

Contratación de servicios de una empresa especializada en Seguridad de la Información para ejercer la función de Responsable de Seguridad de la Información (RSI) y asesoramiento en protección de datos personales

(SC-CP-11/2026)

Información complementaria

Fecha publicación: 30/10/2026

Importante: Plazo de postulación: domingo 08/11/2026 las 23:59 horas.

A continuación, las consultas realizadas con sus respectivas respuestas:

- 1) ***Considerando los avances con relación al marco regulatorio y de gobernanza, ¿tienen alguna medición hecha sobre framework o algún estándar en cuanto al nivel de madurez a nivel institucional?***

Respuesta: Ese trabajo ya se ha venido desarrollando con el proveedor actual y tal como se establece en los TdR, la información y documentación vinculada al estado de situación actual será compartida con la empresa que resulte seleccionada, considerando su carácter confidencial, a efectos de ajustar el Plan de Trabajo preliminar presentado con la oferta y elaborar el Plan de Trabajo definitivo.

- 2) ***En función de la dinámica actual, ¿tienen identificado un promedio de horas mensuales que se utilizan para el RSI y su equipo asociado?***

Respuesta: Desde INEFOP no se establece una dedicación mínima de horas. Dicho aspecto deberá ser considerado por la empresa en su Plan de trabajo inicial al momento de postular en base al alcance y demás información disponible en TdR. Como información complementaria, actualmente INEFOP cuenta con un Comité de Seguridad de la Información que sesiona todas las semanas (1 hora como base), y un Comité de Datos Personales que se reúne quincenalmente. Estas son las instancias periódicas de coordinación actualmente previstas, sin perjuicio del trabajo propio del rol y las actividades asociada al servicio que debe desarrollar la empresa.

- 3) ***Con relación a las pruebas de seguridad y herramientas que se utilicen, deben estar contemplados en la propuesta económica o INEFOP ya cuenta con algunas, sobre todo en cuanto a licenciamiento que se pueda necesitar para desarrollar la tarea***

Y en cuánto a herramientas de concientización, ¿tienen alguna?

Respuesta: INEFOP cuenta con herramientas institucionales que podrán utilizarse para el desarrollo de las actividades previstas en el servicio, según corresponda. No obstante, los oferentes podrán proponer herramientas adicionales que consideren pertinentes para la implementación de su Plan de Trabajo, identificando sus características.

La necesidad de incorporar nuevas herramientas y las condiciones para su utilización serán evaluadas y acordadas con INEFOP, de acuerdo con las prioridades institucionales y las condiciones establecidas en los TdR.

En materia de concientización, INEFOP dispone de una plataforma institucional para capacitaciones internas. La eventual incorporación de otras herramientas podrá ser propuesta por los oferentes y evaluada en el marco del servicio.

- 4) ***¿Entienden que aporta valor adicionar un servicio de respuestas a incidentes de carácter netamente técnicos. O sea, más allá de la atención del RSI en su rol específico, ¿también incluir una respuesta técnica a eventuales incidentes?***

Respuesta: Los TdR contemplan el asesoramiento, la coordinación y el acompañamiento del RSI en la gestión de incidentes de seguridad de la información, pero no establecen como requisito la prestación de un servicio

adicional de respuesta técnica operativa ante incidentes. Por lo tanto, no se requiere que los oferentes incorporen dicho servicio adicional en sus propuestas, a efectos de mantener condiciones comparables para su evaluación.

Sin perjuicio de ello, cada oferente podrá describir las capacidades técnicas de su equipo y los mecanismos de apoyo que propone para la atención de incidentes, en el marco del alcance establecido en los TdR. Estos aspectos podrán ser considerados en la evaluación técnica, conforme a los criterios previstos en el llamado.

5) ***En cuanto a la atención/apoyo permanente que se plantea, ¿tiene que ser para todos los casos o para escenarios críticos?***

Respuesta: En este caso no exige una cobertura permanente 24/7, pero sí se espera que la empresa garantice la asistencia y el acompañamiento necesarios ante eventuales incidentes críticos de seguridad de la información que puedan presentarse. Cada oferente deberá indicar en su propuesta técnica la disponibilidad, modalidad de atención y tiempos de respuesta previstos, conforme a lo solicitado en los TdR.

6) ***Hoy en día el RSI; ¿trabaja con un equipo de seguridad interno de INEFOP o sería parte de la propuesta abarcar la parte táctica y técnica, o sea la operacional?***

Respuesta: Actualmente el RSI trabaja en forma coordinada con el equipo de TI de INEFOP, pero no contamos con una estructura interna especializada en Seguridad de la Información. Se prevé mantener el esquema de trabajo conjunto, en el que el RSI que resulte seleccionado trabajará enfocado en el asesoramiento, la coordinación y el seguimiento de las acciones de seguridad de la información, mientras que el equipo de TI de INEFOP será responsable de implementar las medidas técnicas y operativas que se requieran, en coordinación con el RSI.

7) ***¿El servicio requiere ejecutar ejemplo análisis de vulnerabilidades, pentest?***

Respuesta: Si bien ya tenemos antecedentes de realización de análisis de vulnerabilidades y pruebas de seguridad, se prevé dar continuidad a este tipo de actividades en el marco del servicio contratado. El servicio podrá comprender tanto el asesoramiento y seguimiento de las pruebas realizadas como su eventual ejecución por parte de la empresa adjudicataria, según las necesidades y prioridades institucionales. La modalidad, el alcance y las responsabilidades específicas se definirán de común acuerdo con INEFOP en el Plan de Trabajo.

8) ***¿Existe la posibilidad de postular como un conglomerado de empresas?***

Respuesta: No es posible. La propuesta deberá ser presentada por una única empresa, que será la responsable contractual frente a INEFOP, incluyendo la facturación y el cumplimiento integral del servicio. No obstante, no existe inconveniente en que dicha empresa integre su equipo de trabajo con profesionales vinculados a otras empresas, siempre que se cumplan los requisitos establecidos en los TdR y que la responsabilidad por la prestación del servicio recaiga íntegramente en la empresa contratada.

9) ***Con el objetivo de dimensionar la cantidad de horas del servicio, tal se aclaró todas las configuraciones técnicas específicas las realiza el equipo interno de TI de INEFOP. No obstante, en cuanto a Documentación, mantenimiento de la matriz de riesgos y el respectivo taller, o sea todo lo vinculado a las tareas de gestión, ¿hay algún equipo de INEFOP que lo realiza, o quedaría a cargo de la empresa contratada?***

Respuesta: Esas tareas quedarán a cargo de la empresa seleccionada incluyendo la elaboración y actualización de la documentación, el mantenimiento de la matriz de riesgos y la realización de los talleres que correspondan, de acuerdo con el alcance del servicio y el Plan de Trabajo acordado. No obstante, siempre habrá una asistencia, acompañamiento, intercambio y revisión desde INEFOP, así como las gestiones finales para la formalización y comunicación de dicha documentación a nivel institucional.

10) ***¿Cuáles serían las prioridades que debería abarcar el RSI?***

Respuesta: En términos generales, la prioridad será dar continuidad al Sistema de Gestión de Seguridad de la Información existente, así como avanzar en las mejoras, actualizaciones y acciones de fortalecimiento que correspondan, en el marco del servicio requerido y de las actividades previstas en los TdR. Las prioridades específicas se definirán de común acuerdo con INEFOP al elaborar el Plan de Trabajo definitivo, considerando

el estado de situación institucional y las necesidades identificadas..

- 11) ***¿Cuál fue el último nivel de madurez reportado frente al Marco de Ciberseguridad de AGESIC y qué compromisos o entregas a AGESIC/CERTuy tienen fecha dentro de los próximos 12 meses?***

Respuesta: INEFOP ha realizado evaluaciones de madurez y avanzado en medidas alineadas con el Marco de Ciberseguridad de AGESIC.

Actualmente no se identifican compromisos específicos ni entregas periódicas programadas ante AGESIC o CERTuy para los próximos 12 meses, sin perjuicio de las obligaciones normativas o requerimientos que pudieran surgir.

Los resultados disponibles y las prioridades de mejora se compartirán con el adjudicatario.

- 12) ***¿Cuántos ámbitos de gobernanza integra el RSI (Comité de Seguridad de la Información y otros comités) y con qué frecuencia sesionan? ¿Con qué periodicidad se espera reporte a Gerencia General y al Consejo Directivo?***

Respuesta: El RSI reportará a Gerencia General y asesorará al Consejo Directivo cuando corresponda.

Actualmente el Comité de Seguridad de la Información sesiona semanalmente; el ámbito de protección de datos personales, quincenalmente o a demanda; y las instancias ampliadas con otras áreas se convocan según los temas. La periodicidad de reportes específicos se acordará en el Plan de Trabajo.

- 13) ***¿INEFOP tiene una expectativa de dedicación mínima del RSI (horas o jornadas semanales)? ¿Hay algún monto referencial establecido para este ejercicio? Cantidad de horas del servicio actual***

Respuesta: El TdR no establece una dedicación mínima expresada en horas o jornadas. Cada oferente deberá proponer una disponibilidad y organización del equipo acordes con el alcance, la atención de prioridades y los resultados esperados.

No se establece en las bases un monto referencial de cotización.

- 14) ***¿Cuál es la herramienta o mecanismo de registro y seguimiento de actividades definido por INEFOP? ¿El adjudicatario tendrá acceso con usuario propio, o debe proveer la herramienta?***

Respuesta: INEFOP dispone de herramientas institucionales para el registro y seguimiento de actividades. Los mecanismos de utilización, así como los accesos y permisos correspondientes, se definirán según las necesidades del servicio y las políticas institucionales aplicables.

Sin perjuicio de ello, los oferentes podrán proponer herramientas o mecanismos alternativos en su propuesta técnica, cuya utilización estará sujeta a evaluación y acuerdo con INEFOP.

En todos los casos, el adjudicatario deberá mantener actualizado el registro de actividades, avances, productos y asuntos pendientes, asegurando su trazabilidad y adecuado seguimiento.

- 15) ***¿El equipo del adjudicatario deberá operar con equipamiento y cuentas institucionales de INEFOP, o podrá usar sus propios medios bajo las políticas de INEFOP? ¿Hay restricciones al uso de repositorios o herramientas en la nube del proveedor?***

Respuesta: El equipamiento de trabajo deberá ser provisto por el adjudicatario; INEFOP no prevé entregar computadoras u otros equipos para la prestación.

Cuando resulte necesario, podrá habilitar cuentas o accesos institucionales bajo las condiciones que se establezcan.

El uso de repositorios y herramientas externas, incluidas las soluciones en la nube, deberá ajustarse a las políticas institucionales y contar con la autorización que corresponda.

- 16) ***Dado que el pago es un monto mensual fijo y las líneas de acción son no taxativas, ¿INEFOP admite que la propuesta defina una capacidad mensual de horas asociada al monto, con un mecanismo acordado para requerimientos que la excedan?***

Respuesta: El servicio se contrata por un monto mensual fijo. Cada oferente podrá explicitar en su propuesta la dedicación y capacidad de trabajo previstas, siempre que sean compatibles con el alcance y los resultados esperados.

El TdR no prevé un mecanismo automático de cobro de horas excedentes ni condiciones económicas adicionales por requerimientos que surjan dentro del alcance del servicio.

17) Cuando un ajuste del Plan de Trabajo (nuevas normativas, incidentes, tecnologías) implique mayor esfuerzo que el previsto, ¿cómo se prevé repriorizar? ¿Se reemplazan actividades del plan o puede gestionarse como ampliación?

Respuesta: El Plan de Trabajo podrá ajustarse de común acuerdo entre las partes, redefiniendo prioridades, actividades e hitos en función de nuevas necesidades, riesgos o incidentes. Conforme al TdR, dichos ajustes no implicarán por sí mismos modificaciones del plazo contractual ni de las condiciones económicas adjudicadas.

18) En la línea de vulnerabilidades y pruebas de seguridad, ¿se espera que el adjudicatario ejecute pruebas de penetración dentro del servicio, o solo que asesore, priorice y dé seguimiento a pruebas ejecutadas por terceros? ¿Cuántos ejercicios por año se prevén?

Respuesta: Los TdR contemplan el asesoramiento y acompañamiento en la identificación, análisis, priorización y seguimiento de vulnerabilidades y pruebas de seguridad.

INEFOP cuenta con antecedentes de realización de este tipo de actividades y se prevé darles continuidad. En este sentido, el servicio podrá comprender tanto el asesoramiento y seguimiento de las pruebas ya realizadas como la eventual ejecución de pruebas de seguridad por parte del adjudicatario, según las necesidades y prioridades institucionales.

La modalidad, el alcance y las responsabilidades específicas se definirán de común acuerdo con INEFOP en el marco del Plan de Trabajo. No se establece una cantidad fija de ejercicios anuales.

19) En caso de necesidad de dimensionar las pruebas de seguridad: ¿cuántas aplicaciones web y APIs expuestas tiene INEFOP, cuántas aplicaciones móviles (por plataforma) y cuántos servidores o servicios publicados a Internet? ¿Cuántos segmentos de red interna estarían en alcance? ¿Las pruebas serían con credenciales e información previa (caja gris) o sin ella (caja negra)? ¿Se espera que las pruebas incluyan explotación controlada de las vulnerabilidades y una re-verificación posterior de los hallazgos remediados?

Respuesta: El alcance y las características de las eventuales pruebas de seguridad se definirán en el marco del Plan de Trabajo, considerando los riesgos, las necesidades y las prioridades institucionales.

La información técnica detallada que resulte necesaria será proporcionada al adjudicatario para la definición de las actividades correspondientes.

Para la elaboración de las ofertas, los oferentes podrán tomar como referencia el alcance previsto en los TdR y las características generales de INEFOP, explicitando, cuando corresponda, los supuestos considerados en su propuesta técnica.

20) ¿INEFOP cuenta con monitoreo de seguridad (SOC, SIEM, EDR) propio o tercerizado? ¿Quién realiza hoy la detección y la primera respuesta técnica ante incidentes?

Respuesta: La gestión de incidentes se realiza con intervención de las áreas institucionales competentes, particularmente TI, y el servicio de RSI debe articularse con ellas para asesorar, coordinar y dar seguimiento. Los mecanismos de monitoreo existentes y la distribución operativa de responsabilidades se precisarán con el adjudicatario.

21) ¿Qué horario de cobertura y qué tiempos de respuesta espera INEFOP para incidentes o situaciones prioritarias? ¿Se requiere disponibilidad fuera del horario hábil? Es viable considerar un servicio adicional de respuesta frente a incidentes, pensado para incidentes declarados de prioridad baja, media y alta?

Respuesta: El TdR solicita que cada oferente proponga la disponibilidad, modalidad de atención y tiempos de respuesta para incidentes o situaciones prioritarias. No establece un horario único de cobertura ni niveles de servicio predeterminados.

Las condiciones ofrecidas deberán ser compatibles con la atención de situaciones prioritarias y serán consideradas en la evaluación técnica. Cualquier servicio adicional separado deberá analizarse conforme a las condiciones del llamado.

22) ¿Cuántos incidentes de seguridad de la información se registraron en los últimos 12 meses y de qué severidad?

Respuesta: Los incidentes registrados en el período reciente han sido de baja frecuencia. El detalle y su clasificación serán compartidos con el adjudicatario cuando corresponda.

23) ¿INEFOP cuenta con análisis de impacto (BIA) y planes de continuidad/recuperación vigentes? ¿Cuántas pruebas o ejercicios de continuidad se esperan en el período?

Respuesta: INEFOP cuenta con algunas acciones y medidas vinculadas a continuidad y recuperación, pero aún no dispone de un análisis de impacto en el negocio (BIA) y de un plan integral de continuidad institucional. Se trata de una línea que se espera profundizar durante el servicio. Las actividades y eventuales ejercicios se definirán en el Plan de Trabajo, sin una cantidad anual preestablecida.

24) ¿Cuántos proveedores o servicios contratados críticos se estima evaluar en el período? ¿Existe un procedimiento vigente de evaluación de terceros?

Respuesta: La evaluación de riesgos de seguridad asociados a proveedores y terceros integra el alcance del servicio. Existen prácticas de evaluación que se encuentran en proceso de formalización y aprobación como procedimientos institucionales. La cantidad de proveedores a evaluar y su priorización se definirán según criticidad y necesidades del período.

25) Para concientización: ¿cuál es la población objetivo (funcionarios, equipos técnicos, otros actores externos)? ¿Se esperan campañas de phishing simulado? ¿Cuántas acciones de capacitación por año?

Respuesta: La población objetivo incluye funcionarios, equipos técnicos y otros actores relevantes según cada temática y en caso de corresponder. Se espera que el oferente proponga un enfoque de concientización, incluyendo alcance, modalidades, frecuencia y acciones recomendadas.

Las campañas de phishing simulado podrán considerarse como alternativa, sin que el TdR establezca un número obligatorio de campañas o capacitaciones anuales. Las acciones se acordarán en el Plan de Trabajo.

26) ¿INEFOP cuenta hoy con una plataforma de concientización, e-learning o simulación de phishing (propia o contratada)? En caso afirmativo, ¿cuál es y hasta cuándo está vigente? En caso negativo, ¿espera que el adjudicatario la provea dentro del servicio?

Respuesta: INEFOP dispone de una plataforma institucional para capacitaciones internas.

Hasta el momento no se han realizado simulaciones de phishing; su eventual incorporación podrá ser propuesta y evaluada como parte del asesoramiento.

El TdR no exige expresamente que el adjudicatario provea una plataforma específica de e-learning o simulación.

27) ¿Cuántas bases de datos personales tiene inscriptas INEFOP ante la URCDP y se prevén evaluaciones de impacto en protección de datos en el período? ¿Cuántas?

Respuesta: INEFOP cuenta con 8 bases de datos personales ingresadas a la URCDP que se encuentran en distintos estados del proceso de registración.

Asimismo, se han realizado evaluaciones de impacto en protección de datos personales, cuyo seguimiento y actualización forman parte de las actividades a considerar en el servicio.

El alcance también comprende el asesoramiento para la identificación de otras bases de datos que requieran registro, así como la evaluación de la necesidad de realizar nuevas evaluaciones de impacto y el seguimiento de su implementación.

No se ha establecido una cantidad fija de evaluaciones de impacto para el período, por lo que estas actividades se definirán en el marco del Plan de Trabajo, de acuerdo con las necesidades y prioridades institucionales.

28) ¿Cuántos proyectos, contrataciones tecnológicas o iniciativas de IA se estima que requerirán intervención del RSI desde el diseño en los próximos 12 meses? ¿Existen ya lineamientos de uso de IA aprobados?

Respuesta: INEFOP se encuentra en proceso de aprobación de su Política de Gobernanza de Inteligencia Artificial. El RSI deberá brindar asesoramiento preventivo en proyectos tecnológicos, contrataciones e iniciativas de IA.

La cantidad de proyectos a abordar se determinará de acuerdo con las prioridades y necesidades institucionales; no se ha fijado un número anual.