LA SITUACIÓN DE LAS PERSONAS DEFENSORAS DE DERECHOS AMBIENTALES Y TERRITORIALES

Las personas defensoras ambientales y territoriales son personas o grupos que promueven y protegen los derechos humanos relacionados con el medio ambiente, tanto a nivel nacional como internacional.

DERECHOS FUNDAMENTALES

- Realizar su labor en favor de los derechos humanos de manera libre y sin amenazas.
- Reunirse o manifestarse pacíficamente.
- Formar asociaciones y ONG.
- Recabar, recibir y poseer información relevante.
- Desarrollar y debatir ideas y propuestas.
- Criticar y proponer cambios ante las autoridades públicas.
- Denunciar políticas y acciones contrarias a los derechos humanos, y recibir una respuesta.
- Participar en juicios públicos.
- Obtener protección eficaz de las leyes para garantizar su seguridad.

ACUERDO DE ESCAZÚ

Es un tratado internacional clave para América Latina y el Caribe, enfocado en el:

1. Acceso a la información ambiental
2. Participación pública en la toma de decisiones.
3. Acceso a la justicia en asuntos ambientales, particular destaca la protección de las personas defensoras del medio ambiente.

AGRESIONES

En 2023, CEMDA documentó **123 eventos** de agresión contra personas y comunidades defensoras de derechos humanos ambientales en México.

Un evento de agresión puede contener varios ataques específicos:

282 ataques específicos: amenaza, intimidación, agresión física y verbal, etc.

20 ataques letales (asesinatos).

19 víctimas de desaparición.

64.2% de las víctimas son personas que viven en comunidades:

71 agresiones en contra pueblos indígenas.

1,317 personas afectadas por las agresiones, de las cuales:

344 fueron niños, niñas y adolescentes.

Principales agentes agresores:

Gobierno: 61 agresiones (49.59%)

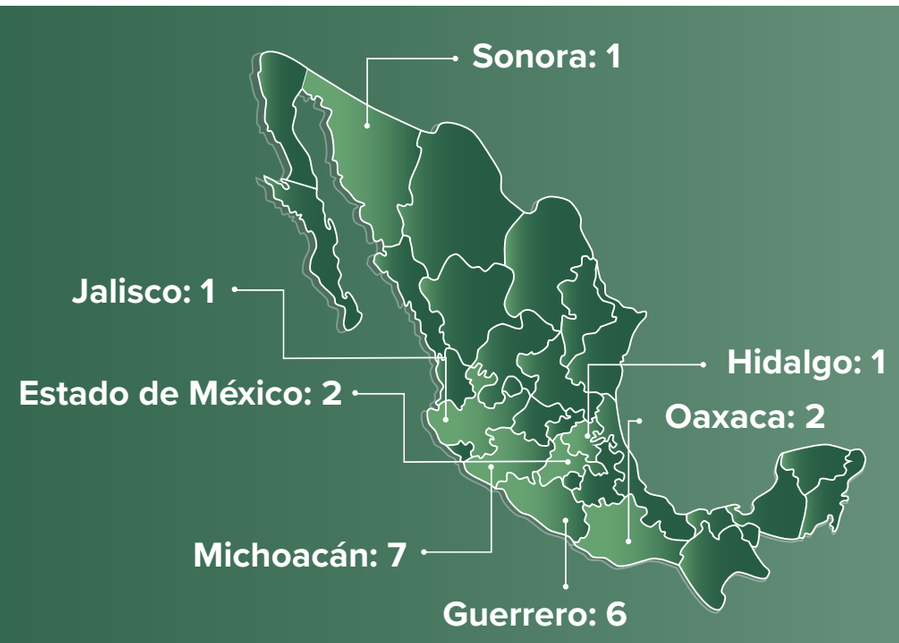
Delincuencia organizada: 37 agresiones (29.6%)

Empresas privada: 19 agresiones (15.45%)

Número de agresiones por tipo:

33 Amenaza
6 Allanamiento
28 Intimidación
5 Tortura y otros malos tratos
26 Agresión física
4 Desaparición
21 Criminalización
5 Desaparición por particulares
19 Homicidio
4 Robo
19 Hostigamiento
3 Violencia de género
18 Difamación
3 Agresión sexual
14 Daño de propiedad
3 Desalojo forzado
14 Estigmatización
2 Desaparición forzada
10 Detención ilegal o arbitraria
2 Discriminación
9 Uso indebido de la fuerza
1 Ejecución extrajudicial
8 Desplazamiento forzado
1 Espionaje
7 Privación ilegal de la libertad
0 Secuestro
6 Despojo
11 Otros

ENTIDADES FEDERATIVAS CON AGRESIONES LETALES EN EL 2023



OPORTUNIDADES PARA LA PROTECCIÓN DE LAS PERSONAS DEFENSORAS

Mecanismo de Protección a Personas Defensoras de Derechos Humanos y Periodistas:

- Atender las causas de fondo
- Medidas de protección apropiadas
- Necesidades diferenciadas:

Reconocer las necesidades particulares de protección para mujeres defensoras y comunidades indígenas, quienes enfrentan agresiones y riesgos únicos.

INTRODUCCIÓN A LOS RIESGOS DE SEGURIDAD

ANÁLISIS DE RIESGO

Primera herramienta de autoprotección para la protección de personas defensoras de los derechos humanos (PDDH)

METODOLOGÍA CUALITATIVA DEL RIESGO

- El **riesgo** es la posibilidad de que ocurra algo
- Cuando esa posibilidad se materializa nos referimos a **amenaza** - suelen ocurrir por factores del exterior
- La amenaza se ve potencializada por todos nuestros puntos débiles a este factor lo llamaremos **vulnerabilidades** - suele ocurrir por factores internos.
- Estos factores se pueden contrarrestar si trabajamos en nuestras fortalezas a este factor lo llamaremos **capacidades** - suelen ocurrir por factores internos.

Por lo tanto obtenemos la siguiente fórmula:

$$\text{RIESGO} = \frac{\text{AMENAZA X VULNERABILIDADES}}{\text{CAPACIDADES}}$$

El riesgo está compuesto de **tres características**:

- **Dinámico:** varía con el tiempo
- **Circunstancial:** depende del contexto
- **Subjetivo:** cada persona puede percibirlo de manera distinta

METODOLOGÍA DEL DIAGNÓSTICO DE SEGURIDAD

6 PASOS GENERALES:

1. **ANÁLISIS DE CONTEXTO:** identificar los fenómenos sociales, políticos, económicos legales, las normas de género, etcétera. Que impactan en el trabajo de la organización.
2. **MAPA DE ACTIVIDADES:** identificar las principales actividades que van en contra de los intereses de los potenciales agresores.
3. **ANÁLISIS DE ACTORES:** identificar los actores (locales nacionales e internacionales), intereses y relaciones.
4. **ANÁLISIS DE INCIDENTES:** identificar cualquier evento que puede comprometer la seguridad de la organización. *No todos los incidentes de seguridad son amenaza, pero sí, todas las amenazas declaradas son incidentes de seguridad*
5. **ANÁLISIS DE CAPACIDADES Y VULNERABILIDADES:** identificar las capacidades y vulnerabilidades de la organización y de sus integrantes.
6. **ANÁLISIS DE RIESGO:** *priorizar las amenazas latentes en función de los pasos anteriores. Evaluar la probabilidad de que ocurra cada una de estas amenazas y su impacto.*

Llevar una bitácora de cada uno de estos pasos nos puede ayudar a realizar un efectivo análisis de riesgo.

TIPOS DE AMENAZAS LATENTES EN MÉXICO

El riesgo está compuesto de tres características:

1. Acciones de intimidación

- Amenazas telefónica, redes sociales, verbales, etc
- Vigilancia y seguimiento demostrativo

2. Acciones de control

- Espionaje de llamadas telefónicas o con micrófono
- Infiltración dentro de la organización
- Vigilancia sobre locales

3. Robo de información

- Cateo y allanamiento a oficinas o domicilio, robo de maletines o mochilas, robo de computadoras, celulares, etc.
- Extracción de objetos dejados en vehículos, examen de la basura

4. Agresiones físicas y ejecuciones

- Golpes, tortura, violencia de género de forma física incluyendo sexual, ejecutaciones.

5. Criminalización

- Difamación pública, montajes judiciales, uso arbitrario del sistema penal

¿CÓMO VALORAR EL RIESGO?

1. **Analizar si existe la posibilidad que alguien nos haga daño intencionalmente (amenaza).** ¿ Es posible que alguien quiera dañar la organización intencionalmente?
2. **Analizar la probabilidad de que pase.** ¿Qué tan probable es que esto ocurra?
3. **Analizar qué tanto daño nos haría si se llevara a cabo la amenaza (impacto).** *Depende de nuestras capacidades y vulnerabilidades.* De acuerdo a las capacidades y vulnerabilidades de la organización, ¿Qué tanto daño tendría la amenaza?

SEMÁFORO DE VALOR DE RIESGO

AMENAZA LATENTE	PROBABILIDAD	IMPACTO
AMENAZAS IDENTIFICADAS	ALTA	ALTO
	MEDIA	MEDIO
	BAJA	BAJO

¿CÓMO RESPONDER AL RIESGO?

- **ACEPTARLO:** nivel de riesgo aceptable.
- **REDUCIRLO**: aumentar capacidades, reducir vulnerabilidades o encontrar la fuente de la amenaza.
- **EVITARLO**: reducir, cambiar o suspender actividades.
- **COMPARTIRLO:** trabajar en red y articulación.
- **IGNORARLO.**

ELEMENTOS PARA LA ELABORACIÓN DE UN PLAN DE SEGURIDAD

5 PASOS PARA ANALIZAR UNA AMENAZA DECLARADA

PASO 1: recoger todos los hechos
PASO 2: destacar patrones
PASO 3: determinar el objetivo ¿por qué?
PASO 4: determinar la fuente ¿Quién está detrás?
PASO 5: evaluar la probabilidad de ataque

ELEMENTOS BÁSICOS DE UN PLAN DE SEGURIDAD

PREVENCIÓN: situaciones específicas o actividades extraordinarias.	**PROTOCOLOS:** Por ejemplo, protocolo para los viajes en zonas de alto riesgo, protocolo para la protección de testigos y víctimas en riesgo.
EJECUCIÓN: actividades ordinarias/normas para el día al día.	**POLÍTICAS PERMANENTES:** Por ejemplo, control del acceso a espacios clave, políticas de seguridad digital, políticas de salud mental, etc.
REACCIÓN: a emergencias o incidentes.	**PLANES DE EMERGENCIA:** Por ejemplo: Plan en caso de secuestro, plan en caso de detención, plan en caso de robo de información sensible, etc.

¿CÓMO DESARROLLAR UN PLAN DE EMERGENCIA?

1. Definir la emergencia

- Definir, consensuar y compartir qué entendemos por una emergencia.

2. Lista de contactos de emergencia

- **Primer contacto:** ¿A quién se tiene que avisar primero dentro de la organización? ¿Con quién se tiene que comunicar si esta persona no está disponible?
- **Red de apoyo:** En caso de emergencia, ¿Hay que avisar a otras organizaciones / personas de confianza?
- **Autoridades:** ¿Hay autoridades locales, estatales o federales que conocen del trabajo de la organización y podrían generar un coste político para reducir las amenazas?
- **Apoyo legal:** ¿La organi zación tiene un abogado?¿Está disponible en cualquier momento para todas las personas de la organización?
- **Apoyo emocional:** ¿A quién se puede recurrir para el apoyo psicológico de emergencia?
- **Apoyo mediático:** ¿Qué medios de comunicación, periodistas o redes mediáticas serían útiles para difundir información que nos ayude en caso de una emergencia?
- **Servicios públicos:** Policía, ambulancia, bomberos, taxi de confianza, otros.

3. Marco general de actuación

- **Primer contacto:** ¿A quién se tiene que avisar primero dentro de la organización?
- **Análisis y documentación:** ¿Quién se encarga de documentar y analizar el incidente?
- **Coordinación/toma de decisión:** Dentro de la organización ¿quién toma la decisión sobre la respuesta a esta emergencia?
- **Apoyo emocional: ¿**Quién se queda en contacto con las personas afectadas para atender sus necesidades?
- **Memoria evaluación: ¿**Quién se encarga de documentar todo lo que sucede a partir del momento inicial en el cual se identifica la
- **Red de apoyo:** En caso de emergencia ¿hay que avisar a otras organizaciones, personas de confianza y/o familiares?
- **Autoridades:** ¿Quién se encarga de tomar la decisión de contactar a las autoridades locales, estatales o federales que conocen el trabajo de la organización?
- **Prensa:** ¿Se contacta automáticamente a la presa en caso de emergencia o se necesita una decisión dentro de la organización antes de contactarla?

4. Niveles de implementación del plan de seguridad

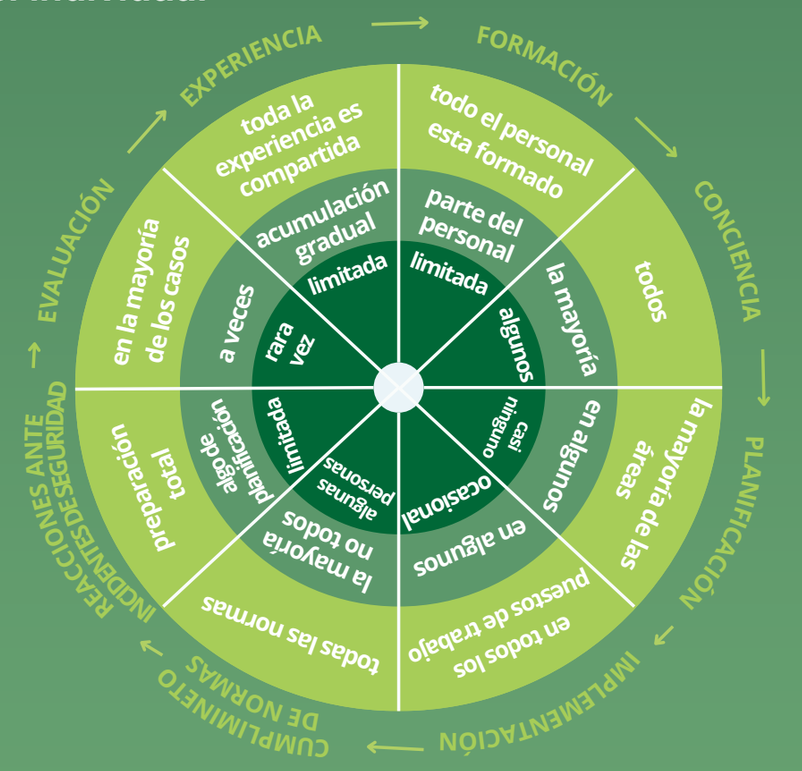
NIVEL 1. COMPROMISO. Individual, institucional, inter organizativo. →

NIVEL 2. DEFINICIÓN DE ESPACIO Y RECURSOS. Compartir, analizar, supervisar y evaluar. ↓

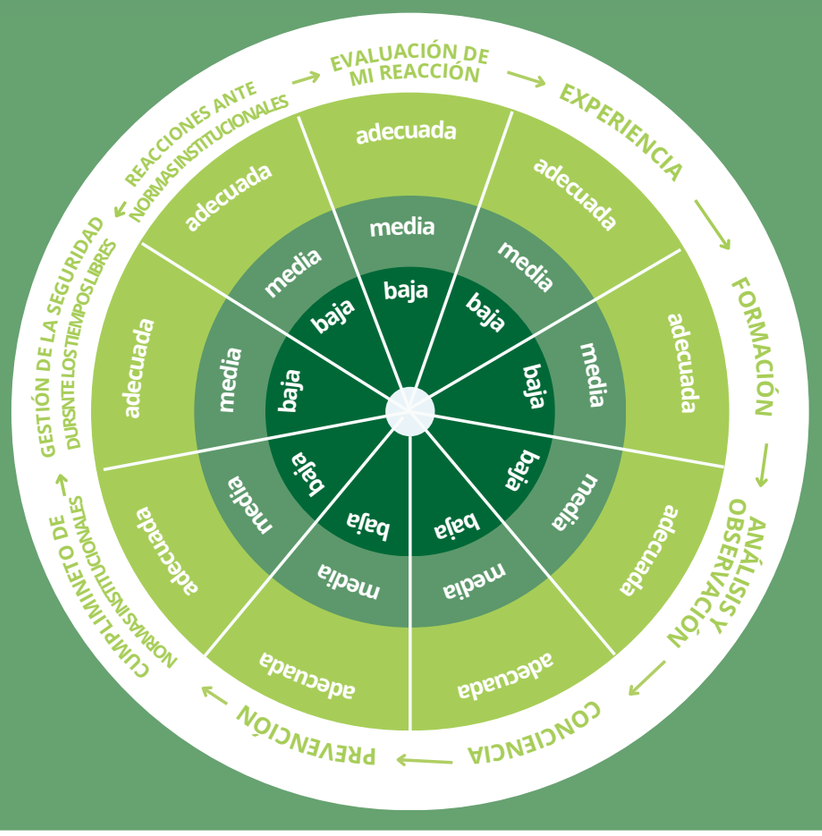
NIVEL 3. ASIGNACIÓN DE RECURSOS. Recursos de apacitación, laborales y materiales. ←

NIVEL 4. DISTRIBUCIÓN DE RESPONSABILIDADES.

5. Evaluar la implementación del plan de seguridad a nivel individual



6. Evaluar la implementación del plan de seguridad a nivel organizativo



PRESENTACIÓN DE LA GUÍA PARA EL ANÁLISIS DE RIESGOS DE SEGURIDAD

PASOS METODOLÓGICOS PARA EL ANÁLISIS DE RIESGOS

1. DEFINICIÓN DEL ÁMBITO GEOGRÁFICO en el que trabaja la organización, así como lapso de tiempo que vamos a analizar:

- ¿Qué tipo de actividad hace mi organización/es?
- ¿En qué localidad y municipio está ubicada mi organización/es?
- ¿En qué comunidades/localidades y municipios trabaja mi organización?

2. ANÁLISIS SITUACIONAL

a. **Sistema político:** ¿Cómo ejercen el poder las instancias oficiales como gobiernos municipales-estatales, partidos políticos, etc.?
b. **Sistema económico:** ¿Cuáles son las actividades económicas centrales en nuestra zona de trabajo (las que generan más riqueza)?
c. **Tejido social:** ¿Qué tan unido o fracturado está el tejido social? ¿Qué elementos generan mayor unidad?
d. **Análisis ambiental:** ¿Qué tan conservado o deteriorado está el ecosistema/s en nuestras zonas de trabajo?
e. **Situación de la infraestructura:** ¿La zona cuenta con una base infraestructural para comunicaciones, transporte, agua, energía, zonas de vivienda, etc, y son accesibles para toda la población?
f. **Presencia y situación de fuerzas de seguridad:** ¿Qué cuerpos de seguridad del Estado están presentes en la zona?
g. **Grupos y actores adversos (delincuenciales):** ¿Hay presencia de grupos delincuenciales en mi zona de trabajo?

ANÁLISIS DE RIESGO INICIAL DE SEGURIDAD							
Amenaza o peligro que nos puede afectar		Valor de la amenaza	Factores de (vulnerabilidad) debilidad		Análisis del riesgo		
Amenaza/ peligro	Situación		Puntos débiles de mi organización	Mitigación ya existente	Nivel de impacto	Probabilidad de impacto	Nivel riesgo inicial

3. IDENTIFICACIÓN DE AMENAZAS Y PELIGROS DE INSEGURIDAD

Amenaza o peligro que nos puede afectar	
Amenaza/ peligro	Situación

Las amenazas son aquellas causas potenciales de daño que provienen de una acción deliberada (como un atentado, robo o secuestro), mientras que los peligros son las causas potenciales de daño que provienen más bien de una acción deliberada (como un accidente de carretera o una inundación).

4. CALCULAR EL VALOR DE LA AMENAZA

Para medir **amenazas y peligros**, vamos a asignar puntajes del 1 al 5 establecidos por algunas afirmaciones a 3 criterios: **intención/capacidad de afectarnos/entorno en el que estamos.** Al terminar esta calificación, sumamos las tres calificaciones asignadas, y ubicamos la suma total en uno de los siguientes rangos:

Valor de la amenaza	Rango de la puntuación	Valor de la amenaza
	3 a < 5	Mínimo
	5 a < 7	Bajo
	7 a < 9	Moderado
	9 a < 11	Substancial
	11 a < 13	Alto
	13 a < 15	Extremo

5. DEFINICIÓN DE FACTORES DE VULNERABILIDAD O DEBILIDAD

Para cada **vulnerabilidad o punto débil** de mi organización, hay que agregar si es que ya existe alguna **mitigación existente**, que son acciones o medidas que reducen esta vulnerabilidad detectada y que ya existen.

Factores de (vulnerabilidad) debilidad	
Puntos débiles de mi organización	Mitigación ya existente

6. ANÁLISIS DEL RIESGO

Análisis del riesgo		
Nivel de impacto	Probabilidad de impacto	Nivel riesgo inicial

a. Nivel de impacto

Insignificante	Menor	Moderado	Severo	Crítico
• Sin lesiones. • Pérdidas y daños mínimos a bienes. • Sin retraso en los programas.	• Lesiones menores. • Posibles pérdidas y daños a bienes. • Atrasos limitados en los programas.	• Lesiones que no ponen en peligro la vida. • Alto nivel de estrés. • Algunos daños y pérdidas de bienes. • Algún retraso en los programas.	• Muertes o lesiones graves. • Pérdidas significativas de vidas. • Atrasos mayores en los programas.	• Incidente de bajas masivas. • Pérdidas mayores o destrucción de bienes. • Cancelación de los programas.

b. Probabilidad de impacto: se califica usando la matriz de probabilidad de impacto para eventos de seguridad, que mide los siguientes criterios:

I. **Intención:** mínimas (0) , bajas (1) , medias (5), altas (30) o máximas (40).
II. **Circunstancias:** mínimas (0) , bajas (1) , medias (2), altas (5) o máximas (10).
III. **Tendencia:** mínimas (0) , bajas (1) , medias (2), altas (5) o máximas (10).
IV. **Probabilidad:** La suma de los tres factores anteriores **(intención + circunstancias + tendencia)**, nos arroja el nivel de probabilidad de que cierta amenaza o peligro se concreten, y dañen a nuestra organización.

Valor	Probabilidad
< 1	Muy improbable
2 a 5	Improbable
6 a 18	Moderadamente improbable
19 a 49	Probable
> 50	Muy probable

c. Cálculo de nivel de riesgo: Una vez calificados tanto el nivel de impacto potencial, como su probabilidad de ocurrir, vamos a colocar los resultados dentro de la tabla siguiente, para determinar el nivel de riesgo:

	Nivel de impacto				
Probabilidad	Insignificante	Menor	Moderado	Severo	Crítico
Muy improbable	Bajo	Medio	Alto	Muy alto	
Improbable	Bajo	Medio	Alto	Alto	Muy alto
Moderadamente improbable	Bajo	Bajo	Medio	Alto	Alto
Probable	Bajo	Bajo	Bajo	Medio	Medio
Muy probable	Bajo	Bajo	Bajo	Bajo	Bajo

7. DEFINICIÓN DE LAS NUEVAS MEDIDAS DE MITIGACIÓN DE LOS RIESGOS

- Para definir las nuevas medidas de mitigación, se revisa cada factor de riesgos, clasificándose en una de las siguientes posibilidades: *Aceptar, Controlar, Evitar o Transferir.*

8. DEFINIR LAS ACTIVIDADES DEL PLAN DE SEGURIDAD, el Cronograma para realizarlas y las personas responsables de llevarlas a cabo:

- Para que el Plan de Seguridad funcione se requiere, además de que cada actividad tenga una persona responsable, contar con un equipo de trabajo que coordine, de seguimiento y actualice el análisis y el plan.
- Se sugiere que tanto el análisis y el plan bien se revisen y actualicen por lo menos una vez por año, o antes si las condiciones y riesgos presentan cambios.

ENFOQUE DE ACCIÓN SIN DAÑO

SENSIBILIDAD AL CONFLICTO (ESC)
Considera los conflictos como fenómenos naturales que indican cambios sociales.

ACCIÓN SIN DAÑO (ASD)
Enfoque integral del marco del Enfoque Sensible a los Conflictos, que reconoce que las iniciativas en contextos conflictivos no son neutrales y tienen potencial de influir significativamente en conflictos existentes.

5 PASOS PARA ANALIZAR UNA AMENAZA DECLARADA

1. Entender el contexto
2. Identificar los divisores y conectores
3. Detalles de nuestro programa
4. Acciones y comportamientos
5. Ajustar para mejorar

1. ENTENDER EL CONTEXTO:

A. Conocer a fondo la comunidad en la que trabajaremos.
- Área de implementación
- Actores
- Problema/conflicto

2. IDENTIFICAR LOS DIVISORES Y CONECTORES

- **Divisores:** Detectar qué aspectos (políticos, económicos, religiosos, etc.) separan a las personas.
- **Conectores:** Reconocer qué une a las personas, como instituciones o líderes que promueven la paz.

3. DETALLES DE NUESTRO PROGRAMA

- El lugar de implementación, el equipo involucrado, los beneficiarios y lo que se ofrecerá (detalles que impactan el contexto del conflicto).

MAPEO DE DETALLES CRÍTICOS

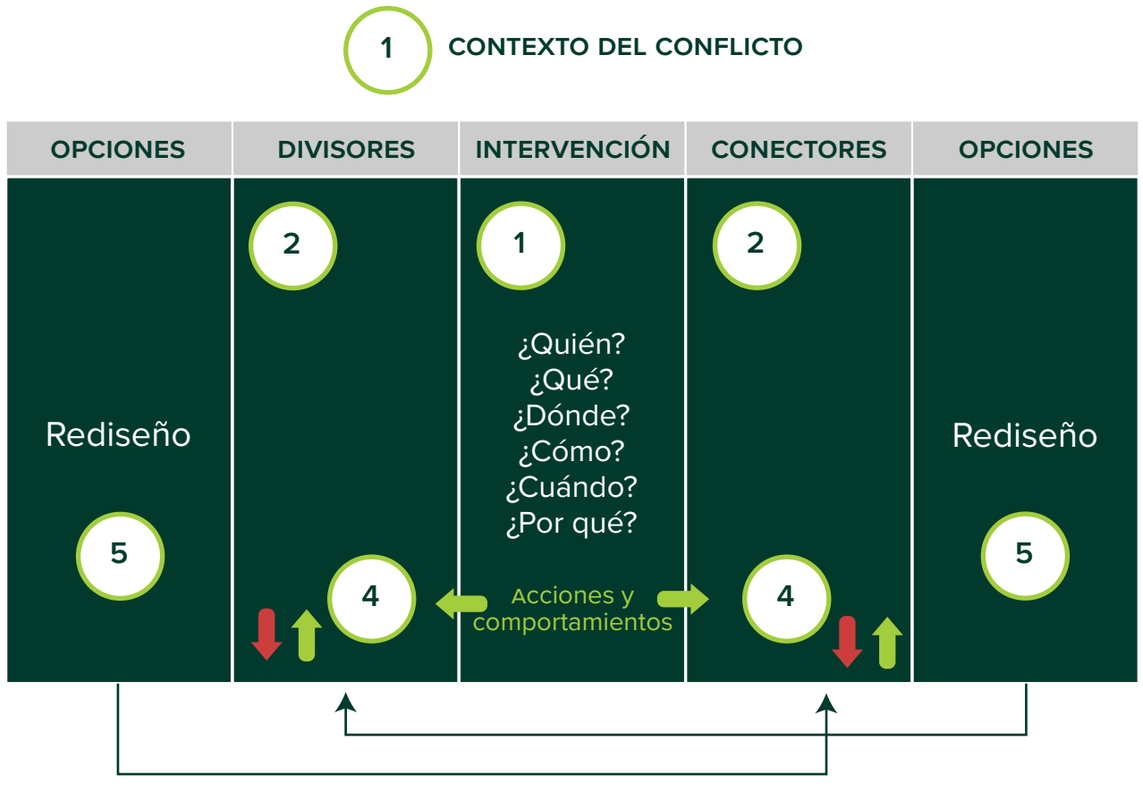
4. ACCIONES Y COMPORTAMIENTOS

- Considerar cómo nuestras decisiones y la conducta de nuestro equipo pueden influir en las divisiones y conexiones.
- **5 patrones de acción o transferencia de recursos:**
  a. Efectos en el mercado
  b. Efectos de distribución
  c. Efectos de información
  d. Efectos de sustitución
  e. Robo
- **5 patrones de comportamiento o mensajes éticos implicitos:** posturas éticas, valores e intenciones que transmitimos con lo que hacemos, decidimos, quiénes forman el equipo, cómo nos comportamos, etc.
  f. Respeto
  g. Responsabilidad
  h. Equidad y justicia
  i. Transparencia

5. AJUSTAR PARA MEJORAR

- Modificar aspectos del programa para minimizar impactos negativos y potenciar los positivos.
- Si ves que estás teniendo un impacto negativo, puedes hacer ajustes EN LOS DETALLES.
- Si ves que estás teniendo un impacto positivo, puedes mantenerlo o aprovechar lo que estás haciendo bien para seguir construyendo sobre ESE DETALLE.

MATRIZ DE ACCIÓN SIN DAÑO



INTRODUCCIÓN A LA SEGURIDAD DIGITAL

LA SEGURIDAD DIGITAL

Busca asegurar la información y los equipos electrónicos con base en tres conceptos clave:

1. **PRIVACIDAD:**
   - El control de tu información.
2. **INTEGRIDAD:**
   - Que tu información no se modifique, no se borre o no se pierda.
3. **DISPONIBILIDAD:**
   - Información disponible cuando la persona usuaria lo necesite.

CLASIFICAR LA INFORMACIÓN

1. **PÚBLICA**
   - Visible y consultable
2. **PRIVADA:**
   - Requiere de más control para acceder a la información.
3. **SENSIBLE:**
   - Es información particularmente riesgosa.

¿DÓNDE ESTÁ LA INFORMACIÓN?

1. **REPOSO LOCAL:**
   - USB,disco duro, computador, etc.
2. **REPOSO EN NUBE:**
   - Google drive, correo electrónico, OneDrive, etc
3. **TRANSMISIÓN:**
   - Moviéndose por internet.

ATAQUES DIGITALES

1. **ATAQUES TÉCNICOS:**
   - Daño, robo o pérdida de dispositivos, denegación de servicios, acceso no autorizado, intervención de dispositivos y sistemas, etc.
2. **ATAQUES DE CONDUCTA HUMANA:**
   - **INTERACCIÓN DIRECTA:** conductas ofensivas o discriminatorias, conductas que incitan al odio, extorsión, acoso, amenazas y hostigamiento.
   - **INTERACCIÓN INDIRECTA:** doxing, distribución de información falsa, suplantación o robo de identidad, vigilancia, bloqueo y control de contenidos, remoción de contenidos.

PASOS DE LA SEGURIDAD DIGITAL

1. **SOSPECHAR:** documentos inesperados, sentido de urgencia.
2. **NO REACCIONAR:** No dar clic en enlaces, no descargar archivos adjuntos.
3. **VERIFICAR LA FUENTE:** correo, enlace, número.
4. **NUNCA ENTREGAR:** Contraseñas, códigos de verificación, datos personales.

SEGURIDAD ANTI MALWARE

1. **SISTEMA OPERATIVO:**
   - Actualizaciones automáticas, instala el mínimo de aplicaciones.
2. **SOFTWARE:**
   - Original y de fuentes confiables.
3. **INTERNET:**
   - Antimalware - Antivirus.

SEGURIDAD DE CONTRASEÑAS

- +16 caracteres
- Frases
- 4-6 palabras aleatorias
- Alfanuméricas
- Símbolos como espacios
- Únicas
- Cambio anual
- No asociables a la identidad

EN CASO DE ATAQUE

1. **¿QUÉ HACER?**
   - Mantener la calma.
   - Documentar con capturas de pantalla y URLs.
   - Identificar el ataque.
   - Contactar a SocialTIC o su punto de contacto de confianza.
2. **¿QUÉ NO HACER?**
   - Borrar correos o mensajes.
   - Formatear dispositivos.

Este material fue realizado en el marco de la Comunidad de Práctica y Aprendizaje en Economía Social y Solidaria (COMPA), implementada por el Programa de las Naciones Unidas para el Desarrollo (PNUD) en México con el apoyo de Fomento Social Banamex y en colaboración con Nuup A.C.