SOCIALTIC

Tecnología digital para el cambio social

Tipología de Ataques Digitales

Febrero 2022, v2
Junio 2020, v1

Elaborado por:
Paul Aguilar
Haydeé Quijano
Juan M. Casanueva
Enrique Garcia

Objetivo de la Tipología

En un espectro de violencia donde las agresiones toman distintas formas, son múltiples y se relacionan, esta tipología busca describir los eventos y elementos asociados a los ataques digitales, algunos de los riesgos que conllevan y medidas digitales de prevención.

La versión web de esta tipología se puede consultar en https://protege.la/ataques

¿Qué es un ataque digital?

Cualquier acción y comportamiento con fines maliciosos mediante el uso de tecnologías de la información y la comunicación (TIC), como teléfonos, sitios web, plataformas de redes sociales y/o correos electrónicos. Los ataques o agresiones digitales tienen como fin generar, incitar o agravar un daño.

Categorías

Esta tipología se encuentra divida en dos categorías principales:

- **Ataques digitales mediante vulneraciones técnicas:** Implican abusar del diseño de la tecnología para modificar o romper aspectos técnicos con fines maliciosos.
- **Ataques digitales mediante conductas humanas:** Implican abusar del componente humano y las relaciones sociales con tal de generar un daño.

Generalmente las dos categorías de ataques se relacionan entre sí.

Consideraciones

a) Enfoque descriptivo

- Los ataques aquí descritos se abordan de manera general, indicando *cómo se manifiestan*, buscando ser útil como punto de inicio para un diagnóstico más profundo. El cómo se realizan se deberá abordar por la persona que utiliza la tipología ya que cada ataque puede tener distintas formas de ejecución o implementación.
- Cada ataque está descrito por individual, sin embargo se debe tener en cuenta que *los ataques se combinan o cruzan* y el cómo derivan en otras manifestaciones y amenazas.
- Contemplamos *algunas posibles amenazas*, ya que el impacto es de manera diferenciada, según quien las ejerce, quien las vive y en qué contexto social, cultural, económico, político están teniendo lugar. Por lo que al realizar un análisis de riesgo, es importante identificar otras posibles vulnerabilidades según el contexto.
- Al utilizar esta tipología para documentar ataques digitales es clave tener en cuenta cómo se atacan grupos y comunidades específicas, por ejemplo mujeres y

comunidades de diversidad sexual. Por lo que esta tipología tendrá que abordarse y complementarse desde una *perspectiva de género e interseccionalidad*.
- Las *medidas de prevención* son algunas propuestas. Para una prevención y atención integral, se deben incluir aspectos físicos, digitales y emocionales de acuerdo a cada caso.

b) Capacidad del agresor

Esta tipología está desarrollada y ordenada considerando las posibles capacidades del agresor, su objetivo y cómo algunos ataques pueden habilitar a otros de manera escalonada. Así como la coordinación y estrategia del agresor/es.

c) Agravantes

Cualquier ataque puede agravar el impacto sobre la víctima u objetivo a través de:
- La combinación y/o cruce de ataques.
- El volumen, persistencia o mayor cantidad de relación entre ataques.
- El contexto de quien es objetivo y vive los ataques así como de quien los ejerce.

Ataques digitales mediante vulneraciones técnicas

Implican el uso de una o varias técnicas que abusan del diseño de la tecnología para modificar o vulnerar aspectos técnicos con fines maliciosos.

Daño, pérdida o robo de dispositivos

- **Descripción:** En dispositivos electrónicos como computadoras, celulares, discos de almacenamiento o USB, guardamos grandes cantidades de información. Estos dispositivos son una puerta a la actividad personal, laboral y de redes de contactos. En caso de daño, pérdida o robo de dispositivos, se puede perder esta información y/o alguien más podrá tener acceso a ella y utilizarla con fines maliciosos.
    - Ej. robo en la calle, transporte público, vehículos privados, habitación o allanamientos de oficinas.
    - Ej. daño por violencia física en manifestaciones, espacios privados o públicos.

- **Posibles impactos:**
    - Pérdida de información por daño (parcial o total) o robo de la misma.
    - Filtración o exposición de información.
    - Acceso a información privada o sensible.
    - Si la información es sensible, puede llegar a comprometer la integridad de una persona o grupo.
    - Debido al acceso a la información, se pueden generar campañas de censura y desprestigio.

- **Medidas de prevención:**
    - Respaldar periódicamente la información en medios de almacenamiento externos.
    - Almacenar los dispositivos en lugares físicamente seguros (a salvo de daños y robo).
    - Elegir el lugar y medio de almacenamiento adecuado en función de la información que se desea proteger o resguardar.
    - Bloquear el acceso de los dispositivos configurando usuarios y contraseñas.
    - Cifrar la información privada y sensible (el cifrado asegura la información con candados y códigos para protegerla).
        - Para cifrado de archivos se puede utilizar Cryptomator
        - Para cifrado de dispositivos completos se puede utilizar VeraCrypt, BitLocker, Filevault o Cryptsetup, dependiendo del sistema operativo.
    - Configurar mecanismos de bloqueo y formateo remoto mediante la opción “Encontrar mi dispositivo” de Google, Apple o Microsoft.

Accesos no autorizados a dispositivos, cuentas y servicios en línea

- **Descripción:** Un acceso no autorizado puede suceder en dos líneas. La primera es a un dispositivo, y la segunda a una cuenta o servicio en línea.

  En un dispositivo puede pasar al no tener configurado un mecanismo de acceso adecuado como contraseña o usuario de inicio de sesión, y puede ser consecuencia de la pérdida o robo del dispositivo.

  En un servicio o cuenta en línea se puede dar por filtraciones o robo de usuarios y contraseñas, por ataques de fuerza bruta (mecanismos automatizados para probar combinaciones de contraseñas) o mediante la suplantación de un sitio web mediante phishing.
  - Ej. Acceso a cuentas en línea de redes sociales, servicios de correo o sitios web.
  - Ej. Acceso físico a un dispositivo perdido o robado.

- **Posibles impactos:**
  - Acceso a información privada o sensible.
    - Filtración o exposición de información.
    - Campañas de censura y desprestigio.
  - Suplantación de identidad.
  - Intervención de dispositivos.

- **Medidas de prevención para dispositivos:**
  - Bloquear el acceso de los dispositivos configurando usuarios y contraseñas.
  - Cifrar la información privada y sensible (el cifrado asegura la información con candados y códigos para protegerla).
    - Para cifrado de archivos se puede utilizar Cryptomator
    - Para cifrado de dispositivos completos se puede utilizar VeraCrypt, BitLocker, Filevault o Cryptsetup, dependiendo del sistema operativo.

- **Medidas de prevención para cuentas y servicios en línea:**
  - Para evitar caer en engaños digitales que permitan accesos no autorizados a cuentas, sigue las acciones recomendadas en Phishing.
  - Utilizar contraseñas seguras
    - Que combinan caracteres alfanuméricos y símbolos, con una longitud mayor de 8 caracteres. Ej. C0ntr4s3ñ4sS3gur4s!
    - Únicas, no repetir en otras cuentas o servicios.
    - Privadas, no compartir con otras personas.
    - Con caducidad, que cambiar por lo menos una vez al año
  - Utilizar la verificación de dos pasos.

        - Utilizar mediante alguna aplicación generadora de códigos cómo Authy, FreeOTP o Google Authenticator.
        - Configurar códigos de recuperación extra.
    - Utilizar un gestor de contraseñas como KeePass.
        - KeePassXC para equipos de computo
        - KeePass2Android para dispositivos Android
        - Strongbox para dispositivos iOS
    - Revisar periódicamente en tus cuentas en línea (cada 6 meses):
        - Conexiones e inicios de sesión (preferentemente cada 2 meses)
        - Configuraciones de seguridad.
        - Configuraciones de privacidad.
        - Filtraciones de datos en Firefox Monitor
    - Conocer las herramientas de reporte y atención de incidentes dentro de las plataformas o servicios en línea.

Phishing

- **Descripción:** El *phishing* es una técnica que se basa en suplantar o falsificar información para incitar a la persona a realizar una acción, como dar clic a un enlace, abrir un archivo infectado, conectarse a una red o sistema falso, o ingresar información en sitios falsos. Generalmente con el objetivo de robar información, infectar un equipo o sistema de información.
    - Ej. correos electrónicos o SMS sospechosos solicitando dar clic a enlaces.
    - Ej. correos electrónicos o SMS sospechosos solicitando enviar o responder información privada, sensible o financiera.
    - Ej. correos electrónicos sospechosos solicitando abrir archivos adjuntos.

- **Posibles impactos:**
    - Robo de información
    - Robo de datos para iniciar sesión en cuentas
    - Accesos no autorizados a cuentas
    - Suplantación de identidad
    - Infecciones e intervenciones de dispositivos

- **Medidas de prevención:**
    - Verificar e identificar
        - Origen de la información (emisor)
        - Veracidad del contenido
        - Veracidad de los enlaces o adjuntos
    - En caso de reconocer información sospechosa o poco confiable, evitar responder, dar clic en enlaces o abrir archivos adjuntos.
    - Evitar compartir información privada o sensible en espacios digitales.
    - Utilizar un navegador web actualizado para identificar sitios sospechosos.
    - Utilizar servicios en línea cómo “Should I Click?”, “URLScan” o “Virus Total” para identificar enlaces maliciosos.
    - Utilizar un antivirus para analizar archivos sospechosos.
    - En caso de requerir abrir archivos que estén potencialmente infectados por

malware se puede utilizar “Danger Zone”.

Denegación de servicios

- **Descripción:** Técnica que busca saturar un servicio o consumir los recursos de un sistema para que colapse y no pueda atender solicitudes. Se suele llevar a cabo con ataques de fuerza bruta y son principalmente dirigidos a un objetivo en específico, el servicio. Cualquier servicio digital o electrónico accesible de manera pública, puede ser atacado, ya sea un sitio web, un servicio de mensajería o una red telefónica o de Internet.
    - Ej. Un sitio web recibe un gran volumen de visitas automatizadas y queda fuera de línea.
    - Ej. Una red de internet como un WiFi en un espacio público recibe un gran volumen de conexiones automatizadas y queda fuera de servicio.
    - Ej. Una red de telefonía móvil recibe un gran volumen de solicitudes o llamadas y ya no puede atender el servicio.

- **Posibles impactos:**
    - Bloqueo parcial o total del servicio.
    - Pérdida de información en un proceso de comunicación ya que el canal de comunicación está caído o saturado.
    - Suplantación o alteración del servicio.
    - Se pueden generar campañas de censura.

- **Medidas de prevención si gestionas un servicio:**
    - Modificar las configuraciones pre-establecidas del servicio.
    - Utilizar infraestructuras robustas y escalables con tal de soportar ataques de gran volumen cómo e.g. utilizar un CDN (*Content Delivery Network*) o infraestructura elástica.
    - Monitorear la actividad del servicio o sistema para detectar actividad sospechosa.

- **Medidas de prevención si utilizas un servicio:**
    - Considerar un servicio de respaldo en caso de emergencia.
    - Considerar herramientas o servicios descentralizados.
    - En casos especiales, considerar servicios offline o analógicos.

Intervención de dispositivos o sistemas

- **Descripción:** Modificación o alteración de un dispositivo (computadora, móvil o servidor) o sistema informático (programas, aplicaciones o servicios en línea), o de su contenido de manera no autorizada, mediante el uso de vulnerabilidades, malware o la modificación de sus componentes físicos.
    - Ej. Infección de un dispositivo por virus descargados mediante *phishing*.
    - Ej. infección de un dispositivo por otros dispositivos infectados, como una USB o un disco externo.

    - Ej. Modificación física del equipo cambiando sus partes por otras.
    - Ej. Acceso no autorizado a un servicio en línea y modificación del mismo.

- **Posibles impactos:**
    - Accesos remotos al dispositivo o sistema.
    - Accesos no autorizados con permisos de administración.
    - Acceso a información privada o sensible.
    - Filtración o exposición de información.
    - Daño, modificación o alteración de:
        - Datos e información
        - Programas, aplicaciones y sistemas operativos
    - Si la información es sensible, se compromete la integridad de una persona o grupo.
    - Pérdida de información.
    - Bloqueo parcial o total del sistema o dispositivo.
    - Suplantación o alteración de la información o los sistemas.
    - Vigilancia y monitoreo.

- **Medidas de prevención para dispositivos:**
    - Evitar caer en *phishing*. Puedes revisar sus medidas de prevención específicas en la sección correspondiente.
    - Respaldar periódicamente la información en medios de almacenamiento externos.
    - Bloquear el acceso de los dispositivos configurando usuarios y contraseñas.
    - Cifrar la información privada y sensible (el cifrado asegura la información con candados y códigos para protegerla).
        - Para cifrado de archivos se puede utilizar Cryptomator
        - Para cifrado de dispositivos completos se puede utilizar VeraCrypt, BitLocker, Filevault o Cryptsetup, dependiendo del sistema operativo.
    - Instalar actualizaciones de seguridad, tanto del sistema operativo como del software (programas o aplicaciones).
    - Instalar y utilizar *antivirus* y un *firewall*.

- **Medidas de prevención para sistemas:**
    - Respaldar periódicamente la información e infraestructura de los sistemas.
    - Cifrar la información privada y sensible de bases de datos o sistemas de almacenamiento.
    - Instalar actualizaciones de seguridad de los sistemas.
    - Utilizar sistemas de monitoreo para identificar actividad, incidentes o eventos sospechosos.

Intervención de líneas o infraestructuras de comunicación

- **Descripción:** Intervenir una infraestructura de comunicación como redes de telefonía fija, móvil e internet, requiere modificar o alterar físicamente su funcionamiento con el fin de interceptar y/o manipular el contenido que viaja en ella.

    - Ej. instalación de antenas no oficiales (*IMSI Catchers , Stingray*)
    - Ej. alteración de las antenas mediante programas u otras antenas repetidoras, para extraer información a fuentes externas.

- **Posibles impactos:**
    - Bloqueo parcial o total del medio de comunicación.
    - Pérdida de comunicaciones e información mientras viaja.
    - Intercepción de información y comunicaciones.
    - Suplantación o alteración de la información interceptada.
    - Vigilancia y monitoreo.

- **Medidas de prevención:**
    - Utilizar medios y herramientas de comunicación cifradas para:
        - HTTPS en sitios web
        - Video y Voz, como Jitsi o Big Blue Button
        - Chat, como Signal
        - Envío y recepción de archivos, como Share Rise Up o Send Tresorit
        - Navegación en Internet con servicios VPN, la red Tor o DNS alternativos
    - Verificar la autenticidad de la información a través de firma o huella digital, o de *hashes*. Ej. llaves o claves de seguridad para cifrado.

Ataques digitales mediante conductas humanas

Implican abusar o aprovecharse del componente humano. En ocasiones involucran también una o varias vulneraciones técnicas.

Como está descrito al inicio en la sección *Consideraciones;* en esta categoría no incluimos **posibles impactos**, ya que estos son de manera diferenciada, según quien ejerce los ataques, quien lo vive y en qué contexto social, cultural, económico y/o político tienen lugar. Por lo que al realizar un análisis de riesgo, es importante identificar otras posibles vulnerabilidades según el contexto.

Las **medidas de prevención** incluyen acciones digitales. Para una prevención y atención integral, se deben incluir aspectos físicos, digitales y emocionales de acuerdo a cada caso.

Reiteramos que al utilizar esta tipología para documentar ataques digitales es clave tener en cuenta cómo se atacan grupos y comunidades específicas: por ejemplo mujeres y comunidades de diversidad sexual. Por lo que esta tipología tendrá que abordarse y complementarse desde una perspectiva de género e interseccional.

Los ataques de esta categoría están divididos en **interacción directa** e **indirecta.**

Los **ataques mediante interacción directa** son aquellos en los que la persona o grupo atacante establece contacto directo con la persona agredida a través de medios digitales, como mensajes en redes sociales, correos electrónicos o chats.

Los **ataques mediante interacción indirecta** no implican una interacción, como cuando recaban información sobre una persona o grupo, o una suplantación de identidad, por lo que suelen ser silenciosos e inadvertidos ya que la persona agredida puede no percatarse de qué está sucediendo.

Estos ataques pueden incluir contenido con fines de causar daño o desinformar, tales como: ofensas, contenido discriminatorio o que incita al odio.

Interacciones directas

Conductas ofensivas, intimidatorias, discriminatorias o que incitan al odio

- **Descripción:** Algunas de estas conductas pueden manifestarse a través de las siguientes expresiones.

  (Asociadas a contextos ofensivos e intimidatorios) Expresiones con el fin de ofender, avergonzar, asustar, humillar, desprestigiar y/o intimidar deliberadamente a otra persona. Ej. Insultos y ofensas a través de redes sociales
    - Ej. Memes ofensivos o imágenes deshumanizantes.

  (Asociadas a contextos discriminatorios) Expresiones que reproducen la desigualdad, buscan otorgar un lugar inferior o insultar deliberadamente a personas o grupos en función de su género, origen étnico, rasgos físicos, religión, origen nacional, orientación sexual, discapacidad u otros rasgos.
    - Ej: Insultos relacionados al cuerpo, tatuajes, color de piel

  (Asociadas a contextos que incitan el odio) Expresiones que incitan o motivan a hacer daño con base en la identificación de una persona o grupo. También aquellas que incrementen el riesgo de violencia, motiven un ambiente de prejuicio y hostilidad, ataques o acciones perjudiciales.
  Los contenidos discursivos que incitan al odio no son libertad de expresión. Si la expresión incita a la violencia se considera conducta de odio.
    - Ej: Imágenes que afirman un ataque: “merece ser golpeada"

  Aunque se pueden mencionar algunos ejemplos y categorías como las anteriores, la generalidad para este tipo de conductas la podemos identificar mediante expresiones o discursos cuyo componente principal está asociado a fenómenos de violencia.

Amenazas

- **Descripción:** Las amenazas anuncian un daño contra la integridad física y el bienestar de un grupo o persona. Con frecuencia incluyen expresiones ofensivas e intimidatorias. Las amenazas en línea no deben tomarse a la ligera, pues generan ansiedad, miedo y alteran el curso de la vida de una persona o grupo.
    - Ej: Mensajes amenazantes a través de chats, correos, llamadas: “sé donde vives, voy a buscarte”.

Acoso

- **Descripción:** Son actos o comportamientos que fomentan un ambiente intimidante, hostil u ofensivo. Son indeseados para quien las recibe y tienen alguna o comparten estas tres características
    A. Son intencionales.
    B. Son de naturaleza repetitiva y sostenida.
    C. Si bien puede que no exista una subordinación, implican un desequilibrio de poder entre un agresor (individual o grupal) y una víctima.

  El acoso opera de manera horizontal entre personas de jerarquías homólogas o de parte de alguien que ocupa una posición mayor a la de la persona acosada.
  El acoso basado en el género está marcado por la intención de agredir a alguien en función de su género y orientación sexual.
    - Ej: “Te voy a seguir mensajeando hasta que respondas”

Hostigamiento

- **Descripción:** Son actos o comportamientos que fomentan un ambiente intimidante, hostil u ofensivo. Implican una manifestación de poder. La relación subordinada en el hostigamiento, es la diferencia con el acoso.
    - Ej. “Mensajes molestos vía chats y que implican una relación laboral”

Extorsión

- **Descripción:** Implica amenazas, chantaje, y/o intimidación con el fin de mantener control sobre una persona, grupo o entidad. Están relacionadas a publicar o distribuir información o contenido privado, sensible o íntimo. Y se puede pedir a cambio dinero, acciones contra la voluntad, o contenido íntimo y privado**.**
    - Ej: “Si no haces lo que te digo, publico tus fotos íntimas”

Acciones inmediatas para ataques digitales de conducta humana por interacción directa

- Buscar apoyo con personas de confianza y organizaciones especializadas.
- Documentar (registrar las agresiones y respuesta de las plataformas).
- Utilizar las herramientas de silenciar, bloquear o reportar.
- Si incurre en un delito y decides hacer una denuncia pública y con las autoridades, aumenta tu seguridad e identifica redes de apoyo.

Medidas de prevención para ataques digitales de conducta humana por interacción directa

- Definir y gestionar perfiles o cuentas digitales según el tipo de información que contengan y su visibilidad.

- Separar o dividir información de acuerdo a cada perfil (público o privado)
- Configurar las opciones de privacidad de cuentas digitales, controlando qué información es visible y quiénes la pueden ver.
- Conocer las normas de comunidad y utilizar las opciones que incluyen las plataformas para dar de baja contenido ofensivo o intimidatorio (silenciar, bloquear o reportar). La respuesta de las plataformas dependerá del tipo de ataque.
- Dependiendo del contexto, contar con un registro de incidentes personales o colectivos (que contenga enlaces, capturas de pantallas y fechas) e incluir acciones y respuestas relacionadas.
- Contar con una red de apoyo que pueda responder ante la solicitud de aspecto físico, legal, digital, emocional.

SOCIALTIC

Interacciones indirectas

Doxing - Búsqueda y distribución sin consentimiento de **información personal, privada, o íntima.**

- **Descripción:** *Doxear* es recopilar información personal o privada para posteriormente ser difundida en espacios públicos con el fin de atacar o dañar a una persona en específico. La información puede ser obtenida de distintas fuentes de acceso restringido, como son redes sociales personales, grupos de mensajería, correos electrónicos, etc. Comúnmente el doxing genera un ambiente de intimidación, acoso y amenaza, y puede escalar a acciones físicas de manera directa.

  Este ataque también puede tomar la forma de divulgación de material gráfico y audiovisual explícitamente sexual o relacionado al rol de género, sin consentimiento y con el fin de causar daño.
  Puede asociarse a una dinámica de extorsión.
  - Ej. Una ex-pareja publica información íntima en redes sociales.
  - Ej. Un grupo opositor tiene acceso a información privada de una persona y publica esta información en redes sociales.

- **Medidas de prevención:**
  - Revisar las configuraciones de seguridad y privacidad de servicios y cuentas en línea, y verificar qué información es pública.
  - Revisar quiénes pueden ver información que es publicada en redes sociales.
  - Realizar un *"auto-stalkeo"* para conocer qué tipo de información existe en internet sobre una persona. El auto-stalkeo consiste en buscar e identificar información publicada sobre una misma(o), también incluye crear alertas asociadas a palabras clave a cerca de una persona o entidad para dar seguimiento de nuevos contenidos relacionados.
  - Evaluar qué información personal podría ser usada para solicitar la baja de contenido de algún espacio digital.

Distribución de información (imágenes, audios, videos o datos) con fines de dañar o desinformar

- **Descripción:** Los intentos para desinformar y desprestigiar tienen lugar cuando una persona o grupos organizados publican en línea contenido negativo, falso, manipulado o sacado de contexto a través de grupos en redes sociales, en servicios de mensajería instantánea, sitios web.

  Este ataque puede tomar la forma de divulgación de material gráfico y audiovisual explícitamente sexual o relacionado a la actividad profesional de la persona con el fin de causar daño.

    - Ej. Un periodista que es despedido de un medio y posteriormente el medio publica contenido sacado de un contexto real que perjudica al periodista en su labor profesional.

- **Medidas de prevención:**
    - Contar con un grupo de apoyo para prevenir y atender situaciones de amenaza. Ej. Contar con un grupo de contra discurso en línea.
    - Establecer y configurar alertas de contenido nuevo en Internet sobre tu persona, e.g alertas sobre contenido de Google

Suplantación y robo de identidad

- **Descripción:** La suplantación de identidad consiste en que alguien se hace pasar por una persona o entidad de manera maliciosa. Esto se puede lograr mediante la creación de perfiles falsos o contenidos en las redes sociales en nombre de alguien más sin necesidad de acceder a cuentas personales u oficiales.

  El robo de identidad consiste cuando la suplantación escala y la identidad falsa comienza a identificarse como real o verídica, esto mediante el robo de accesos (usuarios o contraseñas) de una cuenta en línea o documentos personales.

  El robo y la suplantación de identidad suelen incluir:
    - El acceso a información personal: nombre y apellidos, número de seguridad social, tarjeta de crédito, dirección física, correos electrónicos, teléfono, fotos, videos y/o contactos.
    - La creación de cuentas, perfiles o contenidos falsos en redes sociales usando datos reales o falsos.

    - Ej: “Alguien se está haciendo pasar por mí en Facebook”

- **Medidas de prevención para suplantación de identidad:**
    - Revisar las configuraciones de seguridad y privacidad de servicios y cuentas en línea, y verificar qué información es pública.
    - Identificar los documentos que contienen información personal, manteniéndolos en lugares seguros.
    - Documentar la actividad de las cuentas falsas y reportar a la plataforma que corresponda.
    - Conocer las herramientas de reporte y atención de incidentes dentro de las plataformas o servicios en línea.

- **Medidas de prevención para robo de identidad:**
    - Para evitar caer en engaños digitales que permitan el robo o suplantación de identidad, sigue las acciones recomendadas en Phishing y en Accesos no autorizados a cuentas en línea.
    - Activar notificaciones en servicios y cuentas en línea para identificar actividad sospechosa.

- En caso de notificación de intentos de acceso a cuentas cambiar las contraseñas de estas.
- Revisar inicios de sesión en plataformas, así como las carpetas de correo enviado, basura y spam para identificar actividad sospechosa.
- Conocer las herramientas de reporte y atención de incidentes dentro de las plataformas o servicios en línea.

Vigilancia

- **Descripción:** Acecho e intromisiones reiteradas y obsesivas a una persona o grupo con el fin de dar seguimiento a sus actividades, obtener información privada o sensible y/o enviar información a alguien más.

  Las prácticas de vigilancia pueden ser seguimiento de actividades en espacios físicos y digitales mediante el uso de fuentes de información públicas en Internet como lo son redes sociales, foros, blogs.
  - Ej. “Recibí mensajes de números raros preguntando información personal. También recibo solicitudes de amistad de perfiles desconocidos”

- **Medidas de prevención:**
  - Para prevenir la búsqueda de información y seguimiento de actividades en línea, sigue las acciones recomendadas en Doxing y en Phishing.

Bloqueo o control de la distribución o publicación de información en plataformas, servicios o espacios digitales

- **Descripción:** Consiste en bloquear la generación, circulación o publicación de contenido por parte de proveedores de internet (ISP), plataformas digitales u organismos con poder en la distribución o publicación de información.
  - Ej. Una persona administradora de un espacio digital (como un sitio web) bloquea el acceso de publicación a una persona usuaria de manera arbitraria.
  - Ej. Que un ISP limite el acceso o conexión a servicios en específico brindando preferencia a estos servicios.
  - Ej. Que un ISP favorezca a una fuente de información en específico desfavoreciendo al resto de fuentes.
- **Medidas de prevención:**
  - Utiliza herramientas que aseguren tu privacidad mientras navegas, puedes utilizar el navegador Tor, una VPN o DNS alternativos.
  - Elige canales de comunicación que cuenten con cifrado de extremo a extremo. El cifrado de punta a punta protege tu información mientras viajas en Internet.

Remoción de contenidos publicados en plataformas, servicios o espacios digitales

- **Descripción:** Consiste en remover o borrar contenido para evitar su disponibilidad, ya sea mediante reportes dirigidos a un contenido en específico desde plataformas, medios digitales, o a través de instrumentalizar vía legal una solicitud para remover contenido.
    - Ej. Una persona administradora de un espacio digital (como un sitio web) bloquea o elimina el contenido de una persona usuaria de manera arbitraria.
- **Medidas de prevención:**
    - Cuenta con un registro o documentación de publicaciones y contenidos en línea, esto podría incluir capturas de pantalla o copias de los contenidos.
    - Identifica redes de apoyo que puedan monitorear la remoción de contenidos y respuesta en caso de remoción y otras formas de censura.
- **Medidas de prevención:**
    - Busca la opción de apelar a través de la plataforma.
    - Registra evidencia como pantallazos y respuesta de las plataformas.

SOCIALTIC

Recursos complementarios

Recursos sobre plataformas de redes sociales

Facebook

- Centro de Seguridad
- Normas comunitarias
- Herramientas: bloquear, dejar de seguir u ocultar personas y publicaciones; reportar.
    - *Dejar de seguir*: no verás sus publicaciones en tu News Feed, pero seguirás siendo amigo de ellos.
    - *Bloquear*: impide que la persona pueda agregarte como amigo y ver lo que compartes en tu biografía.*
    - *Eliminar a la persona de tus amigos*: solo tus amigos de Facebook pueden ponerse en contacto contigo mediante el chat de Facebook o publicar en tu biografía. *

      *Al tomar estas acciones, no se tendrá acceso a contenido futuro o contenido previo publicado por esa persona.
    - Reportar una cuenta o los contenidos abusivos que publique
- Recuperar una cuenta vulnerada
- Formulario de robo y suplantación de identidad
- Reportar imágenes íntimas sin consentimiento
- Centro de prevención de bullying para adolescentes, padres y educadores

Twitter

- Centro de ayuda sobre reglas comunitarias
- Formulario de apelación y formularios directos para reportar violaciones a las Reglas de Twitter
- Herramientas: silenciar, bloquear y reportar
    - *Silenciar*: Esta función oculta los tuits o notificaciones de otra persona sin que lo sepa.
    - *Bloquear*: Al bloquear una cuenta en Twitter, impides interacciones. El bloqueo puede resultar útil para controlar las interacciones no deseadas (no te contacten, no vean tus tuits y no te sigan)
    - *Listas de cuentas bloqueadas*: es posible importar listas de cuentas bloqueadas elaboradas por otra persona, exportar tu propia lista de cuentas bloqueadas para compartir con otra persona y manejar diversas listas de cuentas bloqueadas de manera independiente. Esto puede ser útil para aquellas personas que están recibiendo ataques vía interacción directa de un grupo de personas.
    - *Reportar*: Al reportar, el contexto que se proporcione es muy importante. Apoya el reporte con contexto, evidencia (por ejemplo captura de pantalla) y

otros incidentes relacionados. Es posible reportar una cuenta, una lista por contenido abusivo o perjudicial, un tweet o múltiples, y mensajes directos para solicitar que el contenido sea eliminado.
Cualquier persona, puede reportar una violación de los términos de uso o de las reglas de Twitter. Sin embargo, en la medida de lo posible es importante que la persona víctima de la agresión realice el reporte para recibir directamente la respuesta y recomendaciones.

- Alfabetismo y Seguridad Digital: Mejores Prácticas en el uso de Twitter
- Formulario de reporte relacionado a explotación sexual infantil
- Formulario de reporte relacionado a robo o suplantación de identidad
- Formulario de reporte relacionado a comportamiento abusivo y amenazas violentas
- Otros medios de contacto: gob@twitter.com y la cuenta de @TwitterSeguro

Instagram

- Centro de ayuda sobre normas de comunidad
- Reportar una cuenta de suplantación en Instagram
- Reportar contenido abusivo como fotos o videos o spam Utiliza este formulario si tú o a quien apoyes no tienen una cuenta en Instagram
- Reportar casos de acoso u hostigamiento a través de fotos, videos, comentarios o perfiles. Utiliza este formulario si tú o a quien apoyes no tienen una cuenta en Instagram
- Puedes reportar los correos electrónicos sospechosos en cualquier momento escribiendo a phish@instagram.com.

Chats

- **WhatsApp**. Puedes reportar un grupo de chat o un contacto.
- **Telegram**. Puedes reportar contacto, grupo, canal desde las opciones del celular y stickers o bots enviando un correo a abuse@telegram.org e incluyendo enlace y @username a reportar.
- **Signal**. Puedes bloquear un número de teléfono, contacto o grupo.

Sobre responsabilidad de las plataformas y autoridades

Actores con poder regulatorio deben proporcionar información accesible y útil en contextos de ataques digitales para combatir la violencia.

La omisión o falta de información y respuesta por parte de plataformas digitales y autoridades con poder regulatorio sobre herramientas y procesos para prevenir y actuar ante ataques digitales, contribuyen a normalizar y escalar la violencia, así como a la impunidad.

SOCIALTIC

Recursos generales

- Autodiagnóstico
  - https://protege.la/checklist-de-seguridad-digital-%e2%9c%85/
- Acciones preventivas y reactivas
  - https://protege.la/basicos-seguridad-digital/
  - https://protege.la/proteger-cuentas-en-linea/
  - https://protege.la/ataques-en-linea/
  - https://protege.la/que-hacer-si-te-roban-o-pierdes-el-celular/
  - https://protege.la/5-complementos-plugins-basicos-para-tu-navegador/
  - https://protege.la/guia-de-navegacion-segura-y-anonima/
  - https://protege.la/acciones-para-evadir-la-censura-de-informacion-en-internet/
  - https://protege.la/comunicaciones-seguras-en-zoom/
  - https://protege.la/guia-sexting-seguro/
- Configuraciones de privacidad y reportes
  - https://protege.la/seguridad-y-privacidad-en-apps-de-mensajeria/
  - https://protege.la/como-configurar-mi-privacidad-y-seguridad-en-facebook/
  - https://protege.la/herramientas-de-reporte-en-facebook/
  - https://protege.la/como-configurar-privacidad-seguridad-twitter/
  - https://protege.la/herramientas-de-reporte-en-twitter/
  - https://protege.la/como-configurar-privacidad-seguridad-instagram/
  - https://protege.la/herramientas-de-reporte-en-instagram/
  - https://protege.la/herramientas-de-reporte-en-chats/
- Para aprender sobre el temas específicos
  - https://protege.la/que-es-malware-que-tipos-hay-y-como-protegerte/
  - https://protege.la/intervencion-de-dispositivos-y-comunicaciones/
  - https://protege.la/3-tipos-de-phishing-como-identificarlos-y-protegerte/

Fuentes consultadas:

- 13 formas de violencia relacionadas a la tecnología
- Kit de primeros auxilios digitales
- Redes sociales en perspectiva de género
- Infografía sobre acoso en línea (Trollbusters)
- Online abuse 101
- Understanding technology-related violence against women
- Hate speech explained - a toolkit
- Discurso de odio e incitación a la violencia hacia las personas LGBTI
- Ley General de acceso a las mujeres a una vida libre de violencia
- Without my consent
- Seguridad, protección y privacidad de Twitter
- Libres en línea: qué hacer en twitter
- Discurso de odio en LATAM
- Dangerous Speech

- Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial