ASAMBLEA GENERAL

GUÍA PARA LA DELEGACIÓN

Modelo de Naciones Unidas
de la Universidad Nacional de Quilmes

Universidad Nacional de Quilmes

LEVANTA LA MANO

Universidad Nacional de Quilmes Extensión

Ciudadanía digital: participar, expresarse y convivir en el mundo conectado

Hoy en día, lo digital forma parte de prácticamente todo lo que hacemos: estudiamos, jugamos, compramos, opinamos, nos informamos, hablamos con otros, compartimos ideas y participamos en causas que nos importan. Las pantallas no son solo una herramienta para entretenernos: también son espacios donde construimos vínculos, expresamos lo que pensamos y tomamos decisiones. Vivimos en un mundo donde lo digital ya no es algo separado de la vida real, sino una parte importante de ella.

En este escenario, la idea de ciudadanía digital hace referencia al conjunto de derechos, deberes y habilidades que permiten a las personas participar activamente en la sociedad a través de medios digitales. No se trata solo de saber usar tecnologías, sino de hacerlo de manera crítica, ética y responsable. Implica comprender cómo funcionan las plataformas digitales, cómo se produce y circula la información en internet, y qué consecuencias tienen nuestras acciones en el entorno virtual.

La incidencia de lo digital en nuestras vidas nos obliga a repensar derechos como la privacidad, la libertad de expresión o el acceso a la información en contextos donde los datos se recolectan masivamente, los discursos circulan sin control y la desinformación puede tener consecuencias reales. Al mismo tiempo, nos llama a asumir responsabilidades: promover una participación respetuosa, cuestionar prácticas discriminatorias online y defender espacios digitales más justos, seguros y democráticos. La ciudadanía digital es, por lo tanto, un componente esencial de la ciudadanía plena: no es un reemplazo de la participación en el espacio público, sino una extensión de ella en el mundo digital.

Para las y los jóvenes, que crecen y se desarrollan en un mundo atravesado por lo digital, entender y ejercer la ciudadanía digital no es opcional: es parte de su vida cotidiana y de su forma de habitar el mundo. Conocer sus derechos en línea, cuidar su privacidad, expresarse con libertad y responsabilidad, y participar activamente en los debates que circulan en redes son formas de defender la democracia también en los entornos virtuales. Ser parte de esta transformación implica comprometerse con una forma de estar en internet que no solo busca el beneficio personal, sino que también se pregunta cómo construir espacios digitales más inclusivos, respetuosos y solidarios para todos y todas.

1. TIC y Ciudadanía Digital

Las Tecnologías de la Información y la Comunicación (TIC) engloban un conjunto de herramientas, dispositivos, programas, aplicaciones, redes y medios que facilitan la recopilación, procesamiento, almacenamiento y transmisión de información en distintos formatos, como voz, datos, texto, video e imágenes. Gracias a las TIC, las personas pueden comunicarse, acceder a información e interactuar a través de diversos medios, como la radio, la televisión, el teléfono, internet y las redes sociales, de manera rápida y sencilla, sin importar su ubicación.

Su difusión ha transformado profundamente las formas de participación ciudadana, dando lugar a lo que se conoce como ciudadanía digital. Esta implica no solo el acceso a herramientas tecnológicas, sino también el **desarrollo de habilidades críticas** para interactuar en entornos digitales de manera ética, segura y responsable. En este sentido, la ciudadanía digital no se reduce al uso técnico de las TIC, sino que incluye **el ejercicio de derechos y deberes en el espacio virtual**, como la libertad de expresión, el respeto por la diversidad, la protección de datos personales y la lucha contra la desinformación. Así, las TIC se convierten en una vía para ampliar la participación democrática, siempre que se garantice la inclusión digital y se combata la brecha tecnológica.

No obstante, así como las TIC abren nuevas posibilidades para la comunicación y la participación democrática, también pueden ser utilizadas con fines delictivos. El uso indebido de estas tecnologías incluye actividades como el robo de identidad, la difusión de desinformación, el acoso en línea, el fraude digital, y la explotación de niñas, niños y adolescentes a través de internet. A nivel global, preocupa especialmente el crecimiento del *cibercrimen* organizado, que aprovecha las redes digitales para cometer delitos transnacionales, como el tráfico de personas, el lavado de dinero y los ataques a infraestructuras críticas. Frente a estos riesgos, es fundamental fortalecer los marcos normativos, promover la cooperación internacional y fomentar una ciudadanía digital crítica y consciente que contribuya a la prevención de estos usos nocivos.

2. Ciberdelito y Ciberseguridad

Uno de los principales desafíos de la era digital es el **cibercrimen**, que hace referencia a los delitos cometidos en el espacio digital. Al mismo tiempo, la necesidad de defendernos contra estas amenazas ha dado lugar al campo de la **ciberseguridad**, una disciplina dedicada a proteger nuestros sistemas, datos y redes frente a ataques maliciosos.

El **cibercrimen** se refiere a cualquier actividad delictiva que involucra el uso de TIC. Este tipo de crimen puede adoptar diversas formas, como el robo de información personal o financiera, el acceso no autorizado a sistemas informáticos, el fraude en línea, el phishing (suplantación de identidad) o la distribución de malware (programas maliciosos diseñados para dañar dispositivos o robar datos). Los ciberdelincuentes pueden actuar de forma

individual o formar parte de organizaciones criminales que operan a nivel global. En muchos casos, el cibercrimen se lleva a cabo de manera anónima, lo que dificulta la identificación y persecución de los responsables.

El impacto del cibercrimen es amplio, ya que no solo afecta a individuos, sino también a empresas, gobiernos y organizaciones. Las consecuencias pueden incluir pérdidas económicas, daños a la reputación, violación de la privacidad y, en algunos casos, incluso la interrupción de servicios vitales como la atención sanitaria o la infraestructura crítica.

En esta línea, uno de los problemas más graves y preocupantes es el **ciberacoso**. Este fenómeno consiste en el uso de internet y las redes sociales para acosar, intimidar o amenazar a otra persona. Las formas de ciberacoso pueden incluir el envío de mensajes ofensivos o humillantes, la difusión de rumores, la creación de perfiles falsos con el fin de dañar la reputación de alguien, y el envío de imágenes o videos comprometedores sin consentimiento. En algunos casos, el ciberacoso puede escalar hasta convertirse en un acoso constante, provocando efectos devastadores en la víctima, como ansiedad, depresión y, en situaciones extremas, incluso suicidio.

Los **delitos contra la dignidad** en línea también engloban una serie de conductas que afectan directamente el bienestar emocional y psicológico de las personas. Entre estos delitos se incluyen la difamación, la exposición no consensuada de imágenes privadas (como en el caso de la "pornografía de venganza"), y la manipulación de la identidad digital de una persona para perjudicarla o humillarla públicamente. Estos delitos no solo son perjudiciales para la víctima, sino que también pueden generar un clima de inseguridad y miedo en las plataformas digitales, afectando la libertad de expresión y el derecho al respeto en el entorno virtual.

Por otro lado, la **ciberseguridad** se refiere a las prácticas, tecnologías y medidas adoptadas para proteger los sistemas informáticos, redes, dispositivos y datos frente a ciberataques, accesos no autorizados y otros tipos de amenazas digitales. Su objetivo es salvaguardar la integridad, confidencialidad y disponibilidad de la información, así como asegurar que los sistemas operen sin interrupciones causadas por amenazas externas. Para ello, involucra diversas estrategias y herramientas, que incluyen el uso de contraseñas seguras, sistemas de autenticación multifactor, cifrado de datos, firewalls (cortafuegos) y software antivirus. Además, es fundamental la educación y concienciación de los usuarios sobre los riesgos en línea, para evitar caer en prácticas como el phishing o el uso de contraseñas débiles.

Como puede apreciarse, **el cibercrimen plantea serios desafíos para el ejercicio pleno de la ciudadanía digital**. Los delitos en entornos virtuales vulneran derechos humanos y profundizan desigualdades, afectando especialmente a grupos en situación de vulnerabilidad. Frente a ello, las políticas públicas deben promover marcos normativos sólidos, sistemas de justicia especializados, cooperación internacional y estrategias de prevención y alfabetización digital con enfoque de derechos. La construcción de una ciudadanía digital efectiva requiere tanto la protección frente al delito como la creación de condiciones estructurales que garanticen una participación segura, inclusiva y democrática en el entorno digital.

3. ¿Qué es la Asamblea General de la ONU y cómo promueve la ciudadanía digital?

La Asamblea General (AG) de la ONU es el principal órgano deliberativo, normativo y representativo de las Naciones Unidas. Está compuesta por los 193 Estados miembros, y en ella cada uno tiene un voto. Discute temas clave como paz y seguridad, desarrollo sostenible, derechos humanos y cooperación internacional. Si bien sus resoluciones no son legalmente vinculantes, tienen un peso político significativo y orientan la acción global.

AG contribuye a la consolidación de la ciudadanía digital promoviendo marcos multilaterales que regulen el uso de las tecnologías de la información con enfoque en derechos humanos. Impulsa el desarrollo de una convención internacional sobre el uso delictivo de las TIC, fomenta la cooperación internacional contra el cibercrimen y promueve principios de inclusión, acceso equitativo, privacidad y seguridad digital para fortalecer una ciudadanía digital democrática.

Las Naciones Unidas han desarrollado diversas iniciativas y resoluciones que abordan aspectos clave relacionados con la participación y los derechos en el entorno digital. Una de las principales es el Pacto Digital Global (Global Digital Compact), propuesto en el informe "Nuestra Agenda Común" del Secretario General de la ONU. Este pacto busca establecer principios compartidos para un futuro digital abierto, libre y seguro, promoviendo la conectividad universal, el respeto a los derechos humanos en línea y la regulación ética de tecnologías emergentes como la inteligencia artificial.

Así, en diciembre de 2018, la AG aprobó la resolución A/RES/73/27 que refiere a los “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”. El documento establece principios sobre la seguridad de la información en el ciberespacio y el respeto a los derechos humanos en entornos digitales. En este sentido, indica que los Estados deben abstenerse de apoyar actividades que involucren el uso delictivo de TIC, deben adoptar medidas para mejorar la seguridad en el espacio digital y alentar la divulgación responsable de información sobre las vulnerabilidades relacionadas con las TIC.

Los delegados y delegadas pueden acceder al texto de la Resolución a través del siguiente enlace: https://docs.un.org/es/A/RES/73/27

Unos años más tarde, en diciembre de 2024, la AG adoptó una convención histórica contra la ciberdelincuencia: la Convención de las Naciones Unidas contra la Ciberdelincuencia. La Convención se apoya sobre cuatro pilares que buscan establecer un marco legal y operativo común que permita a los Estados enfrentar eficazmente los desafíos que plantea la ciberdelincuencia en el entorno digital global:

1. **Definición y Tipificación de Delitos Cibernéticos:** Establece una lista de delitos relacionados con sistemas, redes y datos informáticos, como el acceso ilícito, la interferencia en datos y sistemas, y el abuso sexual infantil en línea. Cooperación Internacional: Facilita la colaboración entre Estados para la recolección y el intercambio de pruebas electrónicas en delitos graves, fortaleciendo la asistencia legal mutua y la extradición.
2. **Protección de Derechos Humanos:** Subraya la importancia de respetar los derechos humanos y las libertades fundamentales en la lucha contra la ciberdelincuencia, asegurando que las medidas adoptadas no vulneren la privacidad ni la libertad de expresión.
   Asistencia Técnica y Desarrollo de Capacidades: Promueve el apoyo a los países en desarrollo mediante asistencia técnica y capacitación para fortalecer sus capacidades en la prevención y combate de la ciberdelincuencia.

Sugerimos a los delegados y delegadas la lectura de esta Convención, a la que pueden acceder a través del siguiente link:
https://documents.un.org/doc/undoc/gen/n24/372/07/pdf/n2437207.pdf

Para seguir pensando y debatir en el MONUUNQ

Les proponemos a los delegados y delegadas que abran el diálogo desde diferentes ejes: normativo, derechos humanos y cooperación internacional. En esta dirección, formulamos algunas preguntas guías que podrían orientar la participación de las delegaciones:

Eje 1: Marco normativo y regulaciones

- ➔ ¿Qué legislación nacional e internacional tiene cada Estado en relación con la prevención del cibercrimen?
- ➔ ¿Cómo se puede garantizar que las regulaciones no vulneren derechos como la libertad de expresión o la privacidad?

Eje 2: Ciudadanía digital y derechos humanos

- ★ ¿Qué medidas están tomando los Estados para garantizar una ciudadanía digital inclusiva y segura?

- ★ ¿Cómo se puede proteger a los grupos en situación de vulnerabilidad frente a la violencia digital, el ciberacoso y los delitos contra la integridad en entornos digitales?
- ★ ¿Qué estrategias se pueden implementar para fomentar un uso responsable de las TIC entre la ciudadanía?

Eje 3: Cooperación internacional y desarrollo

- ➢ ¿Qué formas de cooperación internacional son necesarias para enfrentar eficazmente el cibercrimen?
- ➢ ¿Cómo pueden los países desarrollados apoyar a los países en desarrollo en materia de infraestructura, formación y transferencia tecnológica?
- ➢ ¿Qué rol deben tener las Naciones Unidas, en particular la Asamblea General, en este proceso?

Propuesta didáctica antes del MONUUNQ: un juego de rol para el aula

Resolver el caso: “Estafa digital por duplicación de SIM”

Simular una audiencia de investigación y resolución de un caso real de ciberdelito, donde los estudiantes representen a distintos actores sociales involucrados, y debatan sobre responsabilidades, soluciones y derechos digitales.

Caso real: Estafa “SIM swapping” y robo de cuentas bancarias en Argentina

Resumen del caso:
En 2020 y 2021, se registraron múltiples casos en Argentina donde personas fueron víctimas de una técnica conocida como **“SIM swapping”** o duplicación de tarjeta SIM. Este método consiste en que los ciberdelincuentes se hacen pasar por la víctima para solicitar un duplicado de su número de celular a la compañía telefónica. Una vez que obtienen acceso a la línea, pueden recibir los códigos de verificación (por ejemplo, los de *token* bancario) y tomar el control de cuentas bancarias o aplicaciones.

Por ejemplo, una de las víctimas relató que dejó de tener señal en su celular por unas horas. Al recuperar el servicio, descubrió que le habían vaciado la cuenta bancaria y tomado créditos a su nombre por varios miles de pesos. Los delincuentes habían accedido a su home banking, cambiaron contraseñas y realizaron transferencias. Aunque denunció el caso, la devolución del dinero fue parcial y el proceso judicial lento.

 Roles sugeridos:

(Se puede dividir el curso en grupos y asignar un rol por grupo)

1. **Las víctimas**
    - Cuentan lo sucedido y cómo le afectó.
    - Reclaman reparación y acceso a la justicia.
    - Exigen mejores políticas de seguridad.
2. **Representante del banco**
    - Defiende el accionar de la entidad.
    - Explica sus protocolos de seguridad.
    - Se enfrenta al dilema: ¿es su responsabilidad?
3. **Representante de la empresa de telefonía**
    - Justifica cómo se otorgó el duplicado de la SIM.

- Detalla las políticas internas de verificación.
  Evalúa qué se podría mejorar.

4. **Abogados/as en derechos digitales**
   - Analizan el caso desde la perspectiva de los derechos de la ciudadanía digital.
   - Reclaman transparencia, seguridad y acceso a justicia digital.
   - Proponen recomendaciones para políticas públicas.

5. **Policía cibernética o fiscalía**

   - Explica los desafíos en la persecución de ciberdelitos.
   - Propone medidas preventivas y legislativas.
   - Informa sobre qué acciones se tomaron tras la denuncia.

6. **Moderador/a del debate o jurado ciudadano**

   - Escucha los argumentos.
   - Realiza preguntas críticas a cada grupo.
   - Emite una propuesta de resolución o plan de acción conjunto.

 Preguntas guía para el debate:

- ★ ¿Quién es responsable del fraude?
- ★ ¿Qué medidas preventivas podrían haberse tomado?
- ★ ¿Qué derechos se vieron vulnerados?
- ★ ¿Cómo debería actuar el Estado ante este tipo de delitos?
- ★ ¿Qué políticas públicas o educativas se podrían implementar?

 Cierre de la actividad:

Cada grupo redacta una **propuesta de medidas de mejora**, que puede incluir:

- Campañas de educación digital.
- Regulaciones para empresas.
- Reformas legales.