TÉRMINOS DE REFERENCIA

"Consultoría para la implementación de la Normativa Nortic A7 e ISO 27001"

1. ANTECEDENTES

En el año 2014, con el apoyo del Programa de Administración Financiera Integrada, la Dirección General de Contrataciones Públicas dedicó esfuerzos a una primera fase de Implementación de un Marco estratégico a nivel de seguridad de sistemas que permitiera alinear los esfuerzos realizados en el área de tecnología de la información, con la estrategia de desarrollo del Sistema Nacional de Contrataciones Públicas (SNCP). Esta consultoría, fue ejecutada la cual, permitió a la Dirección General de Contrataciones Públicas iniciar de forma práctica los primeros esfuerzos para resguardar sus activos de información dentro un marco estratégico de ciberseguridad basados en ISO 27001, definir una propuesta de estructura organizacional para el área de Tecnología de la Información TI y obtener las primeras políticas, normas y procedimientos relacionados con la seguridad de TICs.

Actualmente, la Dirección General de Contrataciones Públicas, ha implementado en 307 instituciones en el Portal Transaccional que utilizan estas herramientas como única vía para gestionar sus procesos de compras, lo que implica que sea necesario asegurar mayores capacidades en seguridad de la información, por lo que se dirige importantes esfuerzos en la revisión de políticas, legislación y procedimientos con miras a garantizar el tratamiento seguro de la información. Asimismo, con dicha implementación se ha iniciado el proceso de desarrollo institucional, de fortalecimiento tecnológico y de automatización de sus procesos internos, para adecuar la institución de cara al cumplimiento de su papel como Órgano Rector del Sistema Nacional de Compras Públicas (SNCP).

Por los motivos antes expuestos, la Dirección General de Contrataciones Públicas necesita contratar una consultoría para implementar las Normas Nortic A7: 2016 y de la Norma ISO 27001:2013 para el cumplimiento de los estándares de seguridad de las tecnologías en la Institución y a su vez continuar con los esfuerzos de implementación de marco estratégico a nivel de seguridad de sistemas basado en ISO 27001.

2. BASE LEGAL

- La Constitución de la República, proclamada el 13 de junio de 2015.
- Ley No. 340-06 del Sistema Nacional de Compras y Contrataciones y normas relacionadas.
- Ley No. 107-13 sobre los derechos de las personas en sus relaciones con la Administración y de Procedimiento Administrativo de fecha 08 de agosto de 2013.
- Ley 53-07 contra crimines y delitos de Alta Tecnología.
- Ley No. 126-02 sobre el Comercio Electrónico, Documentos y Firma Digital.

- Ley 65-00 sobre Derecho de Autor.
- El Decreto No. 543-12 que aprueba el Reglamento de compras y contrataciones de bienes, servicios, obras y concesiones de fecha 06 de septiembre de 2012.
- Decreto No. 350-17 sobre la obligatoriedad del uso del Portal Transaccional.
- Decreto 1090-04 a través del cual se constituye a la OPTIC como dependencia directo del poder ejecutivo y se establecen las funciones del organismo.
- Decreto No. 229-07 el cual es el instructivo de aplicación de Gobierno Electrónico.
- Decreto No. 709-07 sobre las normas y estándares elaboradas por la Optic.
- Decreto No. 615-07, que instruye a la OPTIC a coordinar el procedimiento para la elaboración de los inventarios respecto a los programas incorporados a las computadoras y su licenciamiento.
- Resolución 51-2013, que aprueba los modelos de estructura organizativa permitidos para las unidades de TIC de todos los organismos del sector público.

3. DESCRIPCIÓN DE LA CONSULTORÍA

La consultoría busca implementar, desarrollar y certificar el sistema de administración de seguridad de la Información (SASI) y las políticas y procedimientos concernientes a la Normativa NORTIC A7 e ISO 27001 (ambas) en la Dirección General de Contrataciones Públicas.

4. OBJETIVO GENERAL

Implementar y desarrollar los acápites necesarios para lograr la certifacion de la normativa Nortic A7 e ISO 27001 y en consecuencia el Sistema de Administración de la Seguridad de la Información (SASI), en la Dirección General de Contrataciones Públicas, contemplada en dicho manual de implementación suministrado por la OPTIC y la ISO respectivamente, respondiendo a la estrategia de fomento de buenas prácticas del Estado."

5. OBJETIVOS ESPECÍFICOS

a) Elaborar un Plan de trabajo detallado y un plan de implementación de la Consultoría.

b) Evaluar el Plan Operativo de TIC, elaborar diagnóstico y análisis de brechas inicial de lo existente vs la NORTIC A7 e ISO 27001:2013.

c) Analizar las consultorías relacionadas a la seguridad de la Información que hayan sido previamente ejecutadas en la Dirección a saber, Servicio de Auditoria de calidad de Software, Informe BID Evaluación e-GP Portal de Compras y Contrataciones Públicas Republica Dominicana, entre otros documentos relacionados.

d) Elaborar junto al equipo que designe a estos fines la Dirección General de Contrataciones Públicas los diferentes documentos que conforman el Sistema de Administración de la Seguridad de la Información (SASI), según se detalla a continuación:

   i. Documento de definición y alcance del Sistema de Administración de la Seguridad de la Información (SASI)

ii. Colección de documentos legales y contractuales
iii. Manuales de procedimientos
iv. Manual de instrucciones, lista de tareas y formularios
v. Documento de declaración de aplicabilidad
vi. Cualquier otro requerido por la Nortic A7 e ISO 27001:2013

e) Evaluar las políticas existentes según lo requerido por la NORTIC A7 e ISO 27001:2013.

f) Evaluar los procedimientos existentes según lo requerido por las diferentes políticas, relacionados a la NORTIC A7 e ISO 27001:2013 atendiendo a la operatividad de la Dirección General de Contrataciones Públicas.

g) Realizar auditoria de Vulnerabilidades Tecnológicas y no Tecnológicas.

h) Implementar los procedimientos aprobados con los recursos disponibles y recomendar equipamiento y herramientas requeridos por las normas.

i) Elaborar el plan de recursos y capacidades requeridas para la implementación de las normas.

j) Presentar propuestas para cerrar las brechas identificadas.

k) Elaborar y proponer a la Dirección General los lineamientos estratégicos relativo a la seguridad de la información.

l) Participar en las reuniones técnicas de coordinación según le sea requerido.

m) Elaborar y proponer el Plan operativo de Tecnología en lo concerniente a seguridad y proponer un sistema de seguimiento.

n) Participar activamente en el proceso de certificación en la Nortic A7 e ISO 27001:2013.

o) Realizar otras actividades encomendadas, que contribuyan a la consecución del propósito de esta consultoría.

6. PRODUCTOS ESPERADOS

Fase I: Entrega de plan de trabajo	
Inicio de Proyecto / Entregable 1	Entrega de la metodología, plan de trabajo, de implementación y análisis de riesgo de la consultoría
Fase II: Diagnostico y análisis de brecha	
Entregable 2	**Diagnóstico y análisis de brecha** **Informe de análisis de brecha o cumplimiento de las siguientes normativas.** o Nivel de cumplimiento con la NORTIC A7 o Nivel de cumplimiento con la norma ISO 27001:2013

	○ Oportunidades de mejora y recomendaciones para alcanzar ambas certificaciones.
Fase III: Auditoría de riesgos y vulnerabilidades del sistema de información, identificación de riesgos de seguridad en los diferentes procesos.	
Entregable 3	**Informe de auditoría de vulnerabilidades que no son tecnológicas, vulnerabilidades de los sistemas de información y comunicación aprobado por Departamento de TI:** ○ Identificación y análisis de las fortalezas de los sistemas de información. ○ Verificación del nivel de eficacia de cada control tecnológico y no tecnológico. ○ Evaluación de las vulnerabilidades en los sistemas de información (escaneo de vulnerabilidades y prueba de penetración), acompañada de propuestas de solución. ○ Verificación del nivel de respuesta de la estructura tecnológica en cumplimiento a los requisitos de la norma y el alcance de implementación. **Informe de análisis de riesgo de seguridad de la información aprobado por Departamento de TI** ○ Diseño de Mapas de riesgos de TI, asociado a las amenazas y los controles de seguridad de información. ○ Elaboración de propuesta de mejora y acompañamiento en la implementación del plan de acción.
Fase IV: Documentación y transferencia de conocimientos	
Entregable 4	○Informe de revisión de procesos, entrega de documentos asociados a las Normas Nortic A7 e ISO 27001:2013 y transferencia de conocimiento al personal designado por la Dirección para estos fines. ○Lista de los documentos y registros (políticas, planes y procedimientos) revisados, mejorados o elaborados que han sido implantados en el Sistema de Administración de Seguridad de la Información (SASI).

	o Taller de presentación interna referente a los resultados a la consultoría.
Fase V: Cierre de Proyecto	
Entregable 5	**Informe de cierre del proyecto que incluya:** o Resultados de la auditoría interna del Sistema de Administración de Seguridad de la Información (SASI). o Plan de implementación de las mejoras en la infraestructura tecnológica, identificando las implementaciones que son críticas y que esté alineado a la matriz de riesgo previamente realizada o mejorada. o Participación activa en las certificaciones de las Nortic A7 e ISO 27001:2013.

7. ALCANCE

La consultoría deberá abordar la elaboración, implementación y documentación del sistema de administración de seguridad de la información (SASI) con el objetivo de realizar la certificación de la normativa NORTIC A7 e ISO 27001.

8. ÁMBITO DE EJECUCIÓN DE LOS SERVICIOS

El (la) consultor(a)/Empresa contratado(a) prestará sus servicios en Santo Domingo, Distrito Nacional en las oficinas de la Dirección General de Contrataciones Públicas, según la etapa en la que se encuentre la consultoría y según sea necesario y requerido, para lo cual se le proporcionará el espacio físico adecuado para el desarrollo de sus labores.

La supervisión y coordinación de las actividades del consultor será responsabilidad de quién designe la Dirección General de Contrataciones Públicas.

9. PRODUCTOS ESPERADOS Y CRONOGRAMA DE ENTREGA

Producto	Duración Estimada de Ejecución	Fecha de Entrega a la Dirección	Revisión y Aprobación
1. Plan de Trabajo de la consultoría **(ver Fase I de la sección 6)**	1 mes luego de firmado el contrato.	Al finalizar la cuarta semana luego de firmado el Contrato.	Dirección General de Contrataciones Públicas.
2. Documento de análisis y cierre de brecha. **(ver Fase II de la sección 6)**	1 mes luego de entregado el producto 1.	Al finalizar la cuarta semana luego de entregado el plan de trabajo de la consultoría.	Dirección General de Contrataciones Públicas.
3. Informe de auditoría de vulnerabilidades, plan de recursos y capacidades, Informe de análisis de riesgo, según hallazgos del producto **(ver Fase III de la sección 6)**	2 semanas después de entregado el producto 2	Al finalizar la segunda semana luego de entregado el documento de análisis y cierre de brechas.	Dirección General de Contrataciones Públicas.
4. Plan de Implementación Normativa A7 e ISO 27001. **(ver Fase III de la sección 6)**	2 semanas, después de la entrega del producto 3.	Al finalizar la segunda semana luego de entregado el plan de recursos y capacidades de seguridad de la información e informe de análisis de riesgo	Dirección General de Contrataciones Públicas.
5. Documentación Sistema de Administración de la Seguridad de la Información SASI: • Definición y Alcance SASI • Colección documentos legales y contractuales. • Manual de Procedimientos del SASI. • Manual de Instrucciones, lista de tareas y formularios del nivel operativo. • Documentos de Registros. • Documentación de Procesos.	Un mes luego de entregado el producto 4.	Al finalizar la cuarta semana luego de entregado el plan de implementación Normativa A7.	Dirección General de Contrataciones Públicas.