FGR
FISCALÍA GENERAL DE LA REPÚBLICA

ANEXO TÉCNICO DE LOS LINEAMIENTOS L/002/2021 DE OPERACIÓN DEL REGISTRO NACIONAL DEL DELITO DE TORTURA.

MTRO. OSCAR AARÓN SANTIAGO QUINTOS, Titular del Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, de la Agencia de Investigación Criminal de la Fiscalía General de la República, con fundamento en el lineamiento tercero y en el artículo segundo transitorio de los Lineamientos L/002/2021 de Operación del Registro Nacional del Delito de Tortura, y

CONSIDERANDO

Que los Lineamientos L/002/2021 establecen las directrices para regular el funcionamiento, operación, cooperación y administración del Registro Nacional del Delito de Tortura, que se integrará con los datos proporcionados por los registros de la Fiscalía General de la República; las Fiscalías o Procuradurías de las entidades federativas; la Comisión Nacional de los Derechos Humanos y los organismos públicos de protección de los Derechos Humanos de las entidades federativas; así como de la Comisión Ejecutiva de Atención a Víctimas y de las Comisiones de Atención a Víctimas de las entidades federativas, en términos de los convenios que para tal efecto se celebren y las Bases de Colaboración;

Que el 15 de diciembre de 2021, en el marco de la XLV Asamblea Plenaria de la Conferencia Nacional de Procuración de Justicia, se adoptó el acuerdo "CNPJ/XLV/02/2021. Bases de Colaboración del Registro Nacional del Delito de Tortura" por el cual las personas integrantes del órgano colegiado aprobaron y suscribieron las Bases de Colaboración del Registro Nacional del Delito de Tortura, con lo cual se adhirieron a los Lineamientos L/002/2021 en comento, y

Que el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia o la unidad administrativa que lo sustituya de la Fiscalía General de la República, operará y administrará el Registro Nacional del Delito de Tortura y podrá expedir los anexos técnicos que se requieran para el cumplimiento del objeto de los Lineamientos L/002/2021; por lo que he tenido a bien expedir el siguiente:

ANEXO TÉCNICO

PRIMERA. OBJETO

Establecer los requerimientos técnicos de los servidores, redes de conexión, perfiles de usuario y actividades que se desarrollarán, medidas y parámetros de seguridad de la información, pruebas, validación de información, adecuaciones técnicas que garanticen la integridad y confidencialidad de los datos, y las condiciones en que deben realizarse las conexiones con las Fiscalías o Procuradurías de las entidades federativas; la Comisión Nacional de los Derechos Humanos y los organismos públicos de protección de los Derechos Humanos de las entidades federativas; así como la Comisión Ejecutiva de Atención a Víctimas y las Comisiones de Atención a Víctimas de las entidades federativas.

SEGUNDA. GLOSARIO

1. **Autoridades**: La Comisión Nacional de los Derechos Humanos, las Comisiones Estatales de Derechos Humanos, la Comisión Ejecutiva de Atención a Víctimas, las Comisiones de Atención a Víctimas de las entidades federativas que tengan datos relacionados con casos de tortura y otros tratos o penas crueles, inhumanas o degradantes.

2. **CENAPI**: Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia, de la Agencia de Investigación Criminal de la Fiscalía General de la República.
3. **Confidencialidad:** Medida para garantizar que la información sea accesible sólo a aquellas personas facultadas para tener acceso a la misma.
4. **Control de Acceso:** Mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos de un sistema de información, dejando un registro de dicho acceso.
5. **CSV**: Comma separated values.
6. **DB**: Database, base de datos.
7. **DGTIC:** Dirección General de Tecnologías de Información y Comunicaciones.
8. **Disponibilidad:** Medida para garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma.
9. **Entidad de negocio**: Representa una entidad relevante para una organización, por ejemplo, personas, clientes, proveedores, empleados, productos, cuentas, etcétera.
10. **Fiscalía/Fiscalías**: Fiscalías y procuradurías generales de justicia de las entidades federativas.
11. **ID:** Identificador único.
12. **Información:** Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
13. **Integridad:** Exactitud y totalidad de la información y los métodos de procesamiento.
14. **RENADET versión cliente:** Software para la carga de información a través de plantillas.
15. **RENADET**: Registro Nacional del Delito de Tortura.

16. XLSX: Extensión de archivo utilizada para reconocer hojas de cálculo de la herramienta de software llamada "Microsoft Excel".

TERCERA. RESPONSABLES OPERATIVOS

El CENAPI establecerá los enlaces como responsables operativos de la implementación y, en cumplimiento del presente instrumento, deberán llevar a cabo las siguientes funciones:

I. Realizar las actividades tendentes a cumplir el objeto del presente instrumento;
II. Dar seguimiento a los compromisos derivados del presente instrumento, y
III. Proponer procedimientos, mecanismos y colaboración con las unidades administrativas que resulten competentes.

CUARTA. REQUERIMIENTOS TÉCNICOS

A. Estructura de Comunicaciones

La estructura de comunicaciones es el intercambio de datos entre los servidores del RENADET y las estaciones de trabajo estatales, que se comunican con el servidor nacional, pero no entre ellas.

B. Definición y composición de la plantilla de carga

La plantilla de carga de datos corresponde a un archivo CSV, en formato abierto que permite almacenar datos en forma de tablas, en donde las columnas son separadas por el carácter coma (,). La plantilla contemplará la información relativa a las variables que fueron aprobadas y que hacen referencia al delito de tortura.

Las plantillas de carga de datos serán definidas de tal manera que su organización facilite la generación de las sábanas de información que se transferirán al RENADET a partir de una base de datos relacional,

alineada a la estructura del SENAP la cual será adoptada de manera progresiva, una vez que sea aprobada.

Las plantillas tendrán una relación temática o de negocio con respecto a otra u otras plantillas, lo cual permitirá conocer el entorno del delito de tortura respecto de los hechos presuntamente delictivos.

La relación entre entidades se logrará con la definición de campos identificadores únicos que permitan vincular dichas entidades de negocio.

Con la finalidad de tener un mejor entendimiento y sintetizar la explicación de cada una de las plantillas de carga en formato CSV, se generará un **archivo muestra** en formato XLSX el cual agrupará dichas plantillas en un sólo archivo.

Para efectos de la definición técnica, respecto de los tipos de datos, descripción, catálogos e identificadores, será considerado lo estipulado en el **Diccionario de datos RENADET**, mismo que forma parte integrante de los Lineamientos L/002/2021 de la operación del Registro Nacional de Tortura.

En su caso, también se podrán contemplar protocolos alternativos para la integración de información como los formatos JSON o XML para garantizar la integridad de la información y permitir reglas de validación.

C. Consideraciones de llenado de las plantillas de carga

El llenado de las plantillas de carga se podrá realizar a partir de una base de datos relacional, (comandos o instrucciones) mediante la

automatización de procesos de extracción y transformación de los datos para cumplir con los requisitos del llenado.

Las Fiscalías y Autoridades deberán actualizar la información de manera mensual.

Cada uno de los rubros o entidades de negocio que conforman a las plantillas de carga, deberá contar con sus propias validaciones y reglas de negocio, tanto de carácter general, como específicas para cada rubro.

Ambos casos serán detallados en el documento denominado: *Reglas de negocio para el llenado y procesamiento de las plantillas de carga de datos RENADET.*

C.1 Generación de un nuevo reporte y actualización de información

Las plantillas podrán ser actualizadas con datos ya reportados. Lo anterior se logrará a través del ID identificador de cada entidad correspondiente a la base de datos de cada Fiscalía, así como de las Autoridades.

Las Fiscalías, así como las Autoridades que requieran actualizar registros ya reportados en periodos anteriores, deberán agregarlos a la plantilla correspondiente, manteniendo el campo ID identificador a efecto de que el RENADET lo interprete justamente como una actualización.

La primera carga de datos sólo contemplará un periodo de información por tratarse del primer bloque de datos que se cargará en el RENADET y por lo que hace al llenado de cada plantilla, ésta deberá subirse a la plataforma sin información (vacía), en caso de no tener nada que reportar en relación con el rubro en cuestión.

D. Catálogos

Los campos de cada rubro que corresponden a catálogos estarán representados en el **Diccionario de datos RENADET**, mismo que forma parte integrante de los Lineamientos L/002/2021 de la operación del Registro Nacional de Tortura.

Para que el RENADET pueda reconocer cada identificador de catálogo, debe existir en su base de datos de producción, el correspondiente mapeo de los catálogos propietarios con los catálogos base que serán definidos para el RENADET y que permitan la estandarización de la información. Por tal motivo, ello implica atender un trabajo conjunto entre las áreas involucradas para lograr esta alineación necesaria que permita hablar el mismo idioma en términos de datos estructurados.

Aunado a lo anterior, esta estandarización de catálogos implica mantener una comunicación y actualización constante, por lo que las áreas competentes deberán informar al CENAPI los cambios que pudieran presentarse en cuanto a la definición de cada catálogo involucrado y con ello evitar inconsistencias de información en los reportes.

De igual manera los catálogos del RENADET, deberán estar alineados a los catálogos del SENAP a fin de asegurar el proceso de integración y homologación de ambos sistemas y este último, al ser alimentado por todas Fiscalías, sirva como base para el registro. Una vez que los catálogos del SENAP sean aprobados y sus reglas de negocio se hayan establecido.

Previo a la definición y aprobación de los catálogos y reglas de negocio del SENAP, el RENADET seguirá operando con la Estructura de Registro RENADET vigente.

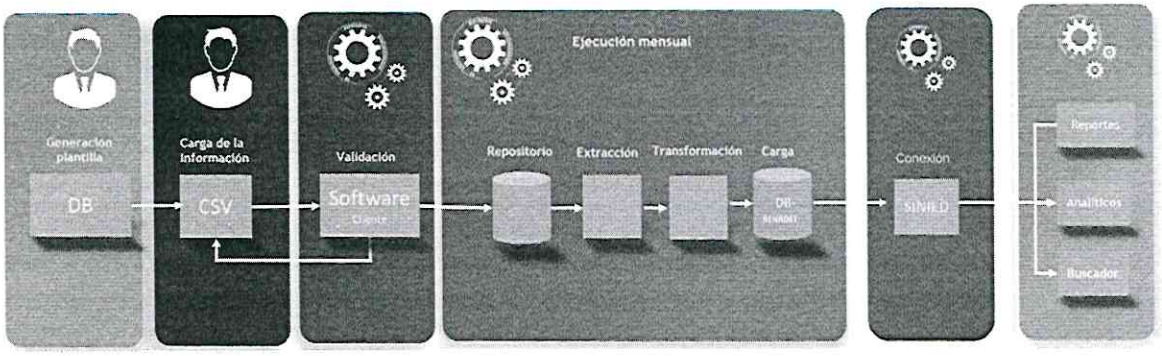
E. Proceso de carga.

Una vez generadas las plantillas de carga por el área correspondiente, el personal designado por cada Fiscalía, así como por las Autoridades que cuente con el acceso autorizado, usará el sistema **RENADET versión cliente** de carga de datos, para validar y posteriormente enviar las plantillas CSV hacia el repositorio central del **RENADET**.

El proceso antes referido, se podrá llevar a cabo antes de la fecha de corte establecida, incluso podrá repetir el proceso las veces que sean necesarias, en caso de requerir hacer alguna modificación a las plantillas.

El **RENADET versión cliente** de carga de datos, devolverá un reporte con la información necesaria para realizar los ajustes en cada una de las plantillas en caso de que el llenado no cumpla con las especificaciones de reglas de negocio y validaciones referidas en el documento que será denominado **reglas de negocio para el llenado y procesamiento de las plantillas de carga de datos**; este proceso se repetirá hasta que el cliente valide las plantillas por completo de manera satisfactoria.

A continuación, se muestra el esquema conceptual del proceso de carga de datos hacia el RENADET.



F. Corrección de errores y ajustes

Cuando sea necesario, podrá realizarse una petición de aclaración o solicitud de corrección de datos en el RENADET, éstas deberán llevarse a cabo por cada Fiscalía, así como por las Autoridades que cuenten con el acceso autorizado, notificando a CENAPI la petición de aclaración o solicitud de corrección correspondiente con su debida justificación a través de las cuentas de correo electrónico de los enlaces asignados. Una vez aprobada por parte de CENAPI, se le comunicará al enlace por los medios electrónicos de comunicación, para que, usando el sistema **RENADET versión cliente** de carga de datos, el enlace remita la actualización de la plantilla de carga de datos CSV para ser ingresadas al repositorio central del **RENADET** conforme al proceso de carga señalado en el inciso E del presente Anexo Técnico.

Todos los registros que sean actualizados como parte del procedimiento de corrección de errores y ajustes contarán con un identificador en el nuevo registro que se cargue, que permita dejar constancia de las modificaciones realizadas.

El procedimiento de corrección de errores y ajustes podrá ser actualizado conforme se determine necesario, así como una vez que se emitan las reglas de negocio del Sistema Estadístico Nacional de

Procuración de Justicia (SENAP), con el objeto de garantizar su alineación e interoperabilidad.

QUINTA. REDES DE CONEXIÓN

La interconexión entre las redes se realizará conforme a los requerimientos siguientes:

- Conexión a una red local (LAN) redundante y exclusiva para el sistema (deseable).

SEXTA. SEGURIDAD DE LA INFORMACIÓN

Se preservará la confidencialidad, integridad y disponibilidad de la información a través de los controles siguientes:

A. Perfiles de Usuario y Actividades

El acceso al RENADET se realizará por niveles y deberá ser tramitado ante el CENAPI, quien a su vez gestionará las cuentas y/o privilegios de cuentas existentes ante la DGTIC, conforme a los perfiles establecidos en los presentes lineamientos.

Los perfiles de acceso de los usuarios y sus actividades se detallan a continuación de manera enunciativa mas no limitativa y podrán ajustarse de acuerdo con las necesidades de la operación:

Administrador. - Este perfil contará con los privilegios de lectura, escritura y corrección de errores y ajustes, así como el alta y asignación de los perfiles de usuario (supervisor, operador o consulta).

Supervisor. – Este perfil de usuario contará con los privilegios de lectura, escritura y corrección de errores y ajustes, de los registros ingresados al sistema RENADET, esto último previo acuerdo con el Administrador.

Operador. – Este perfil de usuario contará con los privilegios de lectura y escritura.
Consulta. – Este perfil de usuario contará con los privilegios de lectura.

Para el otorgamiento de cualquier perfil, se requerirá una petición debidamente fundada y motivada por parte del superior jerárquico del área requirente, misma que podrá realizarse digitalmente con las salvedades de seguridad establecidas en la presente.

De conformidad a lo establecido en el tercer párrafo del lineamiento primero de los Lineamientos L/002/2021, todos los perfiles de usuarios, tanto de las Fiscalías, así como por las Autoridades, tendrán acceso general a la información estadística que se genere de las distintas variables del Registro Nacional de Tortura.

B. Medidas y Parámetros de Seguridad de la Información.
Para salvaguardar la seguridad de la información y los datos personales alojados en la Base, las Fiscalías y las Autoridades deberán contar mínimamente con los controles de seguridad de la información que se describen a continuación:

- Contar con soporte activo, lo cual permitirá el correcto funcionamiento de los equipos de seguridad.
- Todos los usuarios que ingresen al sistema deben firmar la carta de promesa de confidencialidad.
- Avisar de manera inmediata al administrador del Sistema en caso de rotación o baja de personal, para proceder a la cancelación de cuentas de acceso al sistema.

- El reinicio de sesión en los equipos bloqueados se debe hacer mediante el uso de contraseñas.
- Se sugiere que las contraseñas de los equipos que ingresen al Sistema deben ser robustas y contar con por lo menos con 10 caracteres alfanuméricos que incluyan minúsculas, mayúsculas, números y caracteres especiales.
- Lineamientos para el manejo de información (confidencial, reservada).

Asimismo, en el ámbito de sus atribuciones realizarán el Documento de Seguridad que corresponda para la protección de los datos personales a los que tienen acceso, conforme a los términos establecidos por la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.

De igual manera, deberá llevarse a cabo el registro de los accesos y movimientos que realice cualquiera de los perfiles autorizados, mismos que se asentarán en una bitácora expresa para tal efecto, a fin de garantizar la trazabilidad de los accesos y movimientos al sistema.

C. Pruebas de funcionalidad

Las Fiscalías y Autoridades deberán realizar las pruebas correspondientes de comunicación y operación a efectos de asegurar la funcionalidad, el rendimiento y la experiencia del usuario. Estas pruebas servirán para identificar errores de funcionamiento, y deberán ejecutarse antes de publicar el ambiente de producción.

El diseño de las pruebas se ejecutará considerando los siguientes aspectos de forma enunciativa mas no limitativa:

- ✓ Pruebas de rendimiento,
- ✓ Pruebas de escalabilidad,
- ✓ Pruebas de integración, y
- ✓ Pruebas unitarias.

D. Validación de la Información

La validación de los datos ingresados al RENADET será responsabilidad exclusiva de cada una de las Fiscalías y Autoridades, en el ámbito de sus atribuciones, por lo que deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de estos.

E. Adecuaciones Técnicas

Para garantizar la disponibilidad, integridad y confidencialidad de la información alojada en la Base de datos, las Fiscalías y Autoridades deberán contar con las medidas de seguridad que se mencionan a continuación:

- Seguridad perimetral, en los equipos de seguridad tipo firewall, switch, entre otros, se deben configurar políticas específicas, lo cual permitirá restringir accesos no autorizados.
- Contar con equipos de prevención de intrusiones que permitan detener ataques de zonas ajenas a la red.
- Contar con licencias activas en los equipos de seguridad, lo cual permitirá tener acceso a las últimas funcionalidades y versiones, contando con las últimas firmas de seguridad.
- Contar con los parches de seguridad actualizados en los equipos que ingresaran al Sistema.

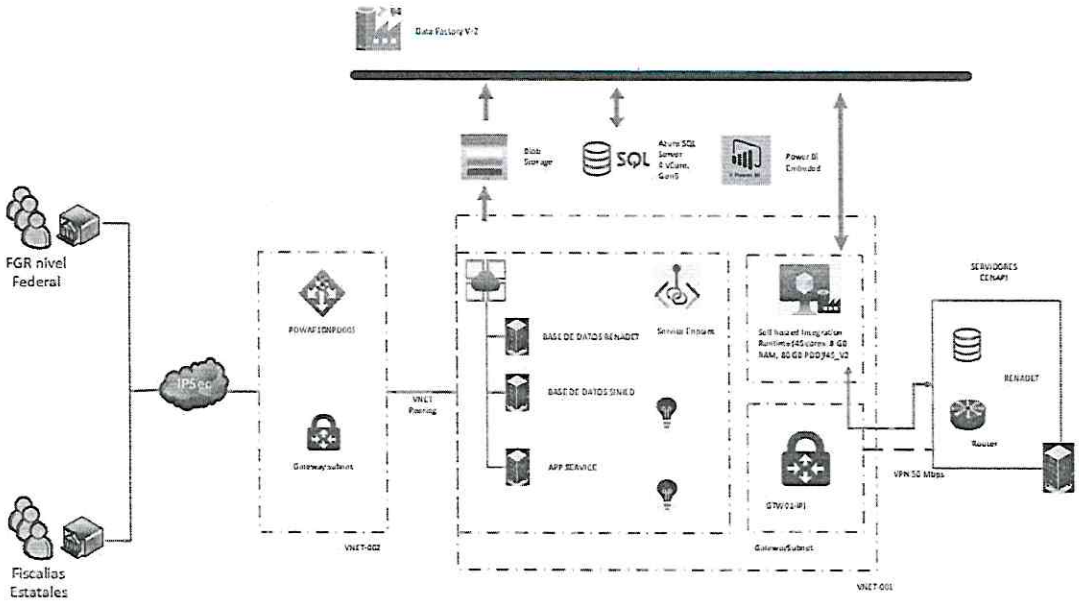
- Contar con antivirus vigente y actualizado.
- Contar con un Plan de Recuperación de Desastres plenamente probados.
- Esquema periódico de respaldo de información que contemple lo siguiente:

  - Respaldo Diario de tipo incremental.
  - Respaldo Semanal de tipo incremental.
  - Respaldo Mensual completo.
  - Respaldo Anual completo.

F. Confidencialidad

El personal de las Fiscalías y Autoridades suscribirá una promesa de confidencialidad, a través del formato que formará parte del presente Anexo Técnico, a efecto de dejar constancia de que, en cumplimiento al Código Nacional de Procedimientos Penales, la Ley General de Transparencia y Acceso a la Información Pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y las demás disposiciones jurídicas aplicables, guardará total secrecía y confidencialidad sobre el contenido de los datos e información a la que tenga acceso y, en consecuencia, se encuentra obligado a darle ese tratamiento, por lo que de ninguna forma tratará de divulgar o revelar, por ningún medio, los datos referidos directa o indirectamente a ninguna persona o entidad, nacional o extranjera.

A continuación, se muestra el esquema de manera general de la aplicación:



G. Certificados de Seguridad

Contar con controles de acceso que permitan el cifrado y acceso a la información y su modificación, sólo a las personas autorizadas.

H. Canales Cifrados para el Acceso a la Información

Contar con controles de acceso que permitan el cifrado y acceso a la información y su modificación, sólo a las personas autorizadas con el uso de esquemas de VPN.

I. Segmentos de Red Exclusivos

Utilizar segmentos reservados de la red, permitirá que se preserve la confidencialidad y disponibilidad de la red.

J. Protección de la Aplicación

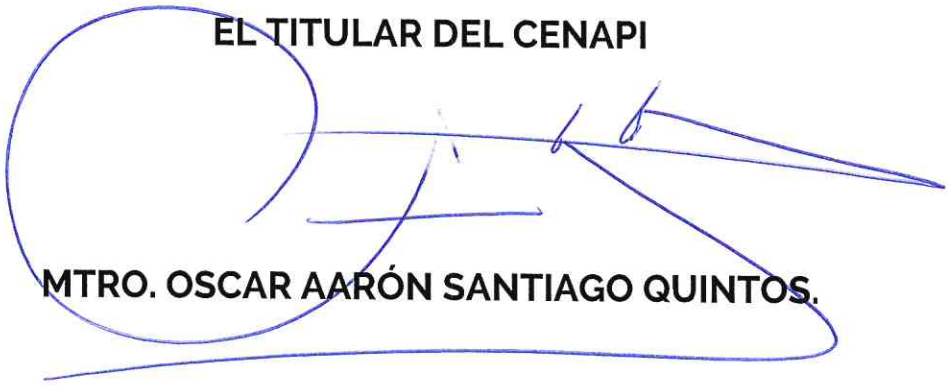
Sólo se permitirá el acceso a las personas que cuenten con los permisos y perfiles autorizados.

K. Monitoreo

Se deben implementar mecanismos de monitoreo de la aplicación, servidores que la soportan, que permitan preservar la disponibilidad e integridad de la información.

Ciudad de México, a 08 de abril de 2022.

EL TITULAR DEL CENAPI



MTRO. OSCAR AARÓN SANTIAGO QUINTOS.

Con esta foja concluye el "**ANEXO TÉCNICO DE LOS LINEAMIENTOS L/002/2021 DE OPERACIÓN DEL REGISTRO NACIONAL DEL DELITO DE TORTURA**".