



3er año, Informática III - Departamento de TIC

Redes e Internet / Seguridad informática

Unidades 3 y 4

Prof. Ricardo Salvador

Sobre este apunte

Este documento incluye contenidos de “Redes de computadoras e Internet” (Unidad 3) y “Seguridad informática” (Unidad 4). Si bien son dos unidades separadas, por su estrecha relación esos contenidos se presentan en una sola secuencia de ocho temas, desde temas lo más concreto y cotidiano (el wifi de tu casa) a lo más abstracto y político (quién decide las reglas de Internet), partiendo en cada tema desde un problema real y cotidiano. Puede verse que la “seguridad informática” no es un asunto aparte, sino algo que aparece en cada nivel de la red: en los dispositivos, en las copias de archivos, en la identidad online y en las reglas que rigen todo el sistema. El objetivo de este apunte es que los conceptos técnicos sirvan como **herramientas para comprender y eventualmente resolver algo**, y no como meras definiciones a memorizar y “devolver” en una evaluación.

El apunte está organizado en tres partes: el desarrollo de contenidos propiamente dicho, una guía de situaciones a resolver y las referencias bibliográficas, por si quieren profundizar algún tema.

Nota 1: Este material fue elaborado con asistencia de la herramienta de inteligencia artificial Gemini (Google). La IA fue utilizada para la generación inicial de estructuras, borradores de texto e ideas mediante un proceso iterativo de peticiones (prompting). El texto final fue completamente revisado, corregido, reescrito y validado pedagógicamente por el autor, quien asume la responsabilidad total de sus contenidos.

Nota 2: Si bien este material fue elaborado por el autor con la asistencia de inteligencia artificial, para la resolución de los problemas planteados al final debe prescindirse de la IA, recordemos siempre que estamos buscando leer, comprender y reconocer ciertos temas en nuestra vida cotidiana, y no solo entregar un trabajo al profesor. En otras palabras, entrenar en lugar de mirar por la tele, o bailar en lugar de tirarnos en un sillón con los auriculares.

Contenidos

1 — ¡El router es mío! Redes locales, topologías y protocolos

Situación problemática. Son las nueve de la noche, tu hermano juega en la consola online, tu vieja mira una serie y vos tenés que entregar un trabajo con la videollamada del grupo cortándose cada dos minutos. Alguien grita “¡reinicien el router!” y, milagrosamente, funciona un rato. Lo mismo pasa en cualquier lugar si todos se conectan a la vez al mismo wifi, como en una previa, con veinte celulares intentando bajar la misma canción al mismo tiempo.

Cómo se explica esta situación. Una red doméstica es una **red de área local (LAN)**: un conjunto de dispositivos conectados entre sí por cable o wifi a través de un **router**, que además los conecta hacia afuera (la **WAN**, la red

del proveedor de internet). La forma en que los dispositivos se conectan entre sí es la **topología** de la red (en estrella, si todos cuelgan de un router central; en malla, si los equipos se conectan entre sí formando una red wifi extendida, como los sistemas mesh que reparten señal por toda la casa). Para que los dispositivos “se entiendan” existen **protocolos**: acuerdos técnicos como el que asigna automáticamente una dirección a cada aparato que se conecta (DHCP) o el que ordena y entrega la información en paquetes (TCP/IP, que se retoma en el Tema 5). El ancho de banda es limitado y se reparte entre todos los dispositivos conectados; por eso la red se pone lenta cuando hay muchos usuarios conectados simultáneamente, y por eso un router tiene una **administración con distintos niveles de permiso**: quien tiene la contraseña de administrador puede priorizar tráfico, bloquear dispositivos o poner controles horarios, mientras el resto de los usuarios sólo usa la red (la “jerarquía de usuarios” implica por lo menos *a. uno o varios administradores* y *b. usuarios*).

Es útil saber esto ya que permite diagnosticar por qué una red anda mal en vez de solo “reiniciar y rezar”, decidir dónde ubicar un router o un repetidor en una casa, y entender qué se puede configurar (por ejemplo, priorizar la videollamada de estudio sobre la descarga de un juego) en vez de sufrir pasivamente una red compartida — algo tan aplicable en una casa como en un comercio o un aula.

2 — El celular que anda lento y lleno de publicidad no deseada: virus, spyware y malware

Cosas que suelen pasar... Instalaste una app “gratis” o desde fuera de la tienda oficial (para desbloquear un juego), o le diste clic a un link que mandó un contacto para “ver una foto tuya en una fiesta” (o cosas por el estilo). Desde entonces el celular anda lento, la batería se gasta el doble de rápido y aparecen publicidad pop-up todo el tiempo, incluso con el celular en reposo.

Conocimiento para resolver esto. Llamamos **malware** (de *malicious software*) en general a cualquier programa diseñado para dañar, espiar o tomar control de un dispositivo sin permiso. Dentro de esa categoría hay varias clases: los **virus**, programas que se adjuntan a otros archivos y se replican cuando estos se ejecutan o comparten; el **spyware**, que se instala de forma oculta para espiar la actividad del usuario (qué escribís, qué mirás, tus contraseñas, lo que “ve” tu cámara) y enviar esa información a un tercero (un indeseable “tercero”); el **adware**, que satura el dispositivo de publicidad no deseada; y el **ransomware** secuestra archivos y pide un rescate para liberarlos (hablaremos de esto más adelante). Los **vectores de infección** más comunes son las **descargas** de fuentes no oficiales, los archivos adjuntos o links de origen dudoso, las **memorias USB** desconocidas (¡también las conocidas!) y los **permisos** excesivos que se le dan a una app sin leerlos. Las **defensas básicas** son: mantener el sistema operativo y las apps **actualizadas** (las actualizaciones suelen incluir parches de seguridad que cierran brechas de seguridad ya conocidas por los que crean malware), usar un antivirus, descargar aplicaciones solo de tiendas oficiales y revisar qué permisos pide cada aplicación.

Saber esto permite reconocer las señales tempranas de un dispositivo comprometido (lentitud repentina, batería que se agota rápido, publicidad excesiva, actividad de datos inexplicable) y tomar decisiones de prevención concretas antes de que el problema escale a robo de información o de dinero, que es lo que se aborda en el Tema 6.

3 — Se te cayó el celular en la pileta (o le entró un ransomware a media Argentina): copias de seguridad

Cosas que pasan... Se te rompió el celular justo antes de un viaje y perdiste años de fotos porque nunca las habías respaldado en otro lado. A una escala mucho mayor, en septiembre de 2023 un grupo de ciberdelincuentes atacó con ransomware a IFX Networks, una empresa que alojaba en la nube los sistemas de decenas de compañías de distintos países, entre ellas varias argentinas. Los atacantes cifraron (encriptaron) y **destruyeron también las copias de seguridad** que la empresa guardaba, y muchas compañías clientes se quedaron sin poder operar porque habían confiado todo su respaldo en ese único proveedor, sin tener otra copia, propia.

Conocer es saber, ¡y conservar nuestros archivos! Una **copia de seguridad (backup)** es una copia adicional de nuestra información; permite recuperarla si el original se pierde, se daña o queda secuestrado (¿se acuerdan del ransomware?). Existen distintos **medios de almacenamiento** para guardarlas: un disco local (el mismo equipo, la opción más débil porque si falla el equipo se pierde todo), un disco externo o pendrive, y el **almacenamiento en la nube** (servidores de terceros accesibles por Internet). Una estrategia clásica es la **regla 3-2-1**: tener al menos tres copias de la información, en dos tipos de soporte distintos, con al menos una copia fuera del lugar físico original (por ejemplo, en la nube o en otra ubicación), de modo que un solo incidente —un robo, un incendio, un ataque informático— no pueda destruir todas las copias a la vez. El caso de IFX Networks muestra justamente por qué “tener todo en la nube” no es sinónimo de estar a salvo: si la única copia depende de un solo proveedor externo, ese proveedor se vuelve un punto único de falla.

Ahora que sabemos esto, tenemos un criterio para decidir cómo proteger archivos propios (fotos, trabajos, proyectos) con una estrategia simple y razonable, y entender por qué las organizaciones importantes no dependen de un solo lugar para guardar su información: la copia de seguridad es, junto con la prevención de malware, la otra mitad de estar preparado ante un incidente.

4 — Wifi para unos, datos carísimos para otros: la desigualdad de acceso en nuestra ciudad

Considerá este caso: un compañero de curso nunca prende la cámara en las clases virtuales y entrega los trabajos tarde. No es desinterés: en su casa no hay wifi fijo, solo un plan de datos móviles limitado que su familia recarga cuando puede, y termina yendo a un Punto Digital municipal o a la casa de un vecino para conectarse.

Parece simple, pero hay algo que saber, que nos da un mejor punto de vista: no alcanza con distinguir quién “tiene” o “no tiene” internet: se habla de **brecha digital de acceso** (si hay o no conexión disponible), **brecha de uso** (con qué frecuencia y calidad se puede usar) y **brecha de apropiación** (si se sabe usar críticamente y eficientemente la herramienta, más allá de lo básico). Un estudio reciente sobre el tema remarca que hoy la brecha no es solo “tener o no tener” sino también la **velocidad y el costo** de la conexión, que sigue penalizando a los sectores de menores ingresos. En Argentina esta desigualdad afecta especialmente a la infancia y adolescencia: estudios sobre el Conurbano Bonaerense mostraron que, entre menores de estratos muy bajos, gran parte no accedía a computadora ni a internet en el hogar. Frente a esto existen políticas públicas concretas: la Ley Argentina Digital (27.078) declara la conectividad de “interés público” y busca garantizar el acceso en condiciones equitativas; y, en Rosario particularmente, la Municipalidad creó desde 2013 los **Puntos Digitales**, espacios gratuitos de acceso a TIC para adolescentes de 13 a 18 años, y desde 1995 funciona **Nodo Tau**, una de las primeras organizaciones del país en montar un servidor comunitario de Internet, hoy dedicada

también a inclusión digital y reciclado de residuos electrónicos.

Esto nos ayuda a entender que el rendimiento escolar o la participación social de alguien no dependen solo de su esfuerzo individual, sino también de la infraestructura a la que tiene acceso; ayuda a identificar y valorar los recursos comunitarios gratuitos que existen en la propia ciudad (Puntos Digitales, bibliotecas populares, Nodo Tau); y nos da herramientas para pensar críticamente sobre las políticas públicas de conectividad, y reclamarlas como el derecho que son, y no sólo consumirlas.

5 — De donde estoy sentado (o parado, ¡o viajando!) a cualquier parte del mundo en milisegundos: qué es y cómo funciona Internet

Cosas que nos pasan: mandás un audio por WhatsApp y en segundos lo escucha un familiar en España. Nadie lo pensó raro hasta que un día, por una falla en un cable en el fondo del mar, medio continente se quedó sin poder navegar bien durante horas. ¿Cómo es posible que algo tan instantáneo dependa de un cable físico que se puede cortar?

Los porqués son importantes. Es que Internet no es “la nube” flotando en el aire: Internet es una **red de redes**, un conjunto descentralizado de miles de redes de computadoras (universidades, empresas, proveedores) que se ponen de acuerdo en usar los mismos protocolos para intercambiar información, principalmente **TCP/IP**, desarrollado a fines de los años 60 y 70 en el marco de ARPANET (la red militar y académica estadounidense que es el antecedente directo de Internet) y estandarizado por Vinton Cerf y Robert Kahn. La información viaja dividida en **paquetes**, que pueden tomar distintos caminos físicos y se reordenan al llegar a destino: por eso Internet no tiene “un centro” que, si se cae, tira abajo toda la red (a diferencia de una red con topología en estrella pura). Esos caminos físicos son reales: cables de fibra óptica submarinos que cruzan océanos, centros de datos, y **proveedores de servicios de Internet (ISP)** que te conectan a esa red mundial. Para que las direcciones numéricas de cada servidor (direcciones IP) sean recordables por humanos existe el **DNS**, que traduce nombres como “instagram.com” a esas direcciones.

Sabiendo esto nos desilusionamos un poco: Internet no es inmaterial ni mágica: es infraestructura física, vulnerable a cortes, desastres naturales o decisiones geopolíticas, y entenderlo ayuda a explicar por qué a veces “se cae Internet” en una región entera. Además, entender su arquitectura descentralizada es la base necesaria para comprender quién puede (y quién no puede) controlar Internet, cosa que veremos al final de este apunte.

6 — Un desconocido te escribe por Instagram y algo no cierra, o no te gusta: tu huella digital, tu privacidad y delitos informáticos

Empecemos con algo feo: un perfil que no conocés empieza a chatear con vos (o con un hermano o hermana menor), se muestra súper amigable, farmea aura, como quien dice, pregunta cosas cada vez más personales y en algún momento pide una foto “de confianza”. En una situación de otro tenor, en febrero de 2024 el área de Seguridad Informática de la Municipalidad de Rosario detectó y desactivó una página web falsa que copiaba exactamente el sitio oficial del municipio para robar datos de tarjetas de crédito a quienes creían estar pagando una multa real. Sin embargo lo feo y lo de otro tenor, tienen puntos en común.

Dicen que querer es poder (no estoy tan seguro), pero seguro que saber sí te hace poderosa/o: tenés que tener claro, muy claro, que todo lo que hacés en Internet (lo que publicás, lo que te gusta, dónde estuviste conectado, qué buscaste) va construyendo tu **huella digital**: un perfil de todo lo que hacés que persiste incluso si después borrás una publicación, porque pudo quedar guardada, compartida o capturada por otros. Cuidar la

privacidad de la información significa decidir activamente qué se comparte, con quién y en qué contexto, no solo “no mostrar la cara”. Cuando alguien usa medios digitales para ganarse la confianza de una persona menor de edad con el objetivo de cometer un delito sexual contra ella, tiene un nombre legal preciso en Argentina: **grooming**, incorporado en 2013 como artículo 131 del Código Penal (Ley 26.904), que prevé pena de prisión para quien contacta a un menor con esos fines. Más en general, la Ley 26.388 (2008) incorporó al Código Penal los llamados **delitos informáticos**: figuras como el acceso ilegítimo a un sistema, el daño informático o el fraude informático, adaptando delitos tradicionales al entorno digital. El caso de la web falsa de la Municipalidad de Rosario es un ejemplo de **phishing**: una técnica de estafa que suplanta la identidad de una entidad confiable para robar datos personales o bancarios; según datos de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), en 2024 se registraron en Argentina más de 34.000 denuncias por delitos informáticos, un 21% más que el año anterior, con el phishing y la usurpación de identidad entre las modalidades más frecuentes.

Ahora estás advertido/a: saber estas cosas te permite reconocer señales de alerta en una conversación online (insistencia, pedidos de secreto, pedidos de material íntimo, urgencia para “resolver algo” con datos personales o bancarios), saber que existen leyes específicas y canales de denuncia ante estas situaciones, y entender que la privacidad es una responsabilidad de cada uno de nosotros, que debemos ocuparnos de gestionar activamente y no como un tema al que reaccionar recién después de un problema.

7 — “¡Yo sólo quería saber el precio de unas zapatillas! y ahora me persiguen los anuncios”: buscadores, algoritmos y la economía de la atención

Nada terrible, buscás una zapatilla en Google por la tarde y a la noche te aparece publicidad de esa misma zapatilla en Instagram, en YouTube y hasta en una app de recetas. Sentís que “te escuchan”, aunque no hayas hablado del tema en voz alta.

Por qué pasa esto: Primero conviene distinguir Internet (la infraestructura del Tema 5) de la **World Wide Web (WWW)**: el sistema de páginas conectadas por hipervínculos y direccionadas por una **URL**, que es apenas uno de los servicios que corren sobre Internet (junto con el correo electrónico, la mensajería, el streaming, etc.). Los **buscadores** no “conocen todo Internet en vivo”: rastrean páginas constantemente, las indexan y luego las ordenan (rankean) según criterios propios cuando alguien busca algo. Las redes sociales usan una lógica parecida con sus **algoritmos de recomendación**: analizan qué mirás, cuánto tiempo te quedás y con qué interactuás (¡eh, la misma huella digital del punto 6!) para decidir qué mostrarte después y mantenerte más tiempo conectado. Esto no es casualidad: es un **modelo de negocio**. Como plantearon el economista Herbert Simon ya en los años 70 y, más recientemente, autores como Tim Wu y Shoshana Zuboff, en un ecosistema saturado de información lo escaso ya no es el contenido sino la **atención humana**, y buena parte de las plataformas “gratuitas” lo son en apariencia: se financian vendiendo esa atención (y los datos que permiten utilizarla) a anunciantes. Esos datos personales no quedan desprotegidos del todo: en Argentina existe la Ley 25.326 de Protección de Datos Personales, que regula qué se puede hacer con la información de una persona y da derecho a acceder, corregir o eliminar esos datos, aunque distintos especialistas señalan que la norma —de 2000— está desactualizada frente a fenómenos como el perfilamiento masivo o la inteligencia artificial, y hay un proyecto de reforma en el Congreso.

**Ahora que sabés esto*, espero que uses las redes sociales y buscadores con un poco más de picardía, es decir una mirada más crítica: entender que el feed no es neutral ni casual, sino diseñado para captar tiempo y atención; reconocer cuándo el propio comportamiento está siendo condicionado por un diseño persuasivo (o saber que casi todo el tiempo tu atención quiere ser “pescada”); y saber qué derechos existen (aunque

limitados) sobre los propios datos personales en Argentina.

8 — ¿Quién decide qué se puede hacer en Internet?: neutralidad de red, gobernanza y derechos digitales

¿A quién no le paso? Una empresa de telefonía ofrece un plan donde usar Instagram y TikTok “no consume datos”, pero mirar cualquier otra página sí. Aparentemente parece un beneficio; otra lectura es que la empresa está decidiendo, de hecho, qué partes de Internet usarás más.

Y todo esto tiene nombre. Este tipo de prácticas (llamadas *zero-rating*) tocan (o tras-tocan) un principio central: la **neutralidad de la red**, la idea de que un proveedor de Internet debe transportar todo el tráfico por igual, sin bloquear, priorizar ni discriminar contenidos, aplicaciones o servicios según le convenga comercialmente. En Argentina este principio está garantizado por ley: la Ley Argentina Digital (27.078) establece en sus artículos 56 y 57 que el Estado debe garantizar el acceso sin limitaciones ni discriminación, y prohíbe expresamente el bloqueo o la discriminación arbitraria de contenidos por parte de los prestadores. Pero que exista una ley no significa que el debate esté cerrado: distintas voces señalan que en la práctica la neutralidad no siempre se cumple del todo, y que la disputa sobre quién controla el tráfico de Internet sigue abierta a nivel mundial. Esto conecta con una pregunta más amplia: **¿quién gobierna Internet?** No hay un “dueño” único ni un gobierno mundial de Internet: existen organismos técnicos internacionales (como los que administran los nombres de dominio) y, en cada país, autoridades regulatorias —en Argentina, el ENACOM— que aplican las leyes locales de telecomunicaciones. Estas decisiones técnicas terminan siendo, en el fondo, decisiones políticas: qué tan libre es la navegación, quién puede vigilar el tráfico, qué datos puede recolectar el Estado o una empresa a través de la red (por ejemplo, cámaras de seguridad conectadas con reconocimiento facial) son debates de **ciudadanía digital** y derechos, no solo de tecnología.

Ahora que sabés esto tenés más criterio para participar como ciudadano informado en debates que definen las reglas del espacio donde los y las adolescentes pasan buena parte de su vida social: entender que esas reglas no son “naturales” sino el resultado de decisiones técnicas y políticas disputables, modificables, y que existe normativa argentina concreta para defender derechos como el acceso equitativo, la no discriminación de contenidos y la protección de datos personales trabajada en los puntos 6 y 7.

Problemas, desafíos y preguntas para resolver con la unidad

¡Importante! Para resolver estos problemas probablemente no servirá recurrir a un párrafo particular, sino que podría necesitarse combinar conceptos de más de un tema, y en varios casos la respuesta es abierta

1. Antes de comenzar...

1. Como siempre, lee todas las consignas: eso te ayudará a contextualizar las respuestas, relacionarlas entre sí y en suma, el trabajo será más fácil de resolver
2. por cada pregunta busca, fotografía o dibuja una imagen que represente la situación planteada: explica por qué la representa.

2. **La red del aula.** En tu escuela hay wifi “gratis” pero solo anda bien en la ciertos lugares. **Proponé un plan para mejorar la red** de la escuela sin comprar equipos nuevos, explicando qué decisiones de topología o administración tomarías, y por qué eso no alcanza para resolver el problema de fondo si un compañero no tiene buena conexión en su casa.

3. **La abuela y el cable submarino.** Tu abuela te dice que antes mandaba cartas y ahora un audio de WhatsApp llega “sin cables, por el aire”. **Redactá una explicación** de por qué en realidad sí hay cables de por medio en gran parte del recorrido, y qué pasaría con la conexión de medio continente si se corta uno de los grandes cables que cruzan el océano.

4. **El juego pirateado.** Un amigo usa el instalador “crackeado” de un juego pago para no comprarlo, y a los pocos días su celular empieza a fallar. **Redactá** usando al menos dos conceptos distintos, qué pudo haber pasado y qué debería revisar antes de asumir que el juego “simplemente no anda bien”.

5. **La foto que creías borrada.** Publicaste una historia a la madrugada, te arrepentiste y la borraste a los diez minutos, pero un compañero la vio y ya la había guardado. **Escribí una explicación**, usando el concepto de huella digital, por qué borrar una publicación no siempre equivale a que “desaparezca”, y qué decisiones previas podrían haber reducido el problema.

6. **“WhatsApp nos vende los datos”.** En un grupo alguien propone migrar todo a otra app “porque es más privada”. **Elaborá un análisis de la situación:** si el problema real que describe esa persona podría tener que ver con cómo se financian estas plataformas y sus políticas de privacidad y qué protección (y qué límites) ofrece hoy la legislación argentina sobre datos personales.

7. **El backup que no existía.** Una pyme guarda toda su facturación en el único disco de la computadora de la oficina. Usando lo aprendido sobre copias de seguridad, **Redactá una explicación** del riesgo concreto está corriendo y proponé una estrategia razonable (no necesariamente cara) para reducirlo.

8. **El mail de ARCA que no era de ARCA.** Te llega un correo a nombre de un organismo oficial pidiendo que actualices tus datos bancarios con urgencia porque “tenés una deuda”. **Explicá** qué tipo de estafa es ésta, qué señales deberían generar sospecha, y qué diferencia hay entre este caso y una amenaza de tipo malware o ransomware.

9. **El plan de la operadora.** Una compañía de celulares ofrece un plan donde Instagram y TikTok “no consumen datos” pero el resto de internet sí gasta. **Contestá:** ¿este tipo de plan respeta la neutralidad de la red que establece la ley argentina? ¿A quién beneficia esa oferta y a quién podría perjudicar a largo plazo (por ejemplo, a una app nueva que compite con Instagram)?.

10. **Concejal por un día.** Si tuvieras que decidir entre instalar más Puntos Digitales en un barrio con poca conectividad o subsidiar planes de datos móviles para adolescentes, ¿qué información necesitarías sobre infraestructura, costos y uso real para tomar una mejor decisión? ****Contestá** fundamentando con al menos dos conceptos de temas distintos.

11. **La señal no llega a tu pieza.** El router de tu casa está en el living y en tu cuarto casi no llega señal para estudiar. **Proponé** dos soluciones técnicas distintas y explicá una ventaja y una desventaja real de cada una (no solo “comprar algo nuevo”).

12. **“Internet es de Google”.** Un amigo asegura que Internet “es de Google, porque ellos tienen todo”. Con lo que leíste en párrafos anteriores sobre la arquitectura y la gobernanza de Internet, **redactá una respuesta** a qué parte de esa afirmación es cierta y qué parte es una confusión entre “una empresa muy grande” y “quién es dueño de la red”.

13. **Contacto sospechoso.** Un perfil desconocido empieza a chatear con un primo o prima de 12 años, es muy amable, le pregunta datos personales y le pide que no le cuente a nadie de esa charla. **Señalá** qué aspecto de la situación debería encender una alarma, más allá de si pide o no una foto, y qué es lo primero que corresponde hacer.

14. **Cámaras con reconocimiento facial.** Un municipio instala cámaras conectadas a internet con reconocimiento facial “por seguridad”. Un vecino dice: “si no hacés nada malo, no tenés nada que esconder”. **Redactá** un contraargumento que combine algo de lo visto sobre datos personales y sobre quién controla (o debería controlar) lo que pasa en una red.

* * *