[Estructura sugerida] *Proceso de selección #:*

TÉRMINOS DE REFERENCIA

Relevamiento, análisis, diseño, normativización y estandarización de políticas y procedimientos de seguridad de la información del Plan de Transformación Digital del INSSJP-PAMI; Elaboración de un BCP y su Plan de Implementación; y Capacitación virtual

ARGENTINA

[Número de la Cooperación Técnica]

Nombre de la Cooperación Técnica: Apoyo a la Transformación Digital del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP)

[Enlace web con el documento aprobado]

1. Antecedentes y Justificación

1.1 El Instituto Nacional de Servicios Sociales para Jubilados y Pensionados de Argentina (INSSJP) es un actor clave en el subsector de la seguridad social, que brinda asistencia médica y servicios sociales a sus 5,3 millones de afiliados de las cuales 90% tiene 60 años o más, siendo mujeres el 63% de la población dentro de este grupo etario. Su población afiliada, la cual incluye a los jubilados y pensionados del régimen nacional contributivo, a beneficiarios de pensiones no contributivas, a los veteranos de guerra de Malvinas, así como a los familiares a cargo de estos tres grupos.

1.2 A partir de un diagnóstico institucional realizado, se han identificado una serie de desafíos en la INSSJP para mejorar la eficiencia en el uso de sus recursos. Estos desafíos dieron lugar al desarrollo de una Estrategia Institucional para 2024-2027 aprobada mediante Resolución N° 1193/2024, destinada a abordarlos, que tiene los siguientes pilares: (i) gestión por resultados trazables y medibles; (ii) desarrollo de herramientas digitales para gestionar las prestaciones y evitar desvíos e ineficiencias; (iii) fortalecimiento del nivel de seguridad de la información de sus afiliadas; y (iv) capacitación del personal para actuar en situaciones de contingencia garantizando la continuidad de la atención.

1.3 Para llevar adelante la Estrategia Institucional, se creó mediante Resolución N° 1272/2024 la Gerencia de Seguridad de la Información y Activos Digitales, cuyas competencias son la planificación, el monitoreo, la evaluación y la articulación de políticas de seguridad de la información que permitan mejorar la calidad de los niveles de seguridad a través de procesos y procedimientos como así también mediante la coordinación con otros Organismos y Dependencias Públicas y Privadas, Nacionales o Internacionales.

1.4 Asimismo, la mencionada Gerencia posee entre sus acciones la propuesta de los lineamientos y mecanismos para monitorear y evaluar periódicamente la implementación de la estrategia de seguridad de la información.

1.5 A tales efectos, se ha suscripto con el Banco Interamericano de Desarrollo una Cooperación Técnica (CT) con recursos no reembolsables con el fin de apoyar la iniciativa

en Seguridad de la Información, vinculada a la Estrategia Institucional 2024-2027, a través de: políticas y procesos mejorados y validados, de un BCP elaborado con un plan de implementación, de capacitaciones virtuales diseñadas e implementadas y de jornadas de sensibilización para el Ecosistema en Salud.

2. Objetivos

2.1 El objetivo general de la Cooperación Técnica es brindar apoyo técnico para fortalecer la implementación del Plan Estratégico Institucional del INSSJP, haciendo foco en la seguridad de la información del ecosistema IT (tecnologías de la información) y OT (tecnologías de operación).

2.2 Los objetivos específicos de la CT son:

a. Relevar y efectuar las mejoras necesarias a las políticas y procedimientos de seguridad de la información, que forman parte del Plan de Transformación Digital.
b. Generar a través de las políticas mejoradas los niveles de seguridad necesarios para fortalecer la disponibilidad, la integridad y el resguardo de la información del INSSJP de acuerdo con los estándares exigidos por la normativa vigente.
c. Proponer y elaborar el BCP (Business Continuity Plan).
d. Concientizar, sensibilizar y capacitar a la mayor cantidad de los agentes y prestadores del INSSJP en Seguridad de la Información, generando visibilidad en la agenda pública del compromiso del Instituto en la temática.
e. Sistematizar las prácticas de sensibilización.

2.3 La referida Cooperación Técnica No Reembolsable se estructura en DOS (2) componentes:

a. Componente 1: Apoyo al marco procedimental certificable y al Plan de Continuidad (BCP) referido a la Seguridad de la Información.

b. Componente 2: Jornadas de intercambio de buenas prácticas y experiencias en la materia.

3. Alcance de los Servicios

3.1 La presente contratación se enmarca en la atención de las actividades del Componente 1: "Apoyo al marco procedimental certificable y al Plan de Continuidad (BCP)". El cual tiene como objetivos:

a. **Marco Procedimental Certificable**. Apoyar mediante el relevamiento de la situación actual de políticas y procedimientos propuestos por la Gerencia sobre la Seguridad de la Información y Activos Digitales en el INSSJP-PAMI, mejoras a través de su normativización y estandarización;
b. **La elaboración de un Plan de Continuidad de Negocios (BCP)** y;
c. **Plan de Capacitación**. El diseño y posterior creación de su capacitación en modalidad virtual que llegue a la mayor cantidad de agentes posibles.

4. Actividades Clave

4.1 El relevamiento y propuesta de las mejoras necesarias a las políticas y procedimientos de seguridad de la información, que forman parte del Plan de Transformación Digital. Para ello se deberán realizar:

4.2 Actividades acordes con el Marco Procedimental Certificable (alcance 3.1.a.)

i. El relevamiento, análisis, diseño, normativización y estandarización de políticas y procedimientos y su validación con las Gerencias respectivas.
ii. Generar a través de las políticas mejoradas los niveles de seguridad necesarios para fortalecer la disponibilidad, la integridad y el resguardo de la información del INSSJP de acuerdo con los estándares exigidos por la normativa vigente.
iii. Incluir el detalle de cuáles de esas políticas y procesos podrán ser certificables por la ISO correspondiente (27001/2022), preparando el material necesario para la certificación.

4.3 Actividades acordes con la elaboración del BCP (alcance 3.1.b.)

i. Proponer y elaborar el BCP (Business Continuity Plan).
ii. La elaboración de un BCP y su propuesta de plan de implementación costeado.

4.4 Actividades acordes con el Plan de Capacitación (alcance 3.1.c.)

i. El diseño y la elaboración de la capacitación virtual necesaria para la propuesta de implementación del BCP, para fomentar una cultura de la seguridad de la información a través de la cabal comprensión y ejercicio de las practicas que permitan elevar los umbrales de seguridad de la Institución.

4.5 Enfoque Metodológico: La empresa debe presentar una propuesta metodológica detallada que incluya el enfoque para el desarrollo de políticas de seguridad, la elaboración del BCP y su implementación, así como el método para realizar las capacitaciones.

4.6 Cronograma: Deberá proporcionar un cronograma detallado del proyecto, incluyendo todas las fases de este.

4.7 Gestión de Calidad: La empresa deberá incluir en su propuesta un plan de aseguramiento de la calidad para cada fase del proyecto

5. Resultados y Productos Esperados

5.1 Políticas y procesos mejorados y validados (alcance 3.1.a.)

a. **Informe de Evaluación Inicial**: Documento que detalle el análisis del estado actual de la seguridad de la información en la organización, incluyendo la identificación de activos críticos, vulnerabilidades, riesgos y brechas normativas.

b. **Informe de Recomendaciones Iniciales**: Propuesta de lineamientos generales para el desarrollo de las políticas de seguridad de la información y estrategias para el BCP.

c. **Políticas de Seguridad de la Información**: Propuesta de documentos de las políticas de seguridad alineadas con el estándar ISO/IEC 27001:2022 y normativas internas. Deberán abordar áreas clave como:
    i. Gestión de Activos de la Información (Identificación, Clasificación, Etiquetado, Uso Aceptable)
    ii. Gestión de las Identidades
    iii. Propiedad Intelectual
    iv. Control de accesos
    v. BYOD
    vi. Criptografía
    vii. Desarrollo Seguro
    viii. Data Loss Prevention
    ix. Protección y resguardo de datos
    x. Gestión de incidentes
    xi. Gestión de configuraciones
    xii. Gestión de Vulnerabilidades
    xiii. Inteligencia de amenazas
    xiv. Monitoreo de actividades
    xv. Pantalla Limpias y Uso aceptable
    xvi. Gestión de Proveedores
    xvii. Seguridad Física
    xviii. Gestión del Cambio
    xix. Continuidad del negocio
    xx. Sincronización de relojes
    xxi. Teletrabajo
    xxii. RRHH / Capacitación

5.2 BCP elaborado con propuesta de plan de implementación (alcance 3.1.b.)

a. Análisis de Impacto en el Negocio (BIA): Informe que incluya la evaluación de impacto de interrupciones en los procesos críticos y las posibles consecuencias para la organización.

b. Plan de Continuidad del Negocio (BCP): Documento integral que detalle los procedimientos a seguir en caso de incidentes, planes de recuperación y estrategias para asegurar la continuidad de los procesos críticos.

c. Plan de Recuperación ante Desastres (DRP): Propuesta de Documento adicional que detalle las acciones específicas para recuperar las infraestructuras y sistemas críticos en caso de incidentes mayores o desastres.

d. Cronograma de Implementación del BCP: Plan sugerido para implementación, incluyendo las fases, actividades, plazos y responsables para la implementación del BCP en todas las áreas de la organización.

e. Plan de Pruebas y Simulacros: Documento que establezca el calendario sugerido y los procedimientos tentativos para realizar simulacros y pruebas del BCP en situaciones simuladas de crisis.

5.3 Producto: Capacitación virtual para la implementación del BCP virtual, diseñada e implementada.

a. Programa de Capacitación: Diseño de un programa de formación para los responsables de implementar y gestionar el BCP, que contemple aspectos teóricos y prácticos.

b. Materiales de Capacitación: Presentaciones, guías y materiales de apoyo necesarios para las sesiones de capacitación.

c. **Reporte de Capacitación**: Informe sobre las capacitaciones realizadas, incluyendo la asistencia, evaluaciones de los participantes y feedback obtenido.
d. **Informe Final del Proyecto**: Documento integral que resuma todas las actividades realizadas durante el proyecto, incluyendo el desarrollo de las políticas de seguridad, la elaboración del BCP, los resultados de las pruebas y simulacros, y las capacitaciones realizadas. Recomendaciones para la mejora continua del BCP y la seguridad de la información, así como un plan de seguimiento para asegurar la efectividad a largo plazo.

6. Calendario del Proyecto e Hitos

6.1 Calendario del Proyecto

	1	2	3	4	5	6	7	8
HITO 1 **Primer entregable: Plan detallado de Tareas** que debe incluir: • Cronograma completo								
HITO 2 **Segundo entregable: Primer Informe de Avance** que detalle: • Informe de Evaluación Inicial (5.1.a) • Informe de Recomendaciones Iniciales (5.1.b) • Programa de Capacitación (5.3.a)								
HITO 3 **Tercer entregable: Segundo Informe de Avance** que detalle • Análisis de Impacto en el Negocio (BIA) (5.2.a) • Materiales de Capacitación (5.3.b)								
HITO 4 **Cuarto entregable: Tercer Informe de Avance** que incluya • Documentos de Políticas de Seguridad de la Información (5.1.c) • Plan de Continuidad del Negocio (BCP) (5.2.b) • Plan de Recuperación ante Desastres (DRP) (5.2.c)								
HITO 5 **Quinto entregable: Cuarto Informe de Avance** que contemple • Cronograma Propuesto de Implementación del BCP (5.2.d) • Plan de Pruebas y Simulacros del BCP (5.2.e) • Reporte de Capacitación (5.3.c)								
HITO 6 **Sexto entregable: Quinto Informe de Avance:** • Informe Final del Proyecto (5.3.d)								

6.2 Hitos del Proyectos

1. **Primer entregable:** ***Plan detallado de tareas:*** su entrega deberá realizarse hasta los 30 días de iniciado el contrato.
2. **Segundo entregable: Primer Informe de Avance**: se entrega deberá realizarse a los 60 días del inicio del contrato.
3. **Tercer entregable: Segundo Informe de Avance**: se entrega deberá realizarse a los 90 días del inicio del contrato.
4. **Cuarto entregable: Tercer Informe de Avance**: se entrega deberá realizarse a los 150 días del inicio del contrato.
5. **Quinto entregable: Cuarto Informe de Avance**: se entrega deberá realizarse a los 180 días del inicio del contrato.
6. ***Sexto entregable: Informe final del Proyecto:*** su entrega deberá realizarse hasta los 240 días de iniciado el contrato.

La duración de la contratación será de 8 (ocho) meses.

7. <u>Requisitos de los Informes</u>

7.1 La organización/empresa/institución seleccionada para este proyecto debe entregar los reportes y productos descritos en la sección 5 para ser aprobados por el BID.

7.2 Todos los informes deben ser en español y enviados en formato digital que permita edición y control de cambios, según lo requerido por el BID, con evidencias del avance en las actividades definidas en el plan de trabajo aprobado al inicio del proyecto.

7.3 Se deberá anexar en forma digital todo el material (documentos, instrumentos, bases de datos, etc.) empleados o producidos para el desarrollo de la consultoría.

7.4 Todos los productos e informes generados por esta consultoría, así como la información a la que se acceda durante o después de la consultoría, son propiedad de las partes contratantes y tienen carácter confidencial, quedando expresamente prohibida su divulgación a terceros (a excepción de las partes contratantes) por parte de la Firma Consultora, a menos que cuente con un pronunciamiento escrito por parte de las partes.

7.5 Los informes deberán contar con una sección de resumen ejecutivo con los principales hallazgos y propuestas; se requerirá una revisión y síntesis de información recabada de fuentes primarias y secundarias. Toda información presentada deberá ser debidamente acompañada de información relativa a su fuente, privilegiando siempre fuentes oficiales de información, y datos de las entrevistas realizadas (incluyendo autorización a publicación de información recogida).

8. <u>Criterios de aceptación</u>

8.1 Los informes entregados serán editados y revisados por la firma consultora para garantizar que no incluyen errores gramaticales o de ortografía.

8.2 Interacción con la Gerencia de Seguridad de la Información para el seguimiento de la consultoría: la firma deberá obtener primero una validación técnica de los productos por parte de la Gerencia de Seguridad de la Información. Luego de ello la Jefatura de

Gabinete del INSSJP-PAMI deberá enviar el informe validado al Banco para una revisión. El Banco dará el visto bueno para el pago del producto.

8.3 La entrega de los productos debe ser hecha a partir de la dirección de correo oficial de la firma seleccionada. Retrasos en la entrega deben ser comunicados con el Banco y aprobados debidamente.

8.4 El trabajo será aceptado y aprobado por el jefe de equipo, definido en la sección 9 de este documento. La aceptación y aprobación será comunicada vía correo electrónico (e-mail). A la aprobación del jefe de equipo el pago correspondiente será desembolsado.

8.5 Los productos no se considerarán aceptados hasta que el Banco no lo exprese de forma electrónica.

9. Otros Requisitos

Hacer referencia al Anexo I del Término de Referencia.

10. Supervisión e Informes

10.1 El Especialista Líder de la División de Salud y Protección Social, Mario Sánchez (SCL/SPH) será el responsable de la supervisión de esta consultoría.

10.2 Será responsabilidad de la Firma coordinar reuniones periódicas con el equipo del BID y del INSSJP-PAMI para recibir insumos y guías que puedan ser necesarias para la realización de las actividades.

10.3 Los comentarios a los informes se realizarán dentro de los 10 días hábiles de recepción, y sujetos a modificaciones adicionales a consideración del equipo técnico del BID.

11. Calendario de Pagos

11.1 La Tasa de Cambios Oficial del BID indicada en el SDP se aplicará para las conversiones necesarias de los pagos en moneda local.

Plan de Pagos			
Entregables	**U$S**	**%**	**Plazo de entrega**
HITO 1 **Primer entregable: Plan detallado de Tareas** que debe incluir: • Cronograma completo	2.000	5	30 días de iniciado el contrato.
HITO 2 **Segundo entregable: Primer Informe de Avance** que detalle: • Informe de Evaluación Inicial (5.1.a) • Informe de Recomendaciones Iniciales (5.1.b) • Programa de Capacitación (5.3.a)	6.000	15	60 días de iniciado el contrato.

HITO 3 **Tercer entregable: Segundo Informe de Avance** que detalle • Análisis de Impacto en el Negocio (BIA) (5.2.a) • Materiales de Capacitación (5.3.b)	6.000	15	90 días de iniciado el contrato.
HITO 4 **Cuarto entregable: Tercer Informe de Avance** que incluya • Documentos de Políticas de Seguridad de la Información (5.1.c) • Plan de Continuidad del Negocio (BCP) (5.2.b) • Plan de Recuperación ante Desastres (DRP) (5.2.c)	14.000	35	150 días de iniciado el contrato.
HITO 5 **Quinto entregable: Cuarto Informe de Avance** que contemple • Cronograma Propuesto de Implementación del BCP (5.2.d) • Plan de Pruebas y Simulacros del BCP (5.2.e) • Reporte de Capacitación (5.3.c)	8.000	20	180 días de iniciado el contrato.
HITO 6 **Sexto entregable: Quinto Informe de Avance:** • Informe Final del Proyecto (5.3.d)	4.000	10	240 días de iniciado el contrato.

Anexo I

INFORMACIÓN PARA LA SOLICITUD DE EXPRESIONES DE INTERÉS (PARA SU PREPARACIÓN POR PARTE DEL BID)

1. Requisitos para la Empresa Proveedora del Servicio

1.1 Experiencia y Trayectoria:

1.1.1 Años de Experiencia: La empresa debe contar con un mínimo de 5 años de experiencia comprobable en proyectos de seguridad de la información, desarrollo de políticas de seguridad, elaboración de planes de continuidad del negocio (BCP) y/o certificación de Sistemas de Gestión de Seguridad de la Información (ISO 27001)

1.1.2 Proyectos Similares: Debe haber ejecutado al menos 3 proyectos similares en organizaciones de tamaño y complejidad comparables, preferentemente en el sector público y/o de salud

1.1.3 Referencias: Deberá presentar referencias documentadas de al menos 3 clientes que avalen la calidad y eficacia de los proyectos realizados

1.2 Competencias Técnicas:

1.2.1 Capacidad Técnica: Debe demostrar capacidad técnica para realizar análisis de impacto en el negocio (BIA), evaluación de riesgos y vulnerabilidades, desarrollo de políticas de seguridad, y elaboración e implementación de BCP.

1.3 Equipo de Trabajo:

1.3.1 Perfil de los Consultores de Seguridad de la Información - BCP: La empresa deberá asignar un equipo multidisciplinario compuesto por profesionales con experiencia en seguridad de la información, gestión de riesgos y continuidad del negocio. Cada miembro clave del equipo deberá contar con al menos 3 años de experiencia en su área de especialización.

1.3.2 Liderazgo: El equipo deberá estar liderado por un gerente de proyecto con al menos 5 años de experiencia en proyectos de seguridad de la información y continuidad del negocio, preferentemente con certificaciones como PMP, CISM o similares.

1.3.3 Capacitación: Deberá contar con expertos en formación para diseñar e impartir capacitaciones sobre BCP a diferentes niveles de la organización.

1.4 Metodología y Planificación:

1.4.1 Enfoque Metodológico: La empresa debe presentar una propuesta metodológica detallada que incluya el enfoque para el desarrollo de políticas de seguridad, la elaboración del BCP y su implementación, así como el método para realizar las capacitaciones.

1.4.2 Cronograma: Deberá proporcionar un cronograma detallado del proyecto, incluyendo todas las fases de este.

1.4.3 Gestión de Calidad: La empresa deberá incluir en su propuesta un plan de aseguramiento de la calidad para cada fase del proyecto.

1.5 Solvencia Económica y Financiera:

1.5.1 Capacidad Financiera: La empresa debe demostrar solvencia económica y financiera para garantizar la ejecución completa del proyecto. Deberá presentar balances y estados financieros de los últimos 3 años.

1.5.2 Seguros y Garantías: Se solicitarán garantías de cumplimiento del contrato, así como pólizas de seguro de responsabilidad civil y profesional vigentes.

1.6 Cumplimiento Normativo y Legal:

1.6.1 Regulaciones Locales: La empresa debe cumplir con todas las normativas y regulaciones locales aplicables en materia de seguridad de la información, protección de datos y continuidad del negocio.

1.6.2 Documentación Legal: Deberá presentar toda la documentación legal requerida, como certificados de inscripción, habilitaciones, y cualquier otra documentación solicitada por la entidad contratante.

2. Perfil Consultor de Seguridad de la Información - BCP

2.1 Requisitos:

2.1.1 Título universitario en Ingeniería en Sistemas y/o estudios universitarios o de posgrado relacionados con la Seguridad de la Información.

2.1.2 Experiencia demostrable de al menos 3 años en desarrollo e implementación de sistemas de gestión de seguridad de la información, desarrollo de políticas de seguridad de la información y planes de continuidad del negocio

2.1.3 Experiencia demostrable de al menos 1 proyecto similar en organizaciones de tamaño y complejidad comparables, preferentemente en el sector público y/o de salud.

2.1.4 Certificado de capacitación que demuestre conocimiento de la Norma ISO 27001:2022.

2.1.5 Experiencia en análisis de impacto en el negocio (BIA) y gestión de riesgos.

2.1.6 Certificación vigente CISSP, CISM, Comptia Sec+ o similar.

2.2 Competencias:

2.2.1 Pensamiento analítico y capacidad para resolver problemas complejos.

2.2.2 Habilidad para gestionar proyectos de manera eficiente y cumplir con plazos establecidos.

2.2.3 Habilidades de comunicación efectiva para liderar capacitaciones y coordinar equipos multidisciplinarios.

2.2.4 Capacidad para trabajar en equipo y colaborar con diferentes áreas de la organización.

2.2.5 Adaptabilidad y capacidad para trabajar en entornos dinámicos.

3. Otra información

3.1 Reunión informativa: se prevé realizar una reunión informativa con las firmas interesadas en presentar sus expresiones de interés a fin de atender a las consultas sobre las definiciones y términos de referencia de la contratación.

[Estructura sugerida] *Proceso de selección #::::::::*

TERMINOS DE REFERENCIA

Jornadas de intercambio de buenas prácticas y experiencias en Seguridad de la Información- Firma Consultora

ARGENTINA

[Número de la Cooperación Técnica]

Nombre de la Cooperación Técnica: Apoyo a la Transformación Digital del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP)

[Enlace web con el documento aprobado]

1. Antecedentes y Justificación

1.1 El Instituto Nacional de Servicios Sociales para Jubilados y Pensionados de Argentina (INSSJP) es un actor clave en el subsector de la seguridad social, que brinda asistencia médica y servicios sociales a sus 5,3 millones de afiliados de las cuales 90% tiene 60 años o más, siendo mujeres el 63% de la población dentro de este grupo etario. Su población afiliada, la cual incluye a los jubilados y pensionados del régimen nacional contributivo, a beneficiarios de pensiones no contributivas, a los veteranos de guerra de Malvinas, así como a los familiares a cargo de estos tres grupos.

1.2 A partir de un diagnóstico institucional realizado, se han identificado una serie de desafíos en la INSSJP para mejorar la eficiencia en el uso de sus recursos. Estos desafíos dieron lugar al desarrollo de una Estrategia Institucional para 2024-2027 aprobada mediante Resolución N° 1193/2024, destinada a abordarlos, que tiene los siguientes pilares: (i) gestión por resultados trazables y medibles; (ii) desarrollo de herramientas digitales para gestionar las prestaciones y evitar desvíos e ineficiencias; (iii) fortalecimiento del nivel de seguridad de la información de sus afiliadas; y (iv) capacitación del personal para actuar en situaciones de contingencia garantizando la continuidad de la atención.

1.3 Para llevar adelante la Estrategia Institucional, se creó mediante Resolución N° 1272/2024 la Gerencia de Seguridad de la Información y Activos Digitales, cuyas competencias son la planificación, el monitoreo, la evaluación y la articulación de políticas de seguridad de la información que permitan mejorar la calidad de los niveles de seguridad a través de procesos y procedimientos como así también mediante la coordinación con otros Organismos y Dependencias Públicas y Privadas, Nacionales o Internacionales.

1.4 Asimismo, la mencionada Gerencia posee entre sus acciones la propuesta de los lineamientos y mecanismos para monitorear y evaluar periódicamente la implementación de la estrategia de seguridad de la información.

1.5 A tales efectos, se ha suscripto con el Banco Interamericano de Desarrollo una Cooperación Técnica (CT) con recursos no reembolsables con el fin de apoyar la iniciativa en Seguridad de la Información, vinculada a la Estrategia Institucional 2024-2027, a través de: políticas y procesos mejorados y validados, de un BCP elaborado con un plan

de implementación, de capacitaciones virtuales diseñadas e implementadas y de jornadas de sensibilización para el Ecosistema en Salud.

2. Objetivos

2.1 El objetivo general de la Cooperación Técnica es brindar apoyo técnico para fortalecer la implementación del Plan Estratégico Institucional del INSSJP, haciendo foco en la seguridad de la información del ecosistema IT (tecnologías de la información) y OT (tecnologías de operación).

2.2 Los objetivos específicos de la CT son:

a. Relevar y efectuar las mejoras necesarias a las políticas y procedimientos de seguridad de la información, que forman parte del Plan de Transformación Digital.
b. Generar a través de las políticas mejoradas los niveles de seguridad necesarios para fortalecer la disponibilidad, la integridad y el resguardo de la información del INSSJP de acuerdo con los estándares exigidos por la normativa vigente.
c. Proponer y elaborar el BCP (Business Continuity Plan).
d. Concientizar, sensibilizar y capacitar a la mayor cantidad de los agentes y prestadores del INSSJP en Seguridad de la Información, generando visibilidad en la agenda pública del compromiso del Instituto en la temática.
e. Sistematizar las prácticas de sensibilización.

2.3 La referida Cooperación Técnica No Reembolsable se estructura en DOS (2) componentes:

a. Componente 1: Apoyo al marco procedimental certificable y al Plan de Continuidad (BCP) referido a la Seguridad de la Información.

b. Componente 2: Jornadas de intercambio de buenas prácticas y experiencias en la materia.

3. Alcance de los Servicios

3.1 La presente contratación se enmarca en la atención de las actividades del Componente 2: "Jornadas de intercambio de buenas prácticas y experiencias en la materia", cuyo objetivo es generar a través de una jornada de Seguridad en la Información en el sistema prestacional, el ecosistema necesario, para sistematizar los principales hallazgos en conjunto con el estado de situación de la Seguridad de la Información en el INSSJP-PAMI.

3.2 Este componente está vinculado con los siguientes los objetivos específicos, anteriormente mencionados: i) Concientizar, sensibilizar y capacitar a la mayor cantidad de los agentes y prestadores del INSSJP en Seguridad de la Información, generando visibilidad en la agenda pública del compromiso del Instituto en la temática; ii) Sistematizar las prácticas de sensibilización.

3.3 La presente contratación se enmarca en el primer objetivo específico y comprende la elaboración de Jornadas de intercambio de buenas prácticas y experiencias en la materia, se espera que la misma sean dos encuentros de Seguridad de la Información multidisciplinaria de 8 hs máximo de duración para 100 asistentes, con la participación de referentes internacionales y nacionales en la materia. Se prevé también la sistematización de las principales conclusiones.

4. Actividades Clave

4.1 Un encuentro de dos jornadas de Seguridad de la Información multisectorial de 8 hs máximo de duración para 100 asistentes, con la participación de referentes internacionales y nacionales en la materia.

4.2 Video/relatoría de las principales conclusiones del evento.

5. Resultados y Productos Esperados

5.1 Un encuentro de dos jornadas para 100 personas a realizarse durante el segundo semestre de 2025, en un salón del Área Metropolitana de Buenos Aires (AMBA). Para ello la firma deberá presentar su propuesta de servicios incluyendo:

i. Lugar: salón a cargo del INSSJP-PAMI - zona AMBA;
ii. Pasajes de avión:
Pasaje para expositor de América del Norte
Pasaje para expositor de Europa;
iii. Alojamiento y comidas para expositores extranjeros:
3 noches de alojamiento y comidas para 2 días
iv. Servicio de catering: catering para 100 personas para 2 días de jornada - café bienvenida; café en intervalo de la mañana; almuerzo; café para intervalo de la tarde.
v. Servicio de traslado para expositores extranjeros: del aeropuerto de Ezeiza al hotel y del hotel al aeropuerto de Ezeiza;
vi.. Realización de cobertura en video y fotografía, entrevistas (al menos 5 speakers seleccionados) en video y fotografía, producción de relatoría, videowall (10m x 4m aprox), provisión de electrónica y operación de proyección, provisión de electrónica y operación de sonido (4 micrófonos inalámbricos, 3 micrófonos headset, parlantes), provisión y operación de cabinas de interprete (2), interprete español-inglés/inglés-español (2 recursos), electrónica de headset de intérpretes y público (al menos 60 unidades), logística de todos los servicios y personal necesario incluyendo ART y fletes.
vii. Imprevistos

6. Calendario del Proyecto e Hitos

- Hito 1. Presentación de las propuestas y presupuestos estimados: agosto 2025
- Hito 2. Realización del evento: segundo semestre 2025 (a confirmar mes de septiembre)
- Hito 3. Presentación de video y relatoría del evento: noviembre de 2025.

7. Requisitos de los Informes

7.1 La organización/empresa/institución seleccionada para este proyecto debe entregar evidencia de los reportes, servicios y productos descritos en la sección 5 para ser aprobados por el BID.

7.2 Todos los informes deben ser en español y enviados en formato digital que permita edición y control de cambios, según lo requerido por el BID, con evidencias del avance en las actividades definidas en el plan de trabajo aprobado al inicio del proyecto.

7.3 Se deberá anexar en forma digital todo el material (documentos, instrumentos, bases de datos, etc.) empleados o producidos para el desarrollo de los servicios.

7.4 Todos los productos e informes generados por estos servicios, así como la información a la que se acceda durante o después del mismo, son propiedad de las partes contratantes y tienen carácter confidencial, quedando expresamente prohibida su divulgación a terceros (a excepción de las partes contratantes) por parte de la Firma Consultora, a menos que cuente con un pronunciamiento escrito por parte de las partes.

7.5 Los informes deberán contar con una sección de resumen ejecutivo con los principales detalles de los servicios prestados; Toda información presentada deberá ser debidamente acompañada de información relativa a su fuente, privilegiando siempre fuentes oficiales de información, y datos de las entrevistas realizadas (incluyendo autorización a publicación de información recogida).

8. Criterios de aceptación

8.1 Los informes/propuestas entregadas serán editados y revisados por la firma consultora para garantizar que no incluyen errores gramaticales o de ortografía.

8.2 Interacción con la Gerencia de Seguridad de la Información y Activos Digitales para el seguimiento de la consultoría: la firma deberá obtener primero una validación técnica de los productos por parte de la Gerencia de Seguridad de la Información y Activos Digitales y de la Gerencia de Comunicación y Relaciones Institucionales. Luego de ello la Jefatura de Gabinete del INSSJP-PAMI deberá enviar el informe validado al Banco para una revisión. El Banco dará el visto bueno para el pago del producto

8.3 La entrega de los productos debe ser hecha a partir de la dirección de correo oficial de la firma seleccionada. Retrasos en la entrega deben ser comunicados con el Banco y aprobados debidamente.

8.4 El trabajo será aceptado y aprobado por el jefe de equipo, definido en la sección 9 de este documento. La aceptación y aprobación será comunicada vía correo electrónico (e-mail). A la aprobación del jefe de equipo el pago correspondiente será desembolsado.

8.5 Los productos no se considerarán aceptados hasta que el Banco no lo exprese de forma electrónica.

9. Otros Requisitos

- Ver detalle de requisitos de la firma en Anexo I.

10. Supervisión e Informes

10.1 El Especialista Líder de la División de Salud y Protección Social, Mario Sánchez (SCL/SPH) será el responsable de la supervisión de esta consultoría.

10.2 Será responsabilidad de la Firma coordinar reuniones periódicas con el equipo del BID y del INSSJP-PAMI para recibir insumos y guías que puedan ser necesarias para la realización de las actividades.

10.3 Los comentarios a los informes se realizarán dentro de los 10 días hábiles de recepción, y sujetos a modificaciones adicionales a consideración del equipo técnico del BID.

- **Calendario de Pagos**

Plan de pagos		
Entregables	%	USD
Propuesta de servicios y presupuesto	50	15.000
Informe/rendición sobre evento realizado	40	12.000
Video/relatoría presentado	10	3.000
Totales	100	30.000

La Tasa de Cambios Oficial del BID indicada en el SDP se aplicará para las conversiones necesarias de los pagos en moneda local.

Anexo I

Requerimientos/antecedentes de la proveedora de servicios logísticos:

- 5 años de experiencia en la organización de eventos y provisión de servicios logísticos (hotelería, pasajes, etc) para sus expositores y participantes; y servicios de video/relatoría en eventos de similar envergadura.

[Estructura sugerida] *Proceso de selección #::::::::*

TÉRMINOS DE REFERENCIA

Producto 2 “Sistematización/documentación de experiencias y lecciones aprendidas en el sector prestacional y de salud" y Producto 3 "La realización de una antología de situación de la seguridad de la información en el sector salud" - Firma Consultora

ARGENTINA

[Número de la Cooperación Técnica]

Nombre de la Cooperación Técnica: Apoyo a la Transformación Digital del Instituto Nacional de Servicios Sociales para Jubilados y Pensionados (INSSJP)

[Enlace web con el documento aprobado]

1. Antecedentes y Justificación

1. El Instituto Nacional de Servicios Sociales para Jubilados y Pensionados de Argentina (INSSJP) es un actor clave en el subsector de la seguridad social, que brinda asistencia médica y servicios sociales a sus 5,3 millones de afiliados de las cuales 90% tiene 60 años o más, siendo mujeres el 63% de la población dentro de este grupo etario. Su población afiliada, la cual incluye a los jubilados y pensionados del régimen nacional contributivo, a beneficiarios de pensiones no contributivas, a los veteranos de guerra de Malvinas, así como a los familiares a cargo de estos tres grupos.

2. A partir de un diagnóstico institucional realizado, se han identificado una serie de desafíos en la INSSJP para mejorar la eficiencia en el uso de sus recursos. Estos desafíos dieron lugar al desarrollo de una Estrategia Institucional para 2024-2027 aprobada mediante Resolución N° 1193/2024, destinada a abordarlos, que tiene los siguientes pilares: (i) gestión por resultados trazables y medibles; (ii) desarrollo de herramientas digitales para gestionar las prestaciones y evitar desvíos e ineficiencias; (iii) fortalecimiento del nivel de seguridad de la información de sus afiliadas; y (iv) capacitación del personal para actuar en situaciones de contingencia garantizando la continuidad de la atención.

3. Para llevar adelante la Estrategia Institucional, se creó mediante Resolución N° 1272/2024 la Gerencia de Seguridad de la Información y Activos Digitales, cuyas competencias son la planificación, el monitoreo, la evaluación y la articulación de políticas de seguridad de la información que permitan mejorar la calidad de los niveles de seguridad a través de procesos y procedimientos como así también mediante la coordinación con otros Organismos y Dependencias Públicas y Privadas, Nacionales o Internacionales.

4. Asimismo, la mencionada Gerencia posee entre sus acciones la propuesta de los lineamientos y mecanismos para monitorear y evaluar periódicamente la implementación de la estrategia de seguridad de la información.

5. A tales efectos, se ha suscripto con el Banco Interamericano de Desarrollo una Cooperación Técnica (CT) con recursos no reembolsables con el fin de apoyar la iniciativa en Seguridad de la Información, vinculada a la Estrategia Institucional 2024-2027, a través de: políticas y procesos mejorados y validados, de un BCP elaborado con un plan

de implementación, de capacitaciones virtuales diseñadas e implementadas y de jornadas de sensibilización para el Ecosistema en Salud.

2. Objetivos

1. El objetivo general de la Cooperación Técnica es brindar apoyo técnico para fortalecer la implementación del Plan Estratégico Institucional del INSSJP, haciendo foco en la seguridad de la información del ecosistema IT (tecnologías de la información) y OT (tecnologías de operación).

2. Los objetivos específicos de la CT son:
   a. Relevar y efectuar las mejoras necesarias a las políticas y procedimientos de seguridad de la información, que forman parte del Plan de Transformación Digital.
   b. Generar a través de las políticas mejoradas los niveles de seguridad necesarios para fortalecer la disponibilidad, la integridad y el resguardo de la información del INSSJP de acuerdo con los estándares exigidos por la normativa vigente.
   c. Proponer y elaborar el BCP (Business Continuity Plan).
   d. Concientizar, sensibilizar y capacitar a la mayor cantidad de los agentes y prestadores del INSSJP en Seguridad de la Información, generando visibilidad en la agenda pública del compromiso del Instituto en la temática.
   e. Sistematizar las prácticas de sensibilización.

3. La referida Cooperación Técnica No Reembolsable se estructura en DOS (2) componentes:
   a. Componente 1: Apoyo al marco procedimental certificable y al Plan de Continuidad (BCP) referido a la Seguridad de la Información.
   b. Componente 2: Jornadas de intercambio de buenas prácticas y experiencias en la materia.

3. Alcance de los Servicios

1. La presente contratación se enmarca en la atención de las actividades del Componente 2: "Jornadas de intercambio de buenas prácticas y experiencias en la materia", cuyo objetivo es generar a través de una jornada de Seguridad en la Información en el sistema prestacional, el ecosistema necesario, para sistematizar los principales hallazgos en conjunto con el estado de situación de la Seguridad de la Información en el INSSJP-PAMI.

2. Este componente está vinculado con los siguientes los objetivos específicos, anteriormente mencionados: i) Concientizar, sensibilizar y capacitar a la mayor cantidad de los agentes y prestadores del INSSJP en Seguridad de la Información, generando visibilidad en la agenda pública del compromiso del Instituto en la temática; ii) Sistematizar las prácticas de sensibilización.

3. La presente contratación se enmarca en el segundo y tercer objetivos específicos y comprende:

   i. La sistematización/documentación de experiencias y lecciones aprendidas en el sector prestacional y de salud para contribuir a la formación de nuevas políticas y planes de seguridad de la información que fortalezcan a todos los actores del sector. Producto: Documentación de las lecciones.

ii. La realización de una antología de situación de la seguridad de la información en el sector de salud en idioma español y en idioma inglés, la cual deberá documentar experiencias, entrevistas y lecciones aprendidas en el sector de salud para contribuir a la formación de nuevas políticas y planes de seguridad de la información que fortalezcan a todos los actores del sector y a las transformaciones digitales que está llevando adelante el Instituto. Producto: Documentación de las experiencias y lecciones que resulten en una guía de buenas prácticas.

4. Actividades Clave

1. La sistematización/documentación de experiencias y lecciones aprendidas en el sector prestacional y de salud para contribuir a la formación de nuevas políticas y planes de seguridad de la información que fortalezcan a todos los actores del sector. Producto: Documentación de las lecciones.

2. Realización de una antología de situación de la seguridad de la información en el sector de salud en idioma español y en idioma inglés, la cual deberá documentar experiencias, entrevistas y lecciones aprendidas en el sector de salud para contribuir a la formación de nuevas políticas y planes de seguridad de la información que fortalezcan a todos los actores del sector y a las transformaciones digitales que está llevando adelante el Instituto.

3. Para ello, la consultora utilizará una metodología mixta, combinando la observación directa durante la jornada de Mejores Prácticas, la recolección de datos primarios a través de entrevistas y la revisión documental de materiales proporcionados por los participantes y expertos.

4. Entrevistas semi-estructuradas: Se realizarán entrevistas con actores clave del sector (directores de TI, especialistas en seguridad de la información, responsables de proyectos), siguiendo un guion que permita capturar tanto experiencias técnicas como lecciones de gestión.

5. Revisión de materiales: La consultora deberá revisar presentaciones, documentos y publicaciones proporcionados por los participantes de la jornada y actores entrevistados.

6. Análisis cualitativo: La información será procesada y sistematizada utilizando técnicas de análisis cualitativo que permitan identificar patrones, buenas prácticas y áreas de mejora.

5. Resultados y Productos Esperados

1. Prácticas de sensibilización sistematizadas:
   i. Documentación de las lecciones realizada y entregada.
   ii. Documentación de las experiencias y lecciones y Guía de buenas prácticas realizada y entregada. Análisis y propuestas de mejora:
      a. Proponer recomendaciones estratégicas basadas en las experiencias documentadas, con miras a mejorar las políticas y procedimientos actuales.

b. Elaborar una guía de buenas prácticas para fortalecer la seguridad de la información en el sector salud, tomando en cuenta las tendencias globales y locales.

6. Calendario del Proyecto e Hitos

- Hito 1. Presentación de las propuestas y presupuestos estimados, agosto 2025
- Hito 2. Informe de sobre la documentación de las lecciones y experiencias, 40 días posteriores a la firma del contrato
- Hito 3. Guía de buenas prácticas; 50 días posteriores a la firma del contrato.

7. Requisitos de los Informes

1. La organización/empresa/institución seleccionada para este proyecto debe entregar evidencia de los reportes y productos descritos en la sección 5 para ser aprobados por el BID.

2. Todos los informes deben ser en español y enviados en formato digital que permita edición y control de cambios, según lo requerido por el BID, con evidencias del avance en las actividades definidas en el plan de trabajo aprobado al inicio del proyecto.

3. Se deberá anexar en forma digital todo el material (documentos, instrumentos, bases de datos, etc.) empleados o producidos para el desarrollo de los servicios.

4. Todos los productos e informes generados por estos servicios, así como la información a la que se acceda durante o después del mismo, son propiedad de las partes contratantes y tienen carácter confidencial, quedando expresamente prohibida su divulgación a terceros (a excepción de las partes contratantes) por parte de la Firma Consultora, a menos que cuente con un pronunciamiento escrito por parte de las partes.

5. Los informes deberán contar con una sección de resumen ejecutivo con los principales detalles de los servicios prestados; Toda información presentada deberá ser debidamente acompañada de información relativa a su fuente, privilegiando siempre fuentes oficiales de información, y datos de las entrevistas realizadas (incluyendo autorización a publicación de información recogida).

8. Criterios de aceptación

1. Los informes entregados serán editados y revisados por la firma consultora para garantizar que no incluyen errores gramaticales o de ortografía.

2. Interacción con la Gerencia de Seguridad de la Información para el seguimiento de la consultoría: la firma deberá obtener primero una validación técnica de los productos por parte de la Gerencia de Seguridad de la Información. Luego de ello la Jefatura de Gabinete del INSSJP-PAMI deberá enviar el informe validado al Banco para una revisión. El Banco dará el visto bueno para el pago del producto.

3. La entrega de los productos debe ser hecha a partir de la dirección de correo oficial de la firma seleccionada. Retrasos en la entrega deben ser comunicados con el Banco y aprobados debidamente.

4. El trabajo será aceptado y aprobado por el jefe de equipo, definido en la sección 9 de este documento. La aceptación y aprobación será comunicada vía correo electrónico (e-mail). A la aprobación del jefe de equipo el pago correspondiente será desembolsado.

5. Los productos no se considerarán aceptados hasta que el Banco no lo exprese de forma electrónica.

9. Otros Requisitos

Ver Anexo I Requisitos de la Firma Consultora

10. Supervisión e Informes

1. El Especialista Líder de la División de Salud y Protección Social, Mario Sánchez (SCL/SPH) será el responsable de la supervisión de esta consultoría.

2. Será responsabilidad de la Firma coordinar reuniones periódicas con el equipo del BID y del INSSJP-PAMI para recibir insumos y guías que puedan ser necesarias para la realización de las actividades.

3. Los comentarios a los informes se realizarán dentro de los 10 días hábiles de recepción, y sujetos a modificaciones adicionales a consideración del equipo técnico del BID.

11. Calendario de Pagos

- La Tasa de Cambios Oficial del BID indicada en el SDP se aplicará para las conversiones necesarias de los pagos en moneda local.

Plan de pagos		
Entregables	%	USD
Plan de Trabajo y cronograma	10	1.000
Informe sobre documentación de lecciones aprendidas	40	4.000
Presentación versión final de guía de buenas prácticas	50	5.000
Totales	100	10.000

Anexo I

REQUISITOS DE LA FIRMA CONSULTORA

La empresa deberá cumplir con los siguientes requisitos:

1. Experiencia mínima de 5 años en la documentación y sistematización de experiencias, capacidad analítica y elaboración de informes técnicos.
2. Capacidad para trabajar en contextos de seguridad de la información y tecnologías aplicadas al sector salud.
4. Disponibilidad de al menos dos profesionales con estudios de posgrado en Cs Sociales y antecedentes demostrables de al menos 5 años en trabajo de campo de observación participante y entrevistas en profundidad a expertos y/o funcionarios públicos de primera línea de gestión y análisis de políticas públicas.
5. Conocimiento de gestión y monitoreo de proyectos.
6. Empresa radicada en el AMBA dada la proximidad geográfica con la ubicación del evento.