COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA

# MÓDULOS DEL CICLO DE CAPACITACIÓN

## Minga Digital por los Defensores y Defensoras Indígenas de la Cuenca Amazónica

PROGRAMA DE Defensores y Defensoras INDÍGENAS

PROGRAMA DE
Defensores y Defensoras
INDÍGENAS

# CICLO DE CAPACITACIÓN

## Minga Digital por los Defensores y Defensoras Indígenas de la Cuenca Amazónica

# MÓDULO 1

## TEMA:

## FICHA DE EMERGENCIA PARA LA DOCUMENTACIÓN DE LA SITUACIÓN DE VULNERACIÓN DE LOS DERECHOS HUMANOS DE LOS DEFENSORES Y DEFENSORAS INDÍGENAS

**Programa Defensa de Defensores y Defensoras Indígenas (PDDD) COICA**

**ABRIL 2022**

COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA

# Índice

# INTRODUCCIÓN

La presente guía tiene como objetivo brindar lineamientos para la implementación de las Fichas de Emergencia que será realizada por los puntos focales del Programa de Defensa de Defensores y Defensoras Indígenas (PDDD) de la COICA y los monitores locales de Ecuador y Colombia como parte del proceso piloto a nivel nacional del PDDD promovido por el Proyecto CISU y la Propuesta Piloto para la implementación del PDDD a nivel nacional, con el soporte técnico de Derecho, Ambiente y Recursos Naturales (DAR).

El levantamiento de esta información tiene como finalidad sistematizar y condensar toda la información relevante recabada en los casos de afectación de los derechos de las y los defensores indígenas. Asimismo, es necesario que se precise la evidencia o los medios probatorios que tengan fotografías, denuncias con otras autoridades (si hubiera), testimonios de testigos, etcétera.

Las fichas de emergencia que servirán como herramientas para la capacitación y levantamiento de información son las siguientes:

- **FICHA Nº 01:** Ficha de emergencia de vulneraciones de derechos de pueblos indígenas en el marco de la COVID-19.
- **FICHA Nº 02:** Ficha de acciones frente a situaciones de emergencia de pueblos indígenas en el marco de la COVID-19.

A continuación, se brindarán lineamientos para completar las fichas referidas.

## REQUERIMIENTOS TÉCNICOS PARA EL ACCESO

El llenado de la ficha se deberá realizar a través del aplicativo móvil, para lo cual será necesario contar con lo siguiente:

- Tener acceso a un ordenador/portátil/laptop o a un teléfono celular móvil.
- Tener acceso a internet (datos, telefonía móvil, inalámbrica, otros).
- Tener acceso a un navegador Google Chrome, Firefox o Internet Explorer.
- Tener disponibilidad en el teléfono móvil para la descarga del aplicativo móvil SAT.

### A. LINEAMIENTOS PARA LA FICHA Nº 01

**Paso 0. ACCESO EN LÍNEA**

Para poder completar la ficha es necesario:

- Descargar el aplicativo móvil e instalar.
- Registrar el usuario.
- Esperar la confirmación.

**Paso 1. IDENTIFICACIÓN DEL DEFENSOR O DEFENSORA INDÍGENA**

En esta sección se debe identificar al defensor o defensora indígena afectada, para ello iniciará especificando:

1) País desde el cual se reporta.
2) Identificar si la amenaza o ataque fue individual o grupal contra la comunidad, resguardo, nacionalidad u otra forma autónomamente reconocida por los pueblos indígenas, considerando que la naturaleza de los/as defensores/as indígenas puede ser individual o colectiva.
3) En caso de que sea individual, indicar género/tipo.
4) Comunidad, resguardo y/o localidad del defensor o defensora indígena.
5) Pueblos o nacionalidades indígenas al que pertenece el defensor o defensora indígena.
6) Rol de la persona defensora en caso se trate de una amenaza o ataque individual, lo que permitirá identificar el nivel de violencia e impacto colectivo en caso se trate de personas con cargos dirigenciales o liderazgos influyentes.

Las preguntas identificadas con un "asterisco (*)", las preguntas 1, 2, 4 y 5, deberán llenarse de manera obligatoria para poder pasar a la siguiente sección.

**Paso 2. IDENTIFICACIÓN DEL RIESGO O ATAQUE**

En esta sección se busca identificar con mayor precisión el tipo de amenaza o ataque, pudiendo escoger cualquiera de las opciones múltiples del listado "Amenazas y ataques cometidos en contra los/las defensores/as indígenas".

El listado no es cerrado, se puede escoger una o varias opciones, aunque no se pretende registrar todas las posibles amenazas o ataques.

En caso de que la amenaza o ataque no figuren en este listado, puede marcar la opción "otro" y a continuación especificar dicha información. La opción de "otros" puede ser usada en simultáneo con las opciones del listado.

Posteriormente, y a partir de las amenazas o ataques identificados, se procede a determinar "¿Qué derechos están en riesgo o fueron vulnerados?", para lo cual visualizará un listado de los posibles derechos involucrados y podrá usar opción múltiple para seleccionar uno o más de uno. Al igual que el listado previo, se considera la opción "otros" a fin de poder especificar uno o más derechos que no hayan sido previstos en el listado referido.

Recordar que ambas preguntas al estar identificadas con asterisco (*) son preguntas que se deben responder de manera obligatoria. Después de ello, deberá marcar el botón "siguiente".

**Paso 3. VÍNCULO DEL RIESGO O ATAQUE CON EL COVID-19**

En esta sección se busca identificar si el riesgo o ataque sufrido por los/las defensores/as indígenas ha surgido o se ha agravado con las medidas tomadas por las autoridades durante la pandemia del COVID-19, con la finalidad de visibilizar los impactos de la emergencia sanitaria en la situación de vulneración de los derechos humanos de los/as defensores/as indígenas.

El listado ofrece múltiples opciones sobre el posible vínculo de esa amenaza o ataque con la pandemia del COVID-19, es decir que puede elegirse más de una opción, al igual que los listados previos, se cuenta con la opción "otro" para especificar otro tipo de vínculos en caso de que no hayan sido considerados en el listado.

**Paso 4. IDENTIFICACIÓN DEL ATACANTE**

Después de haber completado las secciones previas, será importante identificar ¿quién o quiénes son los presuntos atacantes? La respuesta para esta sección tiene como guía un listado del presunto autor, pudiendo marcar más de una opción.

No obstante, considerando la complejidad de los agentes que amenazan y/o agreden a defensores y defensoras indígenas, el listado considera la opción "otro" en caso el presunto autor no figure en la lista inicial. Cuando marque la opción "otro" tendrá un espacio para poder especificar los datos claves del posible atacante; en caso de que no se cuente con mayor información, puede precisar el sector, rubro, institución o área de trabajo del presunto atacante.

Por ejemplo, un dato clave a completar podría ser indicar que se trata de guardiasprivados contratados por una determinada empresa del sector minero.

A continuación, se presentan algunas preguntas orientadoras para brindar datos claves de los presuntos atacantes:

¿Es agente privado de una empresa petrolera, minera, tala de madera, agroindustria u otros similares? ¿es agente público (autoridad/funcionario del Estado)? ¿Tiene derechos legales (concesiones, contratos, títulos otorgados por el Estado, etc) o actúan en el marco de la ilegalidad (minería ilegal, taladores ilegales, narcotraficantes, invasores de tierras, grupos irregulares, paramilitares, guardias privados u otros)?

**Paso 5. RELATO DE HECHOS**

En esta sección es importante detallar la cronología de los hechos y precisar lo que considere más relevante evidenciar. A continuación, se facilita unas preguntas orientadoras para el llenado de esta sección:

- ¿Qué pasó?
- ¿Qué tipo de ataque o amenaza sufrió?
- ¿Cuándo ocurrió?
- ¿Dónde ocurrió?
- ¿Quiénes fueron los agentes de violencia? Puede sumar datos claves que ayuden a una posible identificación de los presuntos atacantes.
- ¿Qué tipo de actividad (económica, extractiva, de infraestructura, otros) está relacionada con el ataque o afectación a esta población?
- ¿Qué derechos fueron afectados?
- ¿Cuáles son los motivos que originaron la vulneración de sus derechos?
- ¿Estas amenazas y ataques están vinculados a su rol como persona defensora?
- ¿Cuáles son los principales riesgos y amenazas que aún continúan?

Asimismo, es necesario identificar a los defensores y las defensoras indígenas más expuestos, la razón por la que se encuentran en especial vulneración y el tipo de violencia que se cometió con esta(s) persona(s).

También puede precisar las acciones por parte del agente de violencia, cómo ingresó al territorio, qué acciones de defensa tomó la organización indígena del lugar, acciones con otras organizaciones aliadas, etcétera.

Para mayor facilidad en el recuento de los hechos, tendrá habilitada una opción adicional a fin de poder subir o grabar un “audio” o “nota de voz”.

**Paso 6. FUENTE DE INFORMACIÓN**

En esta sección se debe señalar con qué fuentes de información contó para llenar la ficha, para lo cual tendrá un listado de fuentes: "directa", "indirecta" y "otros". La fuente directa, consiste en aquella información que obtuvo desde los/as mismos/as defensores y defensoras indígenas que se encuentran en los territorios en dónde se lleva a cabo la amenaza o ataque de/en sus territorios; y la fuente fue indirecta, será aquella que se obtuvo de terceros ajenos al territorio o a los/las defensores/as, como por ejemplo los medios de comunicación, sociedad civil, reporte de alguna autoridad del Estado u ONGs, otros. En caso la fuente de información implique mayores complejidades, podrá marcar la opción otro.

Así mismo, tendrá un apartado en el cual debe adjuntar los medios de verificación a través de un listado con los enlaces de drive (u otra plataforma de almacenamiento disponible), los mismos que deberán ser de acceso permitido para el punto focal de su organización nacional y con acceso para el responsable de COICA.

Estos medios de verificación pueden ser documentos (cartas, demandas, respuestas, informes policiales, acta de comunidad, hojas de amenazas, pantallazos de amenazas digitales como mensajes de texto, mensajes de whatsapp o similares, etc), fotografías (de la destrucción, contaminación, de presuntos atacantes, etc), videos (del momento de la agresión, de las consecuencias de los ataques, etc), audios (testimonios, ataques, amenazas verbales, etc), entre otros medios que se consideren importantes. Por ejemplo: audio de testimonio del defensor o defensora y su enlace del drive en el que se sube el audio mp3.

**Paso 7. IDENTIFICACIÓN DE NUESTRAS ACCIONES REALIZADAS**

Esta sección busca identificar las acciones que han realizado los defensores y defensoras indígenas frente a las amenazas o ataques recibidos, ya sea acciones a un nivel administrativo, es decir ante autoridades del Estado como Ministerios, Defensorías, entre otros, o a un nivel legal, es decir ante el Poder Judicial, Tribunal Constitucional o Corte Suprema, entre otros.

Entre las acciones por ejemplo podríamos identificar el envío de cartas de alerta o solicitudes de intervención de determinadas autoridades, inicio de procesos legales (demandas en diferentes instancias, como la Corte Constitucional u otras), activación de mecanismos de protección para defensores existentes en su país, solicitudes enviadas a la Defensoría del Pueblo, entre otros.

En esta sección no será necesario detalles de la acción identificada, solo se debe responder "sí" o "no", y en caso la respuesta sea afirmativa en ambas preguntas, los detalles de la acción indicada deberán completarse en las secciones de la ficha Nº 02. Esta segunda ficha la podrán encontrar al finalizar la primera ficha, es decir una vez se haya completado todas las secciones de la ficha Nº 01.

**Paso 8. INFORMACIÓN CONFIDENCIAL**

Finalmente, completar la información del contacto que será manejada de forma confidencial por el equipo que gestione la recepción de la información reportada. Para ello, deberá colocar el nombre de los/as defensores/as indígenas y/o persona de contacto, sus datos de contacto como teléfono y correo electrónico en caso cuenten con ello.

En caso de que la información se haya levantado de forma directa, es decir desde las personas, comunidades o nacionalidades que se están viendo amenazadas o afectadas, se deberán precisar las coordenadas UTM identificadas con el equipo de campo proporcionado, ya sea GPS o aplicativo móvil que identifique coordenadas UTM.

Posteriormente, colocar la base o comunidad a la que pertenece, la organización nacional base de COICA a la que pertenece, su nombre y la fecha cuando lo realizó.

## B. LINEAMIENTOS PARA LA FICHA Nº 02

### Paso 1. INFORMACIÓN GENERAL DE LA SOLICITUD O ACCIÓN DE ASISTENCIA A LOS/AS DEFENSORES/AS

En caso de que se haya completado de forma afirmativa ("sí") el paso 7 de la ficha Nº 01, continuará con el llenado de la ficha Nº 02. Iniciará especificando el país desde el cual se reporta, luego completará información mínima para poder conocer sobre la solicitud o acción realizada: ¿Quién presentó la solicitud/carta/demanda? ¿Qué tipo de solicitud se presentó? si fue una carta, una demanda, un informe, una denuncia, una apelación, u otros; el número y fecha de la solicitud presentada (en caso de contar con estos datos), esto a fin de poder contar con el número de registro o de cargo de la entidad respectiva para realizar un posible seguimiento; ¿ante quién se presentó la solicitud? si fue un ente estatal, organismo internacional u ONG que busca garantizar los DDHH de los PPII, u otros.

Luego será importante especificar ¿qué se pidió en la solicitud? para lo cual puede detallar información sobre el asunto de la solicitud y posteriormente detallar puntualmente cuáles fueron esos requerimientos o demandas que se solicitaron.

Por ejemplo:

- Se pidió la intervención policial para la generación de un informe o atestado de los hechos de violencia.
- Dicho informe deberá registrar la destrucción de la vivienda o los medios escritos de las amenazas recibidas.
- Se solicita que se remita el informe o atestado.[1]

1 Un atestado es un documento oficial emitido por una autoridad determinada, o sus representantes, por medio del cual hacen constar algo como verdadero. Por ejemplo se suele usar en las diligencias cuando se averigua un delito.

**Paso 2. ESTADO ACTUAL DE LA SOLICITUD O ACCIÓN**

En esta sección se deberá informar sobre el estado actual de la solicitud que los/las defensores/as u organizaciones/instituciones aliadas hayan presentado en respuesta al riesgo o ataque sufrido. Como la solicitud puede ser indistinta, se presenta una lista de posibles estados de dicha solicitud y, al igual que los listados previos, se prevé la opción "otro" en caso de que el estado de su solicitud no se encuentre en las opciones disponibles.

En el siguiente apartado podrá especificar el estado de dicha solicitud. Por ejemplo, si presentó una solicitud de atención urgente del Ministerio del Interior, y su estado es "derivado", podrá especificar que, si bien fue derivado hace 30 días, aún no se obtiene respuesta de su solicitud. Luego de ello podrá precisar detalles sobre ¿cuál es el estado actual de sus requerimientos o demandas específicas? ello a fin de poder evaluar el nivel de respuesta o cumplimiento de la autoridad que recibió la solicitud. Por ejemplo, si solicitó dos acciones concretas y a la fecha del reporte solo se ha cumplido con una acción, detallar cuál es la que sí se cumplió y cuál sigue pendiente.

Por lo tanto, podrá especificar si los/las defensores/as están recibiendo algún tipo de apoyo y quiénes los/las están brindando dicho apoyo, si se trata de ONGs aliadas, defensorías del pueblo, federaciones, organismos internacionales, autoridades, entre otros.

Así mismo, se podrá especificar si se trata de un tipo de apoyo comunicacional, legal, financiero, social o técnico, y también detallar los datos de contacto de las organizaciones que estén brindando dicho apoyo, a fin de evaluar posibles sinergias en su defensa.

Finalmente, colocar si los/las defensores/as han comunicado algún tipo de pedido específico para la COICA, por ejemplo, apoyo en la visibilización de su caso a través de acciones comunicacionales, legales, ayuda humanitaria, u otros.

**Paso 3. INFORMACIÓN CONFIDENCIAL**

En este último paso se deberá completar la información de contacto que será manejada de forma confidencial por el equipo que gestione la recepción de la información reportada. Para ello, deberá colocar el nombre de los/as defensores/as indígenas y/o persona de contacto, sus datos de contacto como teléfono y correo electrónico en caso cuenten con ello. Además, se sugiere incluir las coordenadas UTM de la zona en el que se dio el ataque o amenaza, o el territorio que se encuentra bajo amenaza y por el que se encuentran bajo amenaza los defensores, con la finalidad de contar con el punto de georeferenciación para contar con un mapeo de la situación de amenazas en los territorios de la cuenca amazónica.

Posteriormente, colocar la base o comunidad a la que pertenece, la organización nacional base de COICA a la que pertenece, el nombre de la persona que llenó el formulario y la fecha de cuando lo realizó.

Para concluir, a partir de toda la información recabada, el monitor local o punto focal deberá seguir el flujo/ruta de validación de las fichas de emergencia a fin de identificar de manera posterior, y dependiendo de los medios disponibles, la estrategia para la atención de los casos y proponer medidas para este. Así como compartir la información a la coordinación técnica del PDDD.

PROGRAMA DE
Defensores y Defensoras
INDÍGENAS

Los módulos han sido elaborados en el marco del Programa Defensa de Defensores y Defensoras, y el proyecto "Protección de defensores de derechos humanos indígenas en la cuenca Amazónica durante la pandemia COVID-19"


COICA ORG

coica_org

coicamazonia.org

@coicaorg

COICA ORG - Oficial

coica@coicamazonia.org

Calle Sevilla N24-358 y Guipúzcoa - La Floresta
Quito - Ecuador
Casilla postal 17-21-753 (593)23226-744


COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA


CON EL APOYO DE:

OXFAM Danmark

DAR DERECHO AMBIENTE Y RECURSOS NATURALES

PROGRAMA DE Defensores y Defensoras INDÍGENAS

# CICLO DE CAPACITACIÓN

## Minga Digital por los Defensores y Defensoras Indígenas de la Cuenca Amazónica

# MÓDULO 2

## TEMA:

## TÉCNICAS PARA EL LEVANTAMIENTO DE DATOS SOBRE LA SITUACIÓN DE VULNERACIÓN DE DDHH DE DEFENSORES Y DEFENSORAS INDÍGENAS

Programa Defensa de Defensores y Defensoras Indígenas (PDDD) COICA

ABRIL 2022

COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA

# Índice

# HERRAMIENTAS PARA EL MONITOREO DE CASOS DE VULNERACIÓN DE DERECHOS HUMANOS DE DEFENSORES INDÍGENAS EN LA CUENCA AMAZÓNICA

## INTRODUCCIÓN

El monitoreo y documentación de los derechos humanos (DDHH) son herramientas indispensables para investigar, registrar y analizar cualquier tipo de información de acciones o situaciones que violenten los derechos de comunidades o de líderes y lideresas indígenas en la cuenca amazónica ya que permite dar mayor legitimidad a las denuncias y cualquier otra acción que se desarrolle en defensa de las reivindicaciones territoriales, la autodeterminación de los pueblos indígenas y la reafirmación de las luchas por los derechos de los defensores y defensoras indígenas amazónicos.

Estas herramientas permiten tener información, cuantitativa o cualitativa, organizada y pruebas sobre cómo sucedieron los hechos, sus posibles causas y consecuencias a través de estudios de casos puntuales en la zona de monitoreo, en este caso, la cuenca amazónica colombiana y ecuatoriana.

El presente módulo brinda herramientas para el seguimiento, monitoreo y documentación de información con énfasis en los derechos humanos, misma que permitirá desarrollar habilidades en las y los monitores comunitarios para registrar la situación de los defensores y defensoras indígenas de la Amazonía ecuatoriana y colombiana en situación de amenaza, violencia, criminalización, persecución y asesinato.

## ¿Qué es el monitoreo?

Es la investigación planificada y sistemática de una realidad social conducida de acuerdo a un esquema predefinido. Es un elemento de acción no violenta cuyo fin es producir un cambio en esa realidad (IIDH y HR, 2004).

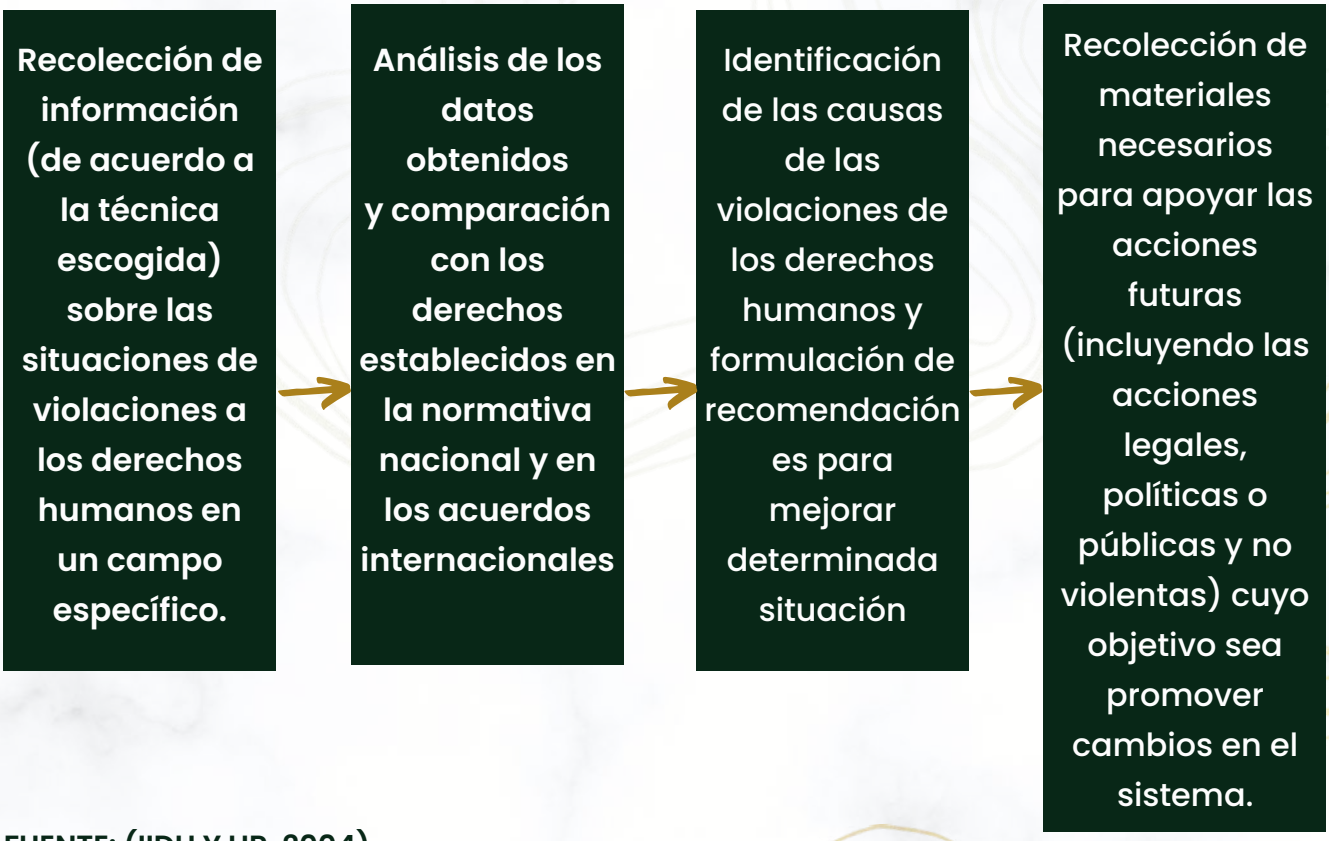
Esta cartilla forma parte del proyecto "Protección de defensores de derechos humanos indígenas en la cuenca Amazónica durante la pandemia COVID-19" ejecutado por la Coordinadora de las Organizaciones Indígenas de la Cuenca Amazónica **(COICA)** y financiado por los aliados OXFAM Ibis- CISU que tiene como finalidad, fortalecer las acciones desarrolladas en el marco del proyecto, así como las estrategias de las organizaciones base para enfrentar la alarmante situación de casos de violencia en contra de líderes y lideresas indígenas en la cuenca amazónica.

La estructura del módulo es la siguiente: primero, se describen las técnicas de levantamiento de información; segundo, se profundiza en el análisis de la técnica de la entrevista; tercero, se recomiendan algunas estrategias para el abordaje de los entrevistados/as; cuarto, se presentan estrategias para el/la monitor/a comunitario/a en el levantamiento de información sensible sobre situación del caso de vulneración de DDHH a defensores y defensoras pueblos indígenas amazónicos y el manejo de la confidencialidad de la información levantada; quinto, se analizan los diferentes tipos de preguntas: preguntas abiertas, cerradas, preguntas de selección múltiple, y respuestas; finalmente, se presentan algunas técnicas para la recopilación de medios probatorios y materiales para incidencia comunicacional (fotos, videos, audios).

## TÉCNICAS PARA EL SEGUIMIENTO, MONITOREO Y DOCUMENTACIÓN DE INFORMACIÓN

Los estudios de monitoreo se realizan para documentar el hecho de que las violaciones a derechos humanos efectivamente existen y recuperar argumentos e información que será necesaria para desarrollar acciones en el futuro. Este tipo de estudios se convierte en el punto de arranque para acciones futuras orientadas al cambio de las condiciones sociales de líderes y lideresas indígenas (IIDH y HR, 2004).

El proceso de monitoreo de los derechos humanos sigue los siguientes pasos:




**FUENTE: (IIDH Y HR, 2004).**

**En este módulo nos interesa conocer las técnicas de investigación que se utilizan para la recolección de información que son las herramientas y procedimientos disponibles para que un monitor o monitora comunitaria pueda obtener dicha información. Estas técnicas pueden ser cualitativas o cuantitativas.**

Las **TÉCNICAS CUALITATIVAS** tienen como objetivo describir determinadas situaciones o procesos en detalle con base a la experiencia y conocimientos de los actores involucrados, en este caso, el de las y los líderes indígenas amazónicas.

Dentro de esta técnica existen diferentes tipos de herramientas para levantar información como:

- Las entrevistas
- La observación de los actores en su contexto
- Las biografías
- Las historias de vida
- Los grupos focales

Las **TÉCNICAS CUANTITATIVAS** tienen como objetivo explicar y predecir determinadas situaciones con base a datos numéricos. Las herramientas para levantar información cuantitativa son:

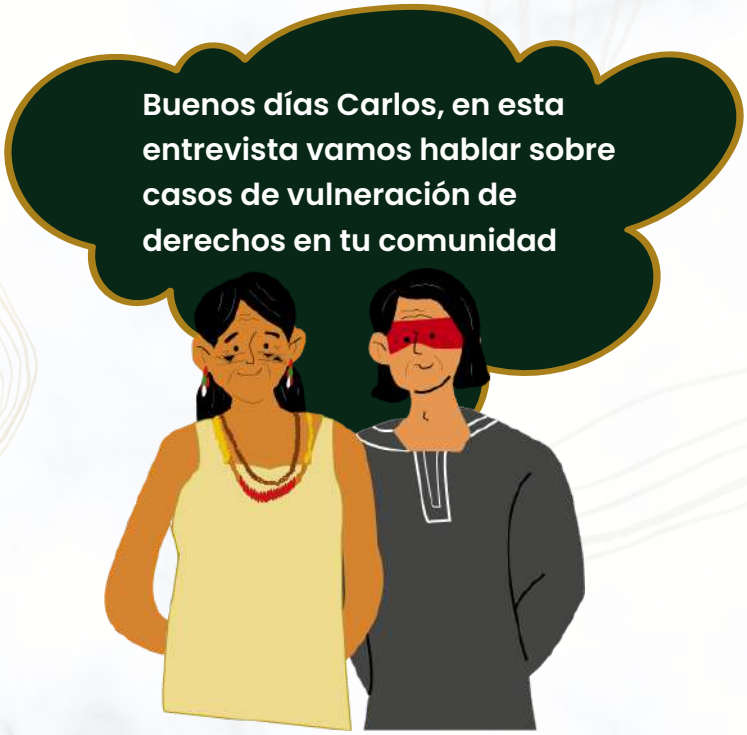
- Censos
- Registros (datos secundarios)
- Cartografía
- Encuestas y cuestionarios

En el monitoreo es más frecuente el uso de técnicas de investigación cualitativa ya que permite el estudio de casos concretos, entendido este como el estudio a profundidad de un evento detallado o de una historia de una persona en concreto, que puede ser utilizado en acciones legales o en campañas informativa (IIDH y HR, 2004).

## TÉCNICA DE LEVANTAMIENTO DE INFORMACIÓN: LA ENTREVISTA

# ¿QUÉ ES UNA ENTREVISTA?

La entrevista es una de las técnicas cuantitativas más comunes para monitorear la realidad social de comunidades, pueblos y nacionalidades. La entrevista consiste en hacerle preguntas directamente a las personas que son víctimas de violación de derechos humanos, para así obtener una aproximación de lo que piensa, siente o ha vivido, que luego podrá ser procesada y presentada en un informe.




En la entrevista, el monitor o monitora comunitaria pretende obtener información relevante de la persona que entrevista de manera directa, en este caso de los líderes o lideresas comunitarias a las que sus derechos han sido violentados. La entrevista suele ser una conversación formal a través de la cual el monitor o monitora es quien toma la iniciativa, ya que es la persona quien realiza las preguntas en todo momento. Sin embargo, la protagonista es la persona entrevistada.

# ¿CÓMO SE REALIZA LA ENTREVISTA?

- **Vía telefónica:** Se realiza a través de una llamada telefónica.
- **Por correo:** Se envía el cuestionario al correo electrónico.
- **Personal:** Se realiza cara a cara.
- **Online:** Se utiliza un medio de internet de comunicación masivo.

## TIPOS DE ENTREVISTAS

Hay tres tipos de entrevistas y depende de los objetivos que tengan las o los monitores comunitarios. Estos se usan dependiendo de la situación en que se necesite realizar una entrevista, se podrá elegir entre una sola opción o una combinación de las siguientes:

### A. ENTREVISTA NO ESTRUCTURADA O LIBRE

Las entrevistas no estructuradas o libres se realizan cuanto no tenemos información suficiente sobre la situación y queremos tener un diagnóstico preliminar para identificar más precisamente el problema. En este tipo de entrevista sólo se define el tema general, lo que permite a la persona que se entrevista discutir sobre todo lo que considera importante. Esta técnica no requiere ningún instrumento escrito (IIDH y HR, 2004).

### B. ENTREVISTA SEMIESTRUCTURADA O SEMILIBRE

Las entrevistas semiestructuradas o semilibres tienen como objeto conocer o abordar una problemática determinada a partir de un guion predeterminado (guía de entrevista) que contiene una lista de preguntas, pero se enlazan otros temas no previstos en la entrevista. Es por eso por lo que se realizan preguntas abiertas con el fin de dar la oportunidad a la persona entrevistada de expresar sus ideas y obtener una información más completa y precisa (IIDH y HR, 2004).

### B. ENTREVISTA ESTRUCTURADA (CON BASE A UN CUESTIONARIO)

Las entrevistas estructuradas o planificadas siguen un orden de preguntas determinadas. Las o los monitores comunitarios planifica las preguntas mediante un cuestionario, o lista de preguntas concretas que serán formuladas a la persona entrevistada. Se empieza con una pregunta general; después, teniendo presente qué tipo de información se necesita, se escribe las preguntas específicas en el cuestionario.

Las preguntas pueden ser **a) CERRADAS** (donde se da una lista de posibles contestaciones):

**Ejemplo:**

**IDENTIFICACIÓN DEL DEFENSOR O DEFENSORA INDÍGENA**

**Indique su país:**

- Colombia
- Bolivia
- Brasil
- Ecuador
- Guyana
- Guyana Francesa
- Perú
- Surinam
- Venezuela

O preguntas **b) ABIERTAS** (donde la persona entrevistada responde dicha pregunta y, el o la monitora comunitaria anota la contestación de la persona entrevistada en detalle) (IIDH y HR, 2004).

**Ejemplo:**

¿Cuál es la comunidad, resguardo y/o localidad?

**¿Puede describir brevemente los sucesos de la amenaza o ataque?**

Las preguntas que son **b) PARCIALMENTE ABIERTAS O MIXTAS** aportan una lista de posibles contestaciones, pero también permiten contestaciones que no están en la lista:

**Ejemplo:**

**IDENTIFICACIÓN DEL RIESGO/ATAQUE**

**¿Cuál fue la amenaza o ataque? ***

- Amenaza (acoso y hostilización/intimidación /insinuaciones o amenazas de violación)
- Criminalización (acoso judicial)
- Violencia física
- Violencia psicológica
- Riesgo a la integridad
- Difamación
- Detenciones arbitrarias
- Violencia de género (física/psicológica/sexual y económica)
- Actos de tortura u otros tratos crueles e inhumanos Secuestro
- Asesinatos
- Afectaciones al territorio
- Daños ambientales (contaminación/derrames)
- Daños a la comunidad (Tentativa de división de la comunidad/tentativa de compra de miembros de la comunidad/deslegitimación de líderes)
- Otro

**Si escogió "OTRO"; por favor indicar aquí:**

## PASOS A SEGUIR ANTES, DURANTE Y DESPUÉS DE LA ENTREVISTA

Las entrevistas a personas víctimas y/o testigos de casos de violación de derechos humanos se pueden realizar mediante los siguientes pasos:


### A) PREPARACIÓN DE LA ENTREVISTA Y CONTACTO PREVIO

El primer paso para elaborar una entrevista es determinar con anticipación los objetivos en función de los temas que se van a tratar, así como, identificar las personas que van a ser entrevistadas con quienes se establece un contacto previo dentro de una atmósfera relajante que permita una comunicación abierta. A cada entrevistado/a, víctima o testigo, se bebe informar que será entrevistada separadamente y en privado para evitar el "efecto simpatía" entre ellos y que uno aprenda los hechos del otro y disminuya la objetividad de la información a recoger (Beltran, s/f). Cuando puedan existir problemas de seguridad (para las personas a entrevistar) se desaconseja la entrevista sobre el terreno, hay que intentar conseguir que se desplacen a un lugar seguro. Dichas condiciones se establecen en el contacto inicial (Beltran s/f).

En esta fase se debe formular las preguntas y secuenciarlas poniendo especial atención en la terminología y en el vocabulario que se utilice, que debe resultar significativo y familiar para las personas entrevistadas. En cuanto a las preguntas, deben estar contextualizadas, evitar ambigüedades, confusiones o dobles sentidos. No deben conducir a una respuesta determinada.

## B) INICIO DE LA ENTREVISTA

En el inicio de la entrevista se recomienda empezar con una explicación clara de la finalidad perseguida. Los primeros minutos de una entrevista son decisivos para poder lograr el éxito, ya que depende en gran medida de la familiarización que establezca la persona entrevistada.

Es mejor que la o el monitor comunitario hable primero, que brinde confianza. Se debe explicar en primer lugar su nombre y cargo en la organización. Después se detalla el trabajo concreto que se está haciendo. Se debe explicar que se va a formular una serie de preguntas bien concretas y que trate de ceñirse o limitarse a las mismas. Se le debe preguntar si desea mantenerse anónimo o si prefiere que el caso se haga público. Se debe explicar claramente si hay algún riesgo en este último caso (Beltrán, s/f).

## C) DESARROLLO DE LA ENTREVISTA

El desarrollo de la entrevista se centra en la forma de interacción que se lleva a cabo para establecer una conversación con la persona entrevistada. Es recomendable trabajar con una entrevista estructurada, con un cuestionario previo que incluyan primero preguntas abiertas y luego preguntas más concretas o cerradas. Se deben tomar notas detalladas de las respuestas, incluyendo una impresión general y credibilidad de las circunstancias y del testigo, circunstancias en que se llevó a cabo la entrevista, y, a menos de que no se pueda por razones de seguridad, se debe mantener anotadas las fuentes y contactos.

Durante el desarrollo de las entrevistas hay que tener cuidado con la utilización de grabadoras o vídeos durante la entrevista. Pueden intimidar al testigo, pueden violar su privacidad o pueden incitarle a “actuar” durante la entrevista, o se debe consultar al entrevistado/a si es posible grabar antes de iniciar la entrevista.

## D) CIERRE DE LA ENTREVISTA

Esta fase es casi tan importante como la del inicio. Antes de terminar hay que verificar los datos recopilados, si no quedó ningún punto sin investigar y si el entrevistado/a no desea añadir algo más. Es recomendable terminar dando una idea general de lo que se va a hacer con la información.

## ESTRATEGIAS PARA EL ABORDAJE DE LOS ENTREVISTADOS/AS

La entrevista a personas que han sufrido o presenciado situaciones de amenaza, violencia, criminalización, persecución y asesinato, es una de las herramientas de investigación de mayor importancia, potencialidad, etc. Pero, al mismo tiempo, es una labor compleja, delicada y de alta sensibilidad que implica importantes cuestiones éticas y de seguridad (Beltrán, s/f). Por lo anterior, se deberá tener en mente los siguientes puntos:

- Respetar los puntos de vista del entrevistado/a, adoptando una actitud imparcial y abierta frente a las ideas que exponga. Además, siempre mostrar interés por la persona entrevistada, de lo contrario le hará sentir incómoda.
- No interponer su ideología, sus sentimientos o sus propios prejuicios en la entrevista.
- Mantener una actitud abierta y positiva que favorezca y facilite la comunicación: utilizar un lenguaje que resulte familiar y significativo para el entrevistado/a.
- Establecer las condiciones de confiabilidad y difusión de la información.
- La relación monitor/a-entrevistado/a tiene que ser amistosa, pero no servicial, ni autoritaria o paternalista.
- Víctimas de tortura, violencia sexual y otras formas de graves violaciones de derechos humanos no deben ser entrevistas a menos que existan mecanismos disponibles de apoyo (por ejemplo, la presencia de un familiar o servicios sociales y asistencia psicológica especializada).

Mujeres que pueden hablar sobre violación u otras formas de violencia contra las mujeres no deben ser entrevistadas sin el consejo o acompañamiento de profesionales de servicios sociales que contribuyan a evitar la revictimización durante la entrevista.

## MANEJO DE LA CONFIDENCIALIDAD Y EL CONSENTIMIENTO INFORMADO

La confidencialidad es uno de los principios fundamentales dentro del monitoreo y un elemento central en la relación entre la organización, las monitoras y monitores comunitarios y las personas entrevistadas, en especial en el caso de las víctimas de violaciones de derechos humanos. Por ello, la regla general es que toda la información que suministran será confidencial a menos que se autorice su difusión a través de medios públicos (Beltrán, s/f).

La información que se genere en casos de agresiones tiene profundas implicaciones dado que puede poner en riesgo a dicha persona (o sus familiares) de sufrir nuevas violaciones de derechos humanos. La confidencialidad está, por tanto, indisolublemente unida a la seguridad (Beltrán, s/n). Al inicio de la entrevista se deben establecer los siguientes principios de confidencialidad:

- Información previa: el monitor/a informa a la persona entrevistada sobre el objetivo de la entrevista incluido el resultado que se espera conseguir.
- Voluntariedad: la persona facilita la información de forma voluntaria, sin coerción, manipulación.
- Compresión y competencia: la persona entrevistada comprende la información que proporciona, así como las implicaciones de su participación.
- Se llega a un acuerdo sobre cómo se utilizará su caso, para qué fines, en qué materiales, de qué manera, con qué restricciones.
- Se garantiza la seguridad y confidencialidad de forma que se reduzca al mínimo los riesgos de seguridad.

**Fuente: Beltrán, s/f.**

Estos principios garantizan que las personas toman decisiones libres e informadas sobre la información que proporcionan y cómo esta se utilizará. También implican que la organización debe obtener su consentimiento previo e informado para actuar a su favor, investigar y documentarse sobre su caso, publicitarlo, utilizar (o no) sus datos personales o imágenes suyas durante la investigación, en los productos finales o en los materiales de campañas comunicacionales posteriores (Beltrán, s/f).

Las y los monitores tiene que garantizar que durante todo el proyecto de investigación-acción (e incluso posteriormente) se respetan los deseos de la persona en relación con la utilización de la información sobre su caso y que, por tanto, no se utilizará para otros objetivos o campañas para los que no exista su consentimiento. Se asegurará que, durante la entrevista, se registra en un soporte el acuerdo sobre el consentimiento informado. Sin ese registro documental el consentimiento no será válido (Beltrán, s/f).

## RECOMENDACIONES GENERALES PARA REALIZAR ENTREVISTAS

A continuación, se describen algunas recomendaciones para llevar a cabo un proceso exitoso en la tarea del monitoreo:

- Mantener el anonimato de los entrevistados: en cualquier entrevista, la colaboración de los entrevistados/as es totalmente voluntaria en todas sus fases. Es por eso que en ningún momento han de desconocer el propósito último de la finalidad de la entrevista y de su colaboración. El anonimato de los entrevistados debe ser estrictamente respetado en caso de que éstos no quieran revelar su identidad.
- El monitor/a debe adoptar todas las precauciones razonables para asegurar que las y los entrevistados no se vean directa o indirectamente perjudicados como consecuencia de su participación en la entrevista.
- Se debe prestar especial atención en la ejecución de entrevistas a menores de edad, sean niños o adolescentes. Por tanto, deberá obtenerse el consentimiento informado de los padres o de un adulto responsable.
- Los entrevistados/as deberán ser informados (normalmente al comienzo de la entrevista) si se están utilizando técnicas de observación o sistemas de grabación, excepto cuando estos se utilicen en lugares públicos. Si un entrevistado así lo deseara, la grabación o parte relevante de la misma deberá ser destruida o borrada. El anonimato de los entrevistados no debe infringirse por el uso de tales métodos.

PROGRAMA DE
Defensores y Defensoras
INDÍGENAS

Los módulos han sido elaborados en el marco del Programa Defensa de Defensores y Defensoras, y el proyecto "Protección de defensores de derechos humanos indígenas en la cuenca Amazónica durante la pandemia COVID-19"


COICA ORG

coica_org

coicamazonia.org

@coicaorg

COICA ORG - Oficial

coica@coicamazonia.org

Calle Sevilla N24-358 y Guipúzcoa - La Floresta
Quito - Ecuador
Casilla postal 17-21-753 (593)23226-744


COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA


CON EL APOYO DE:

OXFAM
Danmark

- Las entrevistas más fáciles, que mejor se pueden preparar y realizar son las que se llevan a cabo con miembros de base de las organizaciones o comunidades. Sin embargo, es necesario entrevistar también a los dirigentes de las organizaciones o comunidades.

# Bibliografía


Beltrán, Esteban (s/f). "Investigación de violaciones de derechos humanos y crímenes de derecho internacional". Disponible en: http://www.derechoshumanos.unlp.edu.ar/assets/files/T%C3%A9cnicas%20de%20Investigaci%C3%B3n..pdf

Instituto Interamericano de Derechos Humanos y Fundación Helsinki para los Derechos Humanos (2004). Monitoreo de los derechos humanos. San José, C.R.

Rull Oscar, et al. (2022). "Como elaborar una entrevista". Disponible en https://sites.google.com/site/redacespecializada/home/cmo-elaborar-una-entrevista

Ruiz Garzon F. (15 de mayo 2021). Como elaborar una entrevista. Disponible en https://www.mat.uson.mx/~jldiaz/ProyectosCD/como_elaborar_entrevistas.pdf

OAS, (3 de febrero del 2020). Recomendaciones generales de cómo hacer una entrevista. Disponible en: https://www.oas.org/juridico/PDFs/mesicic4_ven_rec_gen_rea_entrev.pdf

Cevallos Roberto, (2020). "Catedra de mediación de impacto, Levanta de información Cualitativa". Disponible en: https://terraetica.com/levantamiento-de-informacion-cualitativa-y-cuantitativa.

Hendel Liliana, (2017). "Comunicación, infancia y adolescencia. Guía para periodistas perspectiva de género". Disponible en: https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM1_PerspectivaGenero_WEB.pdf



**Elaborado por:**
**Nataly Torres Guzmán. Eco. Mgt.**
**Consultora**

PROGRAMA DE Defensores y Defensoras INDÍGENAS

# CICLO DE CAPACITACIÓN

## Minga Digital por los Defensores y Defensoras Indígenas de la Cuenca Amazónica

# MÓDULO 3

## TEMA:

**CAPACITACIÓN EN TÉCNICAS PARA EL USO DE GPS Y APLICATIVOS MÓVILES PARA EL LEVANTAMIENTO DE COORDENADAS DE PUNTOS EN LOS QUE HAN OCURRIDO VULNERACIONES DE DDHH A DEFENSORES Y DEFENSORAS INDÍGENAS EN LA AMAZONÍA DE ECUADOR Y COLOMBIA**

**Programa Defensa de Defensores y Defensoras Indígenas (PDDD) COICA**

**ABRIL 2022**

COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA

# CONTENIDO

# CONTENIDO

# CONTENIDO

# CONTENIDO

# I. OBJETIVO

## 1.1. Objetivo general

Fortalecer las redes de seguimiento, monitoreo y documentación de la situación de vulneración de derechos de los defensores y defensoras del territorio amazónico.

# II. CONCEPTUALIZACIÓN DE GPS

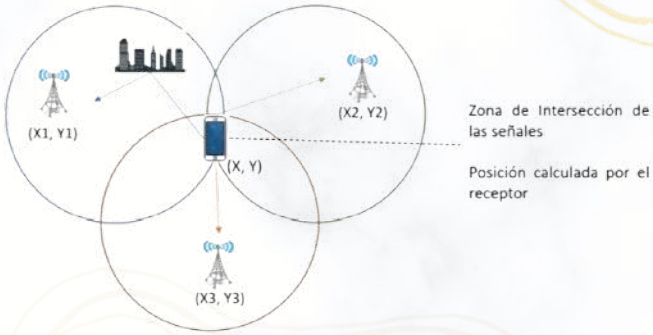
Sistema de Posicionamiento Global GPS, es la revolución en navegación tecnológica que sitúa la localización del usuario en cualquier parte del mundo las 24 horas al día, bajo cualquier condición climática.

El GPS fuñe diseñado por el Departamento de Defensa de los Estados Unidos para uso militar. El sistema GPS se hizo activo a los civiles para utilizarse en aviación, la marina y en el mercado para el recreo. En la actualidad miles de personas utilizan la precisión y la tecnología para realizar deportes, pescar, volar, rastreo para seguridad o practicar el trecking (viajar).

El GPS opera con una constelación de 24 satélites que orbitan alrededor de la tierra. Estos satélites transmiten señales que contienen datos de la hora y orbita para calcular la posición del satélite y los datos de almanaque (registro de datos todos los días del año). Los receptores que se utilizan en la tierra, mar o aire buscan los satélites por el cielo. El GPS necesita recibir buenas señales por lo menos de tres satélites para determinar una posición en la superficie de la tierra.

**Ilustración 1. Satélites (24) que rodean la tierra a 17.700 kilómetros**

**Ilustración 2. Funcionamiento del sistema de posicionamiento GPS**




Para adquirir una posición tridimensional será necesaria una cuarta señal, esta posición determinara la altura o la altitud. En resumen, se requieren como mínimo **cuatro satélites** para la navegación tridimensional (que incluye la altitud) y sólo tres satélites para la navegación bidimensional (sin altitud) sobre la superficie terrestre.

# III. MANUAL PARA EL USO DEL GPS

El presente manual está destinado a proporcionar una comprensión básica de manejo del GPS Garmin eTrex (versión 10, 20 o 30), que puede ayudar a apoyar sus necesidades de georreferenciación y levantamiento de información.

Los receptores GPS ETrex son bastante resistentes. Sin embargo, se debe comprender que estos receptores son pequeñas computadoras, y por lo tanto, debe ser tratado con cuidado. Por ejemplo, nunca guarde el GPS bajo la luz directa del sol o en zonas calientes (baúles de automóviles). Cuando no estás usando su GPS durante largos períodos de tiempo (más de 2 meses), se recomienda quitar las pilas.

El eTrex GPS es totalmente resistente al agua y a prueba de polvo, sin embargo, **no flota**, se debe limpiar el exterior de su receptor GPS simplemente con un trapo húmedo.

Además, cabe señalar que el GPS cuenta con antenas internas. Las antenas se encuentran en la parte superior del GPS (encima de "eTrex"), por lo que se recomienda no obstruir las antenas cuando esté operando su GPS.

La mayoría de los GPS no funcionan en el interior de un edificio, bajo tierra o bajo el agua. Para obtener lo mejor recepción, el GPS requerirá una recepción sin obstrucciones, con cielo despejado. Sin embargo, con el nuevo alto chip GPS de sensibilidad, el eTrex puede recibir consistentemente señales fuertes bajo la densa copa de los árboles.

Se recomienda contar con repuestos de baterías, debido a que el GPS requerirá baterías nuevas (#2 AA) aproximadamente cada 22 horas de uso. El GPS también viene con un cable USB. Este cable se utiliza para conectar al computador. Esto le permitirá descargar o cargar coordenadas, y puede facilitar datos de campo colección.

## 3.1. CONOCIENDO EL GPS

El GPS eTrex 10, 20 o 30 cuenta con seis que debemos estar familiarizados. Estos botones incluyen:

1. 1. El botón de encendido/retroiluminación.
2. El botón Click-Stick o botón controlador.
3. El botón atrás.
4. El botón de alejamiento.
5. El botón de acercamiento.
6. El botón de menú.

Ilustración 3. GPS Garmin eTrex10


**1. El botón de encendido (power):** Es el botón que enciende el GPS. Permite encender y apagar. Este botón también encenderá la luz de fondo (para que pueda usar el GPS por la noche). Tenga en cuenta que el uso de la luz de fondo consumirá las baterías más rápido.

**2. El Click-Stick (controlador mouse):** El Click-Stick es muy similar a un mouse de computadora. Los Click-stick permitirá navegar a diferentes opciones de menú, empujando el Click-stick en una dirección (izquierda o derecha; arriba o abajo). Además, puede utilizar el Click-Stick como botón (pulsando hacia abajo o "adentro") para activar las selecciones resaltadas. Empujando el Click-Stick "in" es similar a hacer clic con el mouse o presionar la tecla "enter" en un teclado de computadora.

Ilustración 4. El Click-Stick funciona como el mouse de la computadora

**3. El botón atrás:** Se usa para salir de un menú o página.

**4. El botón Zoom-out o alejamiento:** Desde la página del mapa, al presionar este botón se habilitará para alejar el mapa. Desde cualquier otra página, presione para desplazarse o mover un control deslizante resaltado hacia arriba.

**5. El botón Zoom-in o acercamiento:** Desde la página del mapa, al presionar este botón se habilitará usted para hacer zoom en el mapa. Desde cualquier otra página, presione para desplazarse o mover un control deslizante resaltado hacia abajo.

**6. El botón Menú:** Presiónelo y suéltelo una vez para ver el Menú de opciones para un página o presione y suelte una segunda vez para mostrar el menú principal desde cualquier página. Si presiona y suelta una vez para ver un menú de Opciones para una página específica y desea salir de ella, asegúrese de presionar el botón Atrás **(no el botón Menú por segunda vez, porque le hará regresar a la página principal de Menú).**

Ilustración 5. Menú principal


## 3.2. PRIMEROS PASOS PARA EL USO DEL GPS

El GPS tiene muchas capacidades y funcionalidades. Esta sección del manual está destinada para mostrar cómo comenzar a usar el GPS y para presentar algunas de las principales capacidades de los GPS que pueden respaldar directamente sus necesidades.

**Waypoints:** Los waypoints son ubicaciones que se graban y se guardan en el dispositivo. Los waypoints pueden marcar dónde estás, a dónde vas o dónde has estado. Puedes añadir detalles sobre la ubicación, como el nombre, la altura o la profundidad. Puedes añadir un archivo **.gpx** que contenga waypoints transfiriendo el archivo a la carpeta GPX

**Empezando...**

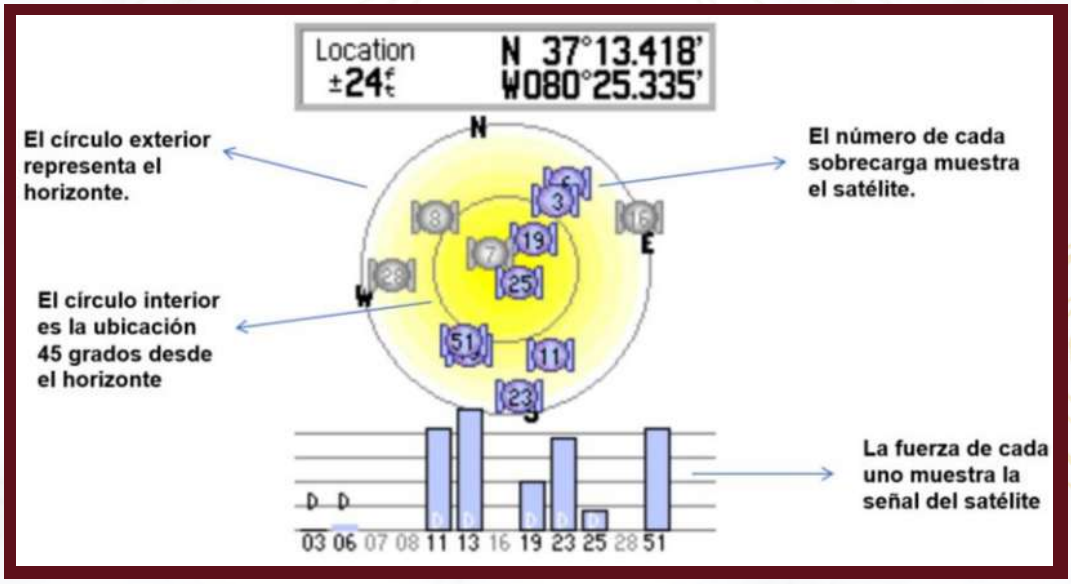
Encienda el GPS presionando el botón de encendido. Utilice el botón Menú para ir a la pantalla principal. **Ir a Menú,** luego seleccione la opción Satélite para ver los satélites actuales.

Normalmente, el GPS tarda un par de minutos en **"localizarse"** en los satélites y determinar una localización. Inicialmente, la ventana de estado puede leer: **Espere... rastreando satélites.**

El GPS estará listo para usar cuando desaparezca la página del satélite y se muestre la página del **mapa**. La página de satélite se puede ver en cualquier momento yendo a la página de menú y seleccionando página de satélite.

Una vez que el receptor GPS esté listo para navegar, se mostrará una ubicación (coordenadas x, y) y un error (±24 pies o 7.3 m) para la ubicación. Aparecerá en la sección superior de la página del satélite.

**Ilustración 6. Pantalla de satélites**



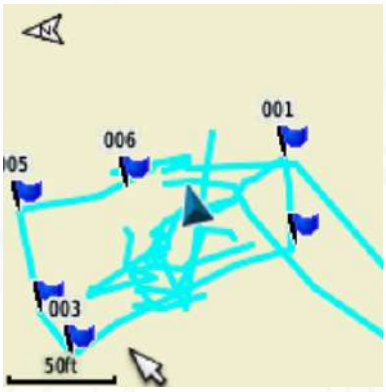

El GPS ahora se ha inicializado y está listo para usarse. El GPS se puede utilizar, por ejemplo, para:

- Identificar y marcar áreas dentro de los árboles para referencia futura (parcelas de investigación, áreas de infestación, etc.).
- Estimar las medidas del área de un campo.
- Estimar el perímetro de un campo (estimar la longitud de la línea de la cerca).

## 3.2.1. PÁGINA DEL MAPA

La Página de Mapa le permite visualizar sus Waypoints y Tracks como mapas que se encuentran en pantalla. Puede acceder desde Menú principal > Mapas. Tiene la capacidad de acercar y alejar estos mapas para obtener más o menos detalle (Ilustración 7).

Ilustración 7. Página del mapa




Su GPS tiene algunos datos de referencia mínimos (eTrex 10 contiene poblados, límites; eTrex 20 y 30 contiene calles principales e interestatales, sombreado en relieve) integrado en el GPS (Ilustración 8). Si usted tiene el modelo eTrex 20 o 30, también puede obtener (es decir, comprar) mapas topográficos digitales y otras imágenes que se puede descargar a su unidad GPS para fines de referencia (de GARMIN en http://comprar.garmin.com). Sin embargo, tenga en cuenta que cualquier mapa que descargue ocupará espacio en la memoria de su unidad (1,7 GB en eTrex 30).

Ilustración 8. Página de mapa 2 con relieve


## 3.2.2. APLICACIÓN 1: PÁGINA DE NAVEGACIÓN (THE TRIP COMPUTER PAGE)

La página de la computadora de viaje también se puede usar para estimar el perímetro o las medidas de distancia.

La página de la computadora de viaje no es tan aplicable para la medición como las opciones descritas anteriormente para estimar el área y el perímetro (ver Aplicación anterior). Sin embargo, las funciones asociadas con la página de la computadora de viaje es algo con lo que debe estar familiarizado. Para estimar el perímetro o la distancia utilizando la página de la computadora de viaje, siga estos pasos.

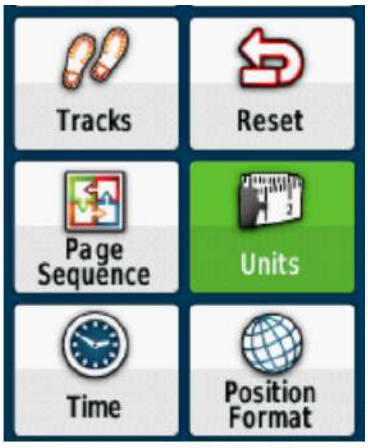
1. Es posible que deba configurar su GPS para asegurarse de que las medidas del perímetro se calculen en metros/hectáreas (por defecto, las unidades de medida están en millas). Para cambiar las unidades de medida, navegue al menú principal (haga clic en el botón Menú dos veces) .

Nota: si se utiliza la opción predeterminada de "estatuto o statute", obtendrá las mediciones del odómetro de viaje en pies hasta que la distancia llegue a 528' (0.1mi.), momento en el cual el receptor cambia automáticamente a centésimas de milla (sin que se utilicen nunca las hectáreas).
Si se selecciona la opción "metros", obtendrá las mediciones del odómetro de viaje en metros hasta que la distancia alcanza 914 metros o las 1000 yardas, momento en el que el receptor cambia automáticamente a centésimas de una milla (sin que se usen nunca los pies). Por estas razones, se sugiere que utilice el técnicas descritas en la Aplicación #3 para estimar medidas de área y perímetro.

Recuerde que 1 yarda = 0,915 metros; 1 pie = 0,305 metros.

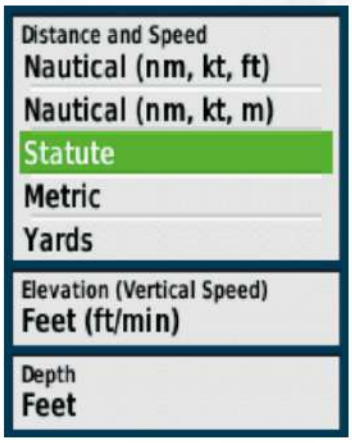
a) En la página del menú principal, use el botón de clic (Click-stick) para seleccionar Configuración (Setup.). En la página del menú de configuración, seleccione Unidades (Units)(ilustración 9) y aparecerá la página de configuración de unidades.

**Ilustración 9. Configuración de unidades (verde)**



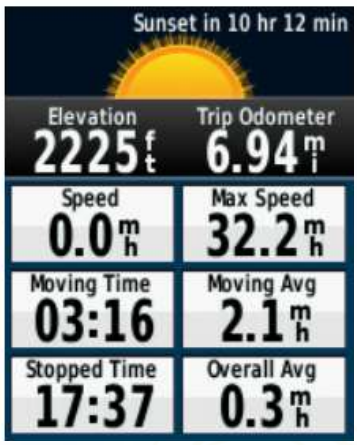
b) En la página de configuración de unidades (Units Setup Page), use el botón de clic (Click-stick) para desplazarse hacia abajo y resaltar Distancia/Velocidad (Distance/Speed). Presiona el Click-stick y aparecerá un menú. En los elementos del menú, seleccione Metric (metros) (Ilustración 10). Esto le permitirá ver las medidas del perímetro en metros (si escoge Statute le permitirá ver el perímetro en pies). Ahora está listo para usar el receptor GPS para calcular el perímetro de un área.

**Ilustración 10. Definir la Unidad de medida**




2. Una vez que haya configurado la unidad para medir el perímetro en unidades estatutarias, vuelva al Menú principal (presione el botón Menú dos veces) y luego seleccione la página Computadora de viaje (**Trip Computer** page) (Ilustración 11).

**Ilustración 11. Configuración de la página de navegación**




3. Para estimar el perímetro de un área, trabajará con la función Odómetro de viaje (Trip Odometer function) en la PÁGINA Ordenador de Viaje (Trip Computer Page). Antes de comenzar, asegúrese de que el odómetro de viaje esté configurado en "cero". Si el odómetro no está en cero, siga estos pasos:

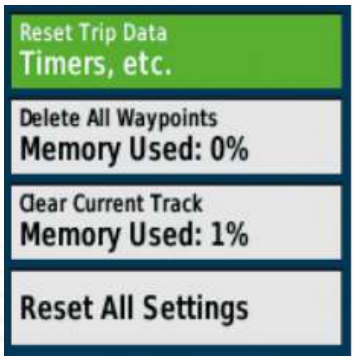
a) Haga clic en el botón Menú una vez para que aparezcan las opciones del Menú de la computadora de viaje.

b) Presione directamente hacia abajo el Click-stick para abrir la página Restablecer (Reset page) (Ilustración 12).

Ilustración 12. Página de restablecer

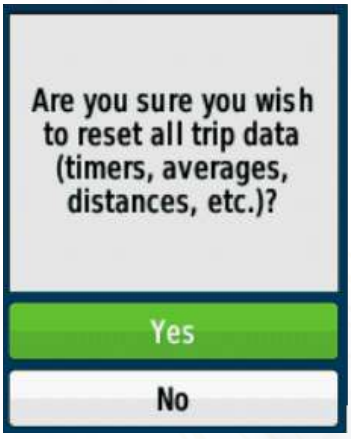

c) Use el botón de clic para seleccionar la opción Restablecer datos de viaje (**Reset Trip Data**) (ilustración 13).

Ilustración 13. Restablecer 2




d) Utilice el botón de clic (click-stick to) para seleccionar Sí (Ilustración 14).

Ilustración 14. Para restablecer



e) Su odómetro de viaje ahora está configurado en cero y está listo para usar. Pulse el botón Atrás (**Back**) y vaya a la página del ordenador de viaje (**Trip Computer Page**.).

4. Ahora que su odómetro de viaje está configurado en cero, comience a caminar por el campo (estacionamiento, o cualquier característica...). Observe que el odómetro cambia a medida que camina. Cuando termine de caminar por el campo, deberá anotar la lectura del odómetro de viaje en un cuaderno. No hay forma de guardar los números del odómetro de viaje dentro del GPS.

### 3.2.3. APLICACIÓN 2: MARCAR Y GUARDAR PUNTOS DE RUTA

Los waypoints permiten marcar y registrar su ubicación actual. Un waypoint es una ubicación "virtual".

Una vez que se establece y guarda un waypoint, puede volver fácilmente al waypoint. Esto es útil para ubicar parcelas de investigación, identificar y reubicar fuentes de contaminación, o para identificar y marcar áreas específicas en un área que ha sido impactada por algún conflicto o enfermedad (al que quizás desee volver en una fecha posterior).

También es posible cargar Waypoints a una computadora de escritorio (usando DNR Garmin o GPS Utility o un programa de software similar).

- Para marcar y guardar su ubicación actual como waypoint:

1. Usted debe caminar hasta el punto en el que desea obtener un waypoint (una ubicación en un puesto con problemas, un área dentro de una parcela que pueden requerir atención adicional, etc.).
2. Presione y sostenga el Click-Stick hasta que aparezca la página Waypoint (Waypoint Page). También puede ir al Menú principal y seleccionar Marcar punto de referencia (Mark Waypoint.).

Ilustración 15. Marcar Waypoint


3. Este GPS asigna automáticamente números de 3 dígitos a los waypoints (en este ejemplo, asignó 001 como el nombre del waypoint). Usted puede personalizar el nombre del punto de referencia.
Para cambiar el nombre del Waypoint, utilice el Click-Stick para resaltar el campo del nombre del waypoint (en el campo de nombre es 001) y haga clic hacia abajo.

4. Escriba el nuevo nombre para el Waypoint, usando el Click-Stick para seleccionar e ingrese los caracteres desde el teclado en pantalla y seleccione **Listo (o Done)** (en letra pequeña, en la parte inferior de la pantalla).

Ilustración 16. Cambiar nombre de waypoint

5. También puede cambiar el símbolo del marcador asociado con el waypoint seleccionando el marcador (con el Click-Stick) y desplazándose por las diferentes opciones. Puedes acceder a más marcadores opciones seleccionando **Puntos de interés o Aire libre** (Points of Interest or Outdoors) en la parte inferior del menú Marcadores (Markers menu).
6. Use el Click-Stick para desplazarse hacia abajo hasta el botón **Listo** (Ilustración 17), cuando seleccione esto, guardará el Waypoint y lo llevará de vuelta a el menú principal **(Main Menu).**

**Ilustración 17. Cambiar de símbolo**


## 3.2.4. APLICACIÓN 3: ENCONTRAR (NAVEGAR HACIA UN WAYPOINT)

El GPS puede servir como un "piloto automático" para navegar de regreso a un Waypoint previamente definido.

- Para navegar de regreso a un waypoint definido previamente, siga estos pasos:

1. Vaya al Menú principal (haga clic en Menú dos veces) y seleccione ¿A dónde? **(Where to).**

**Ilustración 18. ícono a dónde?**

2. Sobre ¿A dónde? **(Where to)**, menú, seleccione **Waypoints** usando el Click-Stick.

1. Use el Click-Stick para seleccionar el Waypoint deseado de la lista (los waypoints suelen en orden alfabético.

**Ilustración 19. Lista de puntos**


3. Seleccione **Ir (Go to)** para crear una línea directa de viaje hasta el Waypoint.

**Ilustración 20. Página ir (go)**

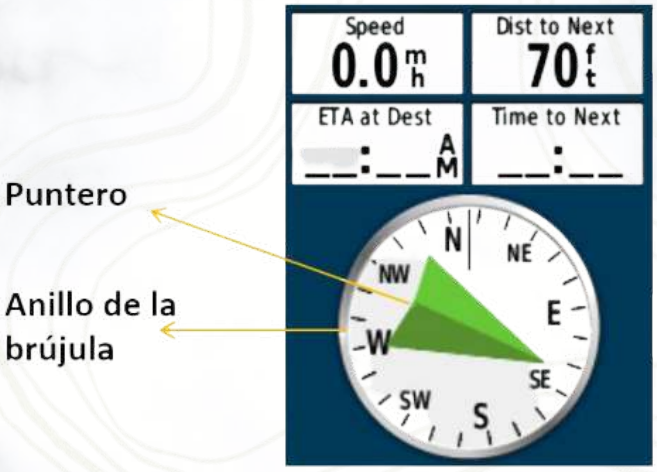

La página del mapa es la página de navegación predeterminada (ilustración 14). En la parte superior de la página habrá navegación direcciones. Estas indicaciones, te indicarán un punto cardinal que te llevará a tu destino (Punto de ruta).

Para usar la **página de la brújula** para la navegación (ilustración 15),vaya al **Menú principal** nuevamente (haga clic en el botón Menú dos veces) y vaya a la página de Brújula (Compass). La flecha en el centro de la brújula sirve como rumbo.

Ponga el puntero, que le dirige al waypoint de destino. La página de navegación también le informa si usted está cerca está del waypoint. También podemos ver la velocidad actual (0 millas/hora), así como una hora estimada de llegada (ETA).

Para dejar de navegar presione el botón Menú dos veces, vaya a Dónde **(Where)** ¿Para? **(To)** y selecciona Detener la navegación **(stop navigation).**

**Ilustración 21. Pantalla de la brújula**




## 3.2.5. APLICACIÓN 4: ENCONTRAR (NAVEGAR HACIA UN WAYPOINT) QUE FUE DEFINIDO POR OTRA PERSONA

Es posible que usted deba navegar a un punto de ruta definido por otra persona (es decir, un propietario, compañero, o un compañero especialista). Esta persona puede haber usado un receptor GPS diferente (o incluso un modelo) y, por lo tanto, puede proporcionarle información de coordenadas (o también puede obtener información de coordenadas de una Información Sistema Geográfico u otro mapa).

Obviamente, su GPS no puede llevarlo a un par de coordenadas (es decir, latitud/longitud, UTM, etc.) si las coordenadas no se almacenan en su GPS como waypoint. Sin embargo, puede crear un waypoint ingresando manualmente información de coordenadas (es decir, latitud/longitud, UTM, etc.) en el receptor GPS.

- Para crear un Waypoint manualmente ingresando sus coordenadas, siga estos pasos:

1. Presione y mantenga presionado el botón de clic para acceder a la página Marcar punto de ruta **(Mark Waypoint Page).**
2. Con el botón de clic, resalte el campo de ubicación (Location Field) en la Pagina Marcar punto de ruta (Mark Waypoint Page) (Ilustración 14). Presiona hacia abajo para seleccionar (marcar en área color verde).

**Ilustración 22. Marcar Waypoint**


3. Ingrese las nuevas coordenadas usando el teclado numérico en la pantalla y las flechas para seleccionar diferentes partes del número de coordenadas (Ilustración 17). Resalte y presione Listo **(Done)** cuando haya terminado.

**Ilustración 23. Colocar nuevas coordenadas**


4. Una vez que las coordenadas del Waypoint se hayan ingresado y guardado manualmente, a continuación, puede utilizar la opción **¿A dónde? (Where to)** función (ver página anterior) para navegar a ese punto de ruta.

Consejo importante: en los Estados Unidos, la primera coordenada (latitudinal) siempre tendrá una "N" como prefijo (ya que se encuentran al norte del Ecuador). La segunda coordenada (longitudinal) siempre tendrá un "W" como prefijo (ya que estamos al oeste del primer meridiano). Además, el primer dígito después de la "W" debe ingresarse como un "cero" (vea la ilustración anterior).

En el caso de Ecuador y Colombia , la primera coordenada (latitudinal) siempre tendrá una "S" como prefijo (ya que se encuentran al sur del Ecuador).

Es muy importante identificar y seleccionar ¡Estos prefijos al ingresar puntos de referencia manualmente en su GPS!

## 3.2.6. APLICACIÓN 5: ESTIMACIÓN DE ÁREAS (MEDIDAS DE ÁREAS)

La estimación de medidas de área en el campo es una tarea necesaria para muchas áreas de aplicación en medición, incluyendo la planificación territorial, la silvicultura y la gestión de los recursos naturales.

Este GPS tiene la capacidad para estimar medidas de área, ¡incluso de polígonos curvos y de forma irregular.

Hay dos métodos para calcular una estimación de área:

1. Herramienta de cálculo de área en la unidad GPS (utiliza pistas o (uses Tracks)).
2. El método de la ruta (The Route method).

Los modelos **Garmin eTrex** hacen que los cálculos de área sean bastante simples. Es importante tener en cuenta que las estimaciones de área tomadas con estas unidades de GPS son solo estimaciones. Muchas variables pueden cambiar el cálculo del área cuando se utiliza el primer método, incluida la cantidad de satélites disponibles y la velocidad de la persona caminando el límite.

- **Estimación de medidas de área, opción 1. Herramientas de cálculo de área (Area Calculation Tool).**

## Descripción general y configuración

A medida que recorre el perímetro de un área, la unidad eTrex registra puntos de seguimiento y utiliza el track log de GPS resultante para calcular internamente el tamaño del tramo cerrado. Este método funciona bien cuando se puede transportar razonablemente el receptor directamente a lo largo del límite de la ruta (Sin pantanos, lagos, acantilados, desfiladeros, pendientes que se interponen en su camino), es posible que deba usar la técnica de ruta como alternativa). El track log activo puede contener hasta 10.000 puntos.

En extensiones de tierra pequeñas y de forma irregular, es posible que desee aumentar el intervalo del registro de seguimiento: la frecuencia con la que se registran los puntos de seguimiento. De lo contrario, perderá precisión cuando el receptor ocasionalmente **"corte esquinas" (cuts corners)** a medida que recorre el límite.

**Vaya a: Menú principal > Configuración (Setup) > Tracks (pistas).** (Nota: asegúrese de están en el menú de Configuración, luego en Tracks, **(no en el Administrador de Tracks).** La página de Configuración del Registro de Tracks abierto, tiene opciones aquí.

**Ilustración 24. Registro de Track**

La configuración predeterminada es **Método de grabación: Automático (Auto)** (es una combinación de distancia y tiempo) e **Intervalo: Normal.** Si elige mantener la configuración automática **(Auto setting)**, puede establecer el intervalo en **Más a menudo o Más a menudo (More Often or Most Often)** para aumentar la frecuencia de los puntos de seguimiento. En lugar de Automático (Auto), puede elegir para grabar por Distancia o Tiempo **(Distance or Time)**, cada uno con sus propias opciones de Intervalo.

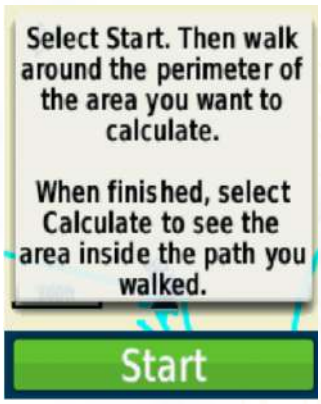
- **Usando la herramienta de cálculo de área**

1. Por lo general, debe borrar el track log activo actual justo antes de comenzar a colocar pistas. Vaya a: Menú principal > Administrador de pistas **(Track Manager)**> Actual Pista **(Current Track)**> Borrar pista actual **(Clear Current Track).** (Si desea guardar la pista anterior registro, primero seleccione GUARDAR o SAVE, luego borre el registro).
2. Vaya a Menú principal > Cálculo de área **(Area Calculation)** (Ilustración 19)

**Ilustración 25. Cálculo de área**


3. La página de cálculo de área tendrá una opción de inicio (Start) en la parte inferior (ver ilustración 20). Una vez que esté en su punto de partida, haga clic en Comenzar Start a usar el Clic-stick.

**Ilustración 26. Inicio de la página de cálculo**

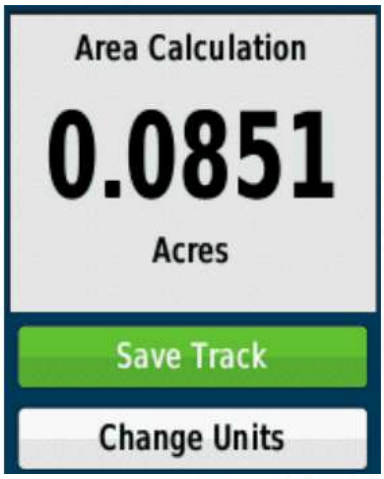


4. Comience a caminar alrededor del perímetro del área que desea calcular. La pantalla muestra su progreso. Acercar o alejar (Zoom in or out) según corresponda para ver tus pistas (tracks). No se desespere si la espesa cobertura de árboles le hace ocasionalmente pierde contacto con los satélites mientras los rastrea. El GPS se "conectar los puntos" y vincular los puntos de seguimiento registrados en un intento de estimar el área encerrada. Ver la pantalla de pista guardada para decidir si se mantuvo o no la integridad de la pista.
5. Una vez que regrese a su punto de partida (starting point), haga clic en Calcular (Ilustración 27). Si no está en su punto de partida (starting point), su receptor completará automáticamente con un tiro directo desde su posición actual a su punto de partida.

Ilustración 27. Calculando área


Los se mostrará el valor del área cerrada (Ilustración 28). Para cambiar unidades **(Change Units)**, Resalte y haga clic en la opción Cambiar unidades para que aparezca una opción selecciona la lista de opciones (pies cuadrados, yardas cuadradas, metros cuadrados, hectáreas, millas cuadradas, etc.

Ilustración 28. Calculando área 2



7. Si necesitará consultar este cálculo de área más adelante, seleccione Guardar ruta **(Save Track).** Se abrirá una página que le permitirá cambiar el nombre de la ruta si necesario.
8. Para ver todas las pistas/ rutas guardadas (saved tracks), vaya a: Menú principal > Administrador de pistas **(Track Manager)** > Rutas Pistas archivadas **Archived Tracks.**

- **Estimación de medidas de área, opción 2. El método de la ruta (The Route Method)**

**Descripción general y configuración**

Para fines de cálculo de área, una ruta es un conjunto secuencial de waypoints perimetrales vinculados entre sí para describir el límite de una extensión de tierra. El método de ruta de cálculo de área tiene algunas ventajas. No es necesario que recorra todo el borde del tramo, siempre que pueda marcar las principales esquinas y vueltas de la línea de límite. Para extensiones muy grandes y para áreas con terreno con restricciones severos, esta puede ser la única técnica GPS práctica.

El método de ruta también le permite realizar comparaciones de superficie estimados de varios tramos después de regresar a la oficina.

La precisión del método de ruta depende en gran medida de su capacidad para localizar y marcar todos los giros clave y vueltas que encierran la ruta (tract). Funciona mejor en áreas rectangulares con límites en línea recta. Los tramos con bordes irregulares y formas extrañas son más difíciles de trabajar y requieren un espacio mucho mayor de números de waypoints para describir con precisión el tramo. El número máximo de waypoints en una ruta es **250 con un máximo de 50 rutas en el eTrex 10** (más almacenamiento en los modelos superiores).

Necesitará el programa GPS Utility instalado en la computadora de su oficina para terminar de calcular el área utilizando este método.

Al usar el método de ruta para calcular el área, una serie de waypoints se identifican (Ilustración 29) en las esquinas, giros y otros puntos de definición a lo largo del área a medir.

Ilustración 29. Waypoint de un área

Los Waypoints luego se asocian con una Ruta y la Utilidad GPS se utiliza más adelante para calcular la medida del área, en particular la ruta, en base a los Waypoints asociados (Ilustración 30).

Ilustración 30. Cálculo del área

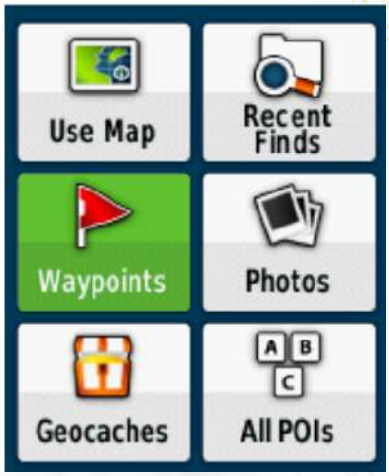
- **Para crear una ruta y calcular el área:**

1. Primero, marque y guarde waypoints de todos los rincones importantes del área desea calcular (consulte: Marcar y guardar waypoints). Eso funciona mejor para guardar estos waypoints con números secuenciales.
2. Desde la unidad GPS, vaya a Menú principal > Planificador de rutas **(Route Planner).** (Ilustración 31).

Ilustración 31. Planificar ruta


3. Seleccione Crear ruta **(Create Route)** y, en la siguiente pantalla, haga clic en **Seleccionar primer punto (Select First Point).** Esto lo lleva al menú de selección de categorías (Ilustración 32). Ir a los puntos de referencia (Waypoints).

Ilustración 32. Waypoints




4. Ahora verá una lista de waypoints para elegir. Seleccione el punto de ruta que marca la primera esquina del área que desea calcular haciendo clic hacia abajo (Ilustración 33). Cuando veas el mapa de este waypoint, haga clic en Usar **(Use.).**

Ilustración 33. Seleccionando waypoint


5. Ahora podrá seleccionar más waypoints, en orden, para completar la ruta repitiendo los pasos 3 y 4.

6. Una vez que haya agregado todos los waypoints a su ruta, puede regresar a Menú principal > Planificador de ruta **(Route Planner).** Desde el menú Planificador de ruta (Route Planner Menu), debería ver el nombre de su ruta (generalmente Ruta 001 si es la primera ruta guardada en su dispositivo). Al seleccionar el nombre de la ruta, puede editar la Ruta (agregar más puntos o eliminar puntos), renombrar, etc. (Ilustración 34).

Ilustración 34. Creación de ruta


7. Una vez que haya regresado a la oficina, descargue su ruta usando el Software gratuito **GPS Utility.** Para ver el resultado cálculo del área, vea sus rutas y seleccione el menú Ver y luego Informes. De esta forma se levantará un informe detallando cada tramo de tu ruta, distancia total y el área delimitada por la ruta.

## 3.2.7. BORRAR DATOS DEL GPS

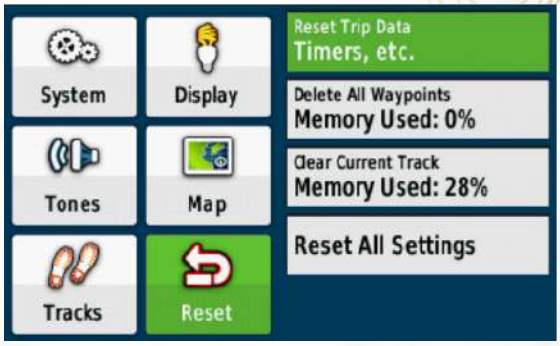
Es posible que deba borrar todos los datos existentes de su receptor GPS para poder comenzar a trabajar nuevamente con una "pizarra limpia (clean slate)".

1. Utilice el botón Menú y navegue hasta el Menú principal (haga clic y suelte dos veces) (Ilustración 35). Utilizar haga clic (click stick) en el botón para seleccionar (**Setup**) la opción Configuración, haga clic en el botón hacia abajo y luego seleccione el elemento Restablecer (**Reset**).

Ilustración 35. Borrar datos en Setup


2. Una vez que el menú Configuración (Setup) esté visible (Ilustración 36), seleccione Restablecer (Reset) de las opciones del menú resaltándolo y presionando directamente hacia abajo con el palo de clic. Esto lo llevará a la página de Opciones de Restablecimiento (Reset Options) (Ilustración 36).

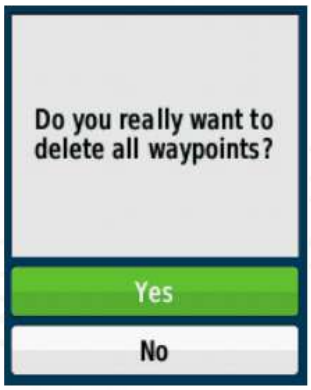
Ilustración 36. Opciones de restablecimiento




Nota: También puede llegar a la página de opciones de reinicio (Reset Options Page) yendo al menú principal, luego al odómetro de viaje (**Trip Odometer**), luego haga clic en el botón Menú una vez.

3. En la página de opciones de reinicio (Reset Options Page), use el botón de clic para navegar en la opción del menú hasta eliminar todos los Waypoints (**Delete All Waypoints**). Haga clic hacia abajo, luego seleccione Sí y haga clic hacia abajo nuevamente para eliminar todos los waypoints (Ilustración 37).

Ilustración 37. Eliminando Waypoints




4. Una vez que haya eliminado todos los waypoints, volverá a la página Opciones de reinicio (Reset options page). Ahora usted puede seleccionar Borrar ruta actual (**Clear Current Track**), seleccione Sí para borrar cualquier ruta o Tracks almacenado en el dispositivo.

Nota: Desde la página Opciones de restablecimiento (Reset options page), también puede restablecer los datos del viaje (Reset Trip Data) de la misma manera, y puede Restablecer todas las configuraciones (Reset All Settings) a los valores predeterminados de fábrica. Si restablece todas las configuraciones (Reset All Settings), tendrá que volver y vuelva a establecer todas sus preferencias (unidades de medida, etc.), por lo que no recomendamos hacer esto.

# IV. APLICACIÓN ODK

Es una estructura para recolección y administración de datos ambientales, sociales, legales, etc. de datos.

ODK es un kit de datos abiertos por sus siglas en inglés (Open Data Kit), creado por programadores afines al open source (código abierto) que desarrollan en el entorno de Google. Reúne varios kits, software o aplicaciones de acceso libre y asequible para todo público que tratan de usar reglas y sentencias fáciles de generar para obtener datos en campo con el uso de equipos móviles que usen el sistema operativo Android creado por Google (OPEN DATA KIT, 2017) (no funciona en equipos con sistema operativo iOS iPhone).

La aplicación ODK Collect, la cual está disponible en el Play Store (aplicación donde se pueden buscar y descargar aplicaciones para el sistema operativo Android). La aplicación brinda facilidades de uso en programación y generación de formularios. Estos formularios pueden ser llenados por los diferentes usuarios que participen en los proyectos de recolección de información

## 4.1 GENERACIÓN DE FORMULARIOS ODK

Un XLSform es un formato estándar creado para ayudar a simplificar la creación de formularios en Microsoft Excel.
XLSForm es un estándar abierto que simplifica la creación de formularios. La creación se realiza en un formato legible por el hombre utilizando una hoja de cálculo. Para obtener más información sobre XLSForm, visite https://xlsform.org/.

El formato básico de cada libro de Excel debe tener tres hojas de trabajo: **Survey** (Encuesta) **Choices** (Opciones) **Settings** (Configuración).

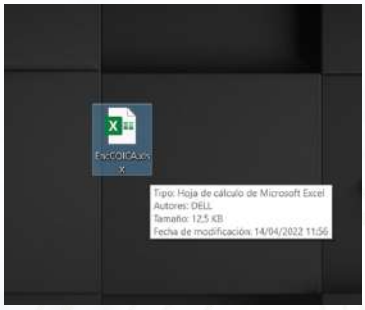
**Ilustración 38. Formato libro Excel**


https://doc.arcgis.com/es/survey123/desktop/create-surveys/xlsformessentials.htm
https://xlsform.org/en/ref-table/

### 4.1.1 HOJA DE TRABAJO SURVEY (ENCUESTA)

Primero se diseña en una hoja Excel con la extensión .xlsx las tres hojas de trabajo y guardamos en el disco local C o En el escritorio, en el ejemplo es EncCOICA.

**Ilustración 39. Hoja Excel extensión.xlsx**

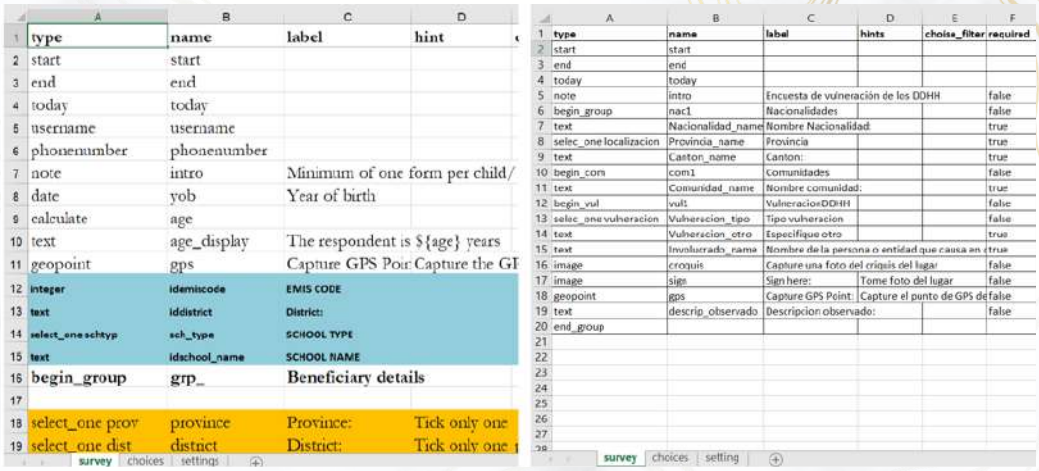



La hoja de cálculo define la estructura general del formulario. Contiene la lista completa de preguntas e información sobre cómo aparecerán en el formulario. Normalmente, cada fila representa una pregunta; sin embargo, hay más características que se describen a continuación y que se pueden agregar al formulario para mejorar la experiencia del usuario.

La hoja de cálculo survey presenta tres columnas obligatorias: **type, name y label o hint.**

- La columna type especifica el tipo de pregunta de XLSForm que se va a agregar. Hay una lista bien definida de tipos de preguntas posibles para esta columna.
- La columna name determina el nombre de la columna de la capa de entidades de ArcGIS en la que se almacenará la respuesta a la pregunta. No se admiten espacios ni caracteres especiales (tilde, ñ) en esta columna. No puede haber dos filas con el mismo contenido.
- Las columnas label y hint contienen el texto para las preguntas. Este es el texto que verá en el formulario. Una pregunta requiere al menos una columna label o hint; se recomienda proporcionar la primera para evitar mensajes de advertencia. Se admiten espacios y caracteres especiales en estas columnas. Como alternativa, puede utilizar columnas de traducción. Ambas columnas también admiten el uso limitado de código HTML y variables que se reemplazarán en su encuesta con la respuesta a otra pregunta.

Ilustración 40. Hoja de trabajo type



| type | name | label | hint |
|---|---|---|---|
| start | start | | |
| end | end | | |
| today | today | | |
| username | username | | |
| phonenumber | phonenumber | | |
| note | intro | Minimum of one form per child/ | |
| date | yob | Year of birth | |
| calculate | age | | |
| text | age_display | The respondent is ${age} years | |
| geopoint | gps | Capture GPS Poir | Capture the GI |
| integer | idemiscode | EMIS CODE | |
| text | iddistrict | District: | |
| select_one schtyp | sch_type | SCHOOL TYPE | |
| text | idschool_name | SCHOOL NAME | |
| begin_group | grp_ | Beneficiary details | |
| | | | |
| select_one prov | province | Province: | Tick only one |
| select_one dist | district | District: | Tick only one |

survey | choices | settings

| type | name | label | hints | choise_filter | required |
|---|---|---|---|---|---|
| start | start | | | | |
| end | end | | | | |
| today | today | | | | |
| note | intro | Encuesta de vulneración de los DDHH | | | false |
| begin_group | nac1 | Nacionalidades | | | false |
| text | Nacionalidad_name | Nombre Nacionalidad: | | | true |
| selec_one localizacion | Provincia_name | Provincia | | | true |
| text | Canton_name | Canton: | | | true |
| begin_com | com1 | Comunidades | | | false |
| text | Comunidad_name | Nombre comunidad: | | | true |
| begin_vul | vul1 | VulneracionDDHH | | | false |
| selec_one vulneracion | Vulneracion_tipo | Tipo vulneracion | | | false |
| text | Vulneracion_otro | Especifique otro | | | true |
| text | Involucrado_name | Nombre de la persona o entidad que causa en | | | true |
| image | croquis | Capture una foto del croquis del lugar | | | false |
| image | sign | Sign here: | Tome foto del lugar | | false |
| geopoint | gps | Capture GPS Point: | Capture el punto de GPS de | | false |
| text | descrip_observado | Descripcion observado: | | | false |
| end_group | | | | | |

survey | choices | setting

## 4.1.2. HOJA DE CÁLCULO (CHOISES)

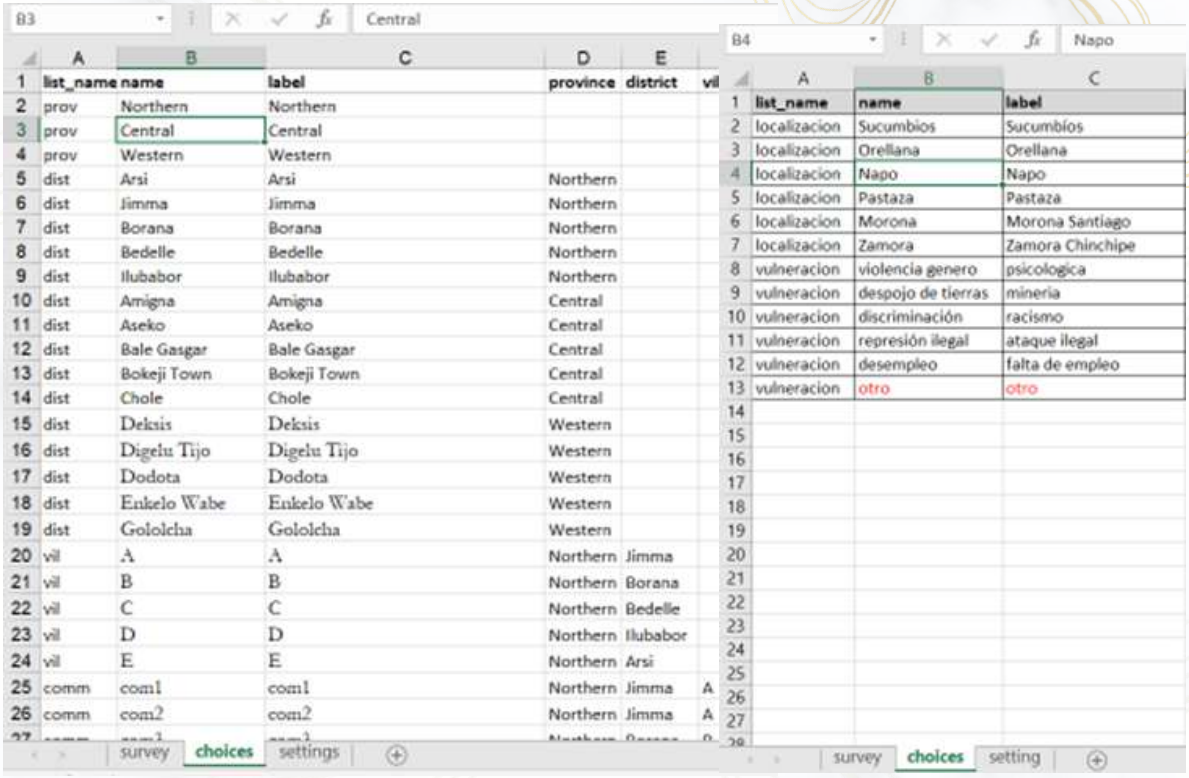
Esta hoja de cálculo se usa para especificar las opciones de respuesta para las preguntas con varias respuestas. Cada fila representa una opción de respuesta. Las opciones de respuesta con el mismo nombre de lista se consideran parte de un conjunto relacionado de opciones y aparecen juntas para una pregunta. También permite reutilizar un conjunto de opciones para varias preguntas (por ejemplo, preguntas de sí o no).

La hoja de cálculo choices tiene tres columnas obligatorias: **list_name, name y label.**

- La columna list_name permite agrupar un conjunto de opciones de respuesta relacionadas. Las opciones con el mismo nombre de lista se presentan como el conjunto de respuestas para una pregunta.
- La columna name especifica el valor que se conserva en ArcGIS. Los valores de la columna name no aceptan caracteres especiales. No se recomienda incluir nombres de opción duplicados en una lista de opciones. Para obtener más información sobre nombres de opciones duplicados, consulte Preguntas con varias opciones.
- La columna label muestra la opción de respuesta tal y como se desea que aparezca en el formulario. Como alternativa, puede utilizar columnas de traducción de etiquetas.

Al crear formularios en Excel, la sintaxis que utilice debe ser precisa. Por ejemplo, si escribe Choices o choice en lugar de **choices**, el formulario no funcionará.

Ilustración 41. Hoja de trabajo choices



| list_name | name | label | province | district | vil |
|---|---|---|---|---|---|
| prov | Northern | Northern | | | |
| prov | Central | Central | | | |
| prov | Western | Western | | | |
| dist | Arsi | Arsi | Northern | | |
| dist | Jimma | Jimma | Northern | | |
| dist | Borana | Borana | Northern | | |
| dist | Bedelle | Bedelle | Northern | | |
| dist | Ilubabor | Ilubabor | Northern | | |
| dist | Amigna | Amigna | Central | | |
| dist | Aseko | Aseko | Central | | |
| dist | Bale Gasgar | Bale Gasgar | Central | | |
| dist | Bokeji Town | Bokeji Town | Central | | |
| dist | Chole | Chole | Central | | |
| dist | Deksis | Deksis | Western | | |
| dist | Digelu Tijo | Digelu Tijo | Western | | |
| dist | Dodota | Dodota | Western | | |
| dist | Enkelo Wabe | Enkelo Wabe | Western | | |
| dist | Gololcha | Gololcha | Western | | |
| vil | A | A | Northern | Jimma | |
| vil | B | B | Northern | Borana | |
| vil | C | C | Northern | Bedelle | |
| vil | D | D | Northern | Ilubabor | |
| vil | E | E | Northern | Arsi | |
| comm | com1 | com1 | Northern | Jimma | A |
| comm | com2 | com2 | Northern | Jimma | A |

| list_name | name | label |
|---|---|---|
| localizacion | Sucumbios | Sucumbíos |
| localizacion | Orellana | Orellana |
| localizacion | Napo | Napo |
| localizacion | Pastaza | Pastaza |
| localizacion | Morona | Morona Santiago |
| localizacion | Zamora | Zamora Chinchipe |
| vulneracion | violencia genero | psicologica |
| vulneracion | despojo de tierras | mineria |
| vulneracion | discriminación | racismo |
| vulneracion | represión ilegal | ataque ilegal |
| vulneracion | desempleo | falta de empleo |
| vulneracion | otro | otro |

## 4.1.3. HOJA DE CÁLCULO (SETTINGS)

La hoja de cálculo settings es opcional y le permite personalizar más el formulario. La personalización disponible incluye un título que se muestra mientras se edita el formulario, un nombre de instancia para identificar de forma única cada formulario completado y un identificador de versión único para la encuesta, entre otros (Fuente: ArcGIS Survey 123, https://doc.arcgis.com/es/survey123/desktop/create-surveys/xlsformessentials.htm.)

## 4.1.4. TIPO DE PREGUNTAS

XLSForm admite diversos tipos de preguntas. Por ejemplo, para recopilar el nombre y la ubicación de una tienda, debe escribir lo siguiente:

| | A | B | C |
|---|---|---|---|
| 1 | type | name | label |
| 2 | text | store_name | What is the name of this store? |
| 3 | geopoint | store_location | Collect the GPS coordinates of this store. |

Fuente: ArcGIS Survey 123
https://doc.arcgis.com/es/survey123/desktop/create-surveys/xlsformessentials.htm.

**Cuadro 1. Tipo de preguntas a realizar en survey**

| Tipo de pregunta | Entrada de respuesta | Tipo de campo predeterminado |
|---|---|---|
| entero | Entrada de número entero. | esriFieldTypeInteger |
| decimal | Entrada decimal. | esriFieldTypeDouble |
| rango | Entrada de un rango determinado de números. | esriFieldTypeInteger |
| texto | Respuesta de texto libre. | esriFieldTypeString |
| select_one list_name | Pregunta con varias opciones en la que el usuario solo puede seleccionar una respuesta. Reemplace list_name con el nombre de su lista de opciones. Puede cambiar el tipo de campo; sin embargo, el nombre de opción siempre se trata como una cadena de caracteres en la aplicación de campo cuando se utiliza en expresiones. | esriFieldTypeString |
| select_multiple list_name | Pregunta con varias opciones en la que el usuario puede seleccionar varias respuestas. Reemplace list_name con el nombre de su lista de opciones. No puede cambiar el tipo de campo y el nombre de opción siempre se trata como una cadena de caracteres en la aplicación de campo cuando se utiliza en expresiones. | esriFieldTypeString |
| rank list_name | Pregunta de clasificación; clasificación de una lista de opciones en orden. Reemplace list_name con el nombre de su lista de opciones. No puede cambiar el tipo de campo y el nombre de opción siempre se trata como una cadena de caracteres en la aplicación de campo cuando se utiliza en expresiones. | esriFieldTypeString |
| nota | Muestra una nota en la pantalla; no acepta entradas. También puede visualizar cálculos ocultos. | esriFieldTypeString |
| geopoint | Captura una coordenada GPS dada. No puede cambiar el tipo de campo. | esriFieldTypeGeometry |
| geotrace | Captura una línea de un mapa. No puede cambiar el tipo de campo. | esriFieldTypeGeometry |
| geoshape | Captura un polígono de un mapa. No puede cambiar el tipo de campo. | esriFieldTypeGeometry |
| fecha | Entrada de fecha. | esriFieldTypeDate |
| hora | Entrada de hora. | esriFieldTypeString |
| dateTime | Acepta una entrada de fecha y hora. | esriFieldTypeDate |
| imagen | Tome una foto. | Adjunto |
| grupo de inicio | Inicia un grupo de preguntas. | No aplicable |
| grupo de fin | Finaliza un grupo de preguntas. | No aplicable |
| begin repeat | Inicia un conjunto de preguntas que se repiten. | No aplicable |
| repetición de fin | Finaliza un conjunto de preguntas que se repiten. | No aplicable |
| calcular | Realiza un cálculo con los valores del formulario. Este tipo de pregunta está oculto y no aparece en el formulario. | esriFieldTypeString |
| username[1] | Cuando se inicia sesión en ArcGIS Online o ArcGIS Enterprise, este campo se rellena automáticamente con el nombre de usuario de la cuenta. Este tipo de pregunta está oculto y no aparece en el formulario. | esriFieldTypeString |
| email[1] | Cuando se inicia sesión en ArcGIS Online o ArcGIS Enterprise, este campo se rellena automáticamente con la dirección de correo electrónico de la cuenta. Este tipo de pregunta está oculto y no aparece en el formulario. | esriFieldTypeString |
| oculto | Un campo que no aparece en el formulario. Use las columnas bind::esri:fieldType y bind::esri:fieldLength para especificar el esquema de datos. | esriFieldTypeString |
| barcode | Escanea un código de barras. | esriFieldTypeString |
| inicio | Fecha y hora de inicio de la encuesta. | esriFieldTypeDate |
| end | Fecha y hora de finalización de la encuesta. | esriFieldTypeDate |
| deviceid | Id. único generado por Survey123 que representa al dispositivo específico con el que se respondió a la encuesta. No es lo mismo que la Identidad Internacional de Equipo Móvil (IMEI, por sus siglas en inglés) del dispositivo móvil, ya que Survey123 se ejecuta en dispositivos que pueden no tener una IMEI. | esriFieldTypeString |
| audio | Grabación de muestras de audio. | Adjunto |
| archivo | Carga un archivo en el dispositivo. | Adjunto |

Fuente: ArcGIS Survey 123

https://doc.arcgis.com/es/survey123/desktop/create-surveys/xlsformessentials.htm

[1]Una opción más flexible es utilizar la función pulldata() para obtener los valores.

### Preguntas con varias opciones

XLSForm admite preguntas select_one (seleccionar solo una respuesta), select_multiple (seleccionar varias respuestas) y de clasificación (ordenar una lista de opciones). Para escribir una pregunta con varias opciones de respuesta, es necesario agregar una hoja de cálculo choices al libro de trabajo de Excel. El siguiente ejemplo muestra una pregunta select_one:

Ilustración 42. Ejemplo de hoja de cálculo choices

| | A | B | C |
|---|---|---|---|
| 1 | type | name | label |
| 2 | select_one yes_no | likes_pizza | Do you like pizza? |
| 3 | | | |

| | A | B | C |
|---|---|---|---|
| 1 | list_name | name | label |
| 2 | yes_no | yes | Yes |
| 3 | yes_no | no | No |

Fuente: ArcGIS Survey 123
https://doc.arcgis.com/es/survey123/desktop/create-surveys/xlsformessentials.htm

La entrada yes_no de la hoja de cálculo survey debe coincidir con la entrada yes_no de la columna list name de la hoja de cálculo choices. Esto garantiza que el formulario muestra la lista correcta de opciones de respuesta para una pregunta concreta.

Cuando se publican las encuestas en ArcGIS con Survey123 Connect, las opciones de las preguntas select_one se convierten en dominios de geodatabase para la capa de entidades de ArcGIS.

Precaución:
A continuación, se enumeran las limitaciones a la hora de utilizar una lista de opciones con nombres de opciones duplicados:

- Los nombres de opciones duplicados no se admiten para las preguntas select_multiple.
- Los nombres de opciones duplicados no se admiten para encuestas multilingües.
- La función jr:choice-name() devuelve la etiqueta de la primera opción duplicada de la lista.
- Cuando se abren desde las carpetas Bandeja de entrada, Borradores, Bandeja de salida, Enviado o Información general, las preguntas select_one se revierten a la primera opción duplicada de la lista.

También puede agregar preguntas con varias respuestas que permitan seleccionar varias respuestas, como las siguientes:

**Ilustración 43. Preguntas con varias respuestas**

| | A | B | C |
|---|---|---|---|
| 1 | type | name | label |
| 2 | select_multiple toppings | favorite_toppings | What are your favorite pizza toppings? |
| 3 | | | |

| | A | B | C |
|---|---|---|---|
| 1 | list_name | name | label |
| 2 | toppings | cheese | Cheese |
| 3 | toppings | pepperoni | Pepperoni |
| 4 | toppings | pineapple | Pineapple |

Fuente: ArcGIS Survey 123
https://doc.arcgis.com/es/survey123/desktop/create-surveys/xlsformessentials.htm

De forma predeterminada, estas opciones aparecen en el orden proporcionado en la hoja choices. En su lugar, puede aleatorizar el orden en el que aparecen estas opciones introduciendo randomize=true en la columna de parámetros.

Precaución:

Todos los valores capturados en una pregunta select_multiple o de clasificación se guardan como una lista separada por comas, por lo que debe evitar el uso de comas en la columna de nombre de su lista de opciones. Tenga en cuenta también que las preguntas select_multiple y de clasificación envían solo el nombre de una opción a la capa de entidades, en lugar del nombre y la etiqueta enviados por las preguntas select_one.

El valor de una pregunta de clasificación permanecerá vacío hasta que el usuario modifique el orden de las opciones. Si se ha establecido un valor predeterminado, el orden predeterminado se aplicará, a menos que el usuario modifique el orden de las opciones.

Una respuesta individual para una pregunta select_multiple se puede devolver con la función selected-at. Lo siguiente devuelve el valor de nombre de la primera respuesta obtenida para una pregunta select_multiple:

selected-at(${species}, 0)

Para enviar la etiqueta de una respuesta, puede usar la función jr:choice-name. Para obtener el valor de etiqueta de la segunda respuesta obtenida de la misma pregunta select_multiple, use lo siguiente:

jr:choice-name(selected-at(${species}, 1), '${species}')

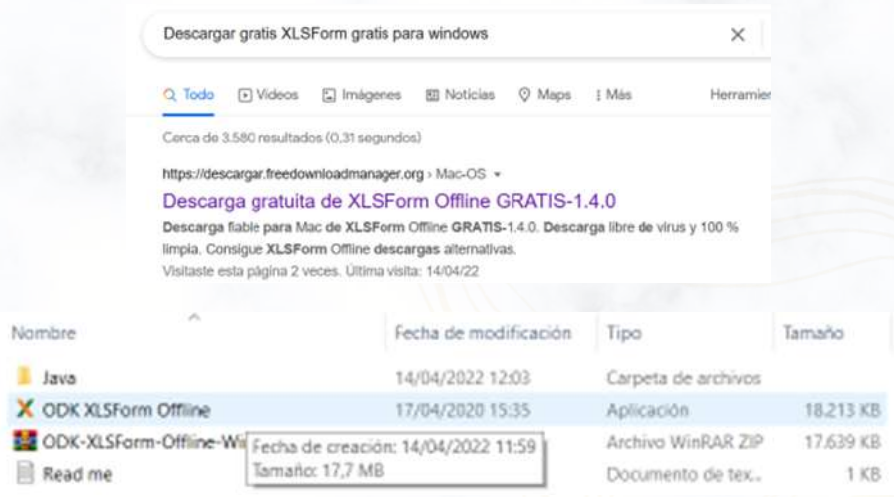
## 4.1.5 CONVERTIR HOJA EXCEL. xlsx A FORMATO XLSForm

Una vez culminado la hoja de trabajo Excel con las tres hojas: survey, choices y settings con las preguntas y respuestas de la encuesta, se procede a subir el archivo Excel a la plataforma ONA.

En el casi que usted no logre subir como archivo Excel a la plataforma ONA se debe a transformar el Excel a formato XLSForm, para lo cual se realiza los siguientes pasos:

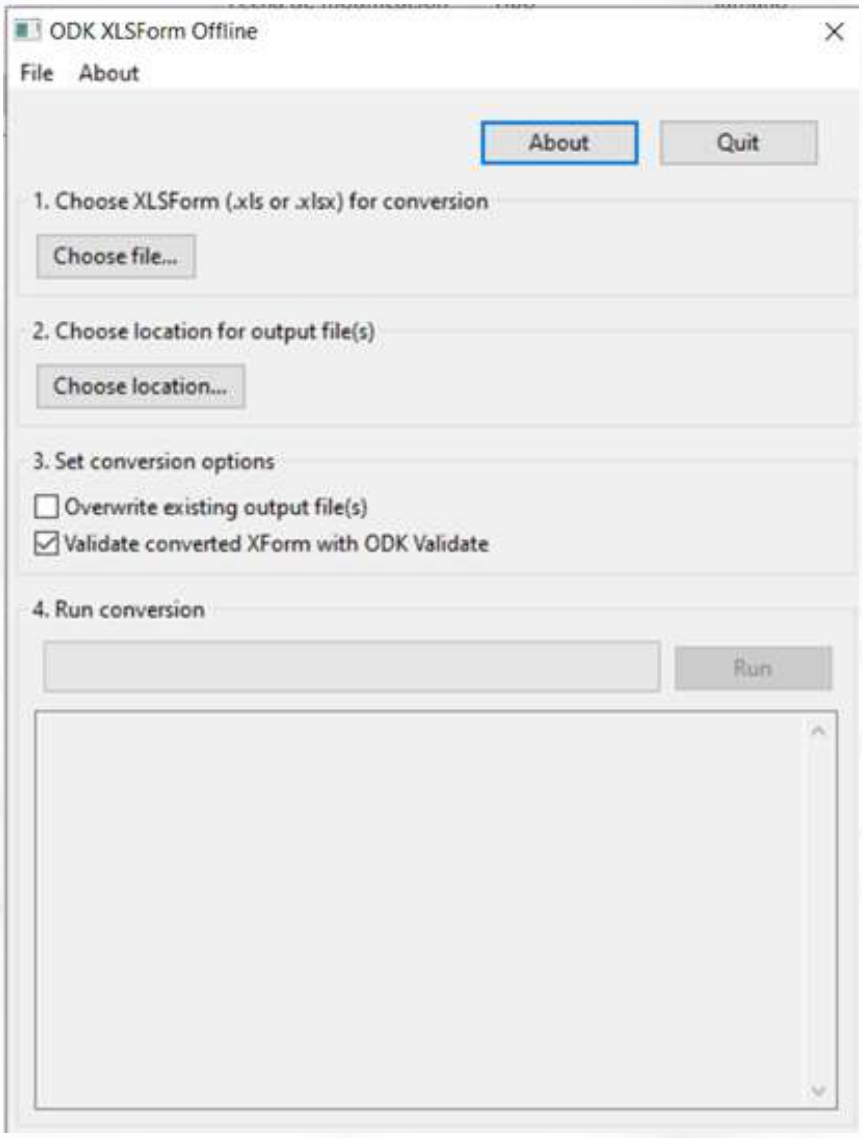
- Proceder a descargar la versión gratuita de XLSForm para Windows

**Ilustración 44. Descargar XLSForm**



- Luego de descargar aparece como ODK XLSForm Offline y damos doble clic para abrir.

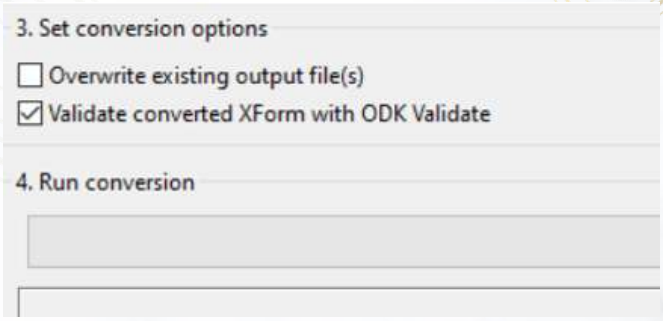

Ilustración 45. ODK XLSForm




El cuadro de diálogo en el ítem 1 se debe seleccionar donde se encuentra guardado el archivo Excel.xlsx y en el ítem 2 se debe seleccionar dónde usted desea guardar el nuevo archivo transformado en formato XLSForm.

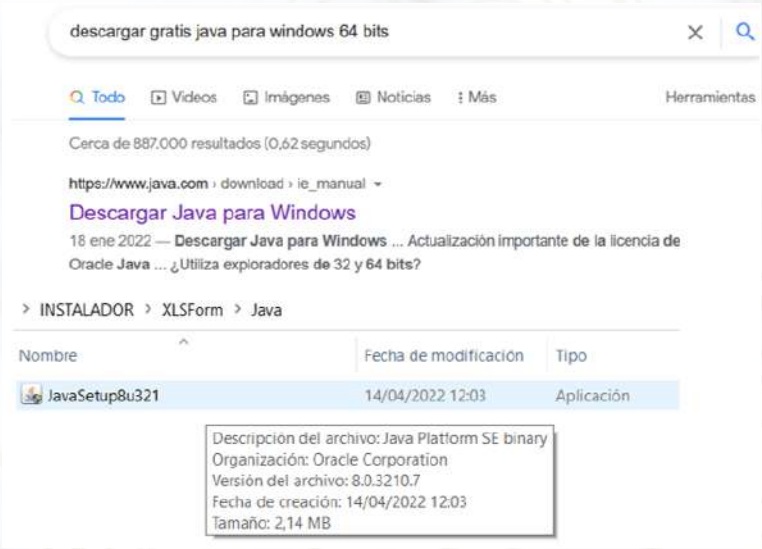
- Debes estar activado la pestaña Validar XForm convertido con ODK **(Validate converted XForm whit ODK Validate)**

Ilustración 46. Área para validar XForm a ODK




En el caso que la pestaña se encuentre desactivada se debe instalar el programa Java para Windows y proceder a instalar.

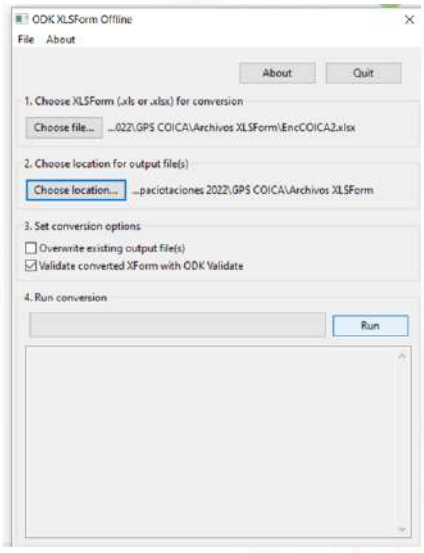
Ilustración 47. Descargar Java gratis para Windows




- Una vez instalado procedemos a transformar el archivo Excel a Formato XForm y ODK.

Dar clic en **Run**

Ilustración 48. Transformar Excel a formato ODK XForm



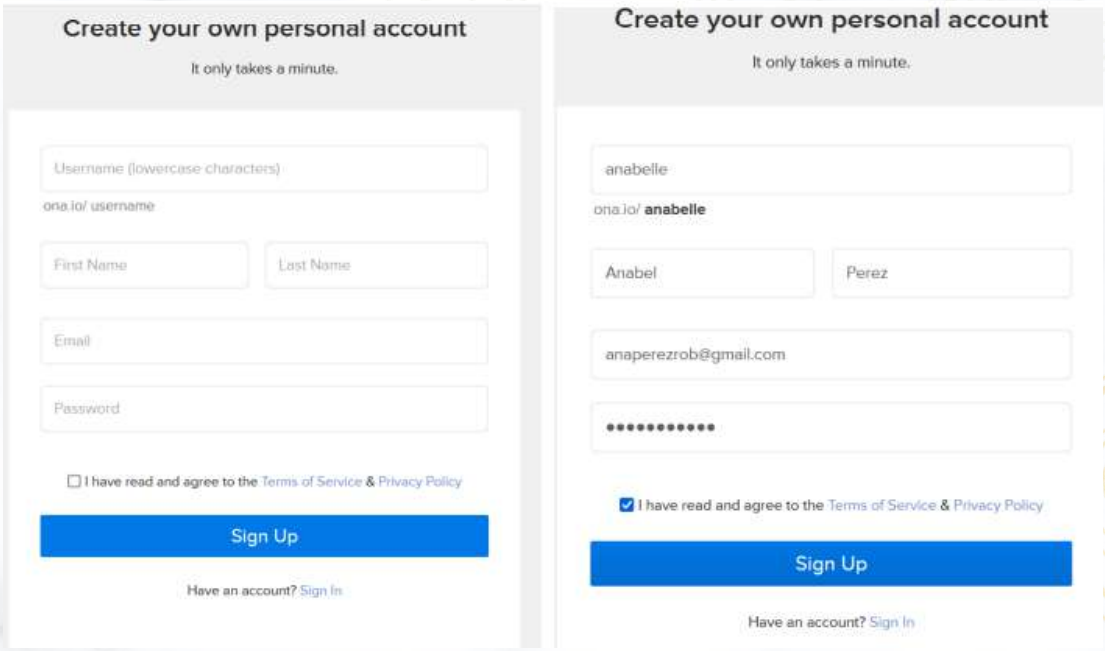
El archivo generado se debe guardar para subir en la plataforma de ONA en formularios.

## 4.2. ACCESO A LA PLATAFORMA ONA

Para cargar un formulario en la plataforma se debe contar con permisos de administrador, los cuales son otorgados únicamente por el dueño del proyecto (la organización).

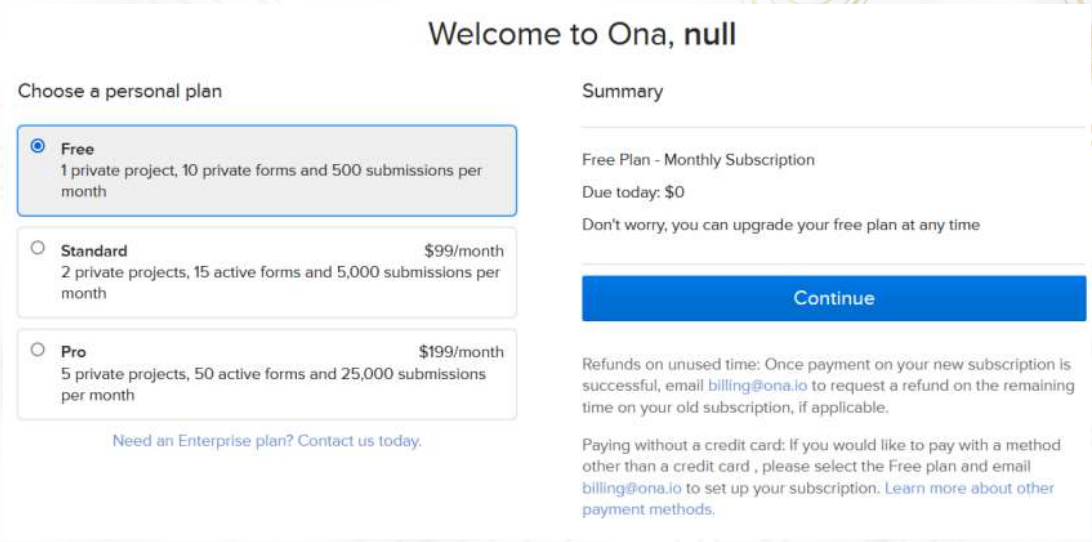
El administrador del proyecto puede asignar los permisos a sus diferentes usuarios a través de correos electrónicos, donde puede controlar si el usuario puede visualizar, editar, borrar o crear formularios según sean sus competencias en el proyecto.

**Ilustración 49. Crear cuenta en plataforma ONA**




Ahora ingresar al sitio WEB: https://ona.io/login
Usuario de ONA:
Contraseña ONA:
Configurar español.

Ilustración 50. Iniciando ONA



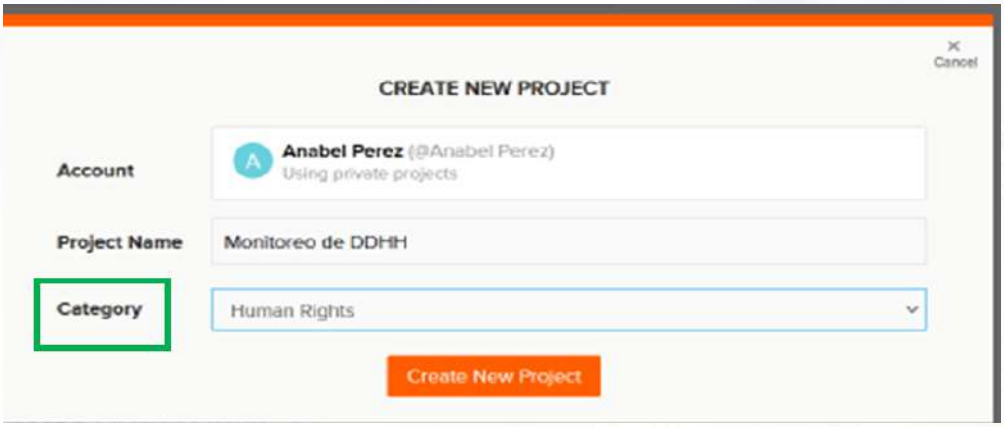


## 4.2.1. CREACIÓN DEL PROYECTO

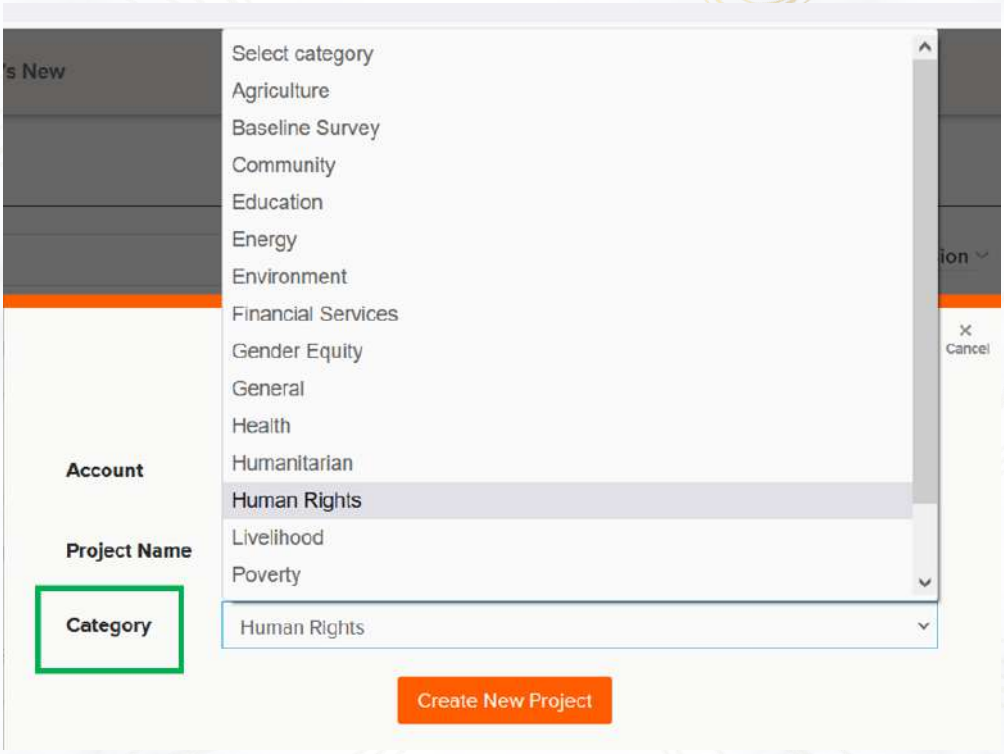
1. Hacer clic en nuevo proyecto.

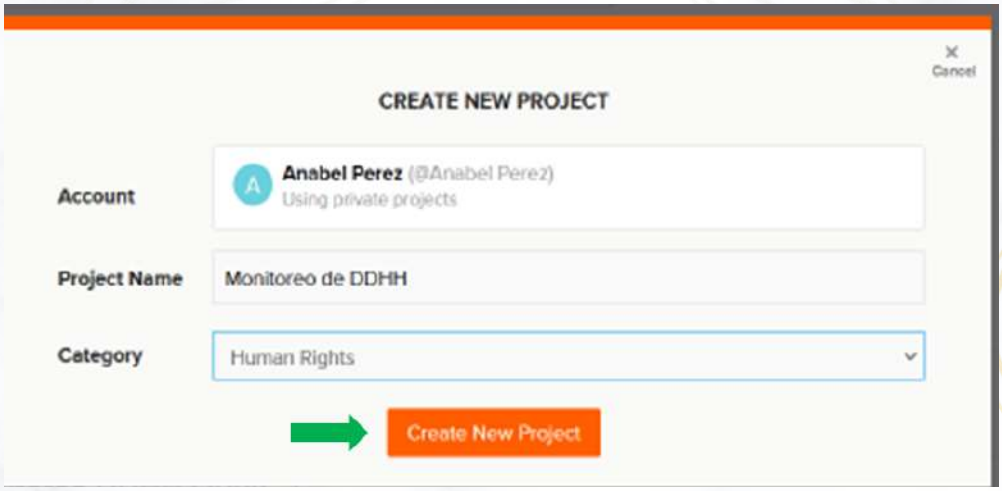
Ilustración 51. Crear un proyecto en plataforma ONA


2. Crear nuevo proyecto.

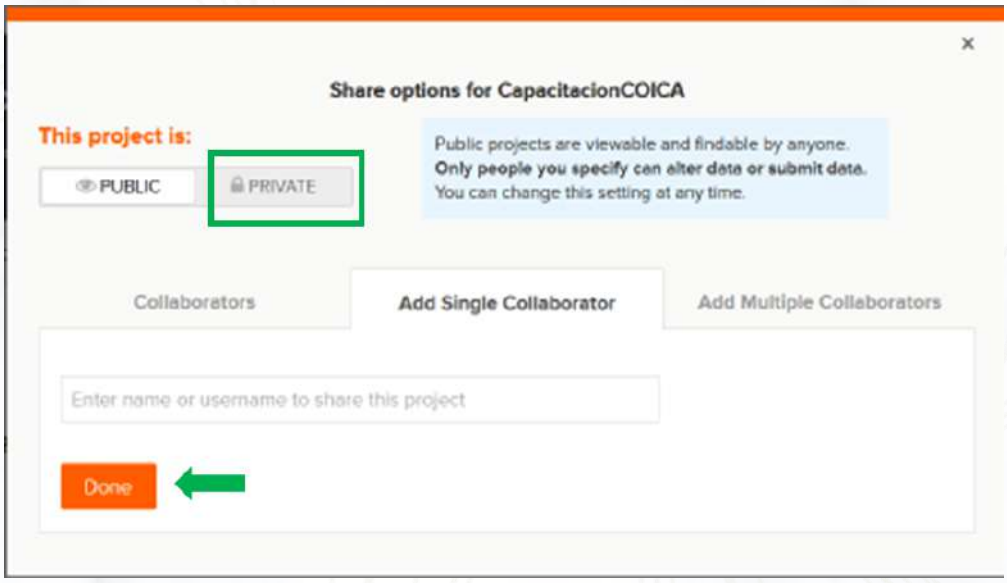


3. Seleccionar la categoría del proyecto.

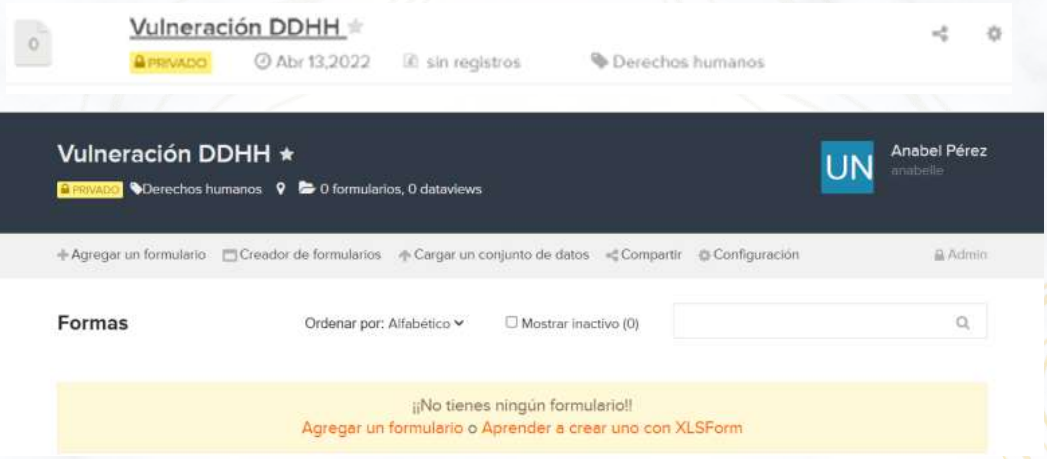



4. Hacer clic en **Private**, para que el proyecto sea privado.
5. Hacer clic el Done.




6.Hacer clic en el proyecto creado para abrirlo.




## 4.2.2. AGREGAR FORMULARIO

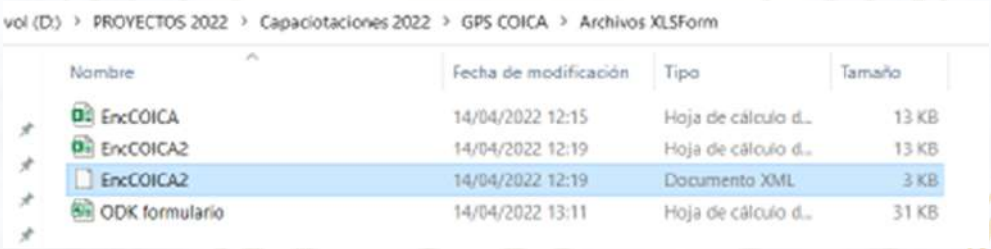
- Hacer clic en Add a form.

Subir el formulario Excel (o el archivo transformado a ODK XForm en el proceso anterior).

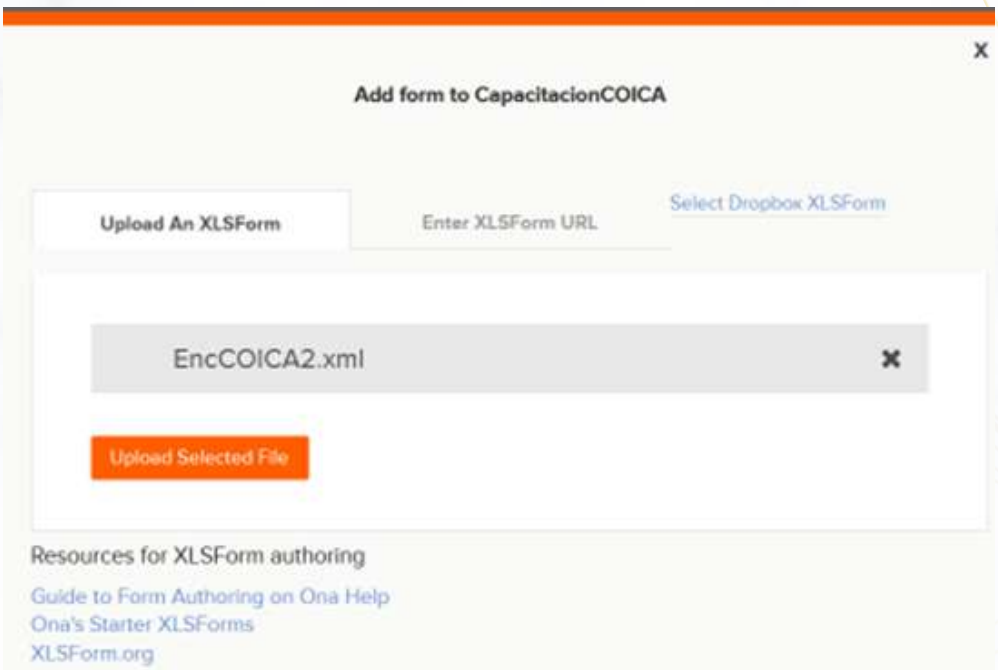
- Hacer clic en Choose file to upload o agregar formulario.

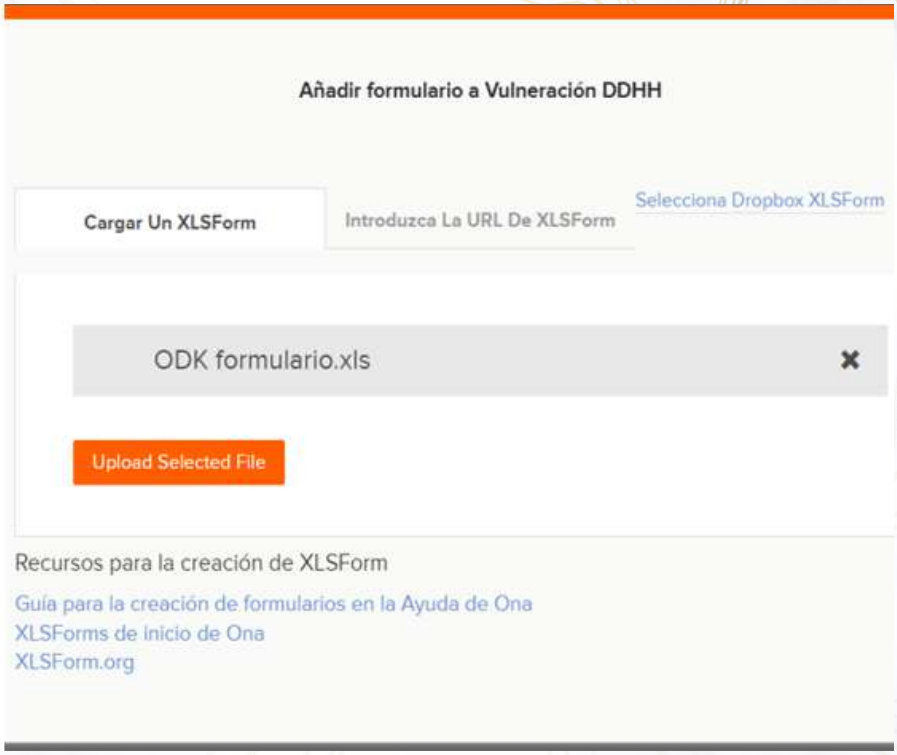

- Seleccionar el archivo que del formulario que se desea subir.

Hacer clic en Abrir.
Recomendación: guardar archivos el Excel 97 - 2003.

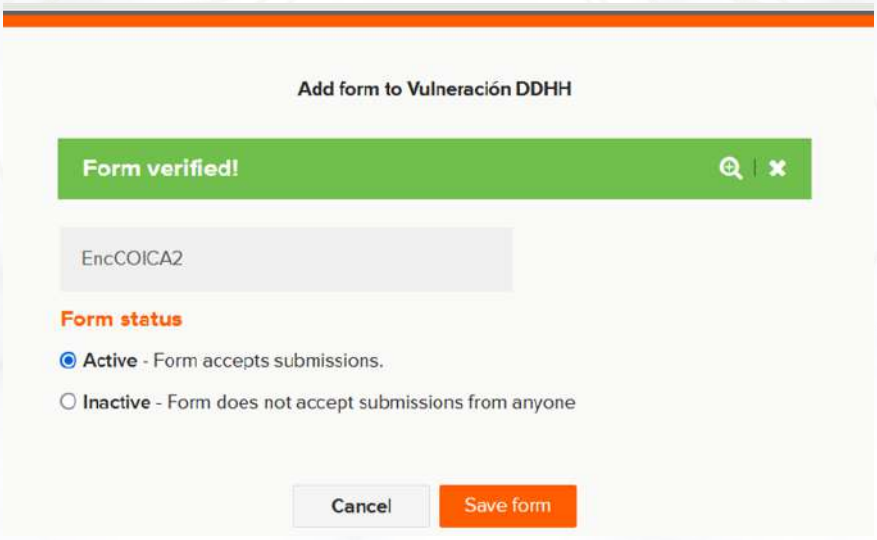



- Seleccionar Upload Selected File.

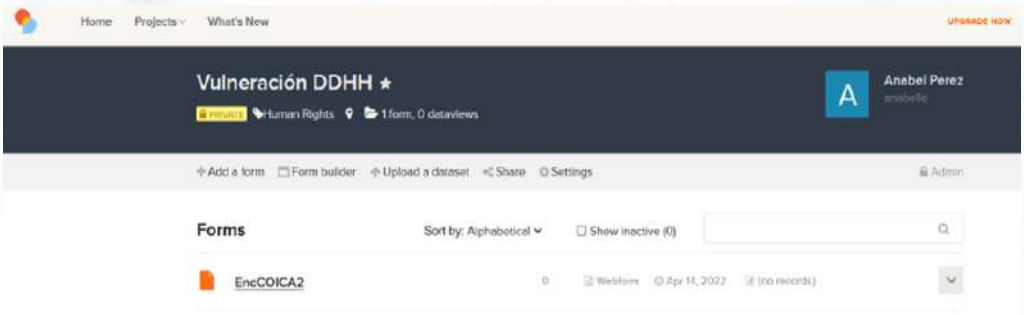





- Seleccionar **Save form.**




De existir algún problema con el formulario, en esta etapa se desplegarán advertencias. Si el formulario está bien, la ficha quedará ya subida en la plataforma y estará disponible para descarga y uso en el celular.
La forma quedará guardada



## 4.2.3. CONFIGURACIÓN DEL CELULAR PARA ACCEDER AL FORMULARIO ODK

1. Descargar ODK en Play Store.

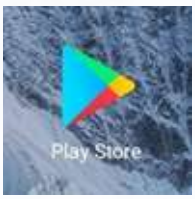
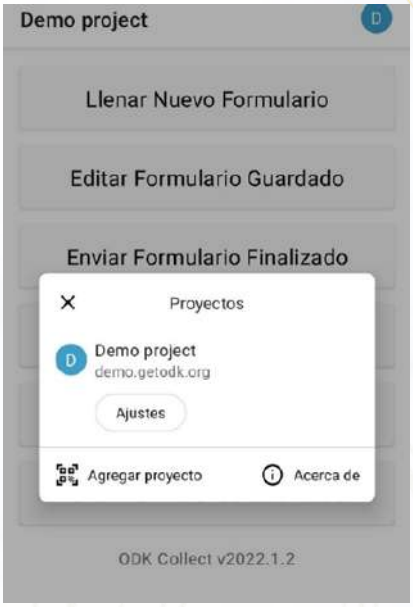



**Ilustración 52. Descargar ODK Collect al celular**

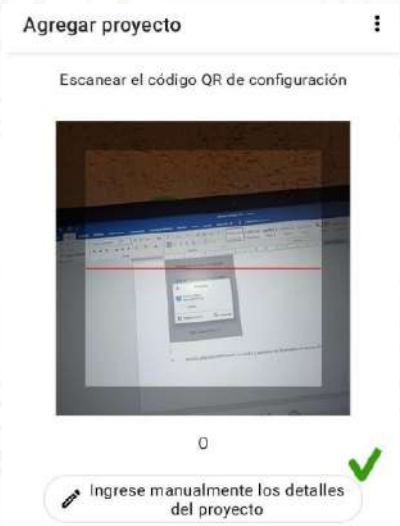

2. Entrar a la aplicación ODK desde su celular.


Una vez en el menú principal, seguir los siguientes pasos para la configuración de ODK en el celular:

Se despliega la pantalla **Agregar nuevo proyecto:**




3. Seleccionar: Ingresar manualmente los detalles del proyecto.




4. En Agregar proyecto seleccionar configuración y seleccionar o agregar una cuenta de correo electrónico.

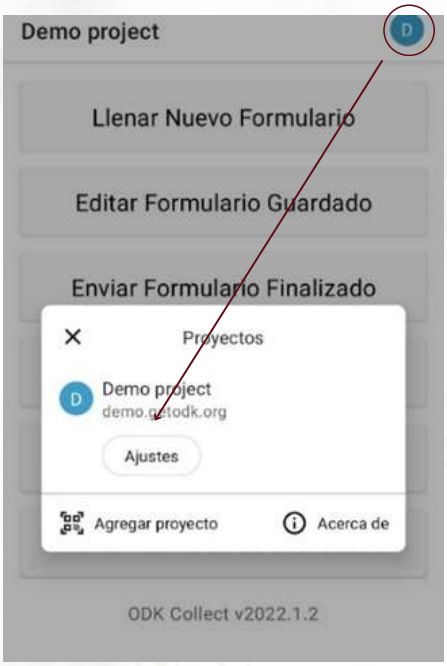

URL: https://odk.ona.io

Usuario: con correos electrónicos o nombre que definan

Clave:

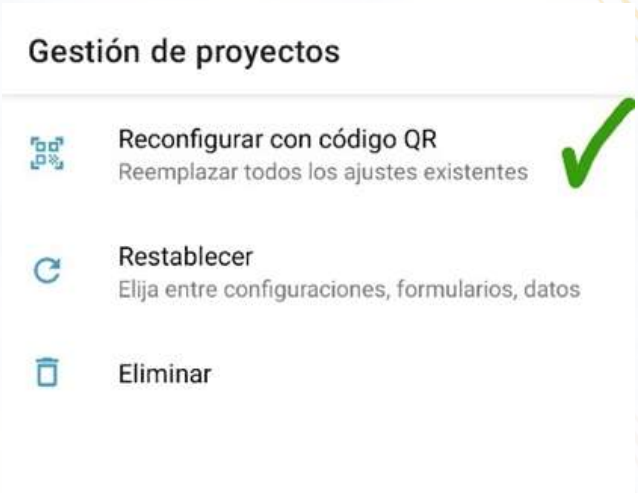
Otra forma para ingresar con usuario y nuevo proyecto es escaneando el código QR

Para lo cual

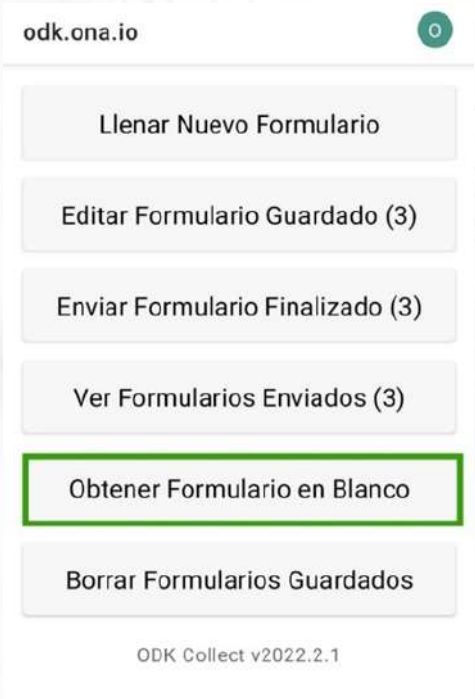


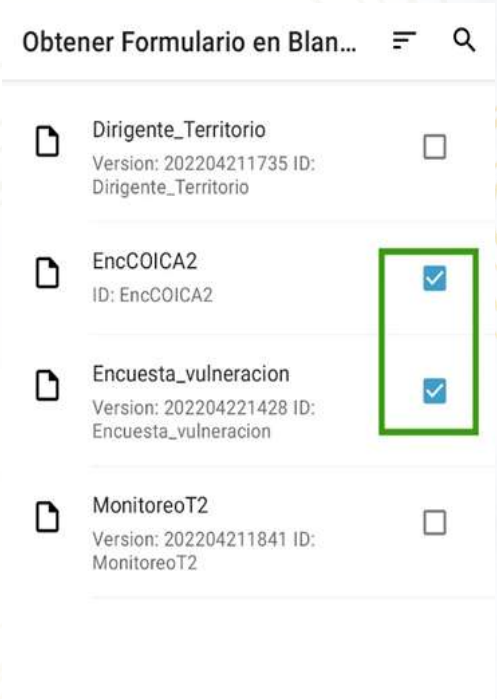

1.En Demo Project seleccionar **Ajustes**

Buscar y seleccionar **Gestión de proyectos – Reconfigurar con código QR** donde se tiene dos opciones **Escanear** el código de otro celular o generar un **Código QR** para que otros usuarios accedan a nuestros formularios.

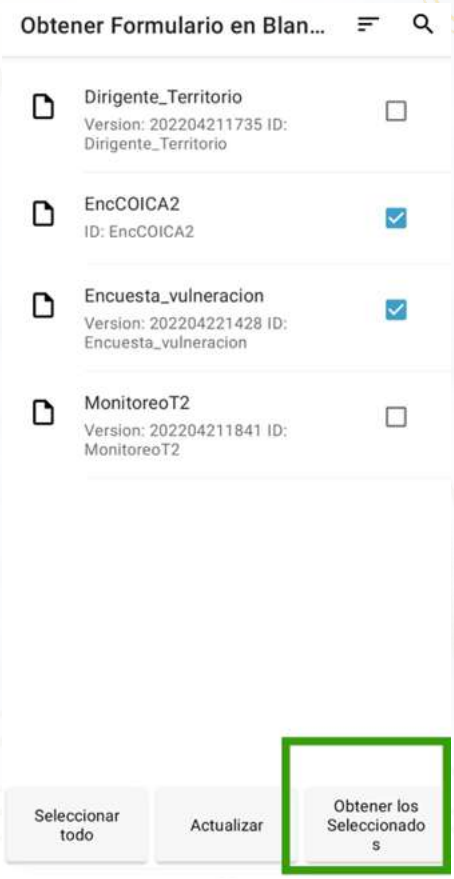




Volver a menú principal y obtener formulario en blanco. Seleccionar el formulario a utilizar.



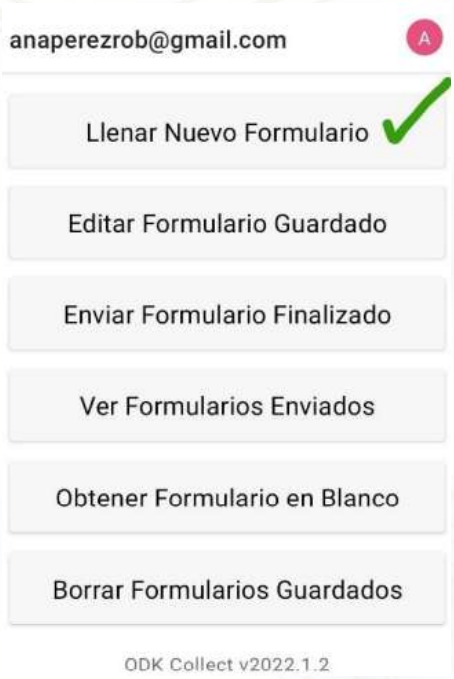



Poner de **Obtener los Seleccionados** y se descargan los formularios.



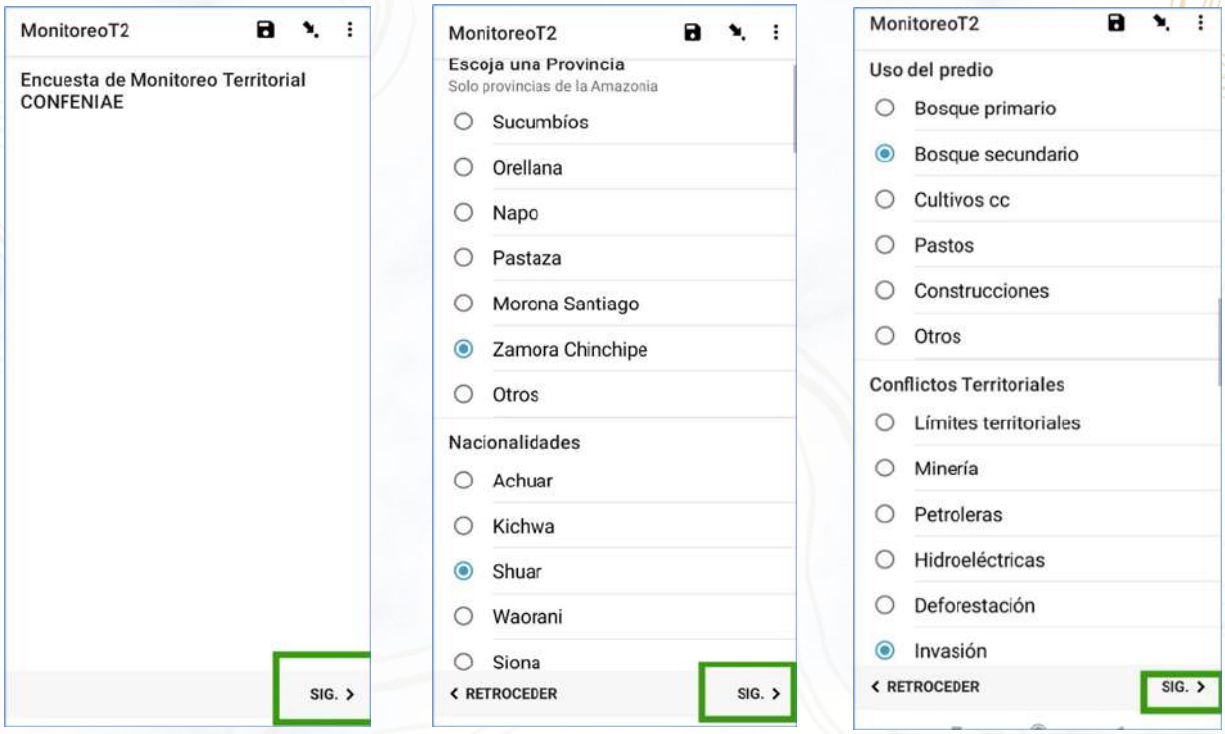

## 4.2.4. LLENAR FORMULARIOS EN EL CELULAR

- Seleccionar llenar Nuevo formulario, luego de ingresar a ODK en su celular.



Seleccione el formulario a llenar.

**Llenar el formulario y hacer clic en guardar y pase a la siguiente pregunta.**

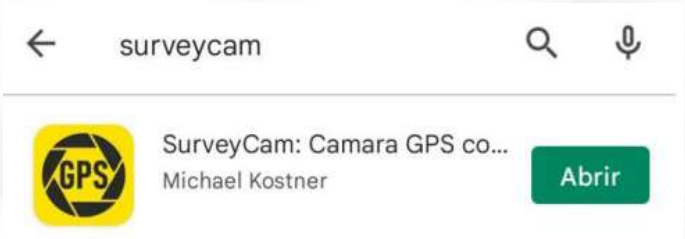



## V. APLICACIÓN SURVEYCAM

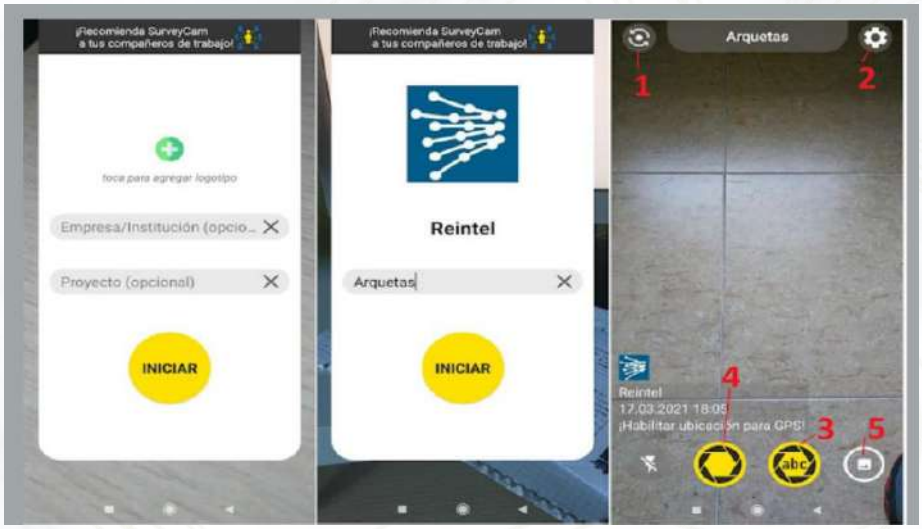
Permite realizar capturas fotográficas georreferenciadas con nuestro smartphone, mostrándonos también una orientación de la exactitud espacial registrada, da la posibilidad de nombrar cada archivo por proyectos/clientes y a la vez guardar notas de cada posicionamiento. Es simple de utilizar e intuitiva para ser empleada por cualquier operador.

### 5.1. CONOCIENDO SURVEYCAM

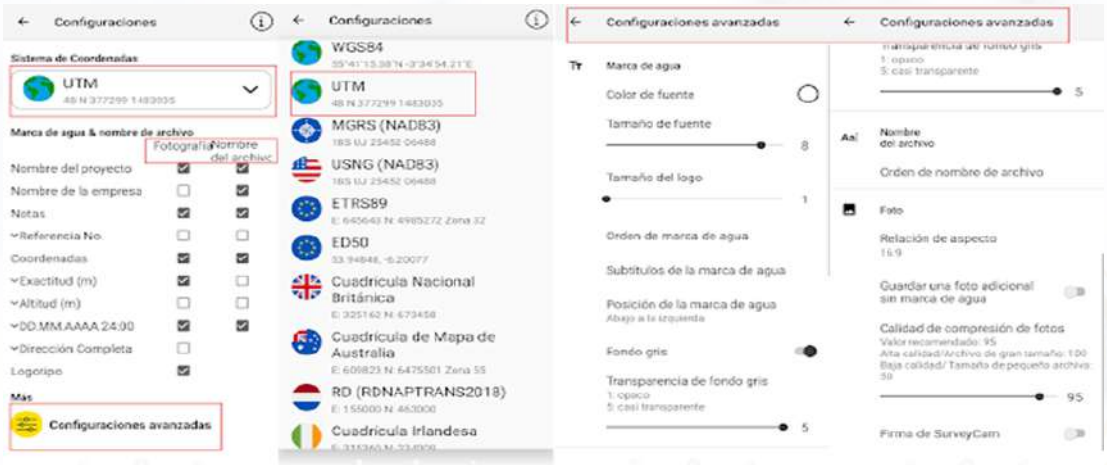
Descargar la aplicación del Play Store la aplicación **SurveyCam.**




Abrir la aplicación SurveyCam en el celular.

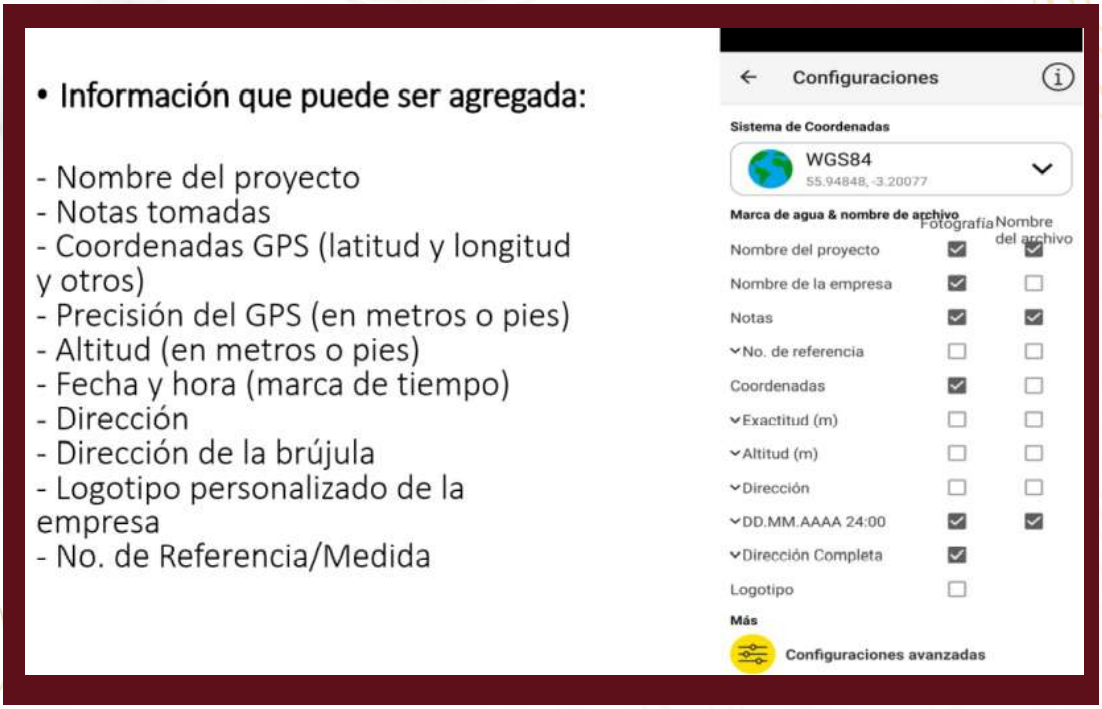




- Lo importante de esta herramienta es la configuración de las opciones: los datos que queremos que aparezcan en la marca de agua o sobreimpresa en la fotografías y la nomenclatura con la que se guardarán los ficheros de las imágenes recogidas.
- De esta manera tendremos clara la relación entre ambos aspectos además de las situación geográfica que es lo fundamental cuando efectuamos levantamientos de un gran número de registros.



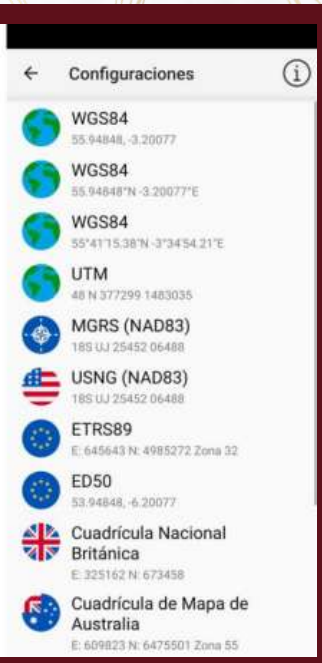
- Con SurveyCam – Cámara GPS, puedes agregar el nombre de un proyecto o de empresa, notas y más información, por ejemplo, un No. de referencia o medida directamente en la app mientras tomas fotografías.
- Datos relevantes adicionales para profesionales, por ejemplo, SurveyCam agregará coordenadas GPS y ubicación de la foto (latitud y longitud y otros formatos de coordenadas), precisión del GPS, altitud, dirección, fecha y hora (marca de tiempo).


- Información que puede ser agregada:



- SurveyCam – Camara GPS permite los siguientes sistemas de coordenadas o cuadrículas:

- WGS84 (latitud y longitud)
- UTM
- MGRS (NAD83)
- USNG (NAD83)
- ETRS89
- ED50
- RD (RDNAPTRANS2018)
- Cuadrícula Nacional Británica (Cuadrícula Nacional OS)
- Mapa de cuadrícula de Australia (MGA2020)
- Cuadrícula Irlandesa
- Cuadrícula Suiza CH1903 + / LV95
- Nueva Zelanda Transverse Mercator 2000 (NZTM2000)




**Elaborado por:**
**Anabel Pérez**

PROGRAMA DE
Defensores y Defensoras
INDÍGENAS

Los módulos han sido elaborados en el marco del Programa Defensa de Defensores y Defensoras, y el proyecto "Protección de defensores de derechos humanos indígenas en la cuenca amazónica durante la pandemia COVID-19".


COICA ORG

coica_org

coicamazonia.org

@coicaorg

COICA ORG - Oficial

coica@coicamazonia.org

Calle Sevilla N24-358 y Guipúzcoa - La Floresta
Quito - Ecuador
Casilla postal 17-21-753 (593)23226-744


COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA


CON EL APOYO DE:

OXFAM
Danmark

PROGRAMA DE Defensores y Defensoras INDÍGENAS

# CICLO DE CAPACITACIÓN

## Minga Digital por los Defensores y Defensoras Indígenas de la Cuenca Amazónica

# MÓDULO 4

## TEMA:

**SEGURIDAD, CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DIGITALES: DEFENSA DIGITAL PARA ORGANIZACIONES SOCIALES**

Programa Defensa de Defensores y Defensoras Indígenas (PDDD) COICA

ABRIL 2022

COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA

# CONTENIDO

# INTRODUCCIÓN

La presente guía es un esfuerzo por sistematizar las experiencias de acompañamiento a organizaciones sociales en las temáticas referentes a seguridad digital. Partiendo de la urgencia de atención que requiere esta área, se proponen seis temas fundamentales para iniciar la defensa digital entre las organizaciones defensoras de derechos humanos, la naturaleza y los territorios.

La defensa digital tiene como principio el desarrollo de capacidades para disminuir los riesgos y amenazas en el uso de las tecnologías, desde una visión en la que la autonomía y protección permita a las organizaciones prepararse para sobrellevar distintos escenarios, fortalecer los procesos internos de la organización y aportar en la continuidad de su trabajo. En ese sentido, esta guía propone fortalecer las capacidades de las organizaciones, desarrollar conocimientos y generar diálogos acerca de las vulnerabilidades, amenazas y riesgos digitales que enfrentan las organizaciones y sus miembros.

Para cumplir con los objetivos planteados, el documento propone los siguientes temas:

**Gestión de riesgos e incidentes digitales:** hace referencia al análisis de riesgos, amenazas e incidentes que comúnmente enfrentan las organizaciones sociales y las personas defensoras de Derechos Humanos; además, se presentan herramientas para leer los peligros y reaccionar frente a ellos.

**Cifrado:** se aborda la temática de encriptación, explicando su significado y mostrando usos posibles a partir de ejemplos fácilmente comprensibles.

**Comunicaciones y correo electrónico seguro:** el contexto actual exige el uso de diferentes medios digitales de comunicación, por esta razón, se analiza, desde la perspectiva de la seguridad y las vulnerabilidades, las ofertas de servicios de mensajería instantánea, videoconferencia y correo electrónico.

**Respaldos:** hoy en día los equipos electrónicos (laptops, computadoras de escritorio, smartphones, tablets, etc.) contienen toda la información laboral y personal de una persona; en este capítulo se revisa la importancia de los respaldos periódicos de datos.

**Malware y actualizaciones:** hace referencia al malware, sus diferentes tipos y las estrategias para mantener la información protegida de posibles ataques.

**Plan de Seguridad Digital:** al final del documento se incluye el marco legal internacional para desarrollar un Plan de Seguridad Digital para avanzar en la ejecución de una estrategia de mitigación y reducción de vulneraciones, riesgos y amenazas digitales.

## Tema 1: Introducción a la Defensa Digital

### Presentación

La protección de las organizaciones y movimientos sociales depende de la capacidad de afrontar y actuar ante posibles incidentes de seguridad, así como de su disposición para generar estrategias de defensa y mantenimiento de herramientas activas de protección. Por este motivo, es fundamental saber identificar los incidentes de seguridad a partir de la comprensión de los riesgos y las amenazas para actuar oportunamente en la protección digital y física de las organizaciones de defensores de DDHH.

Es necesario entender que estos riesgos y amenazas dependen de los contextos en donde se desenvuelve la organización, el momento político y la actitud de sus integrantes. Los riesgos y amenazas son siempre cambiantes, por ello, reconocer los incidentes de seguridad permite generar respuestas acordes a cada contexto y a las necesidades de la organización.

### Incidentes de seguridad

Un incidente de seguridad es cualquier hecho o acontecimiento que pueda afectar la seguridad personal o de la organización, generando un impacto directo sobre el alcance de su trabajo y posibles acciones en contra de las personas o de toda la organización.

Los incidentes de seguridad no son una amenaza en sí mismos, sin embargo, para poder reaccionar frente a ellos, requieren de un proceso de atención, registro y análisis.

El reconocimiento de los incidentes permite cambiar comportamientos o actividades (usos y hábitos de las tecnologías) con el fin de hacer seguro el trabajo de la organización. Los incidentes son indicadores de la situación concreta de seguridad en la que se encuentra la organización y sus integrantes. Por ejemplo, después de identificar varios incidentes de seguridad, una organización puede darse cuenta de que la están vigilando: en ese momento puede hacer algo al respecto. Dichos incidentes son indicativos de la magnitud de la oposición al trabajo de la organización o de la presión que soporta la misma.

Todas las personas que trabajan en la defensa de los Derechos Humanos pueden vivir incidentes de seguridad debido a que su trabajo genera incomodidad a las grandes corporaciones, a los Estados y a las instituciones. Es importante entender que estos agresores potenciales probablemente ya tengan información sobre los movimientos y actividades de la organización y sus participantes. Entonces, la mejor respuesta son las estrategias de protección y mitigación que se puedan construir ante las agresiones en potencia.

**Todas las amenazas son incidentes de seguridad, pero no todos los incidentes de seguridad son amenazas.**

### ¿Por qué suceden las amenazas?

Las amenazas y los riesgos que puede vivir una organización y sus miembros significan que el trabajo que hacen es necesario, y puede haber personas o instituciones que quieran dificultarlo o detenerlo. Para que sea sostenible en el tiempo, es necesario proteger a todos aquellos que trabajan con Derechos Humanos, derechos de la naturaleza y los territorios, sin poner en riesgo la vida de las personas que integran las organizaciones, recordando que las acciones personales tienen un impacto colectivo.

### Amenazas

Una amenaza es una intención y una posibilidad de dañar la integridad física o moral de otra persona. Una amenaza declarada es una indicación de amedrentamiento para que la persona deje de hacer lo que está haciendo. Toda amenaza tiene las siguientes características: un objetivo, un origen y un medio de expresión, es decir, una manera en que se manifiesta.

Una amenaza es una experiencia individual que tiene un impacto doble: emocional y colectivo. No es lo mismo amenazar que constituir una amenaza real, es decir, ejecutarla. Muchas veces, no se hacen efectivas, por lo que es posible diferenciar entre amenazas directas e indirectas.

Las amenazas se asocian directamente con los riesgos, es decir, con las consecuencias potenciales a las que una persona puede enfrentarse si la misma se lleva a cabo.

Existen cuatro puntos para analizar una amenaza que permiten determinar los hechos relacionados con ella: el patrón de cómo se da, el objetivo, el origen y la conclusión razonable sobre dichas amenazas.

### Riesgos

Los riesgos son las vulnerabilidades de una organización o persona en función de las amenazas que experimenta, donde se hace referencia a un posible acontecimiento que causa daño. Es importante notar que los riesgos a los cuales está expuesta una organización o persona se encuentran directamente relacionados con las capacidades de mitigación que desarrollan.

El nivel de riesgo al que se enfrenta un grupo de personas defensoras de Derechos Humanos es mayor en relación a las amenazas recibidas, la vulnerabilidad y la capacidad de reaccionar ante ellas.

Dentro de un análisis de riesgo es fundamental como organización o persona entender las amenazas que se enfrentan, reconocer las propias vulnerabilidades e incrementar las capacidades, en función de que exista el menor riesgo posible.

### Defensa Digital: casos de análisis de riesgos

El ejercicio de hacer un análisis de riesgos permite a las organizaciones incrementar su seguridad y comunicación, y entender sus vulnerabilidades y capacidades.

Es necesario tomar en cuenta que los riesgos y las amenazas cambian con el tiempo, de acuerdo al cambio de contexto, las vulnerabilidades y las capacidades de una organización o persona. Por lo tanto, realizar un análisis de riesgos periódicamente puede ser fundamental para organizaciones que trabajan en contextos complejos o van a realizar una acción que los puede poner en peligro. Por ejemplo: una demanda al Estado por incumplimiento de la Constitución o una demanda a una empresa petrolera por contaminación.

Aumentar las capacidades en defensa digital toma tiempo debido a que es un trabajo que depende del compromiso de la organización y sus integrantes, e implica un hábito que se genera a partir de la práctica constante para disminuir las vulnerabilidades.

En caso de que una organización esté bajo ataque, es importante que pueda buscar apoyo de personas de confianza y abrir un diálogo sobre su situación con el fin de conformar un equipo que maneje la situación.

Para poder realizar un análisis de riesgos se debe tomar en cuenta:

1. Lectura y análisis del contexto.
2. Evaluación del nivel de riesgo al que se enfrenta la organización.
3. Desglose de riesgos: analizar uno por uno para entender y medir su/s impacto/s.
4. Otras cuestiones: ¿Qué hace posible cada riesgo? ¿Qué debe cambiar en la organización para mitigarlo/s? ¿De acuerdo a los componentes del riesgo, cuáles serían los procesos para su mitigación?

Estos cuatro pasos pueden generar claridad sobre cómo proceder en un corto o largo plazo, qué acciones tomar con respecto a la seguridad física, digital y emocional, y en cuanto a medidas legales y de infraestructura.

## Bitácora de incidentes digitales [1] [2]

La bitácora de incidentes digitales tiene el objetivo de registrar eventos, incidentes extraños, amenazas y situaciones de riesgo que afectan a la organización y por lo tanto a sus integrantes. Este documento permitirá hacer un análisis de riesgo con base a las situaciones de riesgo registradas durante un periodo de tiempo.

---

Esta sección ha sido elaborada con base a los siguientes documentos:

1 Eguren, E. Caraj, M. 2009. Protección para los Defensores de Derechos Humanos. Protection International. Bélgica. Primera Edición.

2 Protection International. Formación en Línea. 2020. Disponible en: https://e-learning.protectioninternational.org/?lang=es

La bitácora guarda estos incidentes para el análisis en una perspectiva amplia donde es fácil identificar patrones de vulneraciones como llamadas extrañas, censura de la comunicación, persecución a un integrante de la organización, robo y/o pérdida de equipos o documentos, etc. Esta herramienta permite entender dichas vulneraciones para actuar a partir de capacidades y medidas de seguridad.

La bitácora debería estar a cargo de un grupo de personas de la organización, ubicado en un lugar seguro para recibir una constante alimentación de las situaciones de amenaza.

El registro debe contener la fecha, la hora, el medio y el evento, de manera que se puedan entender los patrones de comportamiento en las agresiones y las vulnerabilidades de la organización y las personas que la conforman.

### Contraseñas

Al salir de la casa o de la oficina, se puede asegurar con llave una puerta para impedir la entrada de personas no invitadas. Tal como en el ámbito físico, en el digital las claves o contraseñas son las llaves que permiten el ingreso a cuentas personales y a los espacios digitales en donde se maneja información privada que no se desea difundir abiertamente. Por este motivo, las contraseñas juegan un rol fundamental en mantener segura la información. Dedicar tiempo a crearlas y cambiarlas periódicamente es una de las formas más básicas de cuidar la información personal y la de la organización.

Siguiendo esta reflexión, resulta pertinente hacerse estas preguntas: ¿Cuándo fue la última vez que modifiqué mi contraseña de correo electrónico? ¿Lo hago con regularidad? ¿Existe información que deseo proteger en mis cuentas?

En este sitio web es posible probar la fortaleza de una contraseña para entender que tan compleja debería ser: **https://howsecureismypassword.net**

Esta herramienta calcula el promedio de tiempo en el que una persona o máquina puede descifrar una contraseña.


Tomado de www.navegandolibres.org

Una contraseña segura debe tener mínimo doce caracteres, mayúsculas, minúsculas, números y símbolos (· $ % $ & /), puede estar en dos idiomas o ser una canción, poema, libro que te gusta, pero sobre todo debe ser única y específica para cada cuenta en particular. Es importante notar que las contraseñas más seguras son las que recuerdas, aunque es mejor evitar utilizar información relacionada directamente a ti y que es pública como: nombres de un familiar (hijo/a, padre, madre), mascotas o de la organización donde trabajas.

Cambiar las contraseñas con regularidad es una barrera importante de seguridad, simple de lograr y muy efectiva. Para guardar las contraseñas no es necesario recordarlas todas, lo más práctico y seguro es manejar un administrador de contraseñas. Anotarlas nunca es recomendable porque puede convertirse en un factor de riesgo.

### Administradores de contraseñas

Existen programas que ayudan a administrar contraseñas, es decir, son bases de datos donde se pueden almacenar de manera segura todas las contraseñas y cambiarlas periódicamente. Para ingresar solo se necesita una contraseña maestra, una llave maestra con la que solo basta recordar una contraseña para ingresar a todas las demás. Estos programas pueden ser individuales o colaborativos; aquí se dan algunos ejemplos:

**Keepass:** Es sumamente popular, puede descargarse en todos los sistemas operativos o en dispositivos celulares
https://keepass.info/

**Psono:** Permite tener contraseñas personales y colaborativas
https://psono.com/

### Práctica

A partir de un ejemplo real o ficticio de incidentes, amenazas y riesgos que haya vivido una organización social, realizar un análisis de riesgos para la misma:

1. Describir a la organización (área de trabajo, equipo y relaciones).
2. Explicar el contexto político, económico, social y cultural de la organización.
3. Describir el caso detallando incidentes, amenazas, riesgos, vulnerabilidades y capacidades.
4. Aplicar la fórmula de análisis de riesgo: RIESGO = Amenaza x Vulnerabilidad / Capacidad.
5. Enumerar los riesgos encontrados.
6. Realizar una bitácora de incidentes de seguridad de este ejemplo, donde se describan cinco incidentes registrados durante un mes. Para poder analizarlos, detallar fecha, medio, descripción, a quién le pasó y quién lo reportó.
7. Instalar Keepass.
8. Crear tu base de datos en Keepass y empezar a administrar tus contraseñas de manera segura.

## Tema 2: Cifrado

### Descripción

El cifrado es uno de los métodos más efectivos para la protección de derechos digitales, principalmente el de la privacidad. Permite asegurar que los archivos, mensajes o demás datos almacenados y procesados en los dispositivos personales y de trabajo estén disponibles solamente para el propietario y para las personas a las que éste decide dar acceso.

Cifrar y encriptar son términos que se usan frecuentemente y en distintos ámbitos, pero: ¿Qué es encriptar? ¿Para qué sirve? ¿Cómo se hace?
Según Wikipedia: "En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo".[3]

### Un caso hipotético

Una mañana llegas a tu lugar de trabajo y descubres que las computadoras y demás dispositivos electrónicos han desaparecido. Imagina que en ese momento tú o la organización en la que participas estaba realizando una investigación sobre violaciones a Derechos Humanos. ¿Qué es lo que harías? Supongamos también que en esos equipos tenías testimonios, evidencias, nombres, direcciones y contactos de las personas que sustentan la denuncia y que, por obvias razones, esa información no debía ser revelada y además imagina que en la investigación han aparecido nombres de varios políticos y funcionarios del gobierno.
En el mejor de los escenarios, quienes se llevaron los equipos los venden por partes o completos, son formateados y toda la información borrada. En el peor de los casos, esos equipos podrían estar siendo analizados y la información que era confidencial podría ser compartida y difundida entre los implicados. Este escenario puede sonar familiar, ya que en muchos países son comunes situaciones como esta. Pero, además, todo se agudiza cuando una filtración de fuentes puede significar el aumento de la vulnerabilidad de la organización y las personas que la integran, siendo objeto de amenazas, difamaciones, demandas y hasta desapariciones forzadas.

3 Wikipedia. Cifrado. Disponible en: https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)

Ahora bien, si en el hipotético escenario se ha incorporado el cifrado de la información, la situación se torna algo menos grave, pues si las claves de descifrado no fueron comprometidas dará igual si los equipos fueron robados para ser vendidos o para buscar en ellos información clasificada, de todas maneras, la información no será accesible para esos terceros, por lo menos no tan fácilmente.

## Glosario

A continuación, se enlistan las definiciones de algunos conceptos para garantizar un entendimiento común que permita el desarrollo del código análogo:

**Mensaje:** Es lo que se quiere transmitir. Para este ejemplo de cifrado se usarán nombres.

**Algoritmo**[4]**:** Es un conjunto de reglas definidas, ordenadas y finitas que permite solucionar un problema, realizar un cómputo, procesar datos o llevar a cabo una tarea. En este caso se usará ROT13[5] como algoritmo de cifrado.

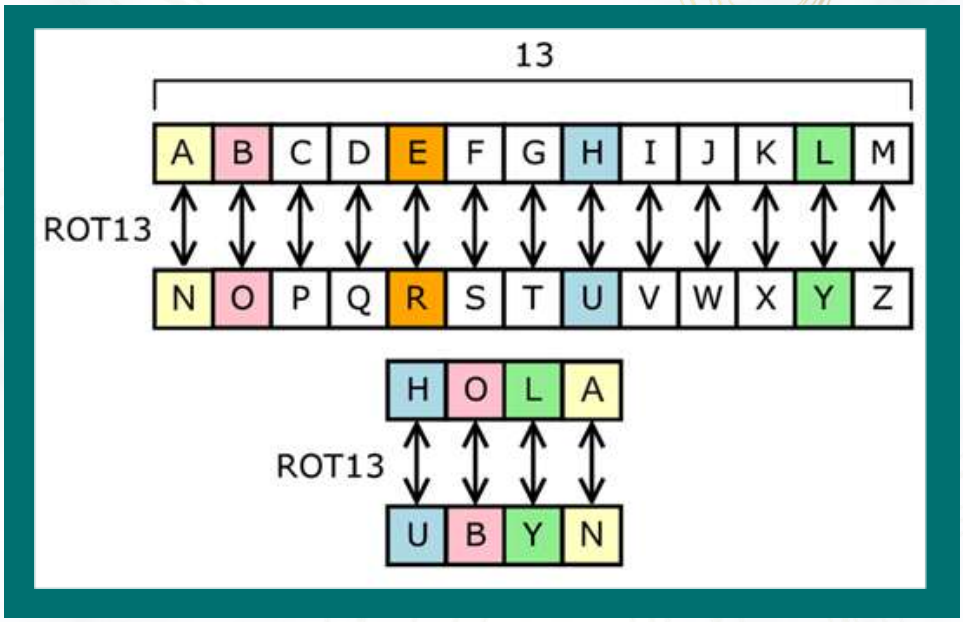
**Llaves:** En el cifrado existen normalmente dos llaves: una pública (es la que se entrega a quienes van a poder leer los mensajes y que se recibe de las personas que envían mensajes cifrados) y la privada (es la que se usa para cifrar los mensajes y que junto con la llave pública de otra persona permite leer los mensajes que se reciben). Las llaves públicas se comparten y las privadas son confidenciales. Para este ejercicio el algoritmo ROT13 será ambas llaves.

**Cifrado:** Es el proceso de transformar un mensaje legible a uno nuevo que solo lo pueden leer las personas a las que se les da permiso, o tienen la llave pública de la persona emisora del mensaje.

**Descifrado:** Es el proceso inverso al cifrado. Significa transformar un mensaje cifrado (ilegible) en uno legible.

Para entender el proceso, se cifra un mensaje utilizando el ROT13, un método que propone hacer un intercambio de letras por sus opuestas conforme a la siguiente ilustración:

4 Wikipedia. Algoritmo. Disponible en: https://es.wikipedia.org/wiki/Algoritmo
5 Wikipedia. ROT13. Disponible en: https://es.wikipedia.org/wiki/ROT13




La ilustración ejemplifica cómo se puede usar el sistema ROT13 para transformar el mensaje “HOLA” en “UBYN”. El proceso es realmente simple: se reemplaza la H por su opuesta U, la O por B, la L por Y y la A por N.

**Práctica**

Para la siguiente práctica, primero realizaremos el siguiente ejemplo para descifrar un código.

Ahora, se aplica el algoritmo para transformar el siguiente nombre:

JUANA VEGA.

Entonces, con la ilustración como referencia, las letras correspondientes al mensaje son reemplazadas por su opuesta correspondiente: la J por la W, la U por la H, la A por la N, la N por la A, la A por la N, el espacio queda tal cual, la V por la I, la E por la R, la G por la T y finalmente la A por la N:

**ORIGINAL**

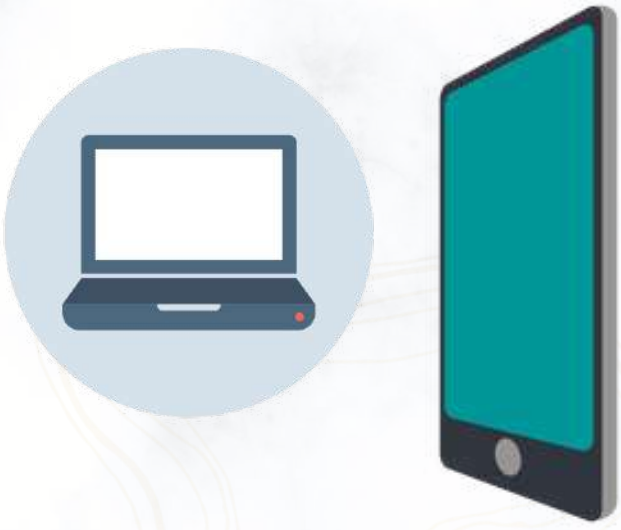
J U A N A V E G A

**CIFRADO CON ROT13**

W H N A N I R T N

El mensaje cifrado finalmente es:

**WHNAN IRTN.**



En este caso, el algoritmo es igual a las llaves antes mencionadas, pues la forma en la que se puede entregar el mensaje "WHNAN IRTN" a otra persona y garantizar su comprensión es indicarle que el procedimiento (algoritmo) que se utilizó para cifrarlo fue ROT13 y que entonces debe usarse el mismo algoritmo para descifrarlo.

**Ejercicio:**
Usando ROT13, descifrar el siguiente mensaje:
**UR QRFPVSENQB ZV CEVZRE ZRAFNWR**

## Cifrar equipos móviles y de escritorio (multiplataforma)

A continuación, se mencionan algunas herramientas y recursos que permiten el cifrado de dispositivos:

### Equipos móviles

**Android:** Google introdujo la funcionalidad "Cifrado de Disco Completo" a finales de 2013 en la versión 4.4 de Android y posteriormente han ido incluyendo mejoras. El proceso es distinto dependiendo de la versión y del fabricante del dispositivo, pero para simplificarlo se puede resumir en los siguientes pasos:

- Ir a la configuración del dispositivo.
- Buscar "Seguridad" y luego "Bloqueo de pantalla".
- Seleccionar "PIN", "Patrón" o "Contraseña" (la mejor opción es la de contraseña).
- Activar la opción "Inicio seguro".

**iOS:** Desde 2014, Apple implementó el cifrado de dispositivos móviles, para activarlo se debe:

- Ir a la configuración del dispositivo.
- Seleccionar "Touch ID & Passcode" (o huella digital).
- Activar "Passcode" (o huella digital).
- Ingresar una contraseña segura.

### Equipos de escritorio

**Veracrypt:** Es un software libre multiplataforma. Esto quiere decir que funciona en varios sistemas operativos y es compatible con GNU/Linux, Mac OS y Microsoft Windows. Su característica más destacada es la compatibilidad entre los sistemas antes indicados:
https://www.veracrypt.fr/code/VeraCrypt/

**LUKS:** Es el sistema de encriptación preferido en los sistemas operativos GNU/Linux. Viene por defecto y es muy fácil de configurar durante la instalación del sistema operativo:
https://github.com/guardianproject/LUKS

**FileVault:** Es el sistema de cifrado de discos que utiliza Apple en sus sistemas operativos Mac OS:
https://support.apple.com/es-co/HT204837

**Bitlocker:** De los sistemas operativos más utilizados en equipos de escritorio, Microsoft Windows fue el último en ofrecer un sistema integrado para el cifrado de discos. Bitlocker fue introducido recientemente en su sistema operativo Windows 10:
https://support.microsoft.com/es-ec/help/4028713/windows-10-turn-on-device-encryption

### Cifrar carpetas

**Veracrypt:** Además de permitir el cifrado de discos completos (unidades de sistema operativo y externas) también permite crear "volúmenes" cifrados, que son "contenedores" en los que podrás almacenar información sensible sin tener que cifrar todo tu disco:
https://www.veracrypt.fr/code/VeraCrypt/

**Cryptomator:** Esta es otra interesante opción. Es un sistema de código abierto, que además de funcionar en sistemas de escritorio también es compatible con Android e iOS. Con este sistema al igual que con Veracrypt, podrás crear "contenedores" cifrados de archivos y compartirlos con otras personas o entre dispositivos:
https://cryptomator.org/

### Práctica

1. Crear un volumen o contenedor cifrado con alguna de las herramientas antes mencionadas, cargar algunos archivos y compartirlos con otras personas.
2. Verificar que un dispositivo móvil esté cifrado.
3. Compartir lo aprendido con otras personas de la organización y discutir las ventajas de proteger la información con métodos de cifrado.

## Tema 3: Comunicaciones y correo electrónico seguro

En este capítulo revisaremos las comunicaciones y el correo electrónico seguro que, al igual que las contraseñas y el encriptado de archivos, son muy importantes porque hoy en día se han convertido en herramientas indispensables en nuestro día a día, ya sea para conversar con un familiar o para interactuar con compañeros de trabajo. Por eso es fundamental saber qué tan seguros son los servicios y cómo podemos protegernos y evitar posibles filtraciones de información sensible para nuestra organización.

### Mensajería instantánea

Hoy en día las aplicaciones de mensajería instantánea son tan comunes que al momento de comprar un teléfono inteligente ya viene con algunas aplicaciones de este tipo instaladas por defecto (WhatsApp, Messenger, Hangouts, etc.).

La mensajería instantánea es una forma de comunicación entre dos o más personas basado en texto y dispone de ciertas características:

1. Gestión de contactos
    - 1.1. Mostrar distintos “estados”
    - 1.2. Mostrar un mensaje de estado
    - 1.3. Registrar y borrar usuarios de la lista de contactos
    - 1.4. Posibilidad de agrupar los contactos
    - 1.5. Posibilidad de utilizar un avatar
2. Conversación
    - 2.1. Tipos de mensajes
        - 2.1.1. Avisos
        - 2.1.2. Invitación a chatear
        - 2.1.3. Mensaje emergente

2.2. Aviso de escritura

2.3. Uso de emoticones o emojis

2.4. Charlas en grupo

3. Otras características

3.1. Envío de archivos

3.2. Posibilidad de interoperar con otros sistemas de comunicación

3.3. Utilización de Bots

Como se puede apreciar, estas son algunas de las características que ofrecen los servicios de mensajería instantánea. Pero se conoce como "mensajería instantánea segura" a aquella que se da cuando dos entidades se están comunicando y no quieren a un tercero leyendo o escuchando.

La gran mayoría de los servicios de mensajería instantánea son gratuitos, lo que lleva a cuestionarse cómo mantienen las infraestructuras que los hacen funcionar. Entonces conviene recordar la siguiente frase: "Cuando un producto o servicio es gratuito, tú eres el producto".

Ahora bien: ¿Cómo puede alguien comunicarse de manera segura? Existen aplicaciones que garantizan que la información que se va a compartir a través de ella no se filtrará a terceros. En el siguiente cuadro se puede ver cuáles aplicaciones son seguras:

| | WhatsApp | Messanger | Telegram | Instagram | Hangouts | SnapChat | Signal |
|---|---|---|---|---|---|---|---|
| Cifrado | Si | No | No por defecto | No | No | No | Si |
| Autodestrucción | No | No | Si | No | No | ¿? | Si |
| Se guarda en Servidores | Si | Si | Si | Si | Si | Si | No |
| Chats Grupales | Si | Si | Si | No | Si | No | Si |
| ¿Quién es el Dueño? | Facebook, Inc. | Facebook, Inc. | Telegram | Facebook, Inc. | Google, LLC | Snap Inc. | Signal Foundation, Signal Messenger LLC |

Como se puede apreciar, no todas las aplicaciones ofrecen el cifrado de las comunicaciones, por lo que en principio estas aplicaciones no son recomendadas para compartir información o archivos confidenciales. Además, en algunos casos en que ofrecen cifrado lo hacen sin garantizar que las comunicaciones no se filtren, por ejemplo, en el caso de WhatsApp, que ha recibido varias acusaciones por filtrado de información de los usuarios.

## Tema 4: Respaldos

### Realizar respaldos de información

En los dispositivos electrónicos se guarda mucha información indispensable en el día a día. ¿Qué pasaría si cuando se trata de acceder a uno de estos documentos no se puede visualizar, ya sea por un fallo del disco, un fallo eléctrico, una infección por la instalación de algún software malicioso o, en el peor de los casos, porque se extravió o fue robado dicho equipo?

La respuesta es simple: se puede recuperar toda la información con un respaldo (siempre y cuando, se haya hecho con anterioridad). Un respaldo hecho oportunamente permite recuperar toda la información y estar nuevamente operativos en cuestión de horas.
En 2017, ESET[6] realizó una encuesta que demostró que el 91% de la comunidad entrevistada en Latinoamérica sí respalda su información. Pero, ¿con qué frecuencia lo hacen?

### ¿Qué información se debe respaldar?

La información que se debe tomar en cuenta a la hora de hacer un respaldo es aquella que sea más difícil de recuperar o recrear (por ejemplo: fotos, trabajos académicos, proyectos y claves).

### ¿Qué tipo de respaldo se debe elegir?

Algunas personas optan por sacar un respaldo total del equipo en cuestión, otras los archivos más importantes y otras solo respaldan archivos de configuración del sistema. Esto depende totalmente de la necesidad de cada persona, ya que se debe tomar en cuenta el espacio de almacenamiento disponible en donde se vaya a almacenar dicho respaldo (disco duro, CD, DVD o incluso en la nube).

(6)Fundada en 1992, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas. Más información disponible en https://es.wikipedia.org/wiki/ESET

### ¿Qué tipo de almacenamiento se debe elegir?

Como se mencionó anteriormente, se debe contar con espacio suficiente para almacenar el o los respaldos. Si se hace en un disco duro externo es recomendable que el uso de éste sea exclusivo para el almacenamiento de respaldos, previniendo un posible deterioro por uso excesivo.

No todos los servicios de almacenamiento en la nube (internet) son recomendados para crear respaldos debido a que no garantizan seguridad de la información ni la restricción de acceso a ella; ese es el caso de Google Drive.

Sin embargo, existen opciones como Mega.nz https://mega.nz/que cifra toda la información que se almacena en ella, o Nextcloud https://nextcloud.com/ que permite levantar una nube propia.

### Frecuencia de respaldo

Como se mencionó anteriormente, si se busca que el tiempo de respuesta ante cualquier daño de un equipo o dispositivo sea rápido, lo ideal es tener un respaldo lo más actualizado posible, minimizando los impactos provocados por la pérdida de información.

### Recursos

Una vez entendida la importancia de realizar respaldos periódicos de la información, surgen las siguientes preguntas: ¿Cómo sacar un respaldo? ¿Basta con copiar los archivos de un lugar a otro? ¿Qué programas se pueden utilizar para esta tarea?
Existen varias herramientas para realizar respaldos. A continuación, se listan algunas de acuerdo al sistema operativo:

- Guía de DragonJar para GNU/Linux.
- Guía de Nettix para MS Windows: Herramientas para Hacer Backup en Windows 10.
- Para Mac OS: La mayoría de alternativas que existen para MS Windows también tienen su versión para Mac OS, por lo que no es necesario listar alternativas que funcionen únicamente para este sistema operativo.

### Prácticas

1. Analizar y ordenar la información que es indispensable y que debe estar respaldada.
2. Analizar qué herramienta es más conveniente para hacer un respaldo.
3. Analizar con qué frecuencia conviene hacer un respaldo de la información importante.
4. Buscar un servicio de almacenamiento que se ajuste a las necesidades para almacenar uno o más respaldos.

## Tema 5: Malware y actualizaciones

### Malware

Iniciemos respondiendo algunas preguntas: ¿De qué protege un antivirus? ¿Qué es un virus informático? Y finalmente: ¿Existen otras amenazas además de los virus? Hace muchos años que se escucha hablar de virus y antivirus. Este capítulo tiene el objetivo de explicar qué es lo importante sobre ellos y cómo proteger los dispositivos de potenciales invasiones.

A pesar de que es común hablar de "antivirus", los programas que reciben ese nombre son en realidad antimalware. El antimalware es un software que pretende proteger equipos y dispositivos contra varios tipos de software y programas maliciosos que afectan a los dispositivos. Para entender mejor este tema se listan algunos de los tipos más comunes de malware:

### Virus informáticos

Se llaman así debido a que su comportamiento es similar al que tienen los virus en los cuerpos orgánicos, es decir:

- Requieren de un anfitrión para reproducirse.
- Una vez que el anfitrión ha sido infectado, realizan múltiples copias de sí mismos.
- Buscan infectar a otros (por uno o diversos medios).

### Los virus buscan:

- Replicarse (crear copias de sí mismos).
- Causar problemas de velocidad en el equipo infectado.
- Saturar los recursos.

Como los virus biológicos que afectan a personas y animales, los virus informáticos destruyen o corrompen el funcionamiento del anfitrión, dejando el sistema sin capacidad de recuperarse. Entonces, cuando se habla de antivirus en informática, se alude a los programas de defensa contra los virus.

### Troyanos

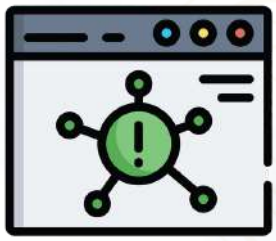
En informática, se llama "troyano" a cualquier programa que toma la forma de otro ocultándose en su interior, y espera a que un usuario, despistado o desinformado, lo ejecute. A partir de ese momento puede tomar control completo del equipo y, desde entonces, permitir a quien lo desarrolló, controlar de manera remota la computadora infectada y todos los dispositivos conectados, incluso permitiendo realizar acciones como encender la cámara sin permiso, leer información de los discos, imprimir documentos o cambiar los parámetros de conexión a internet, entre otras.

### Gusanos

También se los conoce por su nombre en inglés: ***worms***. Este tipo de malware busca destruir y saturar equipos, redes e infraestructura. Se replica rápidamente y es altamente dañino. Este tipo de malware ha llegado a bloquear incluso centrales eléctricas, nucleares y otras grandes infraestructuras de cómputo en todo el mundo. Se puede decir que es un tipo de virus pues comparte varias de sus características, aunque la diferencia fundamental consiste en que no infectan archivos en la computadora.

### Spyware

Este tipo de malware se especializa en espiar. Se trata de un software que pretende recopilar la mayor cantidad de información de su víctima u objetivo, y enviarla a terceros. Existen muchísimos de estos sistemas, inclusive los hay de uso gubernamental y empresarial. Para profundizar un poco más al respecto, se recomienda el artículo NSO Group suplantó a Facebook para instalar malware de vigilancia de R3D, Red de Defensa de Derechos Digitales.[7]



7 Red en Defensa de los Defensores Digitales. NSO Group suplantó a Facebook para instalar malware de vigilancia. Disponible en: https://r3d.mx/2020/05/20/nso-group-suplanto-a-facebook-para-instalar-malware-de-vigilancia/

## Ransomware

Este tipo de software malicioso se ha popularizado porque miles de personas han sido afectadas por diferentes productos de este tipo. ¿Qué es lo que hace? Su nombre lo sugiere: ransom es una palabra inglesa que significa "rescate". Funciona de la siguiente manera: al infectar un equipo o dispositivo, el malware se activa e inicia un proceso de encriptación de todos los documentos no esenciales para el sistema operativo. Este proceso es transparente, ya que se puede notar algo de lentitud en el funcionamiento de la computadora. Una vez que ha terminado el proceso, la información y los archivos dejan de ser accesibles y, normalmente, el fondo de escritorio cambia o aparece una ventana con las instrucciones para el rescate como la que se muestra a continuación:


Algunos de los ataques de ransomware pueden tener solución, aunque la mayoría no; esto significa que los archivos de las personas afectadas permanecerán inaccesibles con la pérdida que ello implica.

## ¿Cómo puede llegar un malware a un equipo?

Los vectores de infección más comunes son dos, el primero ocurre a través del uso de software "pirata". Esto se debe a que, si bien existen personas que desbloquean (o crackean) los programas de la computadora para permitir a otras su uso y socializar el conocimiento, hay terceros que buscan beneficiarse o causar daño durante este proceso.

El segundo modo más común de infección sucede a través de enlaces de internet o archivos, que pueden llegar por medio de correos electrónicos extraños o no deseados, o también por medio del uso de memorias flash u otros dispositivos de almacenamiento.

### ¿Cómo protegerse contra los malwares?

- Usar un antivirus o antimalware en los equipos.
- Al insertar una memoria flash u otro dispositivo de almacenamiento, permitir al antivirus analizarlo.
- Evitar abrir enlaces en mensajes de texto, correos, chats y descargar archivos adjuntos extraños o de remitentes desconocidos.
- Utilizar siempre páginas web seguras (https).
- Actualizar regularmente sistemas operativos y programas.
- Al instalar un antivirus, puede ser más conveniente una versión gratuita que una versión completa "pirata".
- Mantener el antivirus actualizado (solo se puede tener un antivirus funcionando a la vez en cada equipo, poner más de uno puede hacer que el equipo falle).
- Nunca pero nunca hacer caso a anuncios en páginas web en los que se indica que se han detectado amenazas en un equipo. Todos estos anuncios son un engaño.

### Actualizaciones

Se suele pensar que las actualizaciones son molestas e innecesarias. Lastimosamente algunos fabricantes de software como Microsoft han hecho incómoda la experiencia de actualizaciones, a pesar de que constituye un proceso necesario para solucionar problemas o errores detectados en los sistemas y programas. Por ejemplo, una actualización de Windows corrige problemas en el sistema operativo, mientras que una actualización de la base de datos del programa antivirus agrega nuevas capacidades para la detección y eliminación de malware. Sucede lo mismo en el caso de actualizaciones de cualquier otro tipo de aplicaciones en todo tipo de dispositivo.

Las actualizaciones son importantes, pero, en algunos casos, traen también algunos riesgos:

- En algunos casos, el software advierte sobre la necesidad de hacer un respaldo previo y hacerlo puede evitar muchos problemas más adelante.
- Los programas "piratas" suelen recomendar la desactivación de los antivirus o de las actualizaciones del sistema operativo y esto puede causar otros problemas.

Por lo general, el uso del sistema operativo libre GNU/Linux es por defecto suficiente para cualquier persona que usa su computadora para navegar en internet, comprar y vender productos, usar redes sociales, desarrollar documentos y mantener comunicaciones. Por lo tanto, la mejor recomendación en torno a la seguridad digital es comenzar a investigar las bondades de usar sistemas operativos basados en software libre.[8]

Sistemas operativos como Debian, Linux Mint o Fedora, entre otras opciones, traen por defecto una suite de ofimática[9] y sus actualizaciones son libres y gratuitas, por lo que sin mucho esfuerzo es posible tener toda la información resguardada.

### Recursos

Algunos de los antivirus gratuitos con mejor reputación en orden alfabético son los siguientes:

- **AVG:** https://www.avg.com/es-ww/free-antivirus-download
- **Avira:** https://www.avira.com/es/free-antivirus-windows
- **Bitdefender:** https://www.bitdefender.com/solutions/free.html
- **Karsperky:** https://latam.kaspersky.com/free-antivirus
- **Malwarebytes:** https://es.malwarebytes.com/mwb-download

Y algunos recursos sobre actualizaciones:

- **Guía GenBeta**: Cómo actualizar Windows a la última versión (muestra el paso a paso para Windows 7, 8 y 10).
- **Guía de Google:** Cómo consultar y actualizar tu versión de Android.
- **Guía de Apple:** Actualizar el iPhone, iPad o iPod touch.

8 Wikipedia. Software Libre. Disponible en: https://es.wikipedia.org/wiki/Software_libre

9 Según Wikipedia, ofimática es el conjunto de técnicas, aplicaciones y herramientas informáticas que se utilizan en funciones de oficina para optimizar, automatizar, mejorar tareas y procedimientos relacionados. Más información disponible en https://es.wikipedia.org/wiki/Ofim%C3%A1tica

### Práctica

1. Instalar uno o varios de los antimalware/antivirus gratuitos en una computadora y en un teléfono celular. En caso de instalar más de uno, desactivar o desinstalar siempre el anterior, ya que solo uno puede quedar activo.
2. Revisar el estado de equipos con respecto a las actualizaciones automáticas.

## Anexo: Plan de Seguridad Digital [10] [11] [12]

Las principales preocupaciones que tienen las organizaciones a la hora de pensar en su seguridad digital son el marco legal y el soporte de la documentación. Este documento permite sentar las bases y perfilar una estructura formal para abordar una estrategia integral.
La mejor forma de iniciar este proceso es con una reunión interna, lo más amplia posible, en la que se piensen los retos y las necesidades que tiene la organización y todas las personas que la componen. Una lluvia de ideas puede servir como base. Es importante que el proceso se haga hacia adentro de la organización y que todas las personas puedan participar y proponer

Preguntas que pueden guiar la lluvia de ideas: ¿Qué información producimos? ¿Qué información intercambiamos? ¿Manejamos información sensible? ¿Qué medios usamos para trabajar con esta información? ¿A qué riesgos estamos expuestas y expuestos? ¿Qué pensamos que deberíamos hacer mejor a la hora de manejar la información con la que trabajamos?

El presente documento tiene el objetivo de definir un plan de mejoras en Tecnologías de la Información (TI) para la organización, aplicable en un intervalo razonable de tiempo. Se propone un año para la ejecución del plan, estableciendo objetivos medibles y cuantificables que permitan a la organización y a las personas:

---

Esta sección ha sido elaborada con base a los siguientes documentos:
10 Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000, una traducción idéntica de la Norma Internacional ISO/IEC 27000:2016, Information technology — Security techniques — Information security management systems — Overview and vocabulary. El Servicio Ecuatoriano de Normalización, INEN, es el responsable de la traducción de esta Norma Técnica Ecuatoriana.
11 Esquema de Seguridad de la Información EGSI. Registro Oficial Suplemento No. 88 del 25 de septiembre del 2013
12 Política de Seguridad de Información en el Ministerio de Telecomunicaciones y de la Sociedad de la Información, de la República del Ecuador. Acuerdo Ministerial No. 005-2016

- Desarrollar, aprobar e implementar un Plan de Seguridad Digital basado en el Sistema de Gestión de Seguridad de la Información (ISO 27001).
- Actualizar periódicamente el Plan de Seguridad Digital conforme su avance, las necesidades y recursos de la organización.

## PLAN DE SEGURIDAD DIGITAL ANTECEDENTES (MARCO LEGAL NACIONAL E INTERNACIONAL)

El artículo 12 de la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de Naciones Unidas, establece que el derecho a la vida privada es un derecho humano:

*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de Naciones Unidas, consagra al respecto lo siguiente:

1. *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, o lugar físico, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
2. *Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*

[A continuación se sugiere incluir el marco legal de cada país que garantice el derecho a la protección de la comunicación personal y la confidencialidad de los datos digitales]

El presente documento establece un marco de referencia para mejorar la seguridad y gestión de los activos de información de [nombre de la organización] y propone la implementación del Sistema de Gestión de Seguridad de la Información para la Gestión de Seguridad de la Información en lo que sea relevante, pertinente y que brinde valor a la organización.

### Declaración

La organización [nombre de tu organización] implementará un Sistema de Gestión de Seguridad de la Información cumpliendo con los principios de confidencialidad, integridad y disponibilidad de sus activos de información, promoviendo una gestión de riesgos y una cultura de seguridad.

## Descripción

Por medio del presente se busca incorporar en los procesos de gestión interna políticas, normas y procedimientos para la seguridad de la información, así como la aplicación de estándares mínimos en el uso, almacenamiento, acceso y distribución de la información.

Por lo tanto, es absolutamente necesario que todas las personas que participen en la gestión de información de la organización cumplan las normativas que se dicten y estén vigentes, a través de la implantación de un Sistema de Gestión de Seguridad de la Información orientado al resguardo de los activos de información.

El documento, las directrices y los alcances son susceptibles de mejora continua, siendo factibles las modificaciones, actualizaciones y cambios periódicos que la organización considere pertinentes.

## Objetivos

- Identificar, clasificar, categorizar y mantener actualizados los activos de información.
- Identificar a las y los responsables de la seguridad de los activos de información.
- Determinar los roles, responsabilidades y competencias de las y los miembros de la organización que tengan relación con los activos de información.
- Proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información y tecnologías para su procesamiento.
- Detectar, eliminar o mitigar las vulnerabilidades y los riesgos que amenacen los activos de información.
- Establecer, actualizar y difundir normas, procedimientos e instructivos para la manipulación, uso y resguardo adecuado de los activos de información.
- Monitorear y mantener actualizado el Sistema de Gestión de Seguridad de la Información, y establecer los mecanismos de seguimiento y control de los activos de información y tecnologías de procesamiento.
- Difundir el Plan de Seguridad Digital y capacitar a todas las personas que trabajan con la organización.

### Roles y responsabilidades

Para dar seguimiento, continuidad y cumplimiento a lo establecido en la Plan de Seguridad Digital, se establecen los siguientes roles y responsabilidades: **[Definir desde la organización, qué persona o grupo de personas asume los siguientes roles]**

### Oficial de Seguridad digital

Persona que cumple la función de supervisar el cumplimiento del presente plan y de coordinar las funciones del comité. Su función es liderar el establecimiento, la implementación y el mantenimiento del **Sistema de Gestión de Seguridad Digital.**

### Comité o Asamblea de Seguridad de la Información

Es un cuerpo integrado por personas de la organización, destinado a asegurar la implementación del **Sistema de Gestión de Seguridad Digital.** Sus funciones son: proponer, impulsar, promover y revisar periódicamente el Sistema de Gestión de Seguridad Digital.

### Responsable de TI

Persona que cumple la función de cubrir los requerimientos de seguridad informática establecidos y supervisar las tareas de implementación y mantenimiento de sistemas.

### Miembros de la organización

Personas que usan los activos de la información y los sistemas para su procesamiento. Son las y los responsables de conocer, cumplir y hacer cumplir el plan y los procedimientos de seguridad digital. Tienen, además, la responsabilidad de reportar incidentes de seguridad.

### ACTIVIDADES

**[Aquí va el plan, con la forma de un listado de actividades cuyo orden puede variar según la importancia que tengan para la organización. Se trata básicamente de organizar la lluvia de ideas, guiándose por los objetivos planteados. Idealmente las actividades deben establecerse de acuerdo a fechas para su cumplimiento. Pueden tener el formato de una tabla, un cronograma o un simple listado.]**

**Ejemplos de actividades a realizarse:**

1. Incorporar costos de implementación por actividad.
2. Implementar un sistema de videoconferencia seguro.
3. Herramientas y técnicas para mejorar en la seguridad y en el rendimiento de la red institucional de la organización:
   a. Implementar un DNS sobre TLS seguro.
   b. Instalar un Proxy de Red.
   c. Evaluar la posible adquisición de una VPN institucional.
4. Implementar un Sistema de Gestión documental de bajo costo con las mejores funcionalidades disponibles:
   a. Evaluar distintas opciones de software libre (como NextCloud o Alfresco).
   b. Realizar un presupuesto para la implementación y mantenimiento.
      i. Analizar la capacidad de almacenamiento actual y dispositivos de cómputo.
      ii. Costos de almacenamiento.
      iii. Costos de mantenimiento.
   c. Implementar Sistema de Gestión Documental.
5. Implementar mejores prácticas en la gestión y mantenimiento de archivos.
   a. Política y manual para el cifrado de equipos para protección de los activos de la información.
      i. Realizar el cifrado de dispositivos móviles como tablets, celulares, etc.
      ii. Realizar el cifrado de dispositivos de almacenamiento externos como memorias flash, discos rígidos, etc.
   b. Política y manual para comunicaciones seguras.

**Ejemplo de tabla:**

| ACTIVIDAD | PRESUPUESTO | 1° mes | 2° mes | 3° mes | 4° mes | .... |
|---|---|---|---|---|---|---|
| Incorporar costos de implementación por actividad | 0.00 $ | | | | | |
| Implementar Sistema de Videoconferencia seguro | 0.00 $ | | | | | |
| Herramientas y técnicas para mejorar en la seguridad y en el rendimiento de la red institucional de la organización | 0.00 $ | | | | | |

# GLOSARIO

### Sistema de Gestión de Seguridad de la Información (SGSI)

Es un conjunto de procesos que permiten gestionar la seguridad de la información de forma sistemática. Estos procesos serán levantados sobre la base de un enfoque de mejora continua. Un SGSI parte de una evaluación de riesgos en la que se definen medidas de mitigación de aquellos riesgos que se evalúen como inaceptables y contempla una mejora continua con el objetivo de que madure el sistema a lo largo del tiempo.

### Activos de Información

Comprende a los sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información. La información es uno de los activos más importantes de las instituciones y organizaciones, en todas las formas en que ésta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales; y en todos los medios de almacenamiento: magnéticos, ópticos, electrónicos o impresos.

### Seguridad de los Activos de Información

Se trata de proteger, resguardar y asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías implicadas para su procesamiento, a efecto de garantizar la continuidad operacional de la organización.

### Matriz de riesgos

Documento que permite mapear los principales riesgos y amenazas a la seguridad de la información de una organización. También permite describirlos y analizar el estado de cada uno, además de dar pie a un plan para su mitigación.

### Confidencialidad

Se garantiza que la información sea accesible solamente a aquellas personas autorizadas a tener acceso a la misma.

**Disponibilidad**

Se garantiza que las y los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella, toda vez que lo requieran.

**Integridad**

Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

## BIBLIOGRAFÍA


Eguren, E. Caraj, M. 2009. Protección para los Defensores de Derechos Humanos. Protection International. Bélgica. Primera Edición.

Esquema de Seguridad de la Información EGSI. Registro Oficial Suplemento No. 88 del 25 de septiembre del 2013.

Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000. Traducción de la Norma Internacional ISO/IEC 27000:2016, Information technology — Security techniques — Information security management systems — Overview and vocabulary.

Política de Seguridad de Información en el Ministerio de Telecomunicaciones y de la Sociedad de la Información, de la República del Ecuador.Acuerdo Ministerial No. 005-2016.

Protection International. Formación en Línea. 2020. Disponible en https://e-learning.protectioninternational.org/?lang=es

Red en Defensa de los Defensores Digitales. NSO Group suplantó a Facebook para instalar malware de vigilancia. Disponible en: https://r3d.mx/2020/05/20/nso-group-suplanto-a-facebook-para-instalar-malware-de-vigilancia/

Wikipedia. Algoritmo. Disponible en: https://es.wikipedia.org/wiki/Algoritmo
Wikipedia. Cifrado. Disponible en:
https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)

Wikipedia. ESET. Disponible en: https://es.wikipedia.org/wiki/ESET
Wikipedia. Ofimática. Disponible en:
https://es.wikipedia.org/wiki/Ofim%C3%A1tica
Wikipedia. ROT13. Disponible en: https://es.wikipedia.org/wiki/ROT13
Wikipedia. Software Libre. Disponible en:
https://es.wikipedia.org/wiki/Software_libre

**Elaborado por:**

LaLibre.net

**con el apoyo de:**

@ DERECHOS DIGITALES América Latina

PROGRAMA DE
Defensores y Defensoras
INDÍGENAS

Los módulos han sido elaborados en el marco del Programa Defensa de Defensores y Defensoras, y el proyecto "Protección de defensores de derechos humanos indígenas en la cuenca amazónica durante la pandemia COVID-19".


COICA ORG

coica_org

coicamazonia.org

@coicaorg

COICA ORG - Oficial

coica@coicamazonia.org

Calle Sevilla N24-358 y Guipúzcoa - La Floresta
Quito - Ecuador
Casilla postal 17-21-753 (593)23226-744


COORDINADORA DE LAS ORGANIZACIONES INDÍGENAS DE LA CUENCA AMAZÓNICA


CON EL APOYO DE:

OXFAM
Danmark