Corresponde al Expediente N° 22700 – 19714/2018

CONTRATACION DIRECTA N° 382-137-PAB18
ESPECIFICACIONES TECNICAS BASICAS

1.- Objeto

Contratación de un servicio de consultoría especializado de acompañamiento en la implementación de un Sistema de Gestión de Seguridad de la Información, según la serie de normas ISO 27000 (Gestión de Riesgos, Gestión de Vulnerabilidades, Gestión de Incidencias, Gestión de Activos, etc.) y servicios de consultoría especializado para el desarrollo de un Programa de Concientización en Seguridad de la Información y Auditoría.

2.- Glosario de términos y abreviaturas:

A.R.B.A.: Agencia de Recaudación de la Provincia de Buenos Aires.

S.G.S.I.: Sistema de Gestión de Seguridad de la Información.

3.- Vigencia del servicio:

La vigencia del servicio será el siguiente:

- Fase 1: Estimado en catorce (14) semanas, comprendido al menos, dos (2) encuentros semanales de no menos de 6 horas cada encuentro.
- Fase 2: Estimado en tres (3) semanas.
- Fase 3: Estimado en dos (2) semanas.

4.- Características:

El tiempo estimado para la ejecución del proyecto total, en base a la información recabada y de acuerdo a consultas realizadas a personal idóneo, podrá ser de entre 4 (cuatro) y 6 (seis) meses.

El personal destinado por el proveedor a la ejecución de las tareas contratadas, deberá contar con experiencia en el mercado nacional comprobable mediante referencias en servicios del mismo tenor al solicitado.

El servicio deberá incluir tareas relacionadas con la planificación y elaboración de la documentación necesaria, como así también un plan de capacitación y concientización del personal de A.R.B.A. en temas relacionados con la seguridad de la información.

Las tareas mencionadas, deberán abarcar los siguientes aspectos:

Fase 1: Coaching Especializado en Gestión de Seguridad

En esta fase, se requiere la ejecución de las actividades de validación de situación actual del nivel de implementación del S.G.S.I., la revisión de la documentación necesaria para atender a los requerimientos asociados a las Políticas, Normas, Procedimientos y Controles de Seguridad de la Información de A.R.B.A. y, finalmente establecer sesiones de asesoramiento y coaching para orientar en la implementación efectiva del S.G.S.I.

Como actividades principales a realizar durante el desarrollo del servicio de consultoría se requieren:

1. Desarrollo y ejecución de un análisis y validación del S.G.S.I. implementado con el fin de evaluar el nivel actual de cumplimiento de los documentos mandatorios requeridos por el estándar ISO 27001:2013. Como resultado de esta actividad se deberá establecer el conjunto de acciones que A.R.B.A. deberá ajustar bajo la guía y orientación de los consultores designados por el Oferente. El objetivo de esta etapa consiste en el desarrollo de las siguientes tareas específicas:
    a. Analizar la estructura organizacional de A.R.B.A. en términos de roles y responsabilidades en Seguridad de la Información.
    b. Evaluar el cumplimiento y madurez de los procesos de gestión de seguridad de la información respecto del cumplimiento de las cláusulas 4 a 10 del estándar ISO 27001:
        i. Contexto de Negocio
        ii. Liderazgo y Compromiso
        iii. Planificación
        iv. Procesos de Soporte y Apoyo al S.G.S.I.
        v. Operación del S.G.S.I.
        vi. Revisión por la Dirección y Auditoría Interna
        vii. Mejora Continua

c. Evaluar el cumplimiento y madurez de los controles de seguridad de la información respecto de los 114 controles del Anexo A del estándar ISO 27001

   i. Políticas de Seguridad de la Información
   ii. Organización de la Seguridad de la Información
   iii. Seguridad de los Recursos Humanos
   iv. Gestión de Activos de Información
   v. Control de Acceso
   vi. Cifrado
   vii. Seguridad Física y Ambiental
   viii. Seguridad de las Comunicaciones
   ix. Adquisición, Desarrollo y Mantenimiento de Sistemas
   x. Relación con Proveedores
   xi. Gestión de Incidentes de Seguridad de la Información
   xii. Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio
   xiii. Cumplimiento

d. Elaborar el Plan de Acción y Mejora para optimizar aquellos controles y procesos de gestión de seguridad que se encuentren con un desvío claro respecto de los requerimientos del estándar ISO 27001:2013

2. Proveer sesiones para guía y coaching en implementación de un S.G.S.I. según el estándar ISO 27001. Se estiman 2 (dos) sesiones por semana, durante un conjunto de 14 (catorce) semanas. En esta etapa, se tiene previsto la ejecución de las siguientes tareas:

a. Brindar el apoyo y guía (coaching) para orientar al personal responsable del S.G.S.I. de A.R.B.A. a implementar las mejoras identificadas en la etapa anterior de Diagnóstico.

b. Proponer las mejoras a las metodologías y procesos de gestión de seguridad que permitan atender los requerimientos de Auditoría Interna y de futuras auditorías de certificación ISO 27001.

c. Definir y desarrollar conjuntamente con el personal responsable de Seguridad de la Información, de un Tablero de Control para supervisar y establecer los indicadores de gestión del S.G.S.I. implementado en A.R.B.A.

d. Atender a las consultas y clarificar dudas importantes respecto de los procesos del S.G.S.I. y que no hayan sido debidamente comprendidos o bien no cumplen con lo requerido en el estándar ISO 27001:2013.

3. Consultas técnicas remotas las cuales serán respondidas durante las sesiones, o bien mediante emails con el detalle de lo requerido.

    a. Atender a las consultas y clarificar dudas menores respecto de procesos del S.G.S.I. que no hayan sido debidamente comprendidos o bien no cumplen con lo requerido en el estándar ISO 27001:2013.

Fase 2: Programa de Concientización en Seguridad

Esta fase comprende la necesidad de contar con el asesoramiento en la construcción de un Programa de Concientización en Seguridad y sus contenidos principales, para luego ser implementado por el personal responsable de seguridad de la información de A.R.B.A.
Con el fin de optimizar los tiempos y duración del Programa de Concientización, se requiere implementar un Plan que incluya los siguientes componentes:

- Construcción de 1 (una) Presentación digital en formato HTML5 (para ser utilizado en la Intranet de A.R.B.A.), y donde se tratarán los temas y tópicos de seguridad más importantes por parte de A.R.B.A.

- Elaboración de un Cuestionario de Evaluación de Conocimientos (Quiz) al final del Programa de Concientización para evaluar los conocimientos adquiridos.

Este Programa de Concientización deberá incluir, al menos, los siguientes tópicos:

I. Introducción a la Seguridad de la Información

- ✓ Saber qué es la seguridad de la información y por qué es importante
- ✓ Conocer la definición de la terminología y conceptos básicos de la seguridad de la información
- ✓ Reconocer la responsabilidad del usuario en la protección de los activos informáticos de A.R.B.A.
- ✓ Aplicar las mejores prácticas que promueven la seguridad de la información

II. Gestión y Buen Uso de las Contraseñas

- ✓ Reconocer la importancia de una contraseña bien protegida
- ✓ Poder diferenciar entre contraseñas sólidas y débiles
- ✓ Ser capaces de crear una contraseña sólida y fácil de recordar
- ✓ Aplicar las mejores prácticas en selección y protección de contraseñas
- ✓ Buen Uso de contraseñas / No Compartir contraseñas
- ✓ Protección de pantalla / Logout
- ✓ Control de Acceso Lógico a sistemas informáticos

III. Buen uso del Correo Electrónico

- ✓ Conocer y tomar conciencia de las amenazas y los daños a A.R.B.A. y otros organismos debido al uso incorrecto del correo electrónico
- ✓ Reconocer las amenazas presentadas por el spam y los correos falsos (“hoaxes”) y saber qué medidas tomar
- ✓ Poder comunicarse por correo electrónico de manera segura
- ✓ Uso correcto del e-mail y consideraciones sobre el envío de archivos adjuntos. Acciones prohibidas de e-mail

IV. Uso del recurso Internet en el trabajo

- ✓ Reconocer la necesidad de familiarizarse con la Política de Uso Aceptable de Internet en el ambiente de trabajo de A.R.B.A.
- ✓ Tomar conciencia de los daños que puede sufrir A.R.B.A. como consecuencia del uso inapropiado de Internet

- ✓ Aplicar las mejores prácticas para atenuar los riesgos relacionados con la conectividad a Internet
- ✓ Sitios prohibidos de Internet
- ✓ Acciones prohibidas de Internet
- ✓ Uso correcto y seguro de la mensajería instantánea
- ✓ Redes inalámbricas
- ✓ Seguridad e Información en la Nube

V. Ataques y Códigos Maliciosos

- ✓ Conocer y tomar conciencia de las distintas formas de códigos maliciosos
- ✓ Reconocer los factores humanos y técnicos para la prevención de la diseminación de códigos maliciosos
- ✓ Mejores prácticas para atenuar los riesgos de ataques por códigos maliciosos
- ✓ Malware – Virus – Gusanos - Troyanos
- ✓ Piratería de software: un riesgo del negocio
- ✓ Ciber-estafa: Ataques del tipo Phishing

VI. Confidencialidad de Información

- ✓ Copias de respaldo e impresión de información confidencial

VII. Modelo BYOD (Bring Your Own Device)

- ✓ Reconocer la importancia de familiarizarse con la política de uso aceptable sobre dispositivos personales en A.R.B.A.
- ✓ Conocer y tomar conciencia del valor y las vulnerabilidades de los datos que se encuentran en los dispositivos móviles.
- ✓ Uso de tablets y Smartphones en A.R.B.A.
- ✓ Almacenamiento de Información sensible en dispositivos móviles personales.

VIII. Seguridad Física de la Información

- ✓ Reconocer los aspectos valiosos y vulnerables que pueden poner en peligro la seguridad física de la información
- ✓ Aplicar las mejores prácticas para atenuar las violaciones a la seguridad física
- ✓ Escolta de visitantes y tarjetas de seguridad
- ✓ Políticas de escritorios limpios
- ✓ Precauciones con computadores portátiles: Viajes
- ✓ Control de Acceso de Usuarios Remotos

IX. Ingeniería Social

- ✓ Conocer y tomar conciencia de los peligros de la ingeniería social: qué es y cómo funciona
- ✓ Reconocer los métodos y herramientas más comunes de la ingeniería social y aplicar medidas adecuadas para contrarrestarlos
- ✓ Tener una idea sobre cómo piensan los ingenieros sociales
- ✓ Aplicar las mejores prácticas que promueven la protección, seguridad y confidencialidad de la información
- ✓ Redes Sociales – Facebook, Twitter, Instagram, Linkedin.

Fase 3: Auditoría de S.G.S.I.

Durante esta fase, se requiere ejecutar las actividades de Auditoría Interna sobre el S.G.S.I. implementado, para evaluar el correcto cumplimiento de los requisitos y cláusulas de la norma ISO 27001, como así también validar la aplicación de los controles de seguridad implementados en A.R.B.A., incluyendo la revisión de la documentación y aplicación de las Políticas, Normas, Procedimientos y Controles de Seguridad de la Información de A.R.B.A. Como resultado de esta fase, se debe generar el Informe de Auditoría Interna S.G.S.I. para cumplir con la cláusula 9.2 de la norma ISO 27001.

En esta fase se incluirá un auditor de A.R.B.A. para que acompañe en el desarrollo de la misma.

Los requerimientos para esta fase deben incluir, al menos, los siguientes puntos:

a. Planificación y Armado de Cronograma de Auditoría Interna S.G.S.I.: Presentación del Plan de Auditoría Interna.
b. Etapa 1 de Auditoría Interna: Evaluación y Auditoría de Documentación del S.G.S.I. y el cumplimiento de los siguientes requisitos:
    - Alcance del S.G.S.I.
    - Modelo de Gestión de Riesgos (Evaluación y Tratamiento de Riesgos)
    - Compromiso de la Dirección
    - Determinación de las Competencias Profesionales del equipo de recursos comprendidos en el S.G.S.I.

- Información documentada del S.G.S.I.: Control de Documentos y Registros, Manual S.G.S.I., Políticas y Procedimientos de seguridad, etc.)
- Planificación y Modelo de Revisión por la Dirección
- Planificación y Modelo de Auditorías Internas
- Proceso de Acciones Correctivas y Preventivas

c. Etapa 2 de Auditoría Interna: Evaluación y Auditoría de Implementación de los controles de seguridad alcanzados por el S.G.S.I., a ejecutarse en oficinas de A.R.B.A. y atendiendo a los siguientes elementos:
   - Revisión del nivel de madurez y aplicación de los controles de seguridad
   - Revisión por muestreo de registros y evidencias del S.G.S.I.
   - Nivel de aplicabilidad y conocimiento de los funcionarios sobre los procesos alcanzados por el S.G.S.I.
   - Resultados de las Evaluaciones de Riesgos de Seguridad
   - Seguimiento a No Conformidades anteriores y validación del cierre de las mismas
   - Cumplimiento del Proceso de Revisión por la Dirección
   - Y todo otro elemento que sea considerado clave para evaluar al S.G.S.I. implementado.

d. Elaboración de Informe de Resultados de Auditoría Interna: Desarrollo del Informe de Auditoría Interna, poniendo en conocimiento acerca de las observaciones, no conformidades y oportunidades de mejora que surjan de la auditoría. En esta etapa se requiere:
   - Elaboración y Presentación del Informe de Auditoría Interna siguiendo el modelo de documentación definido para el S.G.S.I. de A.R.B.A.
   - Presentación Ejecutiva de los Hallazgos obtenidos durante la auditoría interna.

5.- Requisitos Especiales del Oferente:

Los consultores designados deberán contar con certificaciones vigentes, experiencia comprobable en auditorías e implementaciones de modelos de gestión de riesgos y sistemas de gestión de seguridad de la información (S.G.S.I.), contando en conjunto con al menos las siguientes certificaciones:

- Implementador y Auditor Líder ISO 27001
- Implementador y Auditor Líder ISO 22301

El Oferente deberá presentar la documentación que avale los requisitos requeridos, junto con la documentación del proyecto que pretenda llevar a cabo, incluyendo el detalle de tareas y tiempos, el programa del plan de concientización con el temario ajustado a las buenas prácticas de la industria y el C.V. de los consultores que participarán en las distintas tareas del proyecto.

La ejecución de las tareas solicitadas podrá ser secuencial, a los efectos de no exigir una cantidad elevada de personal del contratante para el seguimiento y ejecución de los trabajos.

6.- Plazo de Cumplimiento y Cronograma estimado:

ENTREGA PARCIAL:

Plan de Acción y Mejora para optimizar aquellos controles y procesos de gestión de seguridad que se encuentren con un desvío claro respecto de los requerimientos del estándar ISO 27001:2013.	Semana 8
Tablero de Control para supervisar y establecer los indicadores de gestión del S.G.S.I. implementado en **A.R.B.A.**	Semana 14
Construcción de 1 (una) Presentación digital en formato HTML5 (para ser utilizado en la Intranet de **A.R.B.A.**), y donde se tratarán los temas y tópicos de seguridad más importantes por parte de **A.R.B.A.**	Semana 16
Cuestionario de Evaluación de Conocimientos (Quiz) al final del Programa de Concientización para evaluar los conocimientos adquiridos.	Semana 16
Auditoría Interna S.G.S.I.	Semana 20