Espacio Curricular: Informática aplicada a Procesos

Curso: **5° "A"**

Prof.: Valeria Reche



SECUENCIA DIDÁCTICA MES MARZO

Objetivos:

- Relevar los conocimientos previos de los estudiantes en relación al uso de las nuevas tecnologías.
- Conocer los medios tecnológicos con los que cuentan en su hogar para realizar tareas virtuales.
- Indagar sobre las expectativas y desafíos que tienen los estudiantes en este nuevo ciclo lectivo.
- Reforzar oralmente protocolo de prevención COVID-19.
- Reflexionar sobre los conflictos y riesgos relacionados con el uso de las redes sociales



Para conocernos realizamos un juego de presentación

TRABAJO PRÁCTICO N°1:

<u>Introducción</u>

Se dialogará con los estudiantes sobre los objetivos y contenidos a abordar en la materia a lo largo del año, haciendo énfasis en el perfil técnico del egresado. Resaltando la necesidad de adquirir conocimientos informáticos los cuales les serán de gran utilidad para su futuro laboral o para continuar estudios superiores.

<u>Desarrollo</u>

Actividad N°1

A continuación, te invito a completar el siguiente cuestionario que tiene como finalidad relevar los conocimientos previos y los medios tecnológicos con los que cuentas para realizar las tareas. Para ello haz click en el siguiente botón. En caso de no tener conectividad responderlo en formato papel.

CUESTIONARIO

Actividad N°2:

Para concluir entre todos confeccionaremos un mural en la plataforma Padlet, en donde cada uno escribirá cuales son las expectativas y desafíos para este año 2022. Para ello haz click en el siguiente botón



O escanea el código QR



En caso de no tener conectividad realizarlo en formato papel (en la carpeta)

Cierre:

En el próximo TP abordaremos algunos temas relacionados sobre cómo debemos comportarnos en la red, haciendo un uso seguro y responsable de internet.

TRABAJO PRÁCTICO N°2:

<u>Introducción</u>

En esta oportunidad abordaremos el tema "Ciudadanía digital"

¿Escucharon hablar de ella? Uds, ¿son ciudadanos digitales?

Aquí un primer acercamiento a través de este video:

https://www.youtube.com/watch?v=3QWFvu-qTZw

Desarrollo:

¿Qué es la Ciudadanía Digital?

El término ciudadanía digital, también conocido como e-ciudadanía o ciber ciudadanía, se refiere al uso de las Tecnologías de Información y Comunicaciones (TIC), y de los

principios que las orientan, para la comprensión de los asuntos políticos, culturales y sociales de una nación.

Dicho de otro modo, se trata de la participación ciudadana a través de entornos e interfaces de tipo digital o electrónico, a través de la Internet y las Redes Sociales.

Las TIC comienzan a configurarse como escenarios en donde se desarrollan intereses diversos, relaciones, información, conflictos, construcción de identidades, entre otros, y como tales reclaman un marco regulatorio que permita una convivencia pacífica. Precisamente por eso, porque los entornos digitales son espacios que "se habitan", es que hablamos de Ciudadanía Digital, como un concepto con el cual trabajar el reconocimiento de derechos y obligaciones que todos tienen en las redes. En este contexto se vuelve fundamental formar a los niños y niñas en el ejercicio de una ciudadanía digital responsable. Les proponemos reflexionar con ellos acerca de los derechos y deberes que se mencionan aquí y seguir ampliando este cuadro.

PARA SER CIUDADANOS DIGITALES TENEMOS...

DERECHOS OBLIGACIONES

- Derecho a la privacidad. Elegir qué datos queremos que sean públicos, cuáles compartir de forma privada, sólo con unos pocos, y cuáles son íntimos.
- Derecho a expresarnos libremente. Aprovechar todas las posibilidades que nos da la Red para opinar, comentar, subir información y producciones propias.
- Derecho a navegar seguros. Que nuestros datos de navegación no nos pongan en riesgo.
- Derecho a ser protegidos por los adultos responsables. En caso de sentirse agredidos, acosados, o amenazados siempre recurrir a un adulto de confianza.
- Derecho a ser respetados y a no ser discriminados.

- Respetar al otro. Como en cualquier otro ámbito, nadie debe utilizar la Red para burlarse, molestar o avergonzar a otro.
- No discriminar. Antes de poner "me gusta" o difundir información de otra persona, reflexionar acerca de cómo reaccionaría cada uno de nosotros ante esa situación.
- No agredir.
- Respetar la privacidad de los demás. No publicar ni reenviar imágenes o datos que pertenecen a la intimidad de una persona.
- Denunciar a las personas o instituciones que violan derechos.

¿Qué es ejercer la ciudadanía digital?

Tal como sucede en las comunidades fuera de línea, un integrante de una comunidad o ciudad digital no es per se un ciudadano de esa comunidad digital.

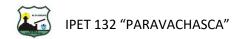
Ser un ciudadano digital implica no solo utilizar las tecnologías, sino también comportarse en relación con ellas; lo cual requiere formarse y desarrollar una serie de competencias y habilidades que nos permitan:

- ✓ El uso provechoso y crítico de las TIC
- ✓ Una participación responsable en las comunidades virtuales.

¿Cómo es un ciudadano digital responsable y saludable?

Es una persona que al momento de relacionarse con las tecnologías:

- Es capaz de usarlas según sus características tecnológicas
- Reconoce y puede controlar sus emociones en el ciberespacio



- Reconoce y respeta la diferencia entre lo íntimo, lo privado y lo público, tanto de sí como de los demás
- Está preparado para hacerse cargo de sus propias decisiones digitales
- Cuida y vela por el respeto a todos los usuarios, inclusive a sí mismo
- Cuida y está comprometido con los derechos de todos los usuarios

Conceptos propios del ejercicio de la ciudadanía digital

- ➡ Identidad digital: se nutre de aquellos contenidos que se suben a la red. Muchos son subidos voluntariamente por nosotros y otros son subidos por terceros sin que nosotros hayamos dado nuestro consentimiento. Nuestra identidad la definen los contenidos existentes en la Web. Tal es la importancia de nuestra identidad digital, que a diario se nos recomienda prudencia para subir contenidos propios y consentimiento para subir contenidos de los demás.
- ♣ Huella digital: son los rastros que vamos dejando por nuestra interacción en las redes, a través de lo que buscamos, elegimos, subimos, compramos, comentamos. Todos estos datos nos pintan como personas: nuestra identidad, preferencias, necesidades y en el mejor de los casos son monetizados por empresas con las que no tenemos ni la menor relación ni conocimiento. En el caso extremo, nuestras huellas digitales son información posible de rastrear por entidades de vigilancia y control. Si bien aún no es posible navegar e interactuar sin dejar rastros, sí podemos gestionar nuestras huellas digitales.
- ♣ Reputación digital: es lo que se dice de una persona o una organización y define su aceptación o rechazo por los demás. En el ciberespacio las palabras no "se las lleva el viento" sino que tienen una permanencia en el tiempo perjudicial para el afectado. Todo puede afectar nuestra reputación digital, un rumor, un meme, un comentario difamatorio o un tuit mal intencionado por parte de alguien. Este tema es complejo porque se barajan dos derechos fundamentales de las personas, el derecho al buen nombre por un lado y el derecho a la libre expresión por el otro.

ACTIVIDAD: Escribe en tu carpeta o en un procesador de textos:



1-¿Qué entendiste por el concepto "Ciudadanía Digital". 2-Sintetiza cuáles son los derechos y deberes tenés ciudadano que como digital. 3- Escribí un ejemplo concreto de cuándo o cómo ejerces como un "ciudadano digital". 4- Para ser un ciudadano digital responsable, ¿Qué se debe tener en cuenta? 5-Según el texto, cada vez que navegamos, publicamos algo o realizamos búsquedas en internet quedan registradas ¿De qué manera?

Cierre:

Reflexionamos sobre el concepto de ciudadanía digital, los deberes y obligaciones de un ciudadano digital

TRABAJO PRÁCTICO N°3:

Introducción:

En esta clase trabajaremos y reflexionaremos sobre los "Riesgos de internet" con el objetivo de adquirir estrategias para reaccionar ante alguna situación de cuidado en el uso de las redes sociales

Desarrollo:

El mundo tecnológico atraviesa cada vez más aspectos de la vida cotidiana. La conectividad establece novedosas formas de vincularnos con el mundo que, hasta hace poco, solo existían dentro de los límites de la ciencia ficción: realizamos videoconferencias con personas en distintos lugares del mundo mientras paseamos un perro, disponemos de la discografía completa de nuestros músicos favoritos con solo presionar un botón que, en realidad, solo existe en una pantalla, etc.

Esta nueva realidad impone nuevas reglas de juego, nos

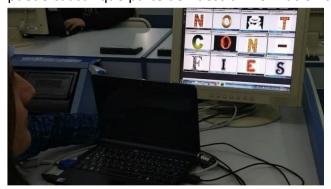
enfrenta a nuevos desafíos y nos expone a ciertos riesgos sobre los cuales debemos ser conscientes.

Debemos conocer cuáles son los protocolos básicos de actuación en Internet. Al igual que conocemos las normas de educación de nuestro día a día y hemos enseñado a los y las niños y niñas a comportarse en diferentes espacios (colegio, casa, en la plaza...), también debemos entender Internet como un espacio más en el que también existen normas de educación. Por supuesto que debemos de alertar de los peligros de no actuar adecuadamente en cualquier espacio, también en la red, pero creemos igual de importante hacerlo inculcando hábitos digitales positivos. Es decir, comprender la responsabilidad en la ciudadanía digital, no ser sólo consumidores sino participantes activos y conocedores de los espacios digitales.

Al usar los sitios, aplicaciones y recursos que nos brinda **internet**, nos exponemos a diferentes situaciones de riesgo. Por un lado, es habitual que publiquemos información que, en caso de caer en manos equivocadas, puede ser usada en nuestra contra. Sobre todo, porque es poco frecuente que tengamos conciencia del alcance de lo que volcamos en la red: quiénes pueden verlo y quiénes no, dónde reside, etc.

Es por este motivo que debemos utilizar métodos seguros para el resguardo y envío de datos en internet. Conocer las herramientas como revisar aplicaciones, limitar lo público y registro de actividad, contraseñas y cifrado (candadito que está al lado del nombre del sitio web al que accedamos), para saber si ese sitio es seguro o no.

En general las redes sociales nos ofrecen la posibilidad de decidir con quién es queremos compartir la información que publicamos en ellas mediante lo que se conoce habitualmente como configuración de privacidad. Sin embargo de forma predeterminada estas configuraciones no tienen los niveles más restrictivos lo cual puede causar que parte de nuestra información sea accesible para más personas de lo



que nos gustaría. Por lo tanto, es recomendable dedicar un tiempo prudencial para ajustarlas y revisar de forma periódica cada una de las aplicaciones que usamos para verificar que sólo sea visible aquello que queramos que sea visible. Se debe ajustar las opciones de sus cuentas de usuario para que no

quede expuesto nada que no quieran que sea público.

No olvidar la importancia que tiene la privacidad en línea. Debemos ser conscientes de que información estamos compartiendo y con quién. Y que lo que publicamos en internet, no desaparece.

Por último, es necesario saber las diferentes modalidades de estafa como abuso informático que operan en internet para estar prevenidos.

El **Phishing (Suplantación de identidad)**, que es el robo de información para ser usada en contra. Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

El **cyberbullying** (ciberacoso en español) es un fenómeno relativamente reciente y estrechamente relacionado con las nuevas tecnologías. Consiste en ofender, insultar o maltratar a alguien a través de internet o de la telefonía móvil. Este tipo de acoso se realiza especialmente entre la población juvenil.

El **sexting** que es la actividad de enviar fotos, videos o mensajes de contenido sexual y erótico personal a través de dispositivos tecnológicos, ya sea utilizando aplicaciones de mensajería instantánea, redes sociales, correo electrónico u otra herramienta de comunicación.

El **grooming** que es una práctica de acoso y abuso sexual en contra de niños y jóvenes que, en la mayoría de los casos, sucede a través de las redes sociales. Afortunadamente, evitar que esto suceda es muy fácil, basta con tomar medidas de prevención y seguridad de navegación en Internet.

La **ciberadicción**, también conocido como trastorno de adicción a Internet (internet addiction disorder, IAD) es un término que se refiere a una supuesta patología que supone un uso abusivo de Internet, a través de diversos dispositivos (ordenadores, teléfonos, tabletas, etc.), que interfiere con la vida diaria.

ACTIVIDAD N°1:

- Lee detenidamente la información anterior, luego analiza cada una de las situaciones e indica a que riesgo hace referencia: Grooming, Sexting, Phishing (Suplantación de identidad), Ciberadicción, , Ciberbullying
 - 1. Pedro ha descargado una imagen del perfil en Facebook de María, y la ha compartido con sus amigos en un grupo de Whatsapp añadiendo comentarios ofensivos. Esto ha provocado que sus amigos sigan ridiculizándola, y que María comience a recibir comentarios de burlas de sus compañeros del centro.
 - 2. «Mi nombre es Carmen y tengo 13 años. Este año, en mi clase, había un chico nuevo, muy guapo y que me gustaba mucho. A muchas de mis amigas también les gustaba, sin embargo, él mostró interés sólo por mí. Además de hablar bastante en clase, cuando llegábamos a casa chateábamos mucho y hablábamos por WhatsApp. Al final empezamos a salir juntos. Un día pensé que le gustaría tener alguna foto mía más íntima, así que me hice una foto en ropa interior y se la envié. Le gustó tanto que me pidió más y se las envié e incluso, le envié alguna en la que estaba desnuda de cintura para arriba. Después de unos meses saliendo juntos, le dejé y parece que a él no le gustó nada. Me ha amenazado con difundir las fotos que tiene mías si no continúo con la relación. No sé qué hacer...»

3



Estimado cliente:

El Banco Canario tratando siempre de estar a la última en la seguridad tecnológica de los datos de nuestros clientes, ha desarrollado un nuevo sistema de seguridad que elimina cualquier posibilidad del acceso de terceras personas a sus datos y cuentas.

Es obligatorio para todos nuestros clientes de Banco Canario usar este nuevo sistema de seguridad, por lo que será necesario que introduzca sus datos de acceso para que el sistema pueda verificarlo. Este proceso le va a costar unos pocos minutos de su tiempo y conseguirá una mayor protección. Si no se verifica en las próximas 48 horas, su cuenta será suspendida temporalmente hasta que su registro sea completado.

Para comenzar el registro por favor haga clic aquí

4.Como cada día, Raquel se dispone a utilizar su cuenta en Twitter, pero al introducir sus datos, la contraseña aparece como inválida y el acceso denegado. Su preocupación es todavía mayor cuando Raquel hace una búsqueda de su nombre en el buscador de la red social y descubre que alguien se está haciendo pasar por ella, publicando comentarios en su nombre. Esta "falsa Raquel" ha accedido al perfil y ha cambiado la contraseña para que su legítima dueña no pueda acceder al perfil.

5.Beatriz tiene 19 años y es **tecnoadicta**. Los primeros síntomas de su adicción aparecieron a los 16: pasaba el día sin compañía, sola con el ordenador y el móvil. Empezó a suspender asignaturas y a descuidar a los amigos y la familia. Sus padres se preocuparon al darse cuenta de que nunca salía y solo hablaba de gente a la que conocía a través de la Red. <u>"A mí no me parecía tan raro</u>, es una forma como otra cualquiera de hacer amigos", cuenta ella. <u>El 21% de los jóvenes</u> está en riesgo de ser adicto a las nuevas tecnologías (El Pais.com)

ACTIVIDAD 2:

De acuerdo a lo que venimos trabajando y a través de este video ustedes podrán apropiarse de las definiciones, que les serán de utilidad para su resguardo.

El peligro de las redes sociales:

https://www.youtube.com/watch?v=Ak3qp4qRAiY&feature=youtu.be

Luego, responde las siguientes preguntas:

- a) ¿Cuáles son los riesgos que podrían originarse de acuerdo al vídeo? ¿realizan algún tipo de acción como las que se ve en el video? Sí/No- En caso de sí, ¿Cuáles?
- b) ¿Alguna de las redes sociales que usas te vincula con otras cuentas que uses?
- c) ¿Cuánta información pueden ver otras personas sobre ti? ¿Todos pueden ver lo mismo?
- d) ¿Tenemos control sobre la información que publicamos en Internet? ¿Por qué?
- e) ¿Puedes bloquear cuentas de desconocidos que intenten contactarte o compartan contenido que te resulta agresivo o desagradable?
- f) Recuerdan alguna situación que hayan escuchado o vivido de acuerdo a las definiciones de cyberbulling, sexting o grooming, ¿Cómo creen que se debería actuar?
- g) ¿Son las TIC una adicción para algunas personas en la actualidad?
- h) ¿Cuándo la exposición pasa a ser perjudicial?

La publicación en las redes sociales

Seguramente formas parte de alguna red social. ¿Sabes quién puede mirar el contenido que compartís en ella y dónde se guarda esa información? Hoy vamos a trabajar sobre estos aspectos de las redes sociales.

1. Elegí dos redes sociales de la tabla y completa los casilleros

Red Social	¿Qué tipo de información se puede compartir?	¿Dónde se guarda la información que se comparte?	¿La información es permanente o transitoria?
Facebook			
Twitter			
Whatsapp			
Instagram			

- **2.** ¿Alguna vez intentaste borrar una foto compartida en alguna red social? ¿Pudiste?
- **3.** ¿Qué pasa con los comentarios asociados a la foto borrada? ¿La foto realmente desaparece de Internet? ¿Qué ocurre si alguien la vio y bajó una copia a su computadora?

Información pública o privada

La información se puede compartir de manera **pública** o **privada.** Al compartir información de manera pública, cualquier persona puede acceder a ella si busca lo suficiente. Un completo desconocido puede ver una foto compartida u otra información sensible. Por el contrario, si se comparte información de manera privada, será accesible solamente para un grupo reducido de miembros de la red social.

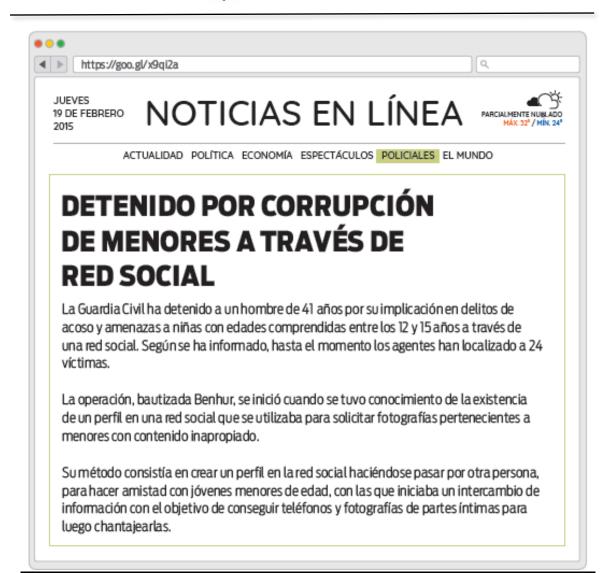
ACTIVIDAD 4:

MENTIRAS Y
PROBLEMAS DE
CIBERSEGURIDAD



Cuando usamos las redes sociales se presentan algunos peligros. ¿Cuáles son? ¿Qué tenemos que hacer en estos casos?

Lee las noticias y responde las preguntas con los compañeros de tu grupo.



JUEVES 11 DE FEBRERO 2016

DIARIO UNO/ENTRE



ACTUALIDAD POLÍTICA ECONOMÍA ESPECTÁCULOS POLICIALES EL MUNDO

PARANÁ: UN ADOLESCENTE FUE ENGAÑADO VÍA FACEBOOK Y TERMINÓ BALEADO

Un adolescente de 14 años salvó su vida de milagro, tras ser baleado por dos personas que intentaban robarle una suma de dinero con la que el menor pensaba comprarles un celular.

Según fuentes policiales, a través de Facebook, el adolescente acordó la compra de un celular. La operación sería concretada en la calle Los Constituyentes. Sin embargo, se trataba de una estafa.

Como suele suceder en estos casos, el engaño comenzó a través de la oferta de un celular de alta gama a un costo muy inferior a su valor real: los delincuentes ofrecían un teléfono de 7000 pesos a 1700.

Con esa suma llegó el menor al lugar pactado, donde lo esperaban los dos delincuentes. Según informó Marcos Antoniow, jefe de la Departamental Paraná de Policía, al advertir que se trataba de un engaño el adolescente quiso escapar corriendo y entonces fue baleado en la pierna y la espalda.

"El chico se asustó e intentó correr, pero fue baleado en la pantorrilla y el omóplato; la segunda bala quedó alojada en la axila", comentó el comisario Marcos Antoniow a Radio La Voz.

Según se supo, la víctima se encuentra fuera de peligro y los delincuentes estarían identificados.

- 1. ¿Qué peligros relacionados con las redes sociales podes identificar en las noticias leídas?
- 2. ¿La misma persona puede tener más de una cuenta en una misma red social?
- 3. ¿Es más fácil mentir en persona o a través de una red social? ¿Por qué?
- **4.** ¿Qué información es mejor no compartir en las redes sociales?

Cierre:

Reflexionamos sobre lo trabajado con el fin de tomar conciencia sobre los distintos riesgos en internet y que medidas de autocuidado adoptar para hacer un uso seguro de la red.

Criterios de evaluación:

- ✓ Presentación de las actividades de forma prolija, ordenada y con letra legible.
- \checkmark Compromiso y responsabilidad en la resolución de la secuencia.
- ✓ Participación y comunicación con la docente para la aclaración de dudas.
- ✓ Comprensión en la interpretación de consignas.
- ✓ Comprensión lectora.