cada país, estado o región donde opere LA AITF.

Plazo
Este Acuerdo y sus Apéndices rigen durante el tiempo de vigencia del convenio a suscribir entre las PARTES y se extiende durante el término de 10 (diez) años contados a partir de su conclusión definitiva.

Mantenimiento de un entorno saludable
LA AITF desea que el Oferente brinden un entorno saludable, seguro y libre de peligros para su salud y seguridad. El Oferente es responsable de utilizar el equipo y los materiales de LA AITF de forma segura.
Si es consciente de algo que podría suponer un peligro para su seguridad, notifíquese a su superior directo inmediatamente.

Políticas de igualdad y no discriminatorio
El Oferente se compromete a no discriminar en ningún momento durante las prácticas de selección, contratación o empleo, en base a la raza, color, edad, sexo, género, identidad de género, expresión de género, orientación sexual, estado civil, etnia, origen nacional, casta, discapacidad, información genética, condición médica, embarazo, religión, afiliación política, afiliación sindical o cualquier otro estado protegido por la ley aplicable.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

Proteger la información

El Oferente reconoce que la protección y la seguridad de la información es un tema crítico y El Oferente se compromete a implementar medidas técnicas y organizativas adecuadas para garantizar la privacidad y seguridad de los mismos.

El Oferente debe entender y se debe comprometer a cumplir con todas las leyes, normativas y regulaciones aplicables relacionadas con las siguientes, incluyendo, pero no limitándose:

- Ley 25.326 PROTECCIÓN DE LOS DATOS PERSONALES y sus actualizaciones vigentes, el decreto regulatorio 1558/2001, así como el resto de las disposiciones emitidas por la Agencia de Información Pública.
- Ley 24.766 LEY DE CONFIDENCIALIDAD SOBRE INFORMACIÓN Y PRODUCTOS QUE ESTÉN LEGÍTIMAMENTE BAJO CONTROL DE UNA PERSONA Y SE DIVULGUE INDEBIDAMENTE DE MANERA CONTRARIA A LOS USOS COMERCIALES HONESTOS. y sus actualizaciones
- Ley de FIRMA DIGITAL en Argentina y sus actualizaciones
- Los convenios y normativas locales e internacionales vigentes en materia de Transferencia Internacional de datos personales, en especial a los países que la Agencia de información Pública de Argentina defina como adecuados.
- Así como cualquier otra ley o regulación que pueda ser aplicable por el servicio que brinda.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

La información confidencial de LA AITF es propiedad exclusiva de ella, y como tal, el Oferente se debe comprometer a cumplir con todas las cláusulas establecidas en los siguientes apéndices:

- Apéndice A–Acuerdo de Confidencialidad
- Apéndice B - Política de Seguridad
- Apéndice C – Política Respaldo y Restauración
- Apéndice D – Política de Replicación de datos

Asimismo, el Oferente se debe comprometer a proporcionar toda la información requerida por LA AITF para garantizar el cumplimiento de este Acuerdo y de cualquier otra política o normativa aplicable en materia de protección de datos y privacidad.

Guía de trabajo de LA AITF

LA AITF proporcionará una guía y políticas sobre los procesos y procedimientos que El Oferente deberá seguir durante la ejecución de sus Servicios.

El Oferente, junto con sus empleados y subcontratistas, se comprometen de manera rigurosa a adherirse a las directrices delineadas en la guía de trabajo proporcionada por LA AITF.

Sera responsabilidad exclusiva del Oferente, asegurar que todos sus recursos humanos involucrados en la colaboración con LA AITF estén completamente informados y cumplan con los procedimientos y expectativas descritos en dicho documento.

LA AITF se compromete a notificar al Oferente de cualquier actualización o modificación en la guía y política de trabajo con una antelación razonable. El Oferente asume la responsabilidad de asegurarse de que sus empleados y contratistas estén debidamente informados y cumplan con las versiones más recientes.

Activos de LA AITF

El Oferente se debe comprometer a respetar y proteger los derechos de propiedad industrial e intelectual de LA AITF y de terceros.
El Oferente no podrá en ningún momento referirse al CONVENIO derivado de este proceso, Acuerdo y/o a los Servicios prestados ni podrá mencionar el nombre de LA AITF en cualquier forma de publicidad, promoción, propuestas, documentación u otra forma de medios de comunicación.
El Oferente no está autorizada a usar las marcas y/o nombres y/o logos y/o cualquier otro derecho de propiedad intelectual de LA AITF sin su autorización previa otorgada por escrito.
El Oferente se deberá comprometer a asegurarse de que sus empleados, colaboradores, subcontratistas y dependientes utilicen los activos y recursos de LA AITF de manera profesional, ética y responsable, cumpliendo rigurosamente con el marco descrito en los apéndices incluidos.

Comunicación

El Oferente se debe comunicar periódicamente las normas de este Acuerdo a sus empleados y subcontratantes, así como garantizar su cumplimiento.
Se alienta al Oferente a plantear cualquier inquietud que surja de su relación con LA AITF o sus empleados o subcontratantes, incluida cualquier sospecha de violación del Acuerdo, enviando un correo electrónico a mcaderini@aif.gob.ar o que se indique mediante comunicación oficial.
LA AITF investigará todas las comunicaciones recibidas, y el Oferente deberá prohibir las represalias contra los que hagan informes de buena fe a LA AITF.
El Oferente deberá informar a LA AITF inmediatamente de cualquier riesgo o incumplimiento detectado, y colaborar activamente con LA AITF para implementar medidas correctivas y preventivas efectivas.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

Acuerdo integral
Este Acuerdo refleja integralmente la voluntad de las PARTES con respecto al objeto del mismo. Ninguna modificación contractual podrá ser considerada como válida y oponible a la contraparte si no estuviera hecha por escrito y firmada debidamente por las PARTES.

Incumplimiento
La EMPRESA adjudicataria deberá aceptar lo establecido en los apéndices A, B, C y D del ANEXO II.

Validez
La declaración de invalidez o nulidad de cualquier cláusula del presente Acuerdo de Cumplimiento no afecta el resto de su contenido.
En prueba de plena conformidad del presente Acuerdo de Cumplimiento y de todos sus apéndices:

- Apéndice A - ACUERDO DE CONFIDENCIALIDAD
- Apéndice B - POLÍTICA DE SEGURIDAD
- Apéndice C –POLÍTICA DE RESPALDO Y RESTAURACIÓN
- Apéndice D –POLÍTICA DE REPLICACIÓN DE DATOS

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

Apéndice A

ACUERDO DE CONFIDENCIALIDAD

INFORMACIÓN CONFIDENCIAL: En el marco de este Acuerdo, queda expresamente prohibido para la EMPRESA la difusión, divulgación o comunicación a terceros de cualquier información que sea considerada como información confidencial (en adelante, "INFORMACIÓN CONFIDENCIAL"). Esta restricción incluye toda la información relacionada con cualquiera de las PARTES y/o que sea procesada por cualquiera de ellas:

(i) de naturaleza interna, autoridades, empleados, asesores, ciudadanos, etc.;
(ii) de naturaleza técnica, como métodos, procesos, know how sobre tratamiento y almacenamiento de información y/o sobre cualquier otro proceso o técnica, software, tecnología, etc.;
(iii) de naturaleza contable, como sus proveedores, precios, costos, compras, ventas, finanzas, ganancias, planes de comercialización, etc.;
(iv) de gestión, como estrategias de organización, información relativa al personal, salarios, beneficios, etc.;
(v) de desarrollo, como investigaciones y desarrollo de nuevas ideas, productos o servicios, o ampliación de los existentes, etc. sin que la enunciación resulte limitativa sino meramente descriptiva y ejemplificativa.
(vi) todo dato, contenido, investigación, procedimiento o instrucción, documentación de naturaleza técnica, financiera, comercial, contable o de otro tipo, correspondiente LA AITF y a todo aquello que pudiera desprenderse de estos documentos y que sea confidencial del Estado.

La información será considerada INFORMACIÓN CONFIDENCIAL siempre que esté comprendida en alguna de las categorías identificadas precedentemente, con independencia del medio y/o soporte en que se almacene y/o transmita.

DESTINO DE LA INFORMACIÓN: La EMPRESA ADJUDUCATARIA no puede utilizar LA INFORMACIÓN CONFIDENCIAL, por sí o a través de terceros, para un destino o finalidad diferentes para el cual esa información ha sido transmitida (indicar negocio, contrato, trabajo, tratativas contractuales, etc., vinculadas con la confidencialidad).

ACTOS PROHIBIDOS: La confidencialidad que La EMPRESA ADJUDICATARIA debe guardar consiste en no realizar ningún acto u omisión que implique divulgar, revelar, difundir, comunicar o usar LA INFORMACIÓN CONFIDENCIAL, por sí o a través de terceros, por cualquier medio –material, gráfico, electrónico, informático, magnético, auditivo, visual o cualquier otro– para una finalidad diferente a la prevista en este Acuerdo.

En caso de duda acerca de si una determinada información, material, documento o diseño puede o no divulgarse o comunicarse a un tercero debe interpretarse en el sentido que la divulgación no se encuentra permitida.

DIVULGACIÓN AUTORIZADA: La EMPRESA ADJUDICATARIA puede divulgar LA INFORMACIÓN CONFIDENCIAL en los casos siguientes:

(i) Autorización emitida por LA AITF por escrito-papel.
(ii) Cuando LA INFORMACIÓN CONFIDENCIAL adquiere carácter o dominio público en el momento de ser relevada.
(iii) Requerimiento de autoridad competente, administrativa o judicial. Ante requerimiento formulado por autoridad judicial o administrativa competente, en el marco de un expediente en curso, quedando aclarado en este caso que:

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

a. La EMPRESA deberá procurar por todos sus medios que la información no sea divulgada más allá de lo estrictamente necesario en dicho expediente; y
b. La EMPRESA deberá dar aviso fehaciente inmediato a LA AITF acerca del requerimiento; y
c. en caso de que LA INFORMACIÓN CONFIDENCIAL contuviera datos personales en los términos previstos Ley 25.326 PROTECCIÓN DE LOS DATOS PERSONALES y sus actualizaciones vigentes, La EMPRESA solicitará a la autoridad competente que la releve del secreto profesional previsto en dicha norma.

SUJETOS COMPRENDIDOS: Toda referencia en este Acuerdo a la EMPRESA ADJUDICATARIA incluye indistintamente: a la EMPRESA, sus representantes legales, asesores, administradores, dependientes, subcontratantes, proveedores, sucursales, agencias, sociedades controladas y a todos aquellos que dependen jurídicamente de él y que reciban o usen LA INFORMACIÓN CONFIDENCIAL.

La EMPRESA ADJUDICATARIA debe celebrar los respectivos convenios de confidencialidad con esas personas o entidades para asegurar el cumplimiento de este Acuerdo o adoptar las medidas necesarias o convenientes para ello.

RESTITUCIÓN: Extinguido el CONVENIO, Acuerdo, trabajo, tratativas contractuales u otros, la EMPRESA ADJUDICATARIA deberá restituir a LA AITF la documentación, los soportes y el material de todo tipo a través de los cuales recibió LA INFORMACIÓN CONFIDENCIAL en el marco de este Acuerdo.

DECLARACIÓN: La EMPRESA ADJUDICATARIA asumirá el compromiso de forma libre y voluntaria y de acuerdo con sus intereses y negocios comerciales, sin que las limitaciones y prohibiciones aquí asumidas afecten su giro y negocios habituales, o le causen daño o perjuicio de algún tipo. Por lo tanto, la EMPRESA ADJUDICATARIA renunciara especialmente a exigir a LA AITF cualquier compensación, retribución o resarcimiento por las obligaciones asumidas en este Acuerdo.

RESPONSABILIDAD: En caso de que la EMPRESA ADJUDICATARIA infrinja las obligaciones de secreto y confidencialidad asumidas en este Acuerdo, generará a favor de LA AITF el derecho de reclamar los daños y perjuicios ocasionados, incluyendo, pero sin limitarse a gastos judiciales y honorarios profesionales devengados en el reclamo y/o en las acciones legales tendientes a proteger LA INFORMACION CONFIDENCIAL.

Asimismo, la violación al deber de Confidencialidad hará pasible a la parte infractora de las sanciones previstas en las leyes 24.766 y 25.326 y de las futuras actualizaciones de dichas leyes, como también lo indicado en la cláusula del CONVENIO DECIMO PRIMERO: RESPONSABILIDAD. b. “Responsabilidad por incumplimiento al deber de confidencialidad”.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

Apéndice B
POLÍTICA DE SEGURIDAD

La EMPRESA ADJUDICATARIA reconoce y acepta el marco de referencia establecido por LA AITF para la operación, protección y seguridad informática, incluyendo todas las normas y procedimientos aplicables. Este marco será revisado por LA AITF regularmente para adaptarlo a cualquier nueva exigencia del entorno o del mercado.

La EMPRESA ADJUDICATARIA entiende y se compromete a implementar y controlar las siguientes medidas técnicas y organizativas tales como a modo enunciativo y no taxativo:

(i) Implementar medidas y tecnologías de seguridad informática, dentro del alcance de los servicios que brinda para LA AITF, como firewalls, sistemas de detección de intrusiones, sistemas de encriptación, entre otros, para proteger la información y datos de la empresa.

(ii) Llevar a cabo revisiones periódicas de la seguridad de la EMPRESA ADJUDICATARIA y de la idoneidad de su programa de seguridad de la información, según lo medido con respecto a los estándares de seguridad del sector y sus políticas y procedimientos.

(iii) Seguir y cumplir con la política de contraseñas de Usuarios establecida por LA AITF. Las contraseñas de acceso a los sistemas son individuales e intransferibles y deben tratarse con el más alto nivel de confidencialidad. En circunstancias excepcionales, cuando existe una autorización previa escrita por LA AITF, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica.

(iv) Seguridad del tratamiento de datos de AITF: Seguridad de la red, la seguridad física de las instalaciones y medidas para controlar los derechos de acceso de los empleados y sus contratistas de la EMPRESA ADJUDUCATARIA.

(v) Procesos para probar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas implementadas por la EMPRESA.

(vi) Aplicar criterios y políticas de seudonimización y encriptación para garantizar un nivel adecuado de seguridad;

(vii) Aplicar medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas y servicios de procesamiento que están siendo operados por el AITF y por la EMPRESAADJUDICATARIA.

(viii) Implementar medidas que permitan a la EMPRESA ADJUDICATARIA realizar copias de seguridad y archivos adecuados, facilitando la pronta restauración de la disponibilidad y el acceso a los datos del AITF en caso de incidentes físicos o técnicos.

(ix) La EMPRESAADJUDICATARIA, está comprometida a facilitar una copia de las certificaciones propias o de terceros involucrados en el servicio en un lapso no mayor a 72hs de hecho el requerimiento.

CAPACITACIÓN: La EMPRESA ADJUDICATARIA entiende y se compromete a invertir en la formación y capacitación del personal en materia de seguridad informática y protección de información para que estén en capacidad de reconocer y prevenir posibles amenazas.

COMUNICACIÓN: La EMPRESA ADJUDICATARIA se compromete a notificar de manera inmediata a LA AITF en caso de cese o cambio de un empleado/contratista, con el fin de retirar, revocar y/o asignar permisos de acceso a la información. Este aviso deberá ser realizado en un plazo menor a las 24 horas del cese o decisión de este. La EMPRESA ADJUDICATARIA garantizará la entrega de todos los activos que LA AITF le haya suministrado al momento del cese o cambio de personal. De esta manera, se asegura la protección de la información y se evita el acceso no autorizado a la misma.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

INCIDENTES: La EMPRESA ADJUDICATARIA entiende y se compromete a establecer procedimientos claros y eficaces para la gestión de incidentes de seguridad informática, para garantizar una respuesta rápida y adecuada en caso de un ataque o incidente.

La EMPRESA ADJUDICATARIA entiende y se compromete a realizar una evaluación constante de los procesos y medidas de seguridad implementados dentro del alcance de los servicios que brinda a LA AITF, para identificar posibles mejoras y ajustes necesarios.

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

Apéndice C
POLÍTICA DE RESPALDO Y RESTAURACIÓN

El presente documento establece la política de backup y restauración para la plataforma de gestión de gobierno de la provincia, abarcando todas las soluciones e infraestructura afectada por la operación devenida de la gestión de gobierno. Esta política tiene como objetivo garantizar la disponibilidad, integridad y confiabilidad de la información crítica para el funcionamiento del gobierno provincial.

Alcance
Esta política se aplica a toda la infraestructura física y virtual de la plataforma de gestión de gobierno, así como a los expedientes electrónicos y bases de datos almacenados en ella. Abarca los siguientes componentes:

Servidores físicos: Los servidores físicos que albergan la infraestructura de la plataforma de gestión de gobierno, incluyendo sistemas operativos, aplicaciones y datos.
Máquinas virtuales: Las máquinas virtuales que operan dentro de la infraestructura de la plataforma de gestión de gobierno, incluyendo sistemas operativos, aplicaciones y datos.
Almacenamiento: Los dispositivos de almacenamiento que albergan los backups de la infraestructura física y virtual, los expedientes electrónicos y las bases de datos.
Redes: Las redes que conectan los componentes de la infraestructura física y virtual, así como los dispositivos de almacenamiento.
Aplicaciones: Las aplicaciones críticas para el funcionamiento de la plataforma de gestión de gobierno, incluyendo todas las aplicaciones intervinientes en la gestión de gobierno.
Datos: Los datos almacenados en la infraestructura física y virtual, incluyendo datos de RRHH, financieros, de expedientes electrónicos y de usuarios.

Objetivos
Los objetivos principales de esta política son:

Proteger la información crítica contra pérdidas accidentales o intencionales: La pérdida de datos puede ocurrir por diversos motivos, incluyendo errores humanos, fallos de hardware o software, ataques cibernéticos y desastres naturales. Una política de backup adecuada garantiza que la información crítica esté protegida y pueda ser recuperada en caso de cualquier incidente.
Minimizar el tiempo de inactividad en caso de un incidente: La indisponibilidad de la información crítica puede tener un impacto significativo en el funcionamiento del gobierno provincial. Una política de backup eficiente permite restaurar la información rápidamente y minimizar el tiempo de inactividad, asegurando la continuidad del negocio.
Garantizar la integridad y la confiabilidad de los datos: La corrupción de datos puede generar información inexacta o incompleta, lo que puede tener graves consecuencias para la toma de decisiones y el cumplimiento de las regulaciones. Una política de backup robusta garantiza que los datos estén protegidos contra la corrupción y que su integridad sea preservada.
Cumplir con las regulaciones y requisitos legales: Existen diversas regulaciones y requisitos legales que obligan a las organizaciones a proteger la información y garantizar su disponibilidad. Una política de backup adecuada permite cumplir con estas regulaciones y evitar sanciones legales.

Esquema de Backup
La política de backup establece un esquema de backup escalonado que abarca la infraestructura física y virtual, los expedientes electrónicos y las bases de datos. El esquema se basa en la frecuencia de actualización de la información y la criticidad de los datos:

Infraestructura física y virtual:

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

- Diario: Realizar un backup completo de la infraestructura física y virtual cada 24 horas. Este backup capturará el estado completo de los sistemas operativos, aplicaciones y datos al final de cada día.
- Semanal: Realizar un backup completo de la infraestructura física y virtual una vez por semana. Este backup complementará el backup diario, proporcionando una copia de seguridad adicional en caso de que se produzca un incidente durante la semana.
- Mensual: Realizar un backup completo de la infraestructura física y virtual una vez al mes. Este backup servirá como archivo de referencia a largo plazo, permitiendo restaurar el sistema a un estado anterior en caso de que sea necesario.

Expedientes electrónicos y bases de datos:

- Diario: Realizar un backup incremental de los expedientes electrónicos y bases de datos cada 2 horas. Este backup capturará los cambios realizados en los datos desde el último backup incremental, minimizando el volumen de datos que se deben copiar.
- Semanal: Realizar un backup completo de los expedientes electrónicos y bases de datos una vez por semana. Este backup complementará el backup incremental diario, proporcionando una copia de seguridad completa de los datos en caso de que se produzca un incidente durante la semana.
- Mensual: Realizar un backup completo de los expedientes electrónicos y bases de datos una vez al mes

Consideraciones

- Seguridad: Los backups deben ser encriptados para proteger la información confidencial. Se deben utilizar métodos de encriptación robustos y reconocidos, y las claves de encriptación deben ser almacenadas de forma segura.
- Retención: Se debe definir una política de retención de backups que establezca por cuánto tiempo se conservarán los backups. La política debe considerar factores como la criticidad de la información, las regulaciones aplicables y las necesidades de recuperación.
- Plan de recuperación ante desastres: Se debe implementar un plan de recuperación ante desastres que establezca los procedimientos para restaurar la información en caso de un desastre mayor, como un incendio, inundación o ataque cibernético. El plan debe incluir la ubicación de los backups de recuperación, los roles y responsabilidades del personal, y los pasos necesarios para restaurar la información y los sistemas.

Pruebas de Restauración

Se deben realizar pruebas de restauración periódicas para garantizar la operabilidad del proceso de backup. Las pruebas deben incluir la restauración de backups de diferentes tipos (diario, semanal, mensual) y la verificación de la integridad y consistencia de los datos restaurados.

Revisión y Actualización

La política de backup y restauración debe ser revisada y actualizada periódicamente para reflejar los cambios en el entorno tecnológico, las necesidades del gobierno provincial y las mejores prácticas en la materia.

Apéndice D
POLÍTICA DE REPLICACIÓN DE DATOS

El presente documento establece la política de replicación de datos en nube para el gobierno provincial, que abarca la plataforma de gestión de gobierno, abarcando todas las soluciones e infraestructura afectada por la operación devenida de la gestión de gobierno. Esta política tiene como

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

objetivo garantizar la disponibilidad y accesibilidad de la información crítica del gobierno provincial en caso de incidentes o interrupciones del servicio.

Alcance

Esta política se aplica a todos los datos almacenados en la plataforma de gestión de gobierno en la nube, incluyendo:

- Máquinas Virtuales
- Bases de datos
- Expedientes electrónicos.
- Archivos adjuntos, imágenes y otros formatos digitales asociados a los datos mencionados anteriormente.

Objetivos
Disponibilidad de datos: Garantizar la disponibilidad de los datos críticos en caso de interrupciones del servicio en la zona de disponibilidad primaria.
Recuperación ante desastres: Facilitar la recuperación de los datos en caso de desastres naturales u otros eventos que puedan afectar la zona de disponibilidad primaria.
Reducción del tiempo de inactividad: Minimizar el tiempo de inactividad en caso de incidentes, permitiendo una rápida restauración de los datos y la continuidad operativa.

Estrategia de Replicación
Se implementará una estrategia de replicación de datos en nube que incluya la replicación de datos dentro y fuera de una misma zona geográfica.

Replicación dentro de la zona geográfica:
Replicación sincrónica: Se replicarán los datos en tiempo real a una zona de disponibilidad secundaria dentro de la misma región de nube. Esto garantizará la disponibilidad inmediata de los datos en caso de una falla en la zona de disponibilidad primaria.
Replicación fuera de la zona geográfica:

Replicación asincrónica: Se replicarán los datos de forma periódica (por ejemplo, diariamente) a una zona de disponibilidad en una región diferente de nube. Esto brindará protección adicional contra desastres naturales u otros eventos que puedan afectar la zona de disponibilidad primaria y secundaria dentro de la misma región.

Criterios y Protocolos
Para garantizar el correcto funcionamiento de las réplicas, se establecerán los siguientes criterios y protocolos:

- Selección de la zona de disponibilidad secundaria: La zona de disponibilidad secundaria debe ser seleccionada cuidadosamente considerando factores como la latencia, la redundancia y el costo.
- Frecuencia de replicación: La frecuencia de replicación se determinará en función de la criticidad de los datos y la tolerancia al riesgo del gobierno provincial.
- Monitoreo y alerta: Se implementará un sistema de monitoreo y alerta para detectar y notificar cualquier anomalía en las réplicas.
- Pruebas de recuperación: Se realizarán pruebas de recuperación periódicas para verificar la funcionalidad de las réplicas y garantizar la capacidad de restaurar los datos en caso de un desastre.
-

Proceso de Simulación Trimestral

Se establecerá un proceso de simulación trimestral para evaluar la efectividad de la política de replicación de datos. La simulación incluirá los siguientes pasos:

Agencia de Innovación
Tierra del Fuego, Antártida e Islas del Atlántico Sur

- Simulación de un desastre: Se simulará un desastre que afecte la zona de disponibilidad primaria.
- Activación de la replicación secundaria: Se activará la replicación secundaria y se restaurarán los datos desde la zona de disponibilidad secundaria.
- Evaluación de la simulación: Se evaluará la simulación para identificar áreas de mejora y actualizar la política de replicación de datos según sea necesario.

Operativa de Utilización de Réplicas en Producción
La operativa de utilización de réplicas en producción se regirá por los siguientes lineamientos:

- Acceso a las réplicas: El acceso a las réplicas estará restringido a personal autorizado y solo se permitirá para fines de recuperación ante desastres o pruebas de simulación.
- Cambio de zona de disponibilidad primaria: En caso de que sea necesario cambiar la zona de disponibilidad primaria, se implementará un proceso de conmutación por fallo que garantice la continuidad del servicio.
- Eliminación de réplicas obsoletas: Las réplicas obsoletas o no utilizadas se eliminarán para liberar espacio de almacenamiento y reducir costos.

Glosario

AITF: Agencia de Innovación de Tierra del Fuego.

Por todo lo descripto, se solicita remitir el mismo al correo electrónico caguado@aif.gob.ar y mcalderini@aif.gob.ar.

Sin más que agregar, saludo atentamente.

Lic. Matías CALDERINI
Secretario de Servicios Digitales

Firmado Electrónicamente por
INGENIERO AGUADO CINTIA ALEJANDRA
Gobierno de Tierra del Fuego
DIRECTOR GENERAL GESTIÓN Y
COORDINACIÓN - SERVICIOS DIGITALES
16/01/2025 10:56