Planear nuestra comunicación celular para organizarnos y actuar [actividad táctica]

A continuación, compartimos unas consideraciones orientativas para grupos que están organizando y/o participando en acciones políticas y usan apps de mensajería/chat.

Puedes usar esta guía para facilitar conversaciones que apoyen a los grupos activistas a considerar los tipos de comunicación que utilizan y diseñar colectivamente protocolos más seguros sobre la gestión y la comunicación en el grupo.

Esta actividad tiene 3 etapas:

- Mapear formas de comunicación y evaluación de riesgos
- Planear: grupos y escenarios.
- Instalar apps (opcional)
- Implementar (opcional)

Si el grupo no ha optado por un aplicativo de chat aún, puede realizar la actividad Conversación, intro + sesiones prácticas: Escoger apps para el celular.

Objetivos de aprendizaje

- adquirir y poner en práctica estrategias y tácticas de seguridad celular para gestionar los impactos de la comunicación celular en nuestras vidas y las de nuestras compañeras y redes activistas;

¿Para quién es esta actividad?

Para participantes con diferentes niveles de experiencia utilizando celulares.

Si va a delegar la responsabilidad de administrar grupos de chat a algunas personas del grupo, planea implementar un diseño y protocolo en el taller.

Tiempo requerido

Aproximadamente **60 minutos** para mapear/visualizar y diseñar y hasta **3 horas** si vas a instalar aplicativos de chat, mapear/visualizar, diseñar e implementar.

Materiales requeridos

- Papel para dibujar y visualizar/mapear.

Mecánica

Mapear formas de comunicación y evaluación de riesgos

Consideraciones: Privacidad

Toma en cuenta que podemos comunicar diferentes tipos de mensajes por signal y algunos mensajes pueden ser más públicos que otros. Mapea los diferentes tipos de comunicación y diseña grupos acorde a vuestras consideraciones de privacidad.

¿Qué tipos de comunicación estableces y qué consideraciones tomas en cada caso?

Puede haber diferentes clases de información -- por ejemplo, información confidencial entre dos personas o sólo debe conocer una persona y documentar sin compartir.

QUIÉN	EJEMPLOS DE TIPO DE COMUNICACIÓN
1 entre un grupo pequeño de personas que se conocen	*ubicación de responsables de la organización/actividad*
2 importante que colaboradoras/voluntarias conozcan o para grupos pequeños coordinarse entre sí	*cambios en la ubicación de la multitud*
3 puede compartirse abiertamente	*hora de inicio de manifestación, grupos que apoyan la acción públicamente*

PLANEAR: Grupos y escenarios

Crea grupos según los diferentes tipos de comunicación.

Sugerimos basarse en las preguntas a continuación. Incluimos recomendaciones para gestionar grupos de comunicación y ejemplos de situaciones para cada tipo. Plantea qué funciona para tu grupo y lo que no, qué cambios puedes realizar.

Membresía/pertenencia

- QUIÉN - ¿quién puede formar parte de este grupo?
- CÓMO - ¿cómo se une alguien al grupo? ¿Cuál es el procedimiento? ¿Necesita haber algun tipo de revisión, presentación o registro?
- CONFIRMACIÓN Y NOTIFICACIÓN - ¿Cómo se avisa al grupo cuando alguien entra? ¿Qué relevancia tiene hacerlo?
- SEGUIR ACUERDOS - ¿Qué se hace si alguien entra al grupo sin seguir el procedimiento?
- INFORMACIÓN PERSONAL - ¿qué tipo de servicio de mensajería/chat están utilizando? ¿las participantes del grupo pueden ver los números de todas? En caso de que alguien quiera/necesite mantener su número privado, hay que tomar esto en cuenta a la hora de formar parte de grupos más grandes.

Saber con quién estás hablando - VERIFICACIÓN

Para cualquier tipo de comunicación ¿cómo verificas con quién estás hablando?

- CARA-A-CARA - ¿es necesario conocerse cara a cara antes de formar parte del grupo? ¿puede entrar sin este contacto si tiene el aval de alguna integrante del grupo?
- SEGURIDAD- VERIFICA que tus mensajes están llegando a los dispositivos correctos. Si estás usando Signal o Whatsapp, VERIFICA LOS NÚMEROS DE SEGURIDAD.
- PALABRAS DE SEGURIDAD - VERIFICA que tus llamadas están llegando a donde tienen que llegar. Si estás usando Signal para llamadas, UTILIZA PALABRAS CLAVES DE SEGURIDAD.

Si utilizas otro aplicativo, ¿quieres seguir algún protocolo para verificar, al inicio de la llamada, que la persona con la que te estás comunicando es la cierta y puedes hablar libremente?

Seguridad de mensajes - configuraciones

Discutan, basándose en el nivel de confidencialidad de la información que se está comunicando, ¿qué acuerdos quieren pactar sobre la configuración de mensajes?

- BORRAR Mensajes - ¿Cuánto tiempo se mantienen los historiales de chat en los dispositivos?
- AUTODESTRUCCIÓN de mensajes - En Signal, puedes programar la desaparición de mensajes automáticamente. ¿Quieres utilizar esta funcionalidad? ¿Cómo y por qué?
- ESCONDE mensajes en tu pantalla de inicio - configura tus apps de chat para que no muestren mensajes en la pantalla. De esta manera, en caso de perder el control de tu dispositivo (lo pierdes, te lo roban o confiscan, etc.), no pueden ver tus mensajes.
- CÓDIGOS - Para información muy confidencial, sugerimos establecer palabras código antes de planear y actuar. Por ejemplo, decir "¡Listxs para tomar un café!" en vez de "¡Listxs para la marcha!".

Planilla para organizar grupos de comunicación

1. Grupos pequeños para información confidencial [se siguen protocolos estrictos de verificación]

Consideraciones/riesgos: el riesgo de personas desconocidas o que no has conocido en persona entrando en el grupo implica que tendrán acceso a información que no quieres que se vuelva pública y potencialmente podrán compartirla.

- Si tienes información confidencial que debe ser compartido sólo entre personas conocidas.
- Grupo muy pequeño (8 personas o menos). Todo el mundo se conoce y se han visto presencialmente;
- Sólo agregan participantes cuando están cara a cara.
- VERIFICAR identidad (en SIgnal, verificar números de seguridad) en persona;
- Si el número de seguridad de alguien cambia, hace falta verificarla de nuevo.
- No compartes más de lo que necesites. Evita tomar riesgos innecesarios.
- ELIMINAR

2. Nodos - grupos pequeños

Consideraciones/riesgos: que personas se unan al grupo y envíen información que no es útilo intencionadamente incorrecta.

- Riesgo de "spamming": interferir en el grupo y hacerlo inservible.
- Entre 2-20 personas. Evitar temas que no son relevantes para el grupo.
- Un grupo grande puede componerse de múltiples nodos con el fin de mantener el enfoque y gestión.
- Los nodos se conectan entre sí para asegurar un flujo de información.
- Puede haber personas de enlace en cada nodo para pasar información al resto del grupo;

3. Grupo abierto / información pública

La información en este grupo será pública y en tiempo real.

A diferencia del resto de los grupos dnde la información se puede filtrar o compartir fuera del grupo sin consentimiento, en este grupo toda la información es pública por defecto.

Seguridad de dispositivos

Si toman tu dispositivo (robo, extravío, confiscación, etc.), evita que otras personas se hagan pasar por tí y lean tus mensajes, contactos, correo, etc. Para más información sobre seguridad de dispositivos, véase la actividad: ¡Respalda! ¡Bloquea! ¡Elimina! También conocido como alguien tomó mi celular: cruzar fronteras, detenciones, incautación y robo

- Configura el bloqueo
- Establece una contraseña robusta y segura
- Cifra tu celular
- Cifra tu tarjeta SIM

Batería y red

¿Qué pasas si alguien no puede usar Signal o el aplicativo que ha escogido el grupo? ¿O no tiene acceso a su dispositivo o internet por algun fallo o corte de red? ¿Tienes un plan B para conectarte a internet? por ej, algún router portable (pero atención, si ocupa la misma red celular y hay un fallo a este nivel, entonces no servirá) ¿Tienen algun plan/protocolo/procedimiento fuera de internet? ¿Tienen cargadores USB o alguna forma de cargar baterías?

Materiales complementarios

- Cómo realizar verificaciones de seguridad y usar palabras clave de seguridad (inglés) - https://theintercept.com/2016/07/02/security-tips-every-signal-user-should-know/
- https://ssd.eff.org/es
- https://ciberseguras.org/?s=celular

image-1605452256072.png
Image not found or type unknown

Revision #4
Created 26 April 2023 00:28:37 by Kira
Updated 28 July 2023 15:03:53 by Kira