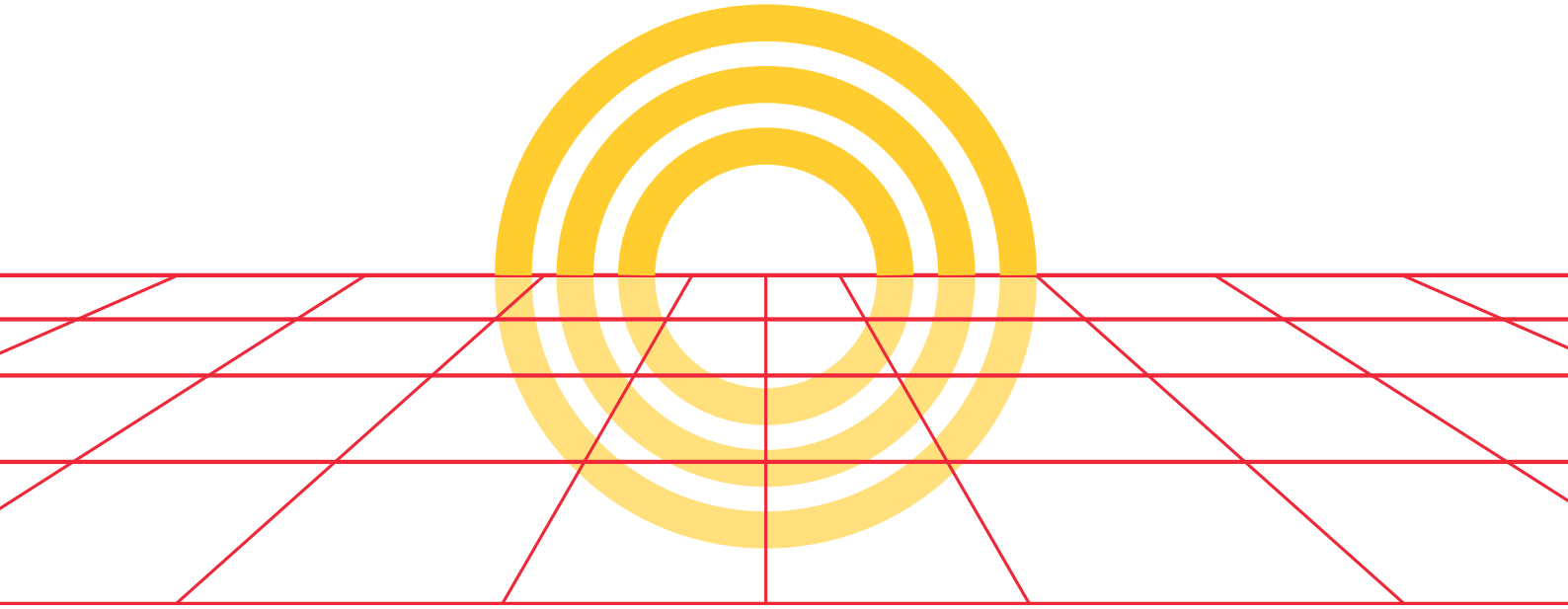

Nota Explicativa

Facilitar el Acceso Seguro a Espacios Digitales

Introducción

El programa de *Inclusión Digital* del ACNUR reconoce que l@s refugiados y otras personas desplazadas tienen el derecho de participar de manera significativa en la revolución digital. El deterioro de muchas situaciones humanitarias con el impacto de la pandemia de COVID-19 ha resaltado la gran importancia de que las poblaciones refugiadas están conectadas y tengan fácil acceso remoto a la información y servicios de protección vitales.

Sin embargo, también se pueden generar grandes riesgos de manera involuntaria hacia las personas desplazadas y las comunidades que l@s acogen cuando se trata de mejorar su acceso e inclusión digital. Estos pueden ser riesgos de fraude online, uso indebido de datos personales de refugiados captados, rastreo de sus actividades en redes sociales, entre otros. Estos se deben comprender, gestionar y mitigar. Es fundamental que las PdI para el ACNUR tengan las habilidades y procesos adecuados para participar de forma segura en línea y garantizar que puedan usar herramientas digitales que ayuden su resiliencia. Junto con el trabajo reciente del ICRC sobre los riesgos de protección de datos en las intervenciones de conectividad, el ACNUR quiere entender más sobre cómo estos riesgos se manifiestan en espacios digitales y cómo se pueden mitigar. El siguiente informe señala algunos de los temas más relevantes y destaca la experiencia de las PdI en dos contextos nacionales investigados (Uganda y Kenia) Connecting With Confidence: Managing Digital Risk.

Contexto

La alfabetización digital es esencial para asegurar que las personas puedan usar la tecnología de manera segura, efectiva y eficiente. La falta de habilidades digitales y conocimientos relevantes sigue siendo una de las barreras más importantes en todo el mundo para el acceso a servicios de conectividad. En una época donde se está pasando por una transformación digital y la asistencia humanitaria se está proporcionando cada vez más por medio de canales digitales, es esencial resolver esta falta de habilidades para garantizar que las comunidades puedan navegar las nuevas modalidades. La alfabetización sobre datos es especialmente importante para que las personas desplazadas no sólo entiendan los sistemas y plataformas que usan, sino también lo que ocurre con los datos que generan/ proporcionan, cómo se procesan, y por quién. Se pueden usar diferentes metodologías para desarrollar estas habilidades y compresión.

Otros riesgos potenciales incluyen:

1. **Conexiones Seguras:** La mayoría de los servicios de conectividad usados por personas desplazadas se proporcionan mediante las conexiones celulares manejadas por Operadores de Redes Móviles (ORMs). En ciertos contextos, la conectividad se proporciona por hotspots de WiFi, centros comunitarios conectados y otras soluciones locales. La naturaleza de estas conexiones puede crear riesgos: Hay algún filtro de contenido? Por cuánto tiempo se retiene la información de l@s refugiados usando un hotspot? Son estas redes seguras o vulnerables a los ataques digitales? Cómo se manejan estos centros y por quien? Hay medidas de seguridad simples que se pueden tomar para gestionar los riesgos a la infraestructura local?
2. **Vigilancia digital:** Cómo se están usando los datos personales online de manera consciente o inconsciente? Cómo pueden los actores externos vigilar, registrar y utilizar la huella digital y el comportamiento en línea de la población? Qué tan conscientes están las PdI sobre estos riesgos y cómo puede afectarl@s en el futuro cuando traten de buscar apoyo o servicios?
3. **Acceso seguro:** Las cuentas online y los dispositivos personales tienen una gran cantidad de información personal valiosa, pero frecuentemente no están suficientemente protegidas- por ejemplo cuando las contraseñas o información sobre las cuentas son compartidas sin entender los riesgos. Es esencial saber las mejores prácticas para minimizar las oportunidades de accesos indebidos o ilegales- por ejemplo cómo manejar contraseñas, configuraciones de seguridad y privacidad, y las implicaciones de compartir las credenciales de acceso a servicios;
4. **Crimen cibernético:** Puede presentarse de diferentes maneras como robo de identidades en línea, fraude financiero, acoso, intimidación, hacking, fraude imitando correos electrónicos, la piratería y falsificación de información o propiedad intelectual;
5. **Abuso en linea y Violencia Sexual y de Genero:** Las redes sociales como Facebook e Instagram se han usado para facilitar la trata humana, “grooming” y explotacion sexual (por ejemplo conectando con potenciales victimas mediante anuncios de trabajo falsos o entablando amistades con niñ@s). El uso extenso de tecnologías digitales también ha incrementado el acoso o interacciones sexuales no deseadas online; afectando especialmente a las niñas y mujeres.

Alcance y Objetivos

El objetivo principal de este reto es encontrar soluciones responsables para disminuir los riesgos digitales que perciben y enfrentan las PdI para garantizar su participación segura e inclusiva en espacios digitales. Estas deben considerar riesgos y barreras específicas que enfrentan diferentes grupos por su género, edad u otra demográfica.

Solicitud

Las propuestas buscarán abordar los riesgos a los cuales las comunidades están expuestas online en un contexto operacional específico por medio de desarrollar sus habilidades digitales y aprovechando esfuerzos e iniciativas previas en esta área. Los proyectos buscarán:

1. Concientizar sobre los riesgos online que viven y perciben las Pdl- especialmente sobre los riesgos más importantes con actividades dirigidas a grupos vulnerables específicos cuando sea relevante y en formatos accesibles;
2. Proporcionar herramientas para: interactuar con o promover la participación segura de las comunidades online, salvaguardando identidades individuales, identificando información clave que se debe proteger, y compartir datos personales de manera responsable;
3. Establecer protocolos y guías para que el personal, socios y Pdl puedan identificar y detectar posibles amenazas online y cómo responder o derivarlas apropiadamente.

Para enviar una propuesta a este reto, haga clic en el botón Aplicar Ahora.

APLICAR AHORA

(*Tendrás que registrarte con tu cuenta de ACNUR*)