Política para compartir información en la Red Autodefensa.Online

La Red busca ser un espacio seguro que permita a sus participantes compartir datos e información de manera segura y confidencial. Para respetar la privacidad de todas las partes implicadas, así como garantizar la confidencialidad y seguridad de nuestras comunicaciones, hemos desarrollado esta política que todas las integrantes de la Red deben aceptar e incorporar a su práctica cotidiana respecto a cómo debe clasificarse, almacenarse, compartirse y destruirse la información intercambiada.

1. Clasificación de la información

Manejaremos toda la información que se produzca e intercambie en el marco de la Red de manera confidencial y no la revelaremos a terceros sin consentimiento previo. Manejaremos la información entrante de manera responsable y la protegeremos contra la divulgación involuntaria a partes no autorizadas. La seguridad de los métodos de almacenamiento y transmisión de la información dentro o fuera de la Red será apropiada a sus niveles de sensibilidad.

Entendemos que existen dos tipos de datos información que pueden ser compartidas en la Red:

- **Información pública.** Se considera que esta información no es confidencial –es decir, que no incluye datos personales identificables o sensibles– y que puede ser distribuida a cualquier persona en cualquier contexto. Esta información está destinada al consumo público. Los correos que incluyan recursos, publicaciones, investigaciones, campañas con vocación de ser difundidas y compartidas con otras personas serán consideradas como datos e información pública.

- **Información confidencial**. Se considera información confidencial a todos los datos o informaciones compartidas a través de los canales de comunicación de la Red –lista de correo, asambleas, grupos de trabajo, chats, documentos del Nextcloud, calendarios, etc.– que no sean alcanzados por la definición de información pública.

En caso de que haya algún dato o información confidencial que tenga que ser compartida con terceras personas –por razones de seguridad, por ejemplo– éstas deberán también aceptar y firmar la presente política.

2. Canales de comunicación

Toda coordinación remota, o iniciativa en línea, se realizará a través de canales seguros que funcionen con software libre y de código abierto y, especialmente si no están cifrados de extremo a extremo, que sean gestionados y alojados por partes de confianza, idealmente por integrantes de la Red Autodefensa.Online. Se evitará el uso de herramientas comerciales o propietarias, especialmente si tienen antecedentes de violar la privacidad de sus usuarios, y/o tienen un historial de facilitar violencias de género en sus plataformas.

Las integrantes de la Red Autodefensa.Online se comunican por una lista de correo segura usando correos no comerciales seguros.

Las integrantes de los grupos de trabajo de la red pueden comunicarse a través de apps de chats seguras y cifradas (Signal, Wire, Riot) y/o por instancias de videoconferencias seguras (instancias propias de BBB y Jitsi o instancias BBB y Jitsi alojadas por sus participantes).