DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Universidad Nacional Autónoma de México

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

PROTOCOLO DE ACTUACIÓN ANTE AMENAZA POR REDES SOCIALES

1. DEFINICIÓN

Con base en la Real Academia Española y su Diccionario del Español Jurídico (2020), se define como amenaza el "anuncio de un mal dirigido a otro, que puede realizarse de forma oral, escrita, o con actos, y con entidad suficiente para infundir miedo y temor". Las amenazas, pueden estar motivadas por la exigencia de dinero o cualquier otra condición como allanamiento, sabotaje, robo, fraude, espionaje o algún otro delito; y puede ser grave cuando es efectuada de forma seria, real y persistente, atentando contra la salud o vida de la víctima o sus familiares.

Existen diferentes tipos de amenazas, pero las más comunes son:

- Amenazas con revelar secretos de otro. Cuando alguien exige de otro una cantidad o recompensa bajo la amenaza de revelar o difundir hechos referentes a su vida privada o relaciones familiares que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés.
- Amenazas contra la pareja. Cuando de modo leve o severo afecte a quien sea o haya sido su esposa(o), que esté o haya estado ligada(o) al ofensor por una análoga relación de afectividad aun sin convivencia.
- Amenazas con armas o instrumentos peligrosos. Es el uso de armas u objetos peligrosos con el fin de obtener un beneficio o bien material de la víctima.
- Los medios para cometer las amenazas en contra de las personas se pueden distinguir en:
  - Presenciales. Aquellos que emplean el uso de armas o instrumentos peligrosos en contra de la víctima y/o mediante el uso de palabras directamente hacia el ofendido.
  - Indirectos o no presenciales. Los que se realizan a través de medios escritos, digitales o auditivos en contra de las víctimas.

Debido a que cualquier persona puede tener alcance a un medio electrónico como los teléfonos celulares y a la rapidez con la que se propaga la información a través de la Internet, las redes sociales, además de un medio de información, se pueden convertir en una herramienta para desprestigiar o amenazar a cualquier individuo, por lo cual es

necesario conocer de forma básica cómo funcionan los aspectos de seguridad de éstas para poder orientar a los usuarios para un manejo responsable y seguro.

En la actualidad las redes sociales más populares son Facebook, Twitter, Instagram, Pinterest, Youtube, SnapChat, TikTok y, especialmente, el servicio de WhatsApp, que actualmente es la alternativa más común de comunicación entre usuarios que van desde niños hasta adultos mayores. También existen algunas de aplicaciones que se están popularizando y que son consideradas de “conquista” como es el caso de Tinder, Badoo o Lovoo. Todas ellas hacen uso del sistema de geolocalización del *smartphone* para mostraral otro usuario el lugar aproximado en el que se encuentra y la distancia que existe entre ambos, lo que representa uno de los principales riesgos de seguridad.

Si bien la finalidad de las redes sociales es el entretenimiento o la absorción de información, es precisamente a través de otra de sus facetas: la interacción entre usuarios, donde se esconden varios riesgos al interactuar con personas desconocidas o incluso conocidas; entre los riesgos se encuentran:

- Sexting. Publicación de fotografías con fines “sexuales” o de "coqueteo".
- Grooming. Acciones emprendidas por un adulto para ganarse la confianza de un menor y tratar de conseguir una cita para abusar sexualmente de él, extorsionarlo o incitar al sexting, entre otras acciones.
- Ciberbullying. Ciberacoso psicológico, generalmente entre los menores de edad, usando los canales sociales y de mensajería.
- Hacking. Suplantación de la identidad al acceder a las cuentas o perfiles de los usuarios.
- Phishing: Obtención de datos personales a través de web ficticias con el fin de realizar hacking sobre alguna persona.

Muchas amenazas no son tomadas en cuenta por sus receptores o no les dan ninguna importancia por no ver en ellas ningún tipo de veracidad. No obstante, existen personas que se pueden sentir intimidadas y que están en su derecho de tomar medidas para restablecer su seguridad.

2. OBJETIVO

Plantear los lineamientos para prevenir y/o subsanar las acciones por amenaza a través de redes sociales a la comunidad de la DGTIC.

3. ALCANCE

El propósito de este documento es concientizar y otorgar información que permita evitar amenazas a través de las redes sociales así como sus consecuencias, que afecten a la comunidad de la DGTIC.

4. PARTICIPANTES

- Comunidad universitaria: alumnos, personal académico y administrativo.
- Titular de la DGTIC.
- Jefe de la Unidad Administrativa de la DGTIC.
- Unidad Jurídica de la DGTIC.
- Brigadistas de Seguridad de la DGTIC.(1)
- Personal de Vigilancia de la DGTIC.
- Dirección General de Análisis, Protección y Seguridad Universitaria (DGAPSU).
- Personal adscrito a la Fiscalía y/o secretaria de seguridad pública o ciudadana, federal o local.

5. CAPACITACIÓN

Se recomienda capacitar y actualizar permanentemente al personal académico, administrativo y de toma de decisiones de la DGTIC que participen en la actuación de este protocolo, en los siguientes temas:

(1) El Titular de la DGTIC, en coordinación con la Comisión Local de Seguridad, definirá el número de personas que integrarán las brigadas y quiénes serán, con el fin de agilizar las medidas de actuación, disminuir su vulnerabilidad y acortar los tiempos de respuesta.

- Curso de redes sociales.
- Acciones a seguir ante amenazas a través de redes sociales.
- Atención a crisis de las víctimas.

6. MEDIDAS PREVENTIVAS DE SEGURIDAD

El Titular de la DGTIC, en coordinación con la Comisión Local de Seguridad, promoverá las siguientes medidas de prevención, que están basadas en las recomendaciones generales de la Policía Ciberdelincuencia Preventiva, dependiente de la Secretaría de Seguridad Ciudadana de la CDMX, así como de la policía del ámbito federal:

- En redes sociales, evitar aceptar solicitudes de desconocidos.
- Evitar publicar información de índole estrictamente personal.
- De ser posible, evitar publicar información y fotografías de familiares.
- Pensar dos veces antes de escribir una publicación.
- Comprobar la configuración de privacidad en cada una de las redes sociales y apps.

Socialice estas precauciones entre la comunidad universitaria, trabajadores y funcionarios de la DGTIC.

7. ACTUACIÓN EN CASO DE AMENAZA POR RED SOCIAL

- Mantener la calma y no tomar medidas impulsivas.
- Hacer del conocimiento de los hechos a personas de confianza, quienes además de servir de apoyo, podrían fungir como posibles testigos.
- Dar aviso de manera rápida y oportuna a las autoridades de la DGTIC, quienes pueden ayudar como mediadores en caso de conciliación, asesores o apoyo legal.
- Si la amenaza pareciera inminente sobre su persona, ponerse en un lugar seguro y dar aviso a las autoridades de la institución marcando al número de emergencias o a través de la app SOS UNAM.

- Si la amenaza es en contra de algún amigo o familiar, y ésta parece inminente, ponerse en contacto con ellos y explicarles la situación para permanecer seguros. Se debe evitar entrar en pánico para no contagiar a los familiares.
- En caso de una amenaza por red social es importante guardar las evidencias, sobre todo si viene de un usuario claramente identificable.
- Para guardar las evidencias de una amenaza, especialmente si son reiteradas, basta con hacer una captura de pantalla en el dispositivo o computadora.
- Si se opta por hacer la captura de pantalla, es imperativo que se realice inmediatamente después de leer la amenaza, ya que, de acuerdo con las instancias policiales, los autores suelen borrarlas casi de inmediato, calculando el tiempo necesario para que la víctima lea el mensaje.
- En el caso de mensajes de audio, se recomienda respaldarlos y/o grabarlos. La mayoría de los teléfonos actuales cuentan con alguna aplicación para grabar audio. De lo contrario, en línea existen diversas apps que tienen este propósito. Se recomienda tener instalada alguna de éstas.
- Una manera apropiada de guardar las conversaciones en la plataforma WhatsApp, es a través de las copias de seguridad. Aquí permanecen los textos, imágenes y audios que un posible acosador realice.
- El afectado por la amenaza también puede poner la situación en conocimiento de la red social donde ha sido emitida. Este procedimiento es totalmente anónimo y muy sencillo, basta con pinchar sobre el comentario y denunciarlo como abuso o spam.
- Una medida muy común y recomendada consiste en bloquear al usuario para evitar recibir mensajes nuevos.
- En caso necesario, la Unidad Jurídica, solicitará el apoyo de la Oficina de la Abogacía General, para interponga una denuncia ante la Fiscalía.

- Es importante señalar que para que una denuncia sea procedente se debe contar con pruebas sólidas, por lo que se deben conservar grabaciones de audio, videos, fotografías o capturas de pantalla que reflejen la amenaza.
- Se debe evitar a toda costa el uso de violencia como medida de prevención ante una amenaza, pues se puede cambiar de víctimas a victimarios en instantes.

TELÉFONOS DE EMERGENCIA

CIUDAD UNIVERSITARIA	
Central de Atención de Emergencias	**55 5616 0523** **55 5616 9071** **55 5616 1288** **55 5616 2390** **55 5616 0914**
Protección Civil	**55 5622 6552** **55 5622 6557**
Bomberos	**55 5616 1560** **55 5622 0565**
Línea de Reacción Puma	**55 5622 6464**
Dirección General de Atención a la Salud (Centro Médico Universitario)	**55 5622 0140** **55 5622 0202**
Sistema de Orientación en Salud	**55 5622 0127**
Secretaría de Prevención, Atención y Seguridad Universitaria	**55 5622 1284** **55 5622 1286**
Dirección General de Análisis, Protección y Seguridad Universitaria	**55 5622 6470** **55 5665 0403**
Denuncia Universitaria	**800 2264 725**

CIUDAD DE MÉXICO

Locatel	**55 5658 1111**
Protección Civil	**55 5683 2222**
Bomberos (Estación central)	**55 5768 3700** **55 5768 3477**
Sistema de Aguas	**55 5654 3210**
Cruz Roja	**55 5395 1111**
Unidad de Contacto del Secretario de Seguridad Ciudadana	**55 5208 9898**
Denuncia anónima	**089**

DIAGRAMA DE FLUJO