

A TRAVÉS DE:

UNIDAD DE ADQUISICIONES Y CONTRATACIONES
INSTITUCIONAL -UACI-

PROMUEVE:

TÉRMINOS DE REFERENCIA
PARA PROCESO DE LIBRE GESTIÓN

**“CONTRATACIÓN DE SERVICIOS DE CONSULTORÍA PARA
REALIZAR UN ANÁLISIS DE SEGURIDAD Y FIABILIDAD DEL
SISTEMA E INFRAESTRUCTURA DEL CORREO ELECTRÓNICO DEL
IAIP”**

Señor oferente:

**Favor leer detenidamente las condiciones que deberá cumplir
su oferta.**

SAN SALVADOR, ENERO DE 2021

Contenido

Antecedentes	3
Justificación	3
Objetivos	4
General	4
Específicos	4
Descripción del servicio esperado	4
Actividades a realizar	5
Productos esperados	5
Recursos y facilidades a ser provistos por el IAIP	6
Forma y lugar de pago	7
Plazo de consultoría	7
Coordinación y administración del contrato	7
Perfil de la persona consultora y criterios de evaluación	7

Antecedentes

El Instituto de Acceso a la Información Pública (IAIP) se encarga de velar por la correcta aplicación de la Ley de Acceso a la Información Pública (LAIP). Entre sus funciones se destacan conocer y resolver los recursos de apelación; conocer y resolver del procedimiento sancionatorio y dictar sanciones administrativas; proporcionar apoyo técnico a los entes obligados en la elaboración y ejecución de sus programas de promoción de la transparencia y del derecho de acceso a la información.

Una de las herramientas más básicas y utilizadas para cumplir con su función es la tecnología de la comunicación, con la cual se busca generar procedimientos expeditos para todos los servicios institucionales, así como brindar respuestas ágiles sin que medie una presencia física en las instalaciones de las partes interesadas.

Así, el correo electrónico forma base fundamental de las actividades diarias que realiza el IAIP, por lo que se vuelve un canal primordial y que debe funcionar de la mejor manera posible, advirtiéndolo, de manera oportuna, cuando no funcione correctamente.

Además, por la pandemia por COVID-19, el correo electrónico se volvió una herramienta importante para la realización de las actividades institucional; y convirtió en canal casi exclusivo de comunicación con entes obligados y público general. Por esta razón, es importante hacer una revisión detallada del buen funcionamiento de esta herramienta para garantizar una comunicación fluida con todas las partes.

Justificación

En sesiones de Pleno, se han manifestado dificultades con respecto al sistema e infraestructura del IAIP, con énfasis al correo electrónico institucional, señalando que los mensajes no llegan al IAIP o a los entes obligados (y viceversa). Por ejemplo, no se pudo recibir documentación enviada por Casa Presidencial, relativa al nombramiento de Comisionados nombrados por la Presidencia de la República; o del proceso que se inició en contra de una Comisionada Suplente. La situación toma mayor envergadura y gravedad por la fiabilidad que se le otorga al correo electrónico frente a alegaciones realizadas con los entes, en las cuales se ha tratado de evidenciar que no se recibió una determinada comunicación, como parte de los procesos administrativos que se siguen desde el Instituto. Existe una alta preocupación sobre la emisión de resoluciones basándose en la poca certeza que produce el sistema; por lo que se considera necesario realizar una indagación detallada que identifique si existe una situación concreta y anómala sobre el sistema e infraestructura manejo del IAIP, con énfasis al correo institucional y su fiabilidad, y la urgencia de detectar qué ha ocurrido.

Objetivos

General

Realizar un análisis de seguridad y fiabilidad del sistema e infraestructura del IAIP, entre ellos el sistema de correo electrónico del Instituto de Acceso a la Información Pública (IAIP).

Específicos

- a. Identificar las fortalezas, vulnerabilidades o debilidades del sistema e infraestructura del IAIP, entre ellos el correo electrónico del IAIP.
- b. Enlistar los hallazgos encontrados en el proceso de análisis al sistema e infraestructura del IAIP, con especial énfasis en el correo electrónico del IAIP, con el objeto de fortalecer la calidad del servicio prestado.
- c. Definir las mejores prácticas y recomendaciones a implementar por la máxima autoridad, para garantizar la seguridad y fiabilidad de la infraestructura tecnológica del Instituto.
- d. Detallar una propuesta de mejora para que el IAIP brinde un servicio de calidad y fiabilidad a los entes obligados a través de su correo electrónico.
- e. Proponer un plan de acción/respuesta de su plataforma tecnológica ante una situación de vulnerabilidad, con especial énfasis al correo electrónico, con el fin de realizar mejoras en los procesos internos.

Descripción del servicio esperado

La consultoría deberá identificar las fortalezas, vulnerabilidades y/o debilidades que pueden ser percibidas y explotadas por personas ajenas que no cuentan con autorización para el manejo de la infraestructura institucional, hackers, personal interno, antiguos empleados, etc. Esto, para tener comprensión amplia y detallada de la infraestructura y sistema de seguridad del IAIP, de tal forma que garantice la confidencialidad, integridad y la disponibilidad de la información en los tiempos estipulados por la Ley de Acceso a la Información Pública.

Con base en los resultados y hallazgos encontrados, se deberán definir las mejores prácticas y recomendaciones a implementar por la máxima autoridad, para garantizar la seguridad y fiabilidad de la infraestructura tecnológica del Instituto; así como detallar los procesos que mejorarán la calidad y fiabilidad del servicio brindado tanto a entes obligados como al público general.

Y, finalmente, se deberá describir un plan de acción o respuesta ante cualquier vulnerabilidad que se presente con el correo electrónico del Instituto.

Actividades a realizar

1. Identificación de fortalezas, vulnerabilidades o debilidades del sistema e infraestructura del IAIP, con énfasis al correo electrónico y los procedimientos de gestión de la plataforma del IAIP.
2. Identificación de posibles mecanismos de ataque que pudiera perjudicar los sistemas e infraestructura del IAIP, con afectación al correo electrónico.
3. Identificación el nivel de preparación del Instituto para la detección, contención y respuesta ante ataques cibernéticos de fuentes externas e internas, en donde se visualice si se cuenta con un plan de acción o respuesta ante dichas acciones.
4. Realización de un análisis que permita ubicar la situación actual del Instituto en relación a las mejores prácticas de ciberseguridad.
5. Identificación de las oportunidades de mejora y recomendar medidas a implementar para cerrar las brechas encontradas
6. Identificación de la necesidad de implementar una herramienta de monitoreo de envíos de correo electrónico, en el que se permita identificar el recurso al que se envió el correo electrónico, el estado del envío, si fue abierto o no y en caso de que hubiese un error, el detalle del mismo, para tomar acciones técnicas y/o legales que ayuden a mitigar este problema.
7. Evaluar la capacidad instalada con que cuenta el IAIP, a nivel tecnológico y humano.

El consultor deberá suministrar un plan de trabajo para evaluar su comprensión de los TDR y la forma en que propone realizar y alcanzar los objetivos del servicio.

Productos esperados

1. El plan de trabajo del consultor, el cual debe de incluir:
 - Descripción y entendimiento del servicio
 - Objetivos y Alcance del trabajo
 - Enfoque y Metodología propuesta
 - Actividades a desarrollar
 - Productos entregables
 - Cronograma del trabajo

2. Un informe que contenga un resumen ejecutivo, escrito en lenguaje común, del análisis realizado donde se detallen, como mínimo, todas las actividades especificadas en estos TDR. El informe también contendrá un componente técnico que especifique actividades realizadas y los resultados de las verificaciones.
3. Una presentación al Pleno del IAIP, en donde se detallen los resultados del análisis y se incluyan los elementos relacionados con las actividades descritas en estos TDR.
4. Un plan de acción para ejecutar las mejoras y recomendaciones a implementar por la máxima autoridad, para garantizar la seguridad y fiabilidad de la infraestructura tecnológica del Instituto.
5. Recomendar la mejor herramienta y/o metodología informática a utilizar (en función del trabajo institucional) que de soporte al IAIP, para el monitoreo de envío de correos electrónicos, el cual permita identificar el recurso al que se envió, el estado del envío, si fue abierto o no y en caso de que hubiese un error, el detalle del mismo, para tomar acciones técnicas que ayuden a mitigar el problema.
6. Detallar dentro del informe ejecutivo, el estado actual de la capacidad de la Unidad de Tecnología, contra las capacidades y el nivel de desempeño con el que debe de contar, con el fin de modernizar la infraestructura y las capacidades técnicas del personal; asimismo, contar con información que respalde la inversión en tecnología y el talento humano.

Recursos y facilidades a ser provistos por el IAIP

1. El IAIP suministrará al consultor la información necesaria de acuerdo al objeto de la consultoría, información sobre la infraestructura, servicios, operación de tecnología, accesos a sistemas, bitácoras de los sistemas, etc., de forma que el alcance de estos TDR se pueda cumplir de forma completa
2. El consultor realizará todas las actividades necesarias para desarrollar el alcance del servicio, incluyendo la recopilación y revisión de la información requerida, determinación y justificación de criterios, procedimientos y metodologías utilizadas, la realización de cálculos y elaboración de informes con los resultados y recomendaciones para el IAIP. Así como entrevistas con el personal involucrado en los procesos contemplados en estos TDR (UTI, GGPD, PLENO, etc.).
3. Para la consultoría, el IAIP gestionará todos los accesos y autorizaciones para las pruebas o auditorías específicas que se realizarán. El IAIP Gestionará la disponibilidad del personal interno que se requiera debe colaborar con el proceso

Forma y lugar de pago

La forma de pago es por cuenta única del Ministerio de Hacienda, a través de la Dirección General de Tesorería, realizará el pago directamente a la cuenta que el proveedor indique en declaración jurada del formato proporcionado en este documento. (Anexo)

El pago por el servicio se realizará contra entrega y aprobación de productos por parte del Pleno del IAIP.

Se establece la siguiente forma de pago:

Dos pagos: 30 % contra entrega y aprobación del plan de trabajo; 70 % contra entrega y aprobación de todos los productos detallados en los TDR.

Plazo de consultoría

El Plazo para la realización de la consultoría es de 45 días calendario, a partir de la fecha de orden de inicio del contrato

Los plazos para el desarrollo del servicio podrán prorrogarse por parte del IAIP, acreditando razones que lo motivan y en caso de ser el contratista, se deberá solicitar previo al vencimiento del plazo, indicando claramente las razones de la solicitud

Fecha prevista de inicio enero 2021. Después de suscribir el contrato el IAIP notificará la orden de inicio

Coordinación y administración del contrato

El oferente contratado deberá coordinar la ejecución del trabajo con la persona delegada por el Pleno del IAIP, quien será la administradora del contrato.

Perfil de la persona consultora y criterios de evaluación

Los servicios serán brindados por un consultor especialista en Seguridad Informática, Sistemas y Redes Informáticas, que pueda verificar sus calificaciones mediante los números de credencial de Certificaciones Especializadas en la rama de Seguridad Informática que incluyan:

- Certificación ISO 27001 – Seguridad de la Información
- Certificación ISO 31000 – Gestión del Riesgo
- Certified Ethical Hacker (CEH) – Hacker Ético Certificado
- Certified Vulnerability Assessor (CVA) – Asesor de Vulnerabilidades Certificado

- Certified Penetration Tester Engineer (CPTE) – Ingeniero en Pruebas de Penetración Certificado
- Certificación COBIT
- Microsoft Certified Professional