Manual de formación

Respuestas centradas en sobrevivientes a la violencia de género facilitada por la tecnología en Guatemala

SEPTIEMBRE **2024**

TRANSFORM DIGITAL SPACES

USAID FROM THE AMERICAN PEOPLE

CIVIL SOCIETY & MEDIA STAND

pact building local promise.

IREX

moonshot

English:

The enclosed training handbook was developed as part of a training delivered by Moonshot to Guatemalan organizations in September 2024 as part of the Transform program. The content of the handbook reflects the specific needs and requests for support from these organizations.
The material was created to accompany the training sessions, rather than as standalone resources. Concepts were fleshed out and discussed in more detail during the training and through follow-up engagement with the training participants. Despite this, we hope the handbook will still be a useful reference for other organizations working on related topics.

Please note that links within the handbook were last reviewed in September 2024 and there are no plans to review and update them in an ongoing way.

Español:

El manual de formación adjunto fue desarrollado como parte de una capacitación impartida por Moonshot a organizaciones guatemaltecas en septiembre de 2024 dentro del programa Transform. El contenido de este manual refleja las necesidades específicas y las solicitudes de apoyo de estas organizaciones.
El material fue creado para acompañar las sesiones de capacitación, más que como recursos independientes. Los conceptos se desarrollaron y debatieron con más detalle durante la formación y a través de un trabajo de seguimiento con los participantes en la misma. A pesar de esto, esperamos que el manual siga siendo una referencia útil para otras organizaciones que trabajen en temas afines.

Téngase en cuenta que los enlaces del manual se revisaron por última vez en septiembre de 2024, y no hay planes de revisarlos y actualizarlos de forma continuada.

Panorama general

Entre el 4 y 6 de septiembre, Moonshot impartirá talleres de capacitación a organizaciones que trabajan en violencia de género facilitada por la tecnología (VGFT), violencia en línea, democracia digital, derechos de las mujeres y temas relacionados en Guatemala. Esta actividad forma parte del trabajo de Moonshot en la actividad Transform Digital Spaces (*Transformar Espacios Digitales* / Transform) para ayudar a las organizaciones de apoyo locales a desarrollar mecanismos en línea confidenciales, centrados en las y los sobrevivientes, seguros y protegidos a través de los cuales todas las y los sobrevivientes de VGFT puedan buscar servicios.

El programa pretende aumentar la capacidad de estos profesionales para prestar apoyo a sobrevivientes de VGFT. La formación abarcará las siguientes áreas básicas:

1. Panorama general de VGFT en el contexto guatemalteco
2. Investigación en línea para construir la base de evidencia en torno a la VGFT en Guatemala
3. Seguridad y bienestar del personal cuando trabaja en la VGFT y con posibles víctimas/sobrevivientes
4. Diseño centrado en el usuario para audiencias vulnerables
5. Campañas digitales de apoyo a sobrevivientes y espectadores de VGFT

Este manual ofrece las ideas clave tratadas en la formación, junto con valiosos recursos y enlaces para llevar a cabo una investigación en línea segura y desarrollar sus campañas digitales.

Introducción a VGFT

▼ Puntos a recordar

Definición

Violencia de género facilitada por la tecnología (VGFT): se define como la amenaza o acto de violencia cometido, asistido, agravado y amplificado en parte o totalmente mediante el uso de tecnologías de la información y la comunicación o medios digitales que se dirige de manera desproporcionada a mujeres, niñas y personas no conformes con su género. Se trata de un continuo de formas múltiples, recurrentes e interrelacionadas de violencia de género que tiene lugar tanto en línea como fuera de línea. (United States Strategy to Prevent and Respond to Gender-Based Violence Globally 2022)

Tipos de VGFT

- **Ciberacoso o acoso en línea**: El uso de las redes sociales (Instagram, TikTok, meta) y otras plataformas de mensajería para degradar, insultar o amenazar a alguien en función de su género o sexualidad.
- **Acecho / Cyberstalking:** El acoso continuo de la presencia en línea, las comunicaciones y la ubicación física de una persona utilizando la tecnología.
- **Doxing:** La publicación de información personal de alguien para amenazarle o acosarle.
- **Discurso de odio:** Cualquier tipo de discurso que pretenda deshumanizar o incitar a la violencia contra un determinado grupo de personas por motivos de raza, sexo, orientación sexual u otras características.
- **Suplantación / imitación de identidad**: Asumir la identidad de alguien en línea para engañar o acosar a otros.
- **Distribución no consentida de imágenes íntimas**: Compartir imágenes o vídeos explícitos sin el permiso de la persona.
- **Desinformación y desinformación de género en línea:** Narrativas falsas o engañosas basadas en el género y el sexo, a menudo con cierto grado de coordinación, para disuadir a las mujeres de participar en la esfera pública. Tanto los agentes estatales como los no estatales utilizan estratégicamente la desinformación sexista para silenciar a las mujeres, desalentar el discurso político en línea y moldear las percepciones sobre el género y el papel de la mujer en las democracias.
- **Sextorsión**: El uso de imágenes o vídeos íntimos para obligar a alguien a realizar actos sexuales o a proporcionar dinero u otras formas de compensación.

Recursos adicionales
Technology-Facilitated Gender-Based Violence: An Overview Suzie Dunn (EN)
Catálogo de recursos digitales del programa Transform
Segur@s en Línea
Toolkit TecnoFeministas Guatemala

El principio de ‘no causar daño’

▼ Puntos a recordar

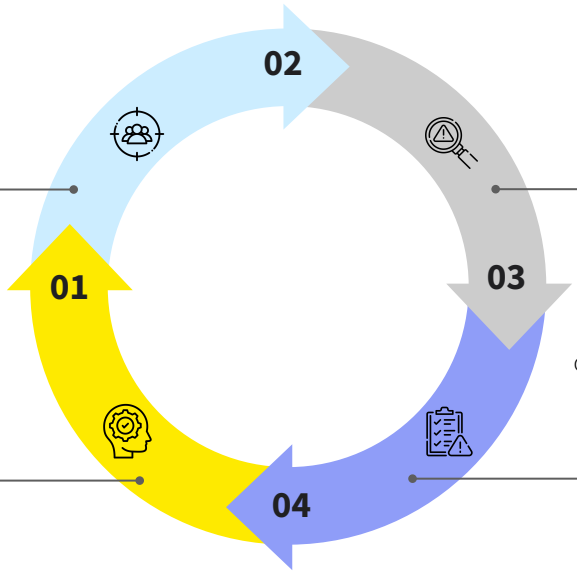
- “No causar daño” es una herramienta para evitar causar daños involuntarios a través de las acciones de una organización o el comportamiento de su personal.

- Cualquier acción, por pequeña que sea, conlleva el riesgo de hacer daño. Para "no causar daño", es necesario:
  - Comprender a tu público, incluidas sus motivaciones, vulnerabilidades y entorno.
  - Identificar cómo las actividades pueden afectar al público en sus contextos específicos.
  - Identificar los riesgos y utilizar un mapa de riesgos para priorizarlos.
  - Revisar constantemente los riesgos y generar opciones
  - Si se produce un incidente, trabajar juntos para mitigarlo e identificar nuevos riesgos

▼ El ciclo ‘no causar daño’

Identifique cómo interactúan las actividades del proyecto con su público y su contexto.

Identifique los riesgos y utilice un mapa de riesgos para ordenarlos por frecuencia e impacto potencial.



Comprenda a su público y sus motivaciones, entorno y vulnerabilidades.

Revise todos los riesgos y genere opciones. Si se produce un incidente, trabaje para mitigarlo e identifique nuevos riesgos.

Enfoque centrado en sobrevivientes

▼ Puntos a recordar

Un enfoque centrado en sobrevivientes se centra en el empoderamiento de los supervivientes mediante la creación de un entorno de apoyo para la sanación. De la violencia de género pueden recuperar o reforzar su sentido de empoderamiento cuando se tiene accesoa servicios de violencia de género centrados en sobrevivientes que defienden estos **cuatro principios rectores**:

1. Garantizar la seguridad de los supervivientes, incluida la prevención y mitigación de nuevos actos de violencia;
2. Proteger la confidencialidad de los supervivientes, incluido su derecho a que la información sobre ellos sólo se comparta con su consentimiento informado y su derecho a elegir si quieren contar sus experiencias y a quién;
3. Demostrar respeto por las necesidades y deseos de los supervivientes y por su derecho a tomar sus propias decisiones, incluidas aquellas que a los proveedores de servicios les resulten difíciles de entender o con las que no estén de acuerdo; y
4. Practicar la no discriminación, garantizando que los supervivientes, en toda su diversidad, puedan acceder y recibir servicios adecuados y un apoyo significativo.

Investigaciones en línea

Consideraciones éticas

▼ Puntos a recordar

→ **Necesidad y proporcionalidad** - Considere por qué el trabajo es necesario para ayudar a salvaguardar el espacio en línea, y cómo la solución propuesta es proporcional a la amenaza a la seguridad pública en cuestión.

→ **Impacto social y no causar daño** - ¿Podría utilizarse lo que produce de una manera que cause daño? ¿Actúa de manera que podría exponer a otros a contenidos o materiales que de otro modo no verían?

→ Derechos humanos

→ Inclusión y diversidad

→ Integridad de los datos

→ Deber de cuidado

→ **Transparencia** - ¿Comparte la información entre sus equipos de forma transparente? Tenga cuidado de compartir lo que ha ido bien y, lo que es más importante, lo que ha ido mal, para que otros puedan evitar esos errores en el futuro.

→ **Responsabilidad** - ¿Qué estructuras de revisión, internas o externas, existen para su trabajo? ¿Cómo se asegura de que las lecciones aprendidas se recogen y abordan rápidamente?

Recursos adicionales

> Marco ético de Moonshot (EN)

> **'Establecer su brújula moral'**
> Este cuaderno de ejercicios (en inglés), en particular la página 6, es un punto de partida útil para considerar una cuestión o dilema ético desde diferentes perspectivas que pueden ayudar a ofrecer ideas o matices particulares que no siempre resultan evidentes a primera vista. Resulta muy útil para poner de relieve que, por lo general, no hay respuestas "correctas", sino distintas compensaciones al seguir determinadas líneas de actuación.

> **'El cuaderno de trabajo de las investigaciones de fuentes abiertas responsables'**
> Esta guía (en inglés), que puede copiarse en Google Drive y adaptarse a proyectos concretos, es un recurso realmente completo para trabajar con rigor las fases del proyecto y la investigación.

Metodología de investigación

▼ Puntos a recordar

El proceso OSINT (Open Source Intelligence)

1. **Seguridad operativa** - Asegúrate de que tu huella digital no es rastreable
2. **Establecimiento de objetivos -** ¿Cuáles son las preguntas a las que desea responder?
3. **Investigación y determinación del alcance** - Para determinar la disponibilidad de datos de interés, así como sus limitaciones.
4. **Identificación** - Técnicas de triangulación
5. **Recopilación** - Fase continua de recopilación de datos a lo largo de un proyecto determinado.
6. **Análisis y procesamiento** - Codificar, clasificar, traducir, refinar y analizar
7. **Compartir** - Preparar un informe o una presentación clara de los resultados y compartirlos de forma segura.

Las preguntas clave de la OSINT

Quién
- ¿Quién realiza el análisis?
- ¿Sobre quién versa el análisis?

Qué
- ¿Qué información se busca?
- ¿Qué se ha encontrado?

Por qué
- ¿Por qué se realiza el análisis?
- ¿Por qué es importante el análisis?

Dónde
¿Dónde se encontró el objeto de análisis?

Cuándo
¿Fecha y hora de las actividades?

Recursos adicionales

Ten en cuenta que la mayoría de estos recursos están en inglés, pero pueden utilizarse fácilmente para investigar en español. Puede utilizar la función de traducción automática de tu navegador para navegar por estas páginas con facilidad.

OSINT framework - Herramienta que intenta ayudar a la gente a encontrar recursos OSINT gratuitos.
Herramienta que intenta ayudar a la gente a encontrar recursos OSINT gratuitos
Recursos de OSINT Techniques
OSINT Techniques Chart - Técnicas OSINT para la investigación de personas
Bellingcat Online Investigation Toolkit
YouTube DataViewer - Comprobar la fuente de un vídeo

Seguridad Digital

▼ Puntos a recordar

Ejemplo de lista de comprobación de seguridad digital

Mi portátil y mi puesto de trabajo son seguros:

- [ ] Tengo una pantalla de privacidad en mi monitor.
- [ ] Las contraseñas del router de mi casa y/o de mi oficina se han cambiado respecto a las predeterminadas.
- [ ] Mi portátil, el cargador y el maletín del portátil no llevan mi nombre completo ni ningún otro vínculo conmigo o con mi organización.
- [ ] Almaceno mis archivos en una ubicación segura aprobada, idealmente una carpeta de almacenamiento en la nube cifrada.
- [ ] Reduzco al mínimo la documentación en papel y dispongo de una trituradora de papel para eliminar de forma segura la información confidencial impresa.

Mis dispositivos autorizados para el trabajo son seguros:

- [ ] Los dispositivos utilizan un código de acceso seguro y, si es posible, tengo activado el ID de huella dactilar o Face ID.
- [ ] Solo utilizo software, dispositivos y aplicaciones aprobados para cumplir con mis obligaciones profesionales.
- [ ] Los dispositivos están cifrados.
- [ ] Uso una VPN cuando me conecto a una red no segura (por ejemplo, wifi pública).
- [ ] He habilitado la autenticación multifactor para cuentas clave (por ejemplo, correo electrónico).
- [ ] He proporcionado una lista actualizada de todos los dispositivos -incluidos los personales- que utilizo para acceder a los datos de la organización.

Tengo una pantalla de privacidad en mi monitor:

- [ ] Utilizo un método de contraseña seguro y evito utilizar datos personales como contraseña (por ejemplo, nombres de mascotas, lugar de nacimiento).
- [ ] No utilizo las mismas contraseñas en varias cuentas.
- [ ] Utilizo un gestor de contraseñas.

Mi presencia en Internet:

- [ ] He revisado mi presencia en Internet para identificar riesgos.
- [ ] He establecido medidas de seguridad y privacidad.
- [ ] Soy consciente del riesgo de phishing y doxxing, y sé cómo informar y responder a un incidente internamente.

Puedo gestionar los riesgos con mi equipo:

- [ ] Tenemos una política organizativa de contraseñas.
- [ ] Conozco el proceso para plantear un problema de seguridad a un/a colega o a un/a responsable de la toma de decisiones.
- [ ] Puedo trabajar con mi equipo para identificar y aplicar medidas paliativas, y sé cómo revisar los incidentes de seguridad.
- [ ] Conozco los pasos necesarios para identificar, notificar y gestionar una violación de la seguridad digital.
- [ ] Soy consciente de que la seguridad digital es una responsabilidad continua y compartida, y de que es esencial saber cómo proteger los datos sensibles y mantenerse seguro en línea.

Recursos adicionales

No se trata de una lista exhaustiva, y con frecuencia aparecen nuevas herramientas, pero asegúrese de que le asesora una fuente creíble y de buena reputación.

Aplicaciones de comunicaciones seguras

- Signal Messenger
- WhatsApp
- Privnote

Software anti-virus

- Avast
- Malwarebytes
- Bitdefender

Cifrado de archivos y unidades de disco

- Para un Mac
- Para Windows

Navegación segura

- NordVPN - Servicio VPN que cifra la conexión a Internet y oculta la dirección IP y la ubicación. Se trata de un servicio de pago que recomendamos como inversión organizativa importante.
- Otras opciones de VPN son Windscribe y TunnelBear.
- Privacy Badger - Extensión del navegador que impide a los anunciantes y a otros rastreadores de terceros rastrear en secreto adónde va y qué páginas consulta.
- uBlock Origin - Extensión del navegador que bloquea anuncios, rastreadores y contenido no deseado.

Pantalla de privacidad

- Tendrás que encontrar la opción adecuada para tu ordenador/dispositivo, pero aquí tienes un ejemplo.

Almacenamiento seguro de datos

- Cifrado en la nube a través de Google
- Cifrado en la nube a través de Microsoft

Protección de las cuentas en línea

▼ Puntos a recordar

El propósito de esta guía es garantizar que todos ustedes tengan acceso a algunas orientaciones rápidas sobre cómo reducir temporal o permanentemente su presencia en línea -esencialmente, hacer privadas las cuentas de las redes sociales, hibernar su cuenta de LinkedIn, etc.

Mantener o no cuentas personales en las redes sociales, y lo que compartes, es una decisión personal, pero hay que asegurarse de que sea una decisión informada.

Tomar estas medidas con sus cuentas personales siempre estará sujeto a la discreción individual, pero como punto general, es importante y útil ser consciente de su huella en línea. Estas directrices han sido adaptadas por los especialistas en seguridad de Security Positive para ayudar a las personas y grupos que necesitan ser conscientes de su seguridad en línea.

Gestión de contraseñas

- Contraseñas seguras que no reutilices
  Generadores de contraseñas seguras disponibles en Diceware y Avast
- Autenticación multifactor (véase más abajo)
- Utilice un gestor de contraseñas como LastPass para crear y mantener contraseñas seguras.
- Cambie sus contraseñas con regularidad (cada 90 días), e inmediatamente si tiene motivos para creer que alguien más la conoce.

Autenticación multifactor en todas las cuentas personales

A continuación se presentan instrucciones específicas sobre 2FA para servicios comunes; consulta www.twofactorauth.org para ver qué otros servicios son compatibles.

- (Gmail, Yahoo!, Outlook)
- Facebook
- Instagram
- X / Twitter
- LinkedIn
- Snapchat
- TikTok
- Youtube
- Whatsapp
- Signal
- Telegram
- iCloud
- Google Drive
- Dropbox
- Paypal (compruebe si aparece algún otro servicio de banca en línea en www.twofactorauth.org)
- Proveedores de sitios web, como GoDaddy y DreamHost.

Ajustes de seguridad por plataforma

Linkedin

- Puedes "pausar" temporalmente tu cuenta para que no se pueda ver tu perfil.
- Esto no lo elimina del índice de Google, pero si haces clic en él, aparecerá una página de error.
- Ten en cuenta que no podrás volver a activarla durante las 24 horas posteriores a la primera pausa de la cuenta.
- Puedes optar por mostrar sólo tu nombre y la inicial de tu apellido

Instagram

- Haz que tu cuenta sea privada.
- Elimina los mensajes antiguos que aparezcan públicamente o que revelen domicilio, número de teléfono, dirección de correo electrónico u otros datos personales.
- Elimina geoetiquetas de Instagram o información de ubicación (EN)
- Impide que tus contactos te etiqueten en fotos sin tu permiso.

YouTube

- Cómo poner un canal de YouTube privado
- (EN) Cómo eliminar publicaciones y vídeos antiguos que aparecen públicamente o que revelan tu dirección postal, número de teléfono, dirección de correo electrónico u otros datos de identificación personal
- Restringir la inserción de vídeos

Facebook

- La gestión de páginas o grupos se realiza a través de cuentas individuales. Asegúrese de que cualquier persona con acceso a sus páginas o grupos está utilizando 2FA.
- Elimine a los administradores que ya no necesiten acceder a sus páginas. Si utiliza su perfil personal para trabajos públicos, considere la posibilidad de cambiarlo a una página pública.
- Cómo hacer privada tu cuenta personal de Facebook.
- Impide que tus amigos te etiqueten personalmente en fotos, actualizaciones de estado o ubicaciones.
- Establece una cuenta de correo electrónico específica para su cuenta de Facebook que no utilice en ningún otro lugar.
- Recibe alertas cuando un dispositivo desconocido inicie sesión en su cuenta.
- No permite las etiquetas de ubicación o la información de ubicación.
- Elimina las publicaciones antiguas que aparezcan públicamente o que revelen su dirección, número de teléfono, dirección de correo electrónico u otros datos de identificación personal.

X (anteriormente Twitter)

- Elimine a los administradores que ya no necesiten acceder a sus páginas. Gestione el acceso con cuidado.
- Si utiliza su perfil personal para trabajos públicos, considere la posibilidad de cambiarlo a una página pública.
- Convierta su cuenta en privada.
- Reciba alertas cuando un dispositivo desconocido acceda a su cuenta.
- No permita etiquetas de ubicación o información de ubicación.
- No permita que sus contactos le etiqueten en fotos sin su permiso.
- Elimine publicaciones, tweets e imágenes antiguas que aparezcan públicamente o que revelen su domicilio, número de teléfono, dirección de correo electrónico u otros datos de identificación personal.

Snapchat

- Haz que tu cuenta de Snapchat sea privada.
- Eliminar Mensajes y Recuerdos antiguos de Snapchat.
- Desactivar la ubicación en Snapchat.
- Otros consejos de privacidad de Snapchat aquí.

TikTok

- Haz que tu cuenta sea privada.
- Elimina los mensajes antiguos que aparezcan públicamente o que revelen tu domicilio, número de teléfono, dirección de correo electrónico u otros datos personales.
- Cambia tu información de ubicación para que no sea tu información real.
- Actualiza tus controles de privacidad

Gestión de su huella en Internet

- Revise las primeras 5-15 páginas de resultados de motores de búsqueda para su nombre
  - Denuncia contenidos sobre productos de Google para su eliminación aquí.
  - Este es un breve manual sobre cómo solicitar la eliminación de datos.
- Lleve un registro de cualquier contenido sensible que encuentre.
- Identifique y elimine las cuentas de redes sociales olvidadas.
- Considera la posibilidad de cambiar tu nombre en las cuentas por un alias o de utilizar un correo electrónico distinto.
- Reciba alertas si su dirección de correo electrónico es objeto de una filtración de datos: regístrese en Have I been pwned?

Bienestar del personal

Algunos principios generales

1. Minimización de riesgos
2. Compartir y comprender la carga
3. Apoyo externo/supervisión
4. Claridad de funciones y expectativas
5. Selección y contratación
6. Dar ejemplo/ cultura de empatía

Prácticas de bienestar inspiradas en la comunidad

Algunas ideas que se compartieron durante la formación sobre cómo podemos cuidarnos y apoyarnos mutuamente como equipo.

Bienestar personal

- Crear espacios de autocuidado y permitir descansos durante el día.
- Practicar pausas activas y cuidar el cuerpo, especialmente durante la menstruación.
- Escucharse a sí misme y no sentir culpa por tomarse tiempo para el autocuidado.
- Respetar los tiempos de comida y establecer momentos sin teléfonos.
- Personalizar el espacio de trabajo y mantener un entorno seguro.
- Personalizar el espacio de trabajo y mantener un entorno seguro.

Bienestar del equipo

- Organizar encuentros de autocuidado y reuniones para mejorar el bienestar colectivo.
- Ofrecer apoyo psicológico mensual y promover un día libre al mes.
- Mantener un espacio seguro para les compañeres de trabajo y evitar saturar las comunicaciones.
- Fomentar la solidaridad y el apoyo entre compañeres.

Prácticas organizacionales

- Establecer horarios de trabajo flexibles y permitir el trabajo desde casa.
- Crear cajas de ideas para actividades y promover un ambiente laboral respetuoso y empático.
- Incluir tiempo para salidas recreativas como un día de playa al año en el presupuesto.

↘ Diseño centrado en sobrevivientes

▼ Puntos a recordar

Cinco principios básicos de diseño

1 **Accesibilidad**

La página de destino tiene que ser accesible para todos los usuarios con discapacidades que afectan al acceso en línea, incluidas las discapacidades auditivas, cognitivas, neurológicas, físicas, del habla y visuales. Además, la accesibilidad también beneficia a las personas sin discapacidad, como las personas mayores cuyas capacidades cambian debido al envejecimiento; las personas con "discapacidades temporales", como un brazo roto o unas gafas perdidas; y las personas con limitaciones situacionales, como estar en un entorno en el que no pueden escuchar audio.

Los principios de accesibilidad de un sitio web van de la mano de su claridad, concisión y facilidad de uso. En el caso de las discapacidades físicas, hay que tener en cuenta que los botones sean grandes y fáciles de pulsar, que el usuario tenga espacio suficiente para rellenar un formulario y que el diseño tenga en cuenta el uso de móviles y pantallas táctiles. En cuanto a las discapacidades cognitivas, hay que informar a los usuarios de los siguientes pasos y plazos, y explicarles qué ocurrirá después de completar un servicio.

2 **Predictibilidad**

Cinco preguntas a las que debe responder un usuario cuando llega a una página de aterrizaje:

- ¿Dónde estoy/qué sitio es éste?
- ¿Para qué sirve?
- Por qué debería estar aquí y no en otro sitio?
- ¿Qué puedo encontrar aquí?
- ¿Qué puedo hacer aquí?

3 **Simplicidad**

- Mejorar la legibilidad de la página de destino
- Mejorar la primera impresión del usuario
- Facilitar que el usuario reconozca la página de destino en futuras visitas
- Se carga más rápido = mejor para conexiones con poco ancho de banda

4 **Privacidad y confidencialidad**

- Políticas de privacidad y preguntas frecuentes
- Reconocimiento directo de los problemas de privacidad
- Formularios de usuario no intrusivos
- Considerar las expectativas de anonimato de los usuarios

5 **Credibility**

- Casos prácticos inspiradores
- Perspectivas de los trabajadores sociales
- Página "Quiénes somos"
- Organizaciones asociadas de referencia

Consideraciones contextuales

Comunicación

Los socios que prestan servicios de intervención deben adaptar el servicio prestado al contexto local. Por ejemplo, si WhatsApp es la plataforma de mensajería más popular en el país, entonces tiene sentido ofrecer a los usuarios vulnerables la entrada a un grupo de WhatsApp en el que puedan hablar con un consejero. Al mismo tiempo, Moonshot siempre recomienda ofrecer múltiples métodos de derivación para permitir diversas circunstancias y preferencias.

Color

La forma en que vemos y percibimos el color depende en gran medida de una serie de factores, como el contexto cultural, nuestra educación y nuestras preferencias personales.

Imágenes y símbolos

Las imágenes y los gráficos deben elegirse con cuidado. Esto se aplica a las imágenes y los símbolos que pueden considerarse tanto un apoyo al punto de vista del usuario como una negación del mismo.

Texto

El tono del texto de la página de inicio debe ser abierto, claro y empático.

Recursos adicionales

Accesibilidad

Las Web Content Accessibility Guidelines (WCAG) son un estándar compartido de accesibilidad al contenido web para particulares, organizaciones y gobiernos. Fueron creadas por el consorcio World Wide Web, que dirige grupos de trabajo específicos para la accesibilidad. El A11Y Project, un proyecto comunitario de accesibilidad web, y el Departamento del Servicio Digital del Gobierno británico también comparten listas de comprobación de accesibilidad muy útiles. Todos estos recursos se encuentran en inglés pero se pueden traducir fácilmente con el traductor del operador que se esté utilizando.
One Click Accessibility es un plugin gratuito que hace que los sitios web de WordPress sean accesibles para personas con discapacidad.

↘ Campañas digitales

▼ Puntos a recordar

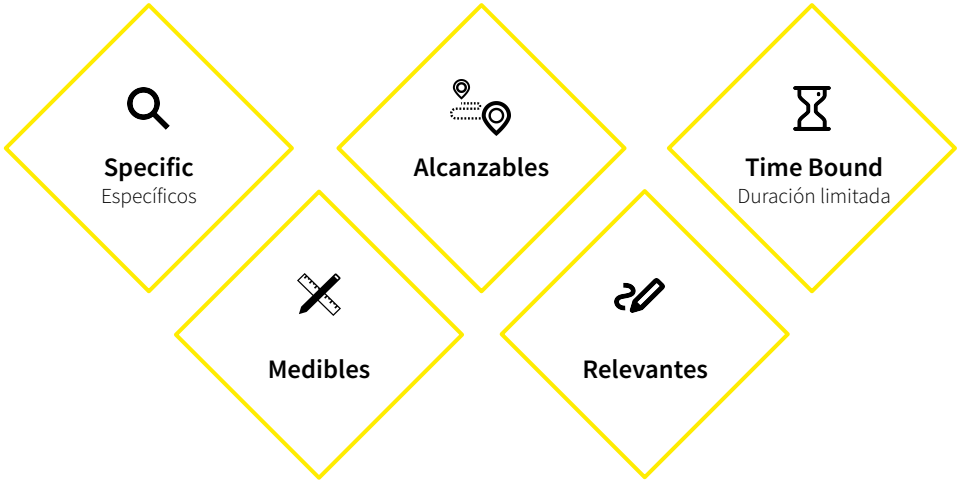
1. Una campaña de comunicación digital consiste en poner en marcha una campaña exclusivamente en plataformas digitales (por ejemplo, redes sociales, herramientas de marketing como Google Ads).
2. Las campañas digitales, especialmente en las redes sociales, pueden utilizarse para combatir la violencia de género, la incitación al odio y el extremismo violento en línea.
3. Para desarrollar una campaña digital, es importante tener en cuenta los principios de la comunicación estratégica: definir su problema y su público, crear el mensaje que desea transmitir, elegir sus plataformas, preparar un plan de comunicación y un presupuesto, y medir su impacto. El marco OASIS es una herramienta importante para planificar campañas digitales.

▼ Marco de planificación de la campaña OASIS

Establecer objetivos

- Antes de planificar la campaña digital, es importante definir el problema y el público al que queremos dirigirnos.
- Definir el problema nos permite comprender los objetivos que hay que alcanzar.
  - El marco SMART (en la página siguiente) se utiliza para definir objetivos específicos, medibles, alcanzables, pertinentes y sujetos a plazos para la campaña digital.

↘ Los objetivos SMART son



Definir su audiencia

1 El público destinatario es el grupo de personas a las que se quiere persuadir con un mensaje específico. Es importante definir el público para crear una campaña digital y un mensaje pertinentes y convincentes.

- A la hora de definir el público destinatario, hay que plantearse preguntas como la edad, la ubicación geográfica, el idioma, los puntos débiles, los intereses y aficiones...

2 La empatía es un elemento esencial en las campañas digitales.

Estrategia y ejecución de campañas

Elección de la plataforma

→ Las campañas digitales pueden lanzarse en multitud de plataformas, como redes sociales, motores de búsqueda, aplicaciones de mensajería y plataformas para compartir audio y vídeo. Considera lo siguiente:

- ¿Dónde puede llegar a el público?
- ¿De qué recursos dispone?
- ¿Existen restricciones legales para determinadas plataformas en tu país?
- ¿Qué conocimientos técnicos necesita?

→ La publicidad de pago en sitios web o motores de búsqueda también es una forma eficaz de llegar rápidamente a tu público destinatario de forma precisa (utilizando elementos como la segmentación por palabras clave). Sin embargo, requiere una inversión financiera y de tiempo bastante importante.

→ También puede recurrirse a la distribución manual (siembra de contenidos o *content seeding*), es decir, colocar manualmente enlaces al contenido de su campaña donde puedan ser vistos por tu público destinatario.

Mensajer@
Es esencial elegir para tu campaña un/a mensajer@ creíble e influyente para el público destinatario.

Branding
¿Cómo se presentará en la campaña?
¿Utilizarás los perfiles de tu organización en las redes sociales o creará canales específicos, quizá anónimos, en las redes sociales?

Mensaje

- El proceso de creación del mensaje principal de la campaña digital, y la forma en que se presenta el mensaje, se denomina *framing*.
- Para enmarcar bien un mensaje, hay que definir el problema que la campaña quiere resolver, así como el público destinatario. Luego hay que presentar el problema al público y proponer una solución utilizando un lenguaje sencillo, convincente y ético.
- Utilizar las emociones es una técnica eficaz para crear mensajes convincentes. Se pueden utilizar emociones positivas, como la alegría y la esperanza, o negativas, como el miedo y la ira. Las emociones pueden transmitirse a través del texto, pero también mediante imágenes y música.

Llamada a la acción
Una buena campaña digital tiene claro si quiere cambiar lo que hace la gente o su forma de pensar sobre un tema concreto. La primera tendrá una clara llamada a la acción, mientras que la segunda tendrá llamamientos más genéricos.

Supervisión y evaluación

Se propone responder a la pregunta: "*¿Hemos conseguido lo que nos habíamos propuesto?*".
La *supervisión* es lo que se hace mientras la campaña está en marcha, mientras que la *evaluación* es lo que se hace al final de la campaña para valorar su rendimiento general.
Para evaluar la campaña, primero tienes que **definir cómo se va a medir el éxito**: ¿cómo sabes que has alcanzado su objetivo? ¿De dónde obtendrás estos datos?

Debes prestar mucha atención a la acogida de la campaña por parte del público destinatario.

- ¿ Cuánto engagement obtienes?
- ¿Cuántos comentarios dejan los usuarios?
- ¿Son comentarios positivos, negativos o neutros?
- ¿El contenido es compartido por muchos usuarios?

Muchas campañas se basan en métricas de plataforma: número de clics, impresiones, visitas al sitio web, número y tipo de comentarios, etc. Las campañas que tienen una clara llamada a la acción también pueden incluir otras métricas: por ejemplo, si la campaña pide a la gente que apoye una iniciativa local, se puede contar el número de personas que realmente la han apoyado como métrica de evaluación. O, si la campaña pide a la gente que firme una petición, puede contar el número de personas que la firman.

Si el nivel de participación no les satisface, se debe analizar a qué se debe.

- ¿Están publicando el contenido en momentos inoportunos? ¿Quizá sería mejor publicarlo en el momento en que su público destinatario está más activo en Internet?
- ¿O hay algún problema con el contenido de la campaña? ¿Quizá el mensaje, su tono o su presentación no atraen a su público destinatario?
- ¿Quizá no está llegando al público adecuado? ¿Las personas que están viendo su contenido son realmente las personas a las que le gustaría llegar?

Algunas de las preguntas más importantes a la hora de evaluar el rendimiento de la campaña son:

1. **Actividades**
   ¿Qué se hizo antes y durante la campaña? ¿Qué se hizo para desarrollar la metodología y el contenido de la campaña? ¿Qué recursos necesitó?

2. **Entregables**
   ¿Qué hizo, creó o produjo para cumplir los objetivos? ¿Realizó un vídeo, un sitio web de la campaña o una serie de dibujos animados?

3. **Aprendizajes**
   ¿Qué información o lecciones aprendierón? ¿Hay algo que haría de forma diferente la próxima vez?

4. **Resultados**
   ¿Qué cambios se han producido como resultado de la campaña?

Recursos adicionales

Sociallymap: Plataforma para automatizar la publicación de contenidos en diferentes redes sociales. También se puede hacer de forma manual a través de la plataforma.

Google Ads Guide (EN): Guía sobre el funcionamiento de la publicidad en Google.

CryptPad: Plataforma de colaboración cifrada y centrada en la privacidad que permite a los usuarios crear y compartir documentos, hojas de cálculo y otros archivos sin comprometer la seguridad de sus datos. Puede utilizarse para crear encuestas y es una alternativa a Google Forms (gratuita).

Recursos gratuitos para la creación de contenidos

Unsplash o freeimages: Imágenes libres de derechos
Bensound: Música libre de derechos
Flaticon: Iconos
Audacity: Editor y grabador de sonido (PC y Mac)
OpenShot: Editores de vídeo (PC y Mac)
Canva: Plantillas de diseño