NORWEGIAN REFUGEE COUNCIL

TÉRMINOS DE REFERENCIA

Consultoría: Evaluación Externa Protección de Datos Colombia

▶ ***Ubicación*** Bogotá

ANTECEDENTES

El Consejo Noruego para Refugiados (NRC) es una organización no gubernamental internacional, independiente, humanitaria, sin ánimo de lucro, establecida en 1946. NRC en América Latina y el Caribe responde a las necesidades y derechos de las personas desplazadas y refugiadas independientemente de su edad, género, condición social, étnica, religiosa o nacionalidad, con un enfoque de acceso a derechos y soluciones duraderas. El compromiso en materia de protección guía todas las acciones humanitarias y respuestas al desplazamiento y es un elemento esencial a la misión de NRC.

NRC ha estado operando en Colombia desde 1991 y ha estado implementando con éxito programas multisectoriales en todo el país. NRC tiene cobertura a nivel nacional y una alta capacidad para trabajar hacia las personas afectadas por el conflicto y otras crisis migratorias presentes en los principales centros urbanos, al tiempo que también puede llegar a comunidades en áreas de difícil acceso y personas con movilidad restringida.

Para proporcionar la asistencia adecuada, NRC debe recoger información, incluyendo datos personales de los beneficiarios de los diferentes programas, además del tratamiento de datos personales de su staff. NRC utiliza los datos personales para cumplir con obligaciones hacia los beneficiarios, empleados, autoridades públicas, donantes, socios y otras partes interesadas.

La política de protección de datos de NRC establece la normativa de la organización sobre cómo proteger la privacidad de los individuos cuyos datos se manejan, de acuerdo con la legislación aplicable y los principios humanitarios. Adicionalmente, el personal, socios y proveedores de NRC que utiliza, en nombre de NRC, los datos personales recopilados por NRC, deben hacerlo de acuerdo al Reglamento General de Protección de Datos de la Unión Europea 2016/679 – RGPD (NRC es una organización con base en Noruega, sujeta al RGPD) y la legislación para la protección de datos aplicable en el país en el cual se recopila y utilizan los datos personales, en este caso Colombia. Esto aplica tanto a los datos personales almacenados en formato electrónico y como a los resguardados en archivos de papel.

Finalmente, NRC está comprometido con la programación segura en sus intervenciones por lo que sigue los estándares mínimos de Programación Segura e Inclusiva (SIP), en cuyo estándar 1E, el NRC incluye la protección de datos personales como un componente a cumplir.

JUSTIFICACIÓN

De acuerdo al RGPD, el principio de responsabilidad proactiva o principio de accountability hace recaer en el responsable o encargado la responsabilidad de (i) implantar aquellas medidas que sean las precisas para garantizar el cumplimiento de la norma; (ii) **demostrar** el cumplimiento y, por lo tanto, la eficacia de las medidas adoptadas y (iii) **revisar** y actualizar dichas medidas. Por tanto, nos encontramos en un entorno normativo en el que la obligación proactiva de cumplimiento con la normativa implica la necesidad de realización de auditorías o evaluaciones externas de cumplimiento.

Así, la realización de auditorías o evaluaciones externas permite:

1. Evaluar los riesgos y verificar si las medidas son suficientes.
2. Identificar y documentar nuevos riesgos.
3. Recomendar y adaptar nuevas medidas en un proceso de continua mejora.

4. Demostrar cumplimiento.

De acuerdo a lo anterior, NRC, en línea con su compromiso hacia la protección de datos personales de su personal y beneficiarios, procede con la contratación de la presente consultoría para la evaluación externa de cumplimiento de protección de datos personales.

OBJETIVOS Y ALCANCE DEL TRABAJO

Objetivo General

El objetivo general de la evaluación externa es verificar el nivel de cumplimiento de la política de protección de datos personales de NRC, los estándares mínimos de Programación Segura e Inclusiva (SIP), la legislación europea de protección de datos personales RGPD y la legislación colombiana sobre protección de datos personales aplicables a las operaciones de NRC en Colombia y establecer un plan de acción para la subsanación de las deficiencias que pudieran detectarse.

Objetivos Específicos

- Identificar oportunidades para mejorar el sistema de protección de datos
- Evaluar riesgos de protección de datos y determinar métodos para tratarlos.
- Comprobar el cumplimiento con requisitos internos y externos de protección de datos personales
- Incrementar o mantener el nivel de confianza del personal y beneficiarios sobre la protección de sus datos personales

Alcance de trabajo

- La consultoría se llevará a cabo en Colombia de manera remota, pero se espera que el/la consultor/consultora visite cada una de las áreas dentro de la operación en Colombia (como mínimo las oficinas principales). A saber: Oficina de País y Centro y Unidad de Respuesta Rápida (URR) en Bogotá, Oficina en Cali del área de Occidente, Oficina en Villavicencio del área de Oriente y Oficina en Cúcuta del área Nororiente.
- La consultoría abarcará las diferentes actividades realizadas por los equipos en NRC Colombia en sus diferentes áreas de acción, a saber: actividades de la unidad de Programas incluyendo las competencias (Educación; Protección; Información, asesoramiento y asistencia legal (ICLA); Medios de vida y seguridad alimentaria, Alojamiento e infraestructura y Saneamiento), M&E y MQR, unidad de soporte (logística, ICT, Finanzas, HR), unidad de incidencia y comunicaciones, así como de la unidad de operaciones.
- El/la consultor/consultora deberá entrevistarse como mínimo con el Equipo de Gerencia de País incluyendo a Gerentes de Soporte y los equipos de gerencia de las diferentes áreas, así como con los equipos en terreno implementando los proyectos del NRC. En los casos en que sea necesario, podrían llevarse a cabo reuniones con el equipo regional relevante.
- El idioma a utilizar en general será el español. Sin embargo, el/la consultor/consultora deberá tener manejo del idioma inglés ya que algunos documentos marco de la organización se encuentran en dicho idioma.

Principales tareas y responsabilidades

Los siguientes son los componentes a revisar por el/la consultor/consultora en los cuales se dan algunos ejemplos orientadores sobre los temas que se espera aborde la evaluación:

- **Revisión aspectos legales**: Serie de medidas cuyo incumplimiento podría conllevar la imposición de sanciones y ello sin necesidad de que exista una lesión previa de los derechos y libertades del interesado. Estas medidas podrían ser las siguientes:

- Tratar los datos personales conforme a las bases legitimadoras establecidas de acuerdo a la política interna, el RGPD y legislación colombiana de protección de datos personales en las diferentes actividades y unidades de NRC Colombia.
- Cumplir con el deber de transparencia hacia el interesado
- Gestionar los ejercicios de derechos de los interesados conforme a la ley aplicable
- Disponer de un registro de las actividades de tratamiento
- Realizar una evaluación de impacto cuando se requiera

- **Revisión aspectos Organizativos**: Mecanismos de gobierno que permitan tomar decisiones al nivel adecuado y con la información suficiente, y una estructura organizativa que permita la involucración/participación de todas las áreas de la organización en la protección del dato:
  - Políticas corporativas de protección de datos, Implementación, conocimiento y apropiación por parte del personal de NRC.
  - Marco de controles en materia de protección de datos.
  - Política sobre el uso de herramientas corporativas, recursos compartidos, etc.
  - Normas internas que contengan los principios y reglas aplicables a la contratación de personal, proveedores, consultores, contratistas, tutores, etc.
  - Guías sobre dispositivos móviles y el uso del teletrabajo.
  - programa de formación periódico general
  - Habilidades del personal de NRC para reconocer, manejar y evidenciar las situaciones que puedan dar lugar a un incidente de protección de datos
  - Documentación relevante para procesos de rendición de cuentas (por ejemplo: consentimientos informados, tablas de retención de la información, notificaciones para uso de información con un propósito diferente de ser necesario, etc)

- **Revisión aspectos técnicos o de seguridad**: Las medidas que se señalan en el texto normativo son aquellas que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento en los términos del artículo 32 de RGPD. En cualquier caso y de conformidad con el principio de accountability, serán las organizaciones las que decidan en cada momento, según el contexto y las actividades de tratamiento llevadas a cabo por la misma, la oportunidad y bondad de las medidas técnicas a implementar. En este sentido, se revisará, por ejemplo:
  - Controles tecnológicos para la seguridad de la información.
  - Medidas para la continuidad de negocio y recuperación ante desastres.
  - Medidas para proteger el uso de herramientas habituales (correo electrónico) como antispam o antiphishing.
  - Protección de Sitios Web.
  - Realización de copias de seguridad y actualización de sistemas operativos.
  - Cifrado de ficheros.
  - Cifrado de discos.
  - Sistemas de control de accesos.
  - Cortafuegos/firewalls.
  - Herramientas que permiten analizar y controlar la actividad del usuario en el envío de información al exterior desde su puesto de trabajo mediante la detección de fugas de información.
  - Gestión centralizada de contraseñas, control de accesos y sesiones: quién accede, cuándo y a qué.
  - Gestión de accesos.
  - Políticas de respuesta ante incidencias y gestión de brechas de seguridad.
  - Gestión de grupos en SharePoint

Productos entregables

- Plan de trabajo y metodología propuesta (con la propuesta de servicios)
- Informe borrador construido a partir de la revisión documental y de sistemas, visitas a terreno y discusiones con el staff relevante.
- Informe final más anexos incluyendo un taller de presentación de hallazgos, buenas prácticas, evaluación de riesgos y principales recomendaciones como se sugiere a continuación.

Informe final:

Del informe final entregado por el o la consultor/consultora se espera tener un mapa claro de acción para lograr el cumplimiento de la operación en Colombia en términos de sus políticas internas, RGPD y legislación nacional de protección de datos. En dicho informe se hará un diagnóstico del estado actual de cumplimiento, se identificarán riesgos que afecten a la operación relacionados a protección de datos personales y se emitirán recomendaciones que se puedan reflejar en un plan de trabajo por parte del equipo de NRC.

El informe final debe contener como mínimo las siguientes secciones:

a. Resumen ejecutivo (uno o dos páginas): brinda una breve descripción general de la evaluación externa, el proceso y los hallazgos clave;
b. Siglas (breve lista) y glosario;
c. Introducción (hasta 3 páginas, incluidas subsecciones): cubre el contexto, una breve descripción general de las actividades de NRC en el país, el contexto del tratamiento de datos en la operación. Con subsecciones sobre: Objetivos de la evaluación: cuál es el objetivo general y cómo se utilizará la información
d. Metodología (hasta 2 páginas): Metodología para realizar la evaluación externa de cumplimiento.
e. Diagnostico (hasta 10 páginas): Diagnostico de nivel de cumplimiento en materia de protección de datos (RGPD y legislación colombiana) respecto de las actividades que hacen parte de la operación colombiana de NRC.
f. Hallazgos (hasta 10 páginas): Deficiencias y vulnerabilidades encontradas o niveles de cumplimiento bajo en materia de protección de datos (GDPR y legislación colombiana) respecto de las actividades que hacen parte de la operación Colombia de NRC y análisis de riesgos de estas deficiencias y como impactan los objetivos de la organización.
g. Recomendaciones: (Hasta 8 páginas) Puede ser en forma de tabla de recomendaciones y puntos de acción necesarios para que la operación pueda alcanzar un cumplimiento óptimo en materia de protección de datos (GDPR y legislación colombiana) respecto de las actividades que hacen parte de la operación Colombia de NRC. Dichas recomendaciones deberán indicar el nivel de riesgo asociado (bajo, medio, alto) así como el área/unidad responsable.
h. Conclusiones finales de la evaluación (no más de 3 páginas).

Comité de revisión

Se conformará un comité de revisión integrado por las partes clave interesadas en el programa que guiará la correcta ejecución de la evaluación. Esto incluye la revisión de los informes preliminares y finales para la difusión de los hallazgos.

Por parte del NRC el comité de revisión estará compuesto por la gerencia de riesgo y cumplimiento, gerencia de ICT, la coordinación de la unidad Administrativa.

DISPOSICIONES INSTITUCIONALES Y ORGANIZACIONALES

El NRC poseerá los derechos de propiedad intelectual de todos los materiales presentados por los consultores en virtud del contrato. Por lo tanto, los consultores deben asegurarse de poseer cualquier material proporcionado al NRC como parte del entregable. Los derechos de reproducción de los informes se otorgarán al NRC y sus agentes contratados. El NRC será libre de reproducir los materiales a voluntad y de otorgar derechos de reproducción.

Deberes del consultor

Los informes deben presentarse en formato Microsoft Word, en español, el informe final deberá presentarse en español en PDF y Word. Los textos no deben tener formato. Los gráficos u otros elementos gráficos deben ser editables (es decir, no deben ser imágenes). Todas las referencias deben citarse conforme a la convención y detallarse en una bibliografía, utilizando el sistema APA. Todas las citas literales deben aparecer entre comillas y no deben tener una longitud excesiva. Todos los datos recopilados en el marco de la consultoría deben enviarse junto con los entregables, en un formato ampliamente reconocido, por ejemplo, Microsoft Excel.

Todo lo que se envíe al NRC debe ser trabajo original de los consultores. Cualquier plagio en cualquier forma, o cualquier otra violación de los derechos de propiedad intelectual, automáticamente descalificará al consultor de recibir cualquier pago adicional conforme al contrato suscrito por el NRC, y el NRC procurará recuperar los pagos ya realizados.

El consultor seguirá la guía de Investigación Ética con Niños con respecto a la participación ética de los niños. Además, se informará plenamente a todos los participantes de estudios u otra interacción sobre la naturaleza y propósito de la interacción y su participación solicitada. Se debe obtener el consentimiento informado para cualquier fotografía, grabación de audio o vídeo, etc., de conformidad con la política de consentimiento del NRC.

El consultor/consultora deberá determinar y asignar los equipos requeridos para garantizar el desarrollo de la consultoría, estos serán de propiedad exclusiva del consultor. El NRC no está en la capacidad de entregar equipos para el desarrollo de la consultoría.

La presente consultoría no establece relación de empleado/empleador entre el NRC y el consultor/consultora y su equipo. Lo anterior significa que el consultor/consultora desarrollará las actividades de manera independiente y los pagos de salarios, prestaciones sociales, seguros de riesgos laborales y de cualquier otro tipo que sean necesarios correrán por su cuenta (la del consultor/consultora) de manera exclusiva. Teniendo en cuenta que la consultoría tendrá una duración de 8 semanas, se espera que el consultor/consultora entregue prueba del pago de prestaciones sociales (salud, pensión y ARL) del personal a su cargo en oportunidad de cada desembolso.

Toda la información que el NRC coloque a disposición de el/la consultor/consultora en razón de esta consultoría será tratado como sensible y confidencial y no podrá ser compartido con terceros. El/la consultor/consultora deberá garantizar la confidencialidad y protección de la información por parte de sus empleados asignados en caso de aplicar. Toda la información a la que tenga acceso el/la consultor/consultora será regresada o destruida una vez finalizada la consultoría.

Deberes del NRC

La provisión oportuna de insumos para revisión documental, acceso temporal a sistemas relevantes, contacto con miembros relevantes del staff en la oficina de país y las áreas a visitar.

CALENDARIO DE EJECUCION Y ESTIMACION DE INSUMOS

#	Descripción	S1	S2	S3	S4	S5	S6	S7	S8
1	Reuniones de arranque y entendimiento, solicitud documental								
2	Revisión documental								
3	Actividades en terreno (Entrevistas staff relevante / observación actividades)								
4	Sistematización y análisis de información y creación de informe borrador construido a partir de la revisión documental y de sistemas, visitas a terreno y discusiones con el staff relevante.								
6	Envío de informe borrador								
7	Correcciones y aportes a informe borrador por parte del comité de revisión (3 días hábiles de revisión)								
8	Informe final más anexos incluyendo un taller de presentación de hallazgos, buenas prácticas, evaluación de riesgos y principales recomendaciones al CMG								

CUALIFICACIONES DE LA PERSONA / EMPRESA CONSULTORA

La persona natural o jurídica que desee postularse deberá cumplir con los siguientes criterios:

- Definir un equipo de trabajo que incluya como mínimo a dos profesionales con experiencia mínima de 5 años en revisión de nivel de cumplimiento de legislación de protección de datos incluyendo la legislación colombiana y RGPD así:
  - Abogado especialista en protección de datos personales en Colombia y RGPD
  - Ingeniero de sistemas con énfasis en seguridad informática. Certificaciones en Ethical Hacking y CISM son bien valorados.
- Se sugiere que el equipo lo constituya un/a consultor/consultora con experiencia en derechos humanos y acción humanitaria, trabajo con población desplazada interna y migrante o refugiada.
- En caso de que la postulación sea por parte de una persona jurídica, su período mínimo de constitución debe ser no menor a 3 años.
- El/la consultor/consultora deberá anexar propuesta técnica que incluya metodología sugerida para presentar realizar la evaluación.

Como características que deberá reunir la consultoría se señalan las siguientes:

- Independencia: la libertad de condicionamientos que amenazan la capacidad del consultor/consultora para desempeñar sus responsabilidades de forma neutral.

- Objetividad: es una actitud mental neutral, que permite a los consultores/consultoras desempeñar su trabajo con confianza en el producto de su labor, y sin comprometer su calidad. La objetividad requiere que los consultores/consultoras no subordinen su juicio al de otras personas en asuntos de su competencia y, asimismo, que no tengan conflictos de interés que condicionen su opinión.
- Efectividad: cumple con los principios fundamentales para la práctica profesional de integridad, competencia y diligencia profesional; es objetiva/objetivo y se encuentra libre de influencias.

DURACIÓN

Ocho semanas a partir de la firma del contrato en caso de no convenir fecha diferente en el mismo.

FORMA DE PAGO

Se dispone de 30.000.000 COP para desarrollar el proceso que incluye el pago de honorarios del equipo consultor, las actividades de campo, los gastos de viaje (de acuerdo al punto 1 de la sección de alcance del trabajo), la documentación de las experiencias y la entrega de productos descritos en los términos de referencia. Las actividades en campo deberán regirse por los lineamientos de seguridad de NRC y normas de bioseguridad de prevención de Covid19.

Los gastos de viaje como alimentación, gastos de transporte aéreo e intermunicipal, taxis, hospedaje se encuentran cubiertos por el valor de la consultoría y deberán ser asumidos por el/la consultor/consultora (de acuerdo al punto 1 de la sección de alcance del trabajo).

La presente consultoría no establece relación de empleado/empleador entre el NRC y el consultor/consultora y su equipo. Lo anterior significa que el consultor/consultora desarrollará las actividades de manera independiente y los pagos de salarios, prestaciones sociales, seguros de riesgos laborales y de cualquier otro tipo que sean necesarios correrán por su cuenta (la del consultor/consultora) de manera exclusiva. Teniendo en cuenta que la consultoría tendrá una duración de 8 semanas, se espera que el consultor/consultora entregue prueba del pago de prestaciones sociales (salud, pensión y ARL) del personal a su cargo en oportunidad de cada desembolso.

Forma de pago:

- A la firma del contrato: 50%
- Visto bueno del iinforme final y presentación al CMG: 50%

POLIZAS:

El Consultor seleccionado deberá contratar pólizas de seguro con las coberturas que se relacionan a continuación, con compañías aseguradoras establecidas en Colombia y autorizadas para explotar el respectivo ramo por la Superintendencia Financiera y aceptables por NRC. El Consultor se obliga a mantener una póliza de iguales condiciones durante la vigencia de sus servicios y cualquier prórroga a la que haya lugar.

- CUMPLIMIENTO: Por un valor asegurado igual al treinta por ciento (30%) del valor del contrato, con una vigencia igual a la estipulada en el presente contrato y seis (6) meses más.
- SALARIOS Y PRESTACIONES SOCIALES: Por un valor asegurado del diez por ciento (10%) del valor del presente contrato, con una vigencia igual a la estipulada en este contrato y tres (3) años más.
- DE BUEN MANEJO Y CORRECTA INVERSIÓN DEL ANTICIPO: Por un valor asegurado equivalente a la suma entregada como anticipo, con una vigencia igual al plazo de ejecución del presente contrato.

DERECHOS DE PROPIEDAD y CONFIABILIDAD: los derechos de propiedad serán del Consejo Noruego para Refugiados. La confiabilidad de la información recolectada es fundamental y la difusión del material sin autorización de la organización podría poner en riesgo de seguridad a los participantes. Cualquier difusión o reproducción del material recolectado deberá contar con la autorización de la organización.

Toda la información que el NRC coloque a disposición de el/la consultor/consultora en razón de esta consultoría será tratado como sensible y confidencial y no podrá ser compartido con terceros. El/la consultor/consultora deberá garantizar la confidencialidad y protección de la información por parte de sus empleados asignados en caso de aplicar. Toda la información a la que tenga acceso el/la consultor/consultora será regresada o destruida una vez finalizada la consultoría.

ELEGIBILIDAD

Las partes interesadas deben presentar los siguientes documentos:

- Persona Jurídica: Cámara de Comercio con al mínimo 30 días de antigüedad, RUT y cedula del representante legal
- Persona Natural: Hoja de Vida, RUT y copia de cédula
- Tres (3) certificaciones de experiencia relevante.
- Propuesta técnica que incluya metodología sugerida para presentar los productos.
- Presupuesto detallado
- Hoja de Vida Equipo Consultor
- Cronograma de Actividades
- Presentar su aplicación al correo electrónico co.tender@nrc.no antes del 26 de abril de 2.022 a las 5:00 pm hora colombiana con el asunto ***BOG2869: Evaluación Externa Protección de Datos Colombia***

Nota: Solamente se evaluarán las propuestas que cumplan con los requisitos solicitados