



Gobierno de Reconciliación  
y Unidad Nacional

*El Pueblo, Presidente!*

Aquí nos ilumina,  
un Sol que no declina  
El Sol que alumbra  
las nuevas victorias  
RUBÉN DARÍO

4★  
2019

MINISTERIO DE HACIENDA Y CREDITO PÚBLICO  
PROYECTO DE MODERNIZACIÓN DEL SISTEMA ADMINISTRATIVO FINANCIERO  
(MHCP-PMSAF)

Convenio No. 5579-NI

**INVITACION A PRESENTAR EXPRESIONES DE INTERES**

**“Auditoría de Seguridad de la Infraestructura Tecnológica del SIGAF”.**

1. El Gobierno de la Republica de Nicaragua, a través del Ministerio de Hacienda y Crédito Público (MHCP), ha recibido un crédito de la Asociación Internacional de Fomento para sufragar el costo del Proyecto de Modernización del Sistema Administrativo Financiero (PMSAF) y se propone utilizar parte de los fondos de este crédito para pagos de contratos de servicios de consultoría para contratar una firma consultora que desarrolle la “Auditoría de Seguridad de la Infraestructura Tecnológica del SIGAF”.
2. El propósito del servicio es: **Evaluar el estado de la seguridad de la información en los centros de datos principal y contingente del MHCP**, junto con la implementación de las mejoras para cumplir con los criterios establecidos en los estándares internacionales ISO/IEC 27001:2005 o más reciente, así como la implementación de un plan de continuidad tecnológico.
3. El Ministerio de Hacienda y Crédito Público (MHCP), invita a **Firmas Consultoras individuales o asociadas** a presentar expresiones de interés para elaborar lista corta, siendo los criterios de evaluación los siguientes:
  - a. Firmas Consultoras individuales o asociadas deben acreditar al menos cinco (5) años de experiencia nacional y/o internacional en temas de seguridad.
  - b. Firmas Consultoras individuales o asociadas deben mostrar evidencia documental de al menos cuatro (4) consultorías exitosas en temas similares o relacionados con el punto 2 de este documento, realizadas a nivel nacional y/o internacional.
4. Las firmas consultoras interesadas deben **presentar en esta etapa:**

**a) Firmas Individuales**

- I. Presentar la expresión de interés firmada por el representante legal.
- II. Documentación legal de la Firma interesada que demuestre haber sido constituida e inscrita en el registro mercantil competente de su país de origen, y documento que acredite las facultades del representante que firme la expresión de interés.
- III. Documentos que demuestren la capacidad financiera de la Firma interesada: Estados Financieros auditados del último período fiscal o Declaración de impuestos del último período fiscal de su país de origen.



**CRISTIANA, SOCIALISTA, SOLIDARIA!**

MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

COORDINACIÓN DE ADQUISICIONES PROYECTO DE MODERNIZACIÓN  
DEL SISTEMA DE ADMINISTRACIÓN FINANCIERA (PMSAF)

Dirección: Palacio de la Cultura 1C al Este, Edificio DGTEC

Telf.: (505) 2222-6326





Gobierno de Reconciliación  
y Unidad Nacional

*El Pueblo, Presidente!*

Aquí nos ilumina,  
un Sol que no declina  
El Sol que alumbra  
las nuevas victorias  
RUBÉN DARÍO

40  
2019

b) Firmas Asociadas

- I. Presentar la expresión de interés firmada por un representante legal debidamente autorizado de cada una de las Firmas interesadas.
  - II. Indicar la figura jurídica con la que llevarán a cabo la asociación, así como la denominación de la misma.
  - III. Presentar la documentación legal de cada una de las Firmas interesadas (Documentación de Constitución legal debidamente inscrita en el registro competente de su país de origen, y documento que acredite las facultades del representante que firma la expresión de interés).
  - IV. Documentos que demuestren la capacidad financiera de las Firmas interesadas: Estados Financieros auditados del último período fiscal o Declaración de impuestos del último período fiscal de su país de origen de cada una de las Firmas interesadas.
5. Las Firmas consultoras serán seleccionadas de acuerdo al método de Selección Basada en Calidad y Costo (SBCC) conforme a los procedimientos indicados en las normas para la selección y Contratación de consultores con Préstamos del BIRF y Créditos de la AIF, edición enero de 2011 (revisadas en el mes de Julio del 2014).

Las expresiones de interés deben enviarse por escrito o correo a la dirección que figura a continuación:

Del Palacio de la Cultura una cuadra al este, Edificio DGTEC – MHCP, Managua, Nicaragua

E-mail: [adquisicionesPMSAF@mhcp.gob.ni](mailto:adquisicionesPMSAF@mhcp.gob.ni). [Felix.osorio@mhcp.gob.ni](mailto:Felix.osorio@mhcp.gob.ni)

Fecha de recepción de expresiones de interés: 20 de marzo del año dos mil diecinueve

Hora: 10:00 a.m.

Oficina de Adquisiciones del PMSAF-MHCP.

Atención Felix Osorio Gutierrez; Coordinador de Adquisiciones (a.i) PMSAF-MHCP

Teléfono: (505) 2222-6326

Se anexa términos de referencia para conocimiento general, de igual manera puede visitar el portal de la Web [www.nicaraguacompra.gob.ni](http://www.nicaraguacompra.gob.ni), en la sección de expresiones de interés.

CON FE Y  
ESPERANZA!



**CRISTIANA, SOCIALISTA, SOLIDARIA!**

**MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO**

COORDINACIÓN DE ADQUISICIONES PROYECTO DE MODERNIZACIÓN  
DEL SISTEMA DE ADMINISTRACIÓN FINANCIERA (PMSAF)

Dirección: Palacio de la Cultura 1C al Este, Edificio DGTEC

Telf.: (505) 2222-6326

MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO  
PROYECTO DE MODERNIZACIÓN DEL SISTEMA DE ADMINISTRACIÓN FINANCIERA  
DEL SECTOR PÚBLICO  
(PMSAF)

Términos de Referencia  
Auditoría de Seguridad de la infraestructura  
tecnológica del SIGAF  
Contrato de Préstamo 5579-NI

Marzo 2019

# Índice

I.	Antecedentes .....	1
II.	Objetivos de la Consultoría.....	1
	a.    Objetivo General .....	1
	b.    Objetivos Específicos.....	1
III.	Requerimientos y alcance del Servicio.....	2
IV.	Actividades Mínimas.....	2
V.	Productos esperados y/o entregables .....	3
VI.	Plazo .....	4
VII.	Perfil de la firma y personal clave con el que deberá contar.....	4
	a.    Perfil de la firma .....	4
	b.    Personal Clave: El equipo de trabajo de la firma consultora deberá, al menos, estar constituido por los siguientes consultores. ....	5
VIII.	Coordinación y Supervisión .....	6
IX.	Otros .....	6

## I. Antecedentes

El PMSAF-MHCP tiene un componente de modernización de la infraestructura tecnológica que permita a las instituciones del sector público acceder de forma centralizada, óptima y segura al SIGAF (Sistema Integrado de Gestión Administrativa y Financiera). Los servicios que se prestan en esta infraestructura tecnológica (TI) son vulnerables de ataques informáticos y su ubicación geográfica tiene un alto riesgo de que ocurra un desastre natural por ser una zona altamente sísmica y volcánica. Esto nos obliga a contar con un sistema de seguridad de la información (SGSI) y un plan de continuidad tecnológico, que garantice el acceso a los datos en caso de cualquier desastre natural u otras amenazas cibernéticas.

Para lograr el objetivo, se requiere contratar una firma consultora que realice una Auditoría de Seguridad de la infraestructura tecnológica del SIGAF alineada a los estándares internacionales ISO/IEC 27001:2005 o más reciente, para evaluar el cumplimiento de los objetivos de control A.10.6 y A.14.1 de la norma antes citada y realizar cambios en la implementación de los controles, que contribuyan a mejorar la seguridad de la información del SIGAF (Sistema Integrado de Gestión Administrativa y Financiera) y otros Sistemas Críticos alojados tanto en el Centro de Datos Principal (CDP) y el Centro de Datos Contingente (CDC) del MHCP.

## II. Objetivos de la Consultoría

### a. Objetivo General

Evaluar el estado de la seguridad de la información en los centros de datos principal y contingente del MHCP, junto con la implementación de un plan de continuidad tecnológico; mediante los criterios establecidos en los estándares internacionales ISO/IEC 27001:2005 o más reciente.

### b. Objetivos Específicos

- Elaborar un diagnóstico del estado actual de la seguridad de la información con relación a los objetivos de control **A.10.6** y **A.14.1** de la ISO/IEC 27001:2005 o más reciente, en ambos centros de datos (CDP y CDC) del MHCP.
- Implementar un plan de mejora basado en los hallazgos del objetivo de control **A.10.6** en ambos centros de datos (CDP y CDC).
- Implementar un plan de continuidad tecnológico basado en los hallazgos del objetivo de control **A.14.1** en ambos centros de datos (CDP y CDC).
- Capacitar al personal de infraestructura de TI de la Dirección General de Tecnología del MHCP basado en el control **A.8.2.2 Concienciación, formación y capacitación para la seguridad de la información** que fortalezca los procesos de gestión de la seguridad de la información.

### III. Requerimientos y alcance del Servicio

- Realizar Auditoría de Seguridad de la infraestructura tecnológica del SIGAF para identificar e implementar mejoras en la seguridad de la red del centro de datos principal y contingente basados en los objetivos de control A10.6 y A14.1.
- Realizar evaluación y recomendaciones de mejoras de acuerdo a los controles 10.5 y 11.4 en ambos centros de datos.
- Elaboración de un plan de continuidad tecnológico (o DRP en inglés) incluyendo los servicios identificados como críticos que se encuentran alojados en ambos centros de datos (CDP y CDC) del MHCP.
- Capacitación de 30 servidores públicos de la DGTEC de acuerdo al control 8.2.2 y a 10 servidores públicos en “Implementador ISO 27001:2013”.
- El taller de sensibilización y la capacitación será realizado fuera de las instalaciones de la institución y la firma consultora debe encargarse de toda la logística, refrigerios y equipos requeridos.
- Se requiere que el personal que participe en esta consultoría, lo haga de forma presencial, en las instalaciones de la DGTEC-MHCP laborando en horas de oficina, de lunes a viernes de 8:00am a 5:00pm. En casos especiales, se pondrán acordar horarios y días fuera de la jornada laboral, en común acuerdo entre PMSAF -MHCP y la firma consultora.
- Toda la documentación relacionada a esta consultoría debe ser entregada en formato editable (ejemplo: Word, Excel, etc.) y PDF.

### IV. Actividades Mínimas

**Fase 1** - Realizar un diagnóstico de la situación actual en los centros de datos principal (CDP) y contingente (CDC) del MHCP, en base a los objetivos de control A.10.6 y A.14.1 considerando al menos las siguientes actividades:

- Taller de sensibilización a todo el personal Infraestructura Tecnológica relacionado con la importancia en la gestión en la seguridad de la información.
- Ejecución de pruebas de penetración interna a diez (10) direcciones IP y pruebas de penetración externa a cinco (5) direcciones IP.<sup>1</sup>
- Presentación de informe de resultado pruebas de penetración con la remediación correspondiente.
- Aplicación de las mejores prácticas de TI para la evaluación de los controles A.10.6, A.14.1, A.10.5 y A.11.4 definidos.
- Presentar Informe de brechas encontradas en los controles.

---

<sup>1</sup> Los sitios en los cuales se realizará la penetración interna y externa se darán a conocer al proveedor adjudicado con la consultoría.

- Capacitación al personal basado en el control 8.2.2 a dos grupos de técnicos (15 por grupo) con un mínimo de 24 horas cada curso.
- Capacitación al personal de seguridad en “Implementador ISO 27001:2013 con Certificación” a un grupo de diez técnicos con un mínimo de 32 horas cada curso.

**Fase 2** - Elaborar un plan de mejoras a los objetivos de control A.10.5, A.10.6, A.11.4, A.14.1 que incluyan: procedimientos, formatos y bitácoras que sean necesarias; así como sugerir nuevos controles para fortalecer la gestión de la seguridad en las redes, considerando al menos las siguientes actividades:

- Definición del plan de implementación de mejoras, que incluya las recomendaciones de los controles indicados.
- Documentar los objetivos de control requeridos A.10.5 y A.11.4.
- Implementar el plan de mejoras de los objetivos de control A.10.6 y A.14.1.
- Implementar mejoras identificadas en las pruebas de penetración.
- Entregar documento de mejoras implementadas.

**Fase 3** - Elaborar el plan y los procesos de continuidad tecnológica en ambos centros de datos, que al menos incluya las siguientes actividades: (A.14.1)

- Análisis de Impacto de las infraestructuras consideradas críticas del MHCP.
- Evaluación de riesgos de TI.
- Estrategias de recuperación de desastres.
- Planes de pruebas de continuidad tecnológica.
- Desarrollo y presentación de Plan y procesos de Continuidad tecnológica.
- Pruebas Operativas del plan de continuidad tecnológica.

**Fase 4** – Cierre del proyecto incluyendo al menos las siguientes actividades:

- Auditar el cumplimiento de la implementación de los objetivos de control seleccionados: A.10.6 y A.14.1 de los estándares internacionales ISO/IEC 27001:2005 o más reciente.
- Entregar Informe final incluyendo los resultados de las cuatro fases.
- Presentar los resultados y próximos pasos a seguir.

**Consideraciones sobre la organización de los equipos en las diferentes fases:**

- Los equipos de trabajo designados a la fase 2 y 3 deberán trabajar juntos durante el desarrollo de la fase 1.
- Las fases 2 y 3 se deberán desarrollar en paralelo como dos subproductos independientes.
- La fase 4 debe ser llevada a cabo por un equipo diferente al que implementó las fases anteriores.

## V. Productos esperados y/o entregables

Deberá entregar al final de cada fase de la consultoría, al menos los siguientes documentos:

**Fase1:**

- Plan de Actividades (cronograma) de la consultoría con los responsables.
- Informe de resultados del Taller de Sensibilización.

- Informe técnico de Pen Test con detalle de tareas, pruebas y herramientas utilizados, así como los riesgos de seguridad identificados y clasificados.
- Documento con requerimientos de seguridad de redes y áreas involucradas en seguridad de Información.
- Informe de diagnóstico y evaluación del cumplimiento de los objetivos de control: A.10.6 y A.14.1 del estándar internacional ISO/IEC27001:2005 o más reciente.
- Certificado de aprobado de las capacitaciones en seguridad de la Información (control 8.2.2).

**Fase 2:**

- Documento detallado de las recomendaciones implementadas y las estrategias a seguir, ajustados al cumplimiento de los objetivos de control: A.10.6 y A.14.1.
- Documentación de la evaluación de los objetivos de control: A.10.5 y A.11.4.

**Fase 3:**

- Documento del Plan de Continuidad Tecnológico basado en el objetivo de control A14.1.

**Fase 4:**

- Informe ejecutivo del cumplimiento de los objetivos de control: A.10.6 y A.14.1 del estándar internacional ISO/IEC27001:2005 o más reciente.
- Informe final de Auditoría.

## VI. Plazo

La duración estimada de la consultoría es de cuatro meses.

## VII. Perfil de la firma y personal clave con el que deberá contar

### a. Perfil de la firma

- **Experiencia General:** Empresa y/o Firma Consultora en Seguridad Informática, con cinco años de experiencia nacional y/o internacional como mínimo.
- **Experiencia Específica:** Presentar Referencias de haber realizado al menos cuatro (4) consultorías exitosas similares a la solicitada en este documento, tanto a nivel nacional como internacional.

- b. **Personal Clave:** El equipo de trabajo de la firma consultora deberá, al menos, estar constituido por los siguientes consultores.

#### Consultor Líder

- Certificaciones
  - Profesional especialista en Tecnologías de la Información y Comunicaciones o carrera a fin.
  - Formación y certificación vigente en ISO27001 y ISO22301 (o equivalente) como mínimo.
  - Deseable certificación en ITIL, Cobit 5, CISM, CISSP, ISO 27005, CISA, PMP, entre otros.
- Experiencia General
  - Al menos cinco años de experiencia en proyectos de Consultoría relacionados en algunas de las siguientes áreas: auditoría informática; implementación de infraestructura relacionada a seguridad informática; certificación de infraestructura relacionada a la seguridad de la información; y procesos de continuidad tecnológica.
- Experiencia Específica
  - Haber liderado al menos tres (3) proyectos exitosos de Auditoría, Consultoría y Seguridad en instituciones de gobierno o similares.
- Deberá de adjuntar CV y soportes que corroboren la experiencia requerida para esta consultoría con contactos de las empresas (Nombre, correo y Teléfono).

#### Consultor en Seguridad Informática

- Profesional especialista en Tecnologías de la Información y Comunicaciones o carrera a fin.
- Certificación en Ethical Hacker (CEH) o equivalente como mínimo.
- Experiencia general: Al menos tres años de experiencia en seguridad informática y herramientas de TI, entre las que se encuentran IPS, Firewall, UTM, WAF, Router y Sistemas Operativos.
- Experiencia Específica: Participación en al menos dos (2) proyectos exitosos similares a lo requerido en esta consultoría.
- Deberá de adjuntar CV y soportes que corroboren la experiencia requerida para esta consultoría con contactos de las empresas (Nombre, correo y Teléfono).

#### Consultor en Gestión en la Seguridad de la Información

- Profesional especialista en Tecnologías de la Información y Comunicaciones o carrera a fin.
- Certificación en Implementador del ISO27001:2005 o más reciente, como mínimo.

- Experiencia general: Al menos tres años de experiencia en al menos gestión, implementación, certificación o auditoría de seguridad de la información.
- Experiencia Especifica: Participación en al menos dos (2) proyectos exitosos similares a lo requerido en esta consultoría.
- Deberá de adjuntar CV y soportes que corroboren la experiencia requerida para esta consultoría con contactos de las empresas (Nombre, correo y Teléfono).

#### Consultor en Procesos de Continuidad Tecnológico

- Profesional especialista en Tecnologías de la Información y Comunicaciones o carrera a fin.
- Certificación en ISO22301 (o equivalente) como mínimo.
- Experiencia general: Al menos tres años de experiencia en seguridad informática y herramientas de TI, entre las que se encuentran IPS, Firewall, UTM, WAF, Router y Sistemas Operativos.
- Experiencia Especifica: Participación en al menos dos (2) proyectos de Continuidad Tecnológica exitosos similares a lo requerido en esta consultoría.
- Deberá de adjuntar CV y soportes que corroboren la experiencia requerida para esta consultoría con contactos de las empresas (Nombre, correo y Teléfono).

## VIII. Coordinación y Supervisión

La supervisión de las actividades y aprobación de los productos descritos en estos términos será responsabilidad del área de Infraestructura del PMSAF- MHCP.

## IX. Otros

- La empresa y/o firma consultora deberá firmar acuerdo de confidencialidad y de no divulgación (NDA).