CONTRATO DE SERVICIOS PROFESIONALES DE CONSULTORÍA EN SEGURIDAD INFORMÁTICA PARA EL REGISTRO NACIONAL DE LAS PERSONAS NATURALES DE HONDURAS

Nosotros, **JORGE ARTURO REINA GARCIA**, mayor de edad, casado, hondureño. Ingeniero Civil, con tarjeta de identidad No.0801-1960-04641 y de este domicilio, actuando en mi condición de Director del **REGISTRO NACIONAL DE LAS PERSONAS**, nombrado por el Soberano Congreso Nacional mediante Decreto Legislativo No.93-2009 de fecha 14 de Mayo de 2009 y consecuentemente representante legal de la Institución, quien en lo sucesivo se denominará **EL REGISTRO** por una parte y por otra parte el señor **NAIM OSMAN LENIGAN GARCÍA**, mayor de edad, casado, Ingeniero en Sistemas y de este domicilio, con tarjeta de identidad numero 0801-1980-02550, actuando en su condición personal, en adelante denominado como **EL CONTRATISTA** hemos convenido en celebrar, como al efecto celebramos, **CONTRATO DE SERVICIOS PROFESIONALES DE CONSULTORÍA EN SEGURIDAD INFORMÁTICA PARA EL REGISTRO NACIONAL DE LAS PERSONAS DE HONDURAS**, que se regirá por la legislación vigente de Honduras y en especial, por las estipulaciones que aquí se pactan, bajo las clausulas siguientes: **PRIMERA: OBJETO DEL CONTRATO**: EL **REGISTRO** manifiesta: Que enfrenta serias dificultades para definir e implementar una política publica en materia de seguridad informática, pero no cuenta con el recurso humano, ni material, ni tecnológico para definirla, lo que establece la necesidad de adquirir esas capacidades mediante los servicios de consultoría que le permitan acceder a los recursos que requiere, ampliando este criterio hasta determinar que la implementación de esta solución se ejecute mediante un proyecto llave en mano. **SEGUNDA: TRABAJO A EJECUTAR POR EL CONTRATISTA: EL CONTRATISTA,** manifiesta: Que es consultor especializado en el área de seguridad informática y tiene como metas y se compromete a ejecutar, de acuerdo con EL REGISTRO, las siguientes:

Meta General;

Elaborar un diagnóstico revisar y evaluar controles, sistemas, procedimientos, equipos de cómputo, de comunicaciones y los sistemas institucionales para determinar y proponer las mejores alternativas para garantizar la seguridad de la información y los accesos a la misma, generando una política de seguridad integral.

Metas Específicas,

- Determinar fortalezas y debilidades internas y externas en seguridad de la información en el RNP.
- Analizar mediante matrices de control, la revisión, aprobación, aplicación, seguimiento y mantenimiento de los controles establecidos en la institución en el manejo y acceso a la información.

- Evaluar los procedimientos de acceso, control de operación, seguridad física, seguridad lógica, manejo de equipos y sistemas.
- Evaluar cómo se administran los dispositivos de almacenamiento informático.
- Evaluar controles de mantenimiento y manejo de fallas en sistemas y equipos.
- Diseñar la política de seguridad, conjuntamente con los clientes y proveedores, alineada a las necesidades del RNP.
- Establecer controles, procesos y política en las diferentes áreas del RNP.
- Asegurar el cumplimiento de los estándares de seguridad definidos.
- Minimizar los riesgos de seguridad que amenacen la continuidad del servicio.
- Monitorear todos los puntos de conexión de la red, para asegurar la disponibilidad de datos, la conectividad y el funcionamiento de los sistemas remotos. Establecer medidas de administración ajustadas a los criterios de los administradores y supervisores, evitando accesos no autorizados.
- Asegurar el acceso oportuno a la información, incluyendo los respaldos en caso de daños o pérdida producto de accidentes, atentados o desastres.
- Velar por el adecuado funcionamiento de los equipos y prever las acciones a ejecutar ante una falla, robo, incendio, boicot, desastres naturales, fallas en la alimentación eléctrica, u otro factor que afecte la infraestructura informática.
- Establecer normas para minimizar los riesgos a la información o infraestructura informática, horarios de funcionamiento, restricciones de acceso a ciertas áreas, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y lo necesario para estructurar los niveles de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general.

Alcance

El Contratista se compromete a prestar los servicios ofertados, respetando los roles de cada actor, la metodología propuesta, aplicando los correctivos necesarios para minimizar los riesgos que se pueden enfrentar en la ejecución o con posterioridad a la misma.

Como mínimo las áreas que deberá cubrir son:

1. Política de Seguridad

Relevar la información de la situación actual en esta área, para que en base a la evaluación de las fortalezas, debilidades, oportunidades y amenazas definir la política de seguridad del RNP, la cual proveerá la guía, las normas, los procedimientos y los controles a la estructura administrativa del RNP, sus usuarios y entidades relacionadas, de los criterios y acciones que regirán la seguridad de la información en relación a los requerimientos institucionales y a las leyes y regulaciones aplicables.

Productos a Generar en esta área:

Un documento diagnóstico de situación de la seguridad de la información en el RNP, un documento contentivo de la política de seguridad de la información del RNP y un documento contentivo de la estrategia de implementación, de socialización y divulgación de la política al interior y con los usuarios externos.

2. Organización de la Seguridad de la información

Proceso para elaborar el plan de implementación del modelo de gestión de la seguridad de la información en el RNP, con la propuesta de la estructura organizacional, roles y procesos para gestionarlo.

Productos a Generar en esta área:

Las matrices resultantes del proceso de evaluación de la calidad, del respaldo documental del compromiso de respeto a la política de seguridad de la información, por empleados, funcionarios y ejecutivos del RNP, documento donde se define la estrategia de coordinación para implementarla, asignando responsabilidades, estableciendo los procedimientos, controles y autorización de servicios de proceso de información, que determine los niveles y tipos de acuerdos de confidencialidad, los listados de contactos, de autoridades internas, externas al RNP y con grupos de interés especiales, considerando los procedimientos de certificación o revisión independiente de la política, identificando los riesgos externos relacionados con las partes, las consideraciones de la seguridad para los clientes y en los acuerdos con terceras partes

3. Gestión de Activos

Relevamiento de la información de la situación actual, para que en base a su evaluación, diseñar las políticas, procedimientos y controles para definir, implementar y mantener la protección de los activos organizacionales.

Productos a Generar en esta área:

Inventario de activos, identificando la unidad de asignación y la propiedad, su condición actual, documento donde se determinen los criterios de clasificación de la información y de los activos, diseñando el etiquetado y el manejo de la información.

4. Seguridad de los Recursos Humanos

Sensibilizar a los empleados, contratistas y usuarios de servicios tercerizados acerca de sus responsabilidades y seleccionar los más adecuados para ejecutar los roles asignados, y reducir los riesgos de robo, fraude o uso inadecuado de las instalaciones.

Productos a Generar en esta área:

Preparar los manuales de organización que contengan los roles y las responsabilidades de los actores, evaluar el personal existente, reclutar, seleccionar y contratar el personal que hiciere falta.

En base a la normativa laboral establecida, definiendo las responsabilidades de la dirección en la aplicación de políticas, sensibilizar, formar y concientizar a los participantes sobre la seguridad de la información, definir los procesos, procedimientos y controles disciplinarios, determinar y establecer las responsabilidades en la terminación de los contratos, establecer procedimientos de devolución de activos y de manejo de los derechos de acceso.

5. Seguridad Fisica y del Entorno

Fortalecer las medidas y normativa para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información del RNP.

Productos a Generar en esta área:

Documento diagnostico de la seguridad física y del entorno, en el que se definan los perímetros, los tipos y controles de acceso físico, los requerimientos de oficinas, recintos e instalaciones y de protección contra amenazas externas y ambientales, documento de conceptualización del trabajo en áreas seguras, incluyendo las áreas de carga, despacho y acceso público, la ubicación y protección de los equipos, analizar, evaluar y determinar los trabajos de protección a los servicios de suministro, a la seguridad del cableado, periodicidad, procedimientos y controles del mantenimiento preventivo y correctivo de los equipos, de la seguridad de estos fuera de las instalaciones, en la eliminación y en el retiro de activos.

6. Gestión de Comunicaciones y Operaciones

Generar manuales para asegurar la operación correcta y segura de los servicios de proceso local y remoto de la información.

Productos a Generar en esta área:

Recopilar la documentación de configuraciones, la estructura administrativa y documentar los procedimientos de operación, de la gestión del cambio, elaborar los manuales de organización, donde se describan las funciones, las instalaciones de desarrollo, prueba y producción, de las de prestación de los servicios tercerizados monitorearlos y revisarlos, controlar la gestión de los cambios y de la capacidad de los proveedores, establecer los procedimientos de recepción y de aceptación de los

sistemas implementados por terceros, los controles contra códigos maliciosos, o contra los códigos móviles, establecer e implementar los procedimientos de respaldo de la información, de los controles de las redes y de la seguridad de sus servicios, en la gestión de los medios removibles y su eliminación, establecer los procedimientos de manejo de la información, las políticas, procedimientos acuerdos y medios físicos para intercambiar la información, flexibilizar el proceso de comunicación interna mediante la mensajería electrónica, para mejorar los sistemas de información del negocio, establecer los niveles de seguridad en comercio electrónico, en las transacciones en línea, para generar mayor y mas confiable Información disponible para el público, sin descuidar las pistas de auditoría y el monitoreo del uso del sistema, la protección de la información del registro, a niveles del administrador y del operador, del registro de fallas, sincronizador de relojes.

7. Control de Acceso

Controlar el acceso a la información.

Productos:

Definir los procedimientos, procesos y controles a aplicar para establecer una política de control de acceso, que incorpore el registro de usuarios, los perfiles asociados, con la identificación de la gestión de privilegios, contraseñas para usuarios, los derechos de acceso, el uso permitido de las contraseñas, los procedimientos de manejo y monitoreo del equipo de usuario desatendido, considerando privilegiadamente el concepto de establecer la política de escritorio despejado y de pantalla despejada, así como la política de uso de los servicios de red, incluyendo la autentificación de usuarios para conexiones externas, identificando los equipos en las redes, estableciendo subredes y separando algunas comunidades de usuarios, enfatizando en el control de conexión a la misma, así como en el control de enrutamiento de la red, para determinar los procedimientos de ingreso seguros, con la adecuada identificación y autenticación de usuarios, con su sistema de gestión de contraseñas, usando apropiadamente las utilidades del sistema, controlando los tiempo de inactividad de la sesión, la limitación del tiempo de conexión, la restricción de acceso a la información, el aislamiento de los sistemas, dispositivos y datos sensibles, dando especial tratamiento a la computación y comunicaciones móviles y al trabajo remoto.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Garantizar que la seguridad es parte integral de los sistemas de información.

Productos a Generar en esta área:

Manual de análisis y especificación de los requisitos de seguridad en los procesos, que contenga la aplicación de métodos de validación de los datos de entrada, de control de procesamiento interno, de integridad del mensaje, de validación de los datos de salida, que defina y establezca la política sobre el uso de controles criptográficos, gestión de llaves de seguridad, control del software operativo, protección de los datos de prueba del sistema, control de acceso al código fuente de los programas, procedimientos de control de cambios, revisión técnica de las aplicaciones después de cambiar el sistema operativo, restricciones en los cambios a los paquetes de software, fuga de información, desarrollo de software contratado externamente, control de vulnerabilidades técnicas.

9. Gestión de los Incidentes de la Seguridad de la Información.

Asegurar que los eventos y las debilidades de la seguridad de la información en los sistemas de información se conocen oportunamente de forma que se pueden tomar acciones correctivas oportunas.

Productos:

Manual de procedimientos, controles y mecanismos de monitoreo para establecer la generación periódica o controlada de los reportes de los eventos de seguridad de la información, de las debilidades de la seguridad, de las responsabilidades y procedimientos a aplicar para resolverlos, generándose la memoria institucional correspondiente y estructure un modelo dinámico de aprendizaje en base a los incidentes de seguridad de la información, cuidando permanentemente los procesos de recolección de evidencia.

10. Gestión de la Continuidad del Negocio.

Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

Productos:

Propuesta en que se definan las estrategias, los procesos, procedimientos que aseguren la inclusión de la seguridad de la información en la gestión de la continuidad del negocio, documento de análisis del escenario de la continuidad del negocio y la evaluación de riesgos, que contemple el desarrollo y la implementación de los planes de continuidad incluyendo la seguridad de la información, estructura para planificar la continuidad del negocio, pruebas, mantenimiento y reevaluación de los planes.

11. Cumplimiento

Asegurar el cumplimiento de Leyes, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad.

Productos:

Resumen de identificación de la legislación aplicable, derechos de propiedad intelectual (DPI), protección de los registros de la organización, protección de los datos y privacidad de la información personal, prevención del uso inadecuado de los servicios de procesamiento de información, reglamento de los controles criptográficos, de cumplimiento de las políticas y normas de seguridad, verificación del cumplimiento técnico, controles de auditoría de los sistemas de información, protección de las herramientas de auditoría de los sistemas de información.

En base al diagnóstico de los diferentes dominios y sus controles, se podrán realizar las recomendaciones pertinentes, según los hallazgos identificados.

Entregables

- Matriz de control y evaluación de dominios y controles norma ISO 27002.
- Matriz de riesgo de los principales riesgos identificados con sus recomendaciones, nivel de impacto, dominio afectado y su plan de acción.
- Propuesta de mejora.

EL CONTRATISTA asume todos los riesgos de su personal con sus propios medios cumpliendo por su propia cuenta todas las obligaciones que puedan derivarse de la relación laboral entre **EL CONTRATISTA** y sus trabajadores o empleados.

TERCERA: OBLIGACIONES DE EL REGISTRO: El Registro Nacional de las Personas proporcionará a **EL CONTRATISTA** toda la información y documentación que sea requerida para la elaboración del objeto de este contrato, asimismo se obliga a pagar el valor pactado para la ejecución del mismo, y a designar un equipo de trabajo para la definición detallada del alcance y acompañamiento permanente para la puesta en marcha del proyecto.

CUARTA: DURACION E INICIO DEL CONTRATO: El Presente contrato tendrá una duración de 30 dias hábiles contados a partir de la fecha de suscripción del presente contrato.

QUINTA: MONTO DEL CONTRATO Y FORMA DE PAGO: El monto del presente contrato es de **SEIS CIENTOS OCHENTA Y SEIS MIL CIEN LEMPIRAS** (Lps 686,100.00) pagaderos en la forma descrita a continuación:

15 % del monto establecido al aprobar la consultoría y su plan de trabajo.

45 % del monto total al entregar el borrador del informe final (entrega de la Matriz de riesgo, la de control y la de propuesta de mejora).

40 % Contra la aceptación del informe a satisfacción del EL REGISTRO.

SEXTA: EL REGISTRO pagará los montos antes señalados una vez que **EL CONTRATISTA** entregue los informes de trabajo a EL REGISTRO, quien una vez que los revise y apruebe, dará la correspondiente orden de pago. Si tras la entrega de cada parte del sistema especificada en el plan de trabajo hubiere correcciones que hacer, EL CONTRATISTA dispondrá de cinco (5) días calendario para verificar y validar los resultados o productos entregados. Si encontrare errores o deficiencias, lo notificará por escrito a EL CONTRATISTA, para que las corrija y someta a revisión de nuevo, hasta subsanarlos, una vez realizados los arreglos, se hará una nueva entrega, Si los errores detectados afectan a funcionalidades básicas, e implican que no puede ponerse en operación, la fecha de la entrega con los errores subsanados será la fecha de entrega válida.

Los JEFES DE IDENTIFICACION del Registro Nacional de las Personas, son interlocutores válidos: para llevar a cabo las comunicaciones necesarias durante la ejecución del contrato.

Si pasados 30 días tras la entrega EL CONTRATISTA no indicara problemas o deficiencias, se entenderá que la entrega ha sido validada por EL REGISTRO.

SÉPTIMA: GARANTIAS DE CUMPLIMIENTO: EL CONTRATISTA se obliga a presentar la garantía de cumplimiento a favor de **EL REGISTRO** por un monto equivalente al 20% del valor del contrato, misma que tendrá vigencia de 90 días después de la entrega de los trabajos recibidos a entera satisfacción del RNP, la garantía podrá ser un pagaré a favor de **EL REGISTRO.**

OCTAVA: CONFIDENCIALIDAD.- EL CONTRATISTA se obliga permanentemente a no transferir, transmitir ni divulgar por medio alguno, publicaciones, conferencias, informes o cualquier otra forma, a personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras, los datos e información obtenidos de la ejecución de éste contrato sin la autorización expresa y por escrito de **EL REGISTRO**, especialmente toda la información contenida en las fichas dactilares u otros medios, cualquier otra insertada o capturada en las terminales, aceptando que salvo lo que expresamente esté pactado o haya sido objeto de precisión durante el proceso que dio lugar a la celebración del presente contrato, todos los datos e información comunicados por **EL REGISTRO** o a los cuales tuvo acceso **EL CONTRATISTA**, son propiedad exclusiva de **EL REGISTRO**, por lo que en este acto **EL CONTRATISTA** asume la obligación de confidencialidad y discreción total.

Se considerará como información confidencial de **EL CONTRATISTA** y no podrá divulgarse sin su autorización expresa y por escrito: **a)** El software (programas), incluyendo cualquier mejora del mismo y cualquier otra modificación efectuada, o aplicación desarrollada por ellos, que no sea de dominio público; **b)** Cualquier información o datos remitidos a **EL REGISTRO** por **EL CONTRATISTA** calificados por éste como "confidenciales" o sujetos a alguna reserva de confidencialidad similar.

NOVENA.- PROPIEDAD INTELECTUAL. EL CONTRATISTA , da por aceptado y acreditan el derecho de explotación derivados de la Ley de Propiedad Intelectual, de la política pública generada del presente contrato y de los sistemas informáticos derivados del mismo, asi como de todos los sub-productos: documentación técnica de análisis y diseño, documentación de planificación y pruebas, etc. son propiedad de **El REGISTRO.** Además **EL CONTRATISTA** garantiza que los trabajos y servicios prestados a **El REGISTRO** objeto de este contrato no infringen ni vulneran los derechos de propiedad intelectual o industrial o cualesquiera otros derechos legales o contractuales de terceros, cualquier reclamo será solventado por él.

DECIMA.- GARANTÍA EN EL TIEMPO.

Una vez entregada y validada cada parte, se iniciará un periodo de garantia del correcto funcionamiento y adecuación a los requisitos de rendimiento y calidad de 6 meses. La garantía cubrirá el servicio de mantenimiento correctivo por El Contratista, con un tiempo de respuesta a las notificaciones de incidencias inferior a las 8 horas laborables y un tiempo de reparación acorde al esfuerzo técnico necesario para su reparación.

La garantia no cubre operaciones de mantenimiento adaptativo o perfectivo.

DECIMA PRIMERA.- SOLUCION DE CONFLICTOS Y LA LEY APLICABLE: Si existiere alguna desavenencia con motivo o en ocasión de la ejecución e interpretación de este contrato y la misma no fuere solucionada por el buen entendimiento extrajudicial, ambas partes se someterán a la jurisdicción y competencia del Juzgado de Letras de lo Contencioso Administrativo del Departamento de Francisco Morazán, por lo tanto se prohíbe el arbitraje; para todo lo no previsto en el presente contrato se aplicarán las disposiciones legales del ordenamiento jurídico vigente en la República de Honduras aplicables a este contrato.

DECIMA SEGUNDA: CAUSAS DE RESOLUCION: Ambas partes podrán invocar la resolución del contrato por cualquiera de las causas siguientes: 1.- El grave o reiterado incumplimiento de las cláusulas convenidas 2.- La falta de constitución de garantía de cumplimiento del contrato 3.- La suspensión definitiva o la suspensión temporal, por 15 días, de los trabajos por parte de **EL CONTRATISTA,** sin la debida justificación. En caso de fuerza mayor o caso fortuito, se estará a lo acordado con **EL REGISTRO.**

4.- La muerte de **EL CONTRATISTA** si no pudieran concluir las obras sus sucesores. 5.- El mutuo acuerdo de las partes. 6.- El incumplimiento de las obligaciones de pago por **EL REGISTRO**. 7.- Las demás que establezca expresamente el contrato y la Ley de Contratación del Estado. Ambas partes manifiestan su conformidad con el contenido de las cláusulas de este contrato, obligándose al fiel cumplimiento de las mismas.

Si el contrato se rescinde sin producir la entrega de los productos en la forma dispuesta en el mismo, las partes acuerdan colaborar de buena fé, especialmente EL CONTRATISTA para facilitar, una nueva contratación para darle continuidad a los trabajos, o para que EL REGISTRO pueda continuar con los trabajos, y a facilitar la transferencia del conocimiento y sub-productos generados.

A la resolución del contrato, EL CONTRATISTA, independientemente de las entregas parciales realizadas, entregará a EL REGISTRO los productos y documentación producida, con un sistema de clasificación y acceso que permita identificar las versiones de cada componente.

En fe de lo anterior y para constancia firmamos el presente contrato en la ciudad de Tegucigalpa Municipio del Distrito Central, Departamento de Francisco Morazán a los veinte (20) días del mes de junio de dos mil doce (2012).

Ing. JORGE ARTURO REINA IDIAQUEZ
EL REGISTRO

Ing. NAHÍ OSMAN LENIGAN GARCÍA
EL CONTRATISTA