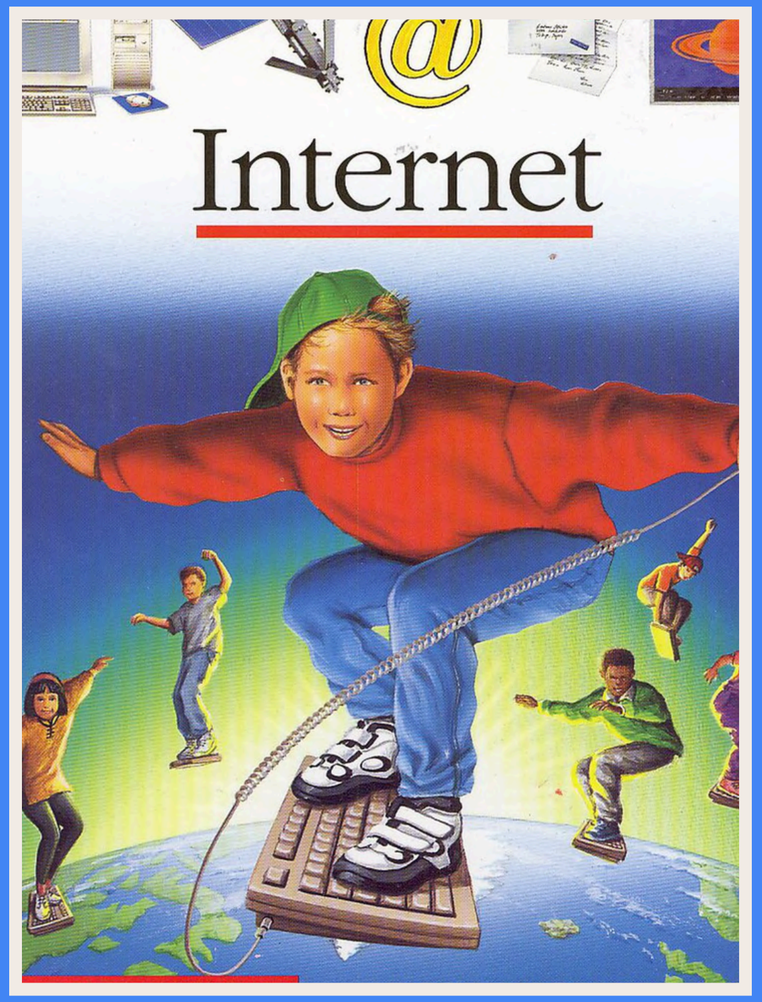
3.6 Conexiones

3.6 Conexiones



INTRODUCCIÓN

Para la conexión entre los equipos de una red, conectar una red local a internet o bien conectar varias redes entre sí, se necesitan unos dispositivos intermedios y unos medios de transmisión, que vimos en sesiones anteriores. En muchos casos, es necesario realizar una serie de pasos o configuraciones para que funcionen correctamente y que posean una cierta seguridad.

REDES CABLEADAS I

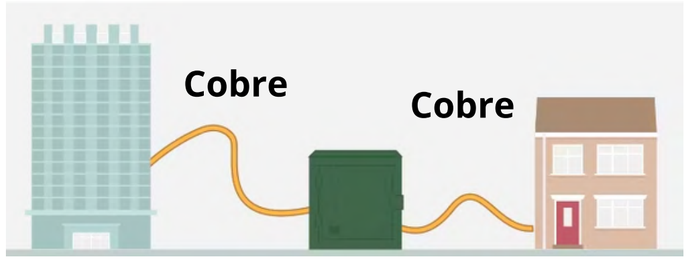
Cómo ya trabajasteis en la tarea1, existen diferentes tipos de cables que podemos utilizar en una red cableada y dentro de los cables de par trenzado podemos diferenciar entre 3 tipos distintos en función del apantallamiento que utilicen y también de la categoría a la que correspondan.

En el caso de los cables de par trenzado se utilizan conectores **RJ45** para conectarlos a los puertos **RJ45** de los distintos dispositivos. En el caso de la fibra óptica se habla de **FTTx(F**iber **T**o **T**he **X)** que significa “fibra hasta el/la x”. Así, podemos hablar de FTTH (Home), FTTB (Building) ó FTTN (Node).

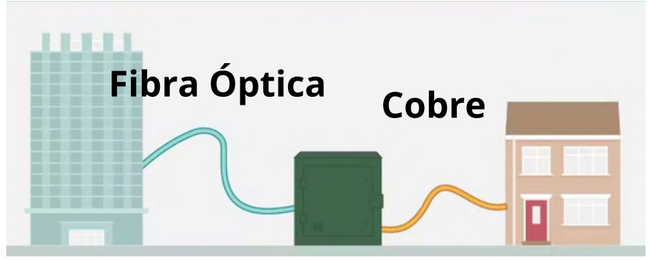
NOTA: Los consejos de FTTH Europeo, Norteamericano y Asia-Pacífico acordaron definiciones unicamente para FTTH y FTTB pero no hay definiciones formales para FTTC y FTTN

REDES CABLEADAS II

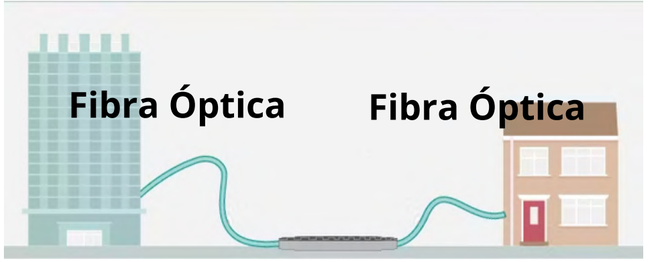
ADSL



FTTC



FTTH



REDES CABLEADAS III

Como ya vimos Ethernet es el estándar de redes de área local, o LAN, para equipos informáticos y está definido en el **IEEE 802.3**. Entre los tipos de Ethernet están los estándares Ethernet, Fast Ethernet y Gigabit Ethernet. El siguiente estándar, Terabit Ethernet, ofrece velocidades mucho mayores que los anteriores.

Cada uno de los tipos de redes Ethernet se caracteriza por la velocidad, la palabra «Base» y una letra que indica el tipo de cable que se va a utilizar y la longitud máxima que se puede alcanzar entre segmentos. Si se necesita cubrir distancias mayores es necesario utilizar un repetidor, que recibe la señal y la amplifica y la regenera.

REDES CABLEADAS IV

Los tipos de cables más utilizados son los citados en la Tabla de debajo. Los valores 100, 1000 y 10G indican la velocidad en bits por segundo a la que viajan las señales por el cable. «Base» es la codificación de la señal y las letras finales son el tipo de cable, donde T y TX son para par trenzado, y FX y LX son para fibra óptica.

Nombre	Tipo de cable	Distancia máxima del segmento	Velocidad máxima
100Base-T	Par trenzado	100 m	100 Mbps
100Base-FX	Fibra óptica	2 km	100 Mbps
1000Base-T	Par trenzado	100 m	1 Gbps
1000Base-LX	Fibra óptica	5 km	1 Gbps
10GBase-T	Par trenzado	100 m	10 Gps
10GBase-LX	Fibra óptica	10 km	10 Gps

REDES INALÁMBRICAS

Las redes inalámbricas proporcionan mucha flexibilidad, facilidad de uso y movilidad a las redes informáticas ya que evitan tener que utilizar cableado, pero a la vez constituyen un alto punto de riesgo.

La conexión se realiza a través de un punto de acceso o un router wifi y se suele utilizar un dispositivo móvil o un portátil para la conexión. El uso de este tipo de redes es muy común en portátiles y dispositivos móviles, pero también en ordenadores de sobremesa y se están imponiendo debido a las ventajas de poder disponer de una red sin tener que cablear. El **inconveniente** principal es, sobre todo, la **seguridad** de la conexión.

REDES INALÁMBRICAS II

Dentro de las redes inalámbricas, podemos diferenciar entre dos tipos de conexión, atendiendo a como se establece la conexión entre los elementos que intervienen:

- **Modo Ad hoc.** En este modo no existen puntos de acceso o routers y los dispositivos cliente se comunican entre sí directamente. Un ejemplo de esto es el uso de Bluetooth o WI-FI Direct.
- **Modo infraestructura.** Es necesario el uso de puntos de acesso o routers para la conexión de los dispositivos. Es la que se utiliza normalmente en empresas y hogares. A través de un punto de acceso o del router, se accede a los distintos recursos de la red como: Dispositivos, servidores, impresoras...

REDES INALÁMBRICAS III

Las redes inalámbricas de área local cumplen los estándares **IEEE 802.11**, de los que hay diversas variantes dependiendo de la frecuencia de la banda en la que se transmite, la velocidad o tasa de transferencia y la seguridad. Hasta el estándar Wifi 4 se denominaba por el nombre del estándar.

Estándar	Banda	Velocidad máxima
IEEE 802.11a	5 GHz	54 Mbps
IEEE 802.11b	2,4 GHz	11 Mbps
IEEE 802.11g	2,4 GHz	54 Mbps
Wifi 4 (IEEE 802.11n)	2,4 GHz y 5 GHz	450 Mbps
Wifi 5 (IEEE 802.11ac)	5 GHz	3,5 Gbps
Wifi 6 (IEEE 802.11ax)	2,4 GHz y 5 GHz	9,6 Gbps
Wifi 6E (IEEE 802.11ax)	2,4 GHz, 5 GHz y 6 GHz	9,6 Gbps

La tasa de transferencia puede ser total, que son los bits de datos y de control trasmitidos por segundo, o efectiva (throughput), que son solo los bits de datos.

Un router de doble banda puede trabajar con las bandas de frecuencia de 2,4 y 5 GHz.

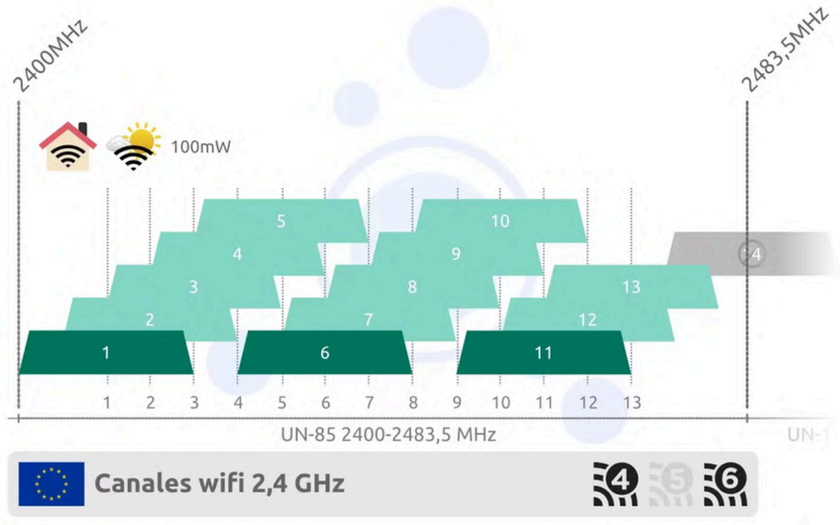
REDES INALÁMBRICAS IV

Dentro de las redes inalámbricas, hay que hablar también de una serie de conceptos:

- **Banda.** Son los rangos de las frecuencias en las que operan. Como vimos en la tabla, las más comunes son las que operan en:
    - **2.4 GHz.** La más antigua y compatible con casi todos los dispositivos. Todos los routers la incorporan. **Muchos IoT solo funcionan en esta banda.**
    - **5 GHz**. Incorporado hace casi una década, a día de hoy está presente en prácticamente la totalidad de dispositivos.
    - **6 GHz.** Utilizado por el estándar Wifi 6E y cuya implantación comenzó en 2021. No todos los dispositivos son compatibles.

REDES INALÁMBRICAS V

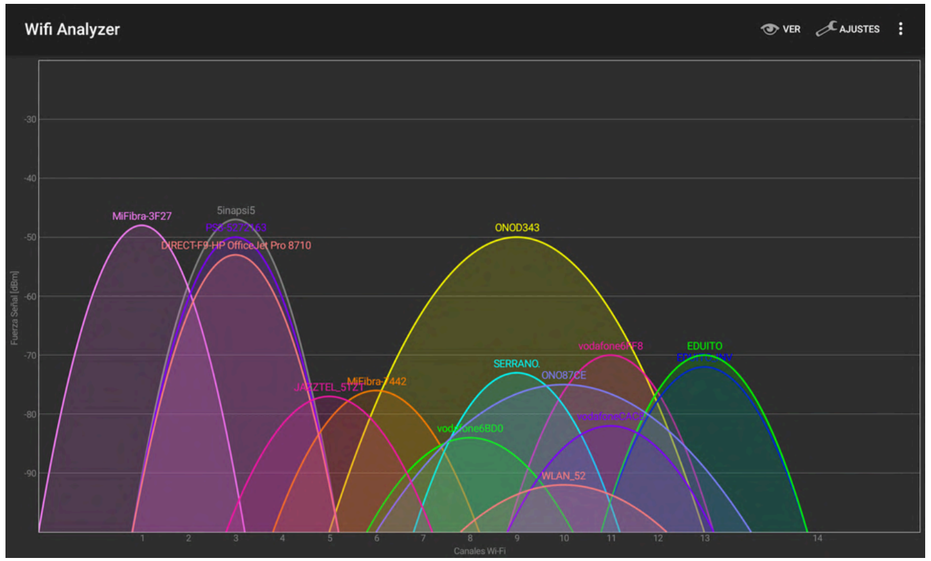
- **Canales.** Es como se dividen las bandas. Cada banda tiene un número determinado de canales. Podríamos compararlo cómo los carriles de una carretera. Cada banda, tiene un número determinado de canales.



OJO: No todos los canales están disponibles, existen una serie de canales que no se pueden usar.

REDES INALÁMBRICAS VI

- **Interferencias.** Ocurre cuando la señal se degrada debido a otras fuentes de señal. Por así decir, es como un bar, cuando habla mucha gente al mismo tiempo, lo que produce dificultades para entender lo que se dice.



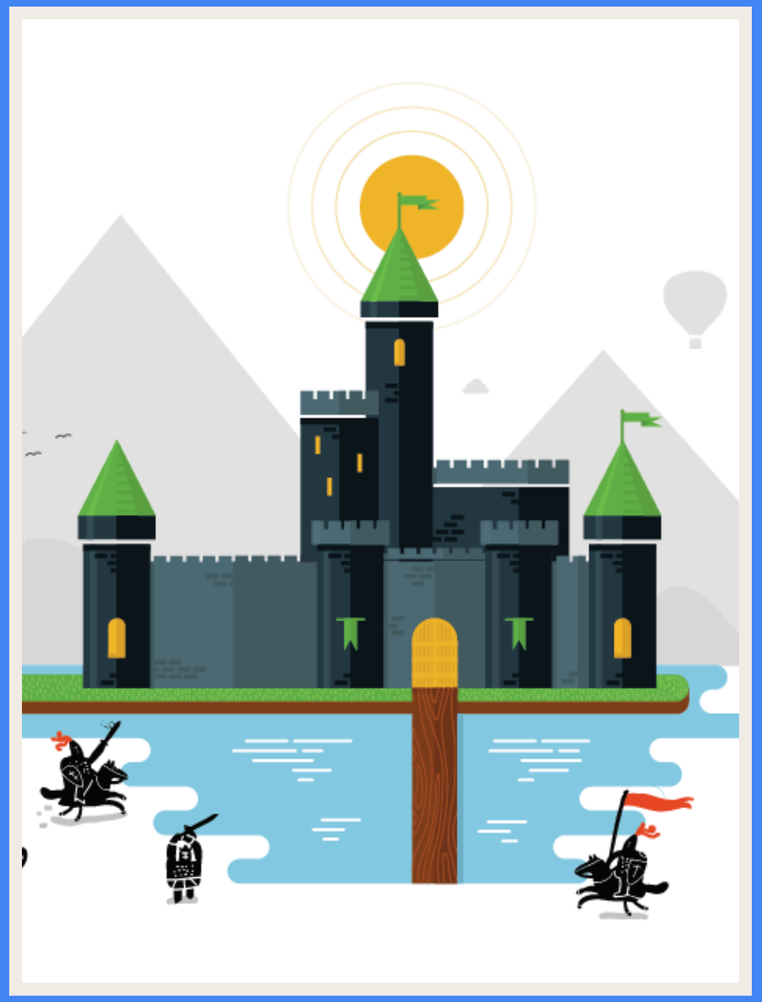
Ejemplo de uso del canal 2.4 GHz

REDES INALÁMBRICAS VII

SSID (Service **S**et **Id**entifier). Es el nombre público que identifica una red local inalámbrica, es decir, una WLAN. Es una secuencia alfanumérica de un máximo de 32 caracteres. Este sistema de identificación de redes distingue entre mayúsculas y minúsculas. También se admiten algunos símbolos especiales, como los puntos o los guiones bajos. El SSID debería ser único en cada red para ayudar a diferenciar entre las diversas redes que se encuentran dentro del alcance del adaptador inalámbrico.

3.7 Seguridad

3.7 Seguridad



INTRODUCCIÓN

La seguridad en redes informáticas se asemeja a los castillos medievales en su estrategia defensiva. Del mismo modo que los castillos empleaban altas murallas, torres de vigilancia y fosos como barreras contra los asaltos, formando un sistema defensivo multicapa, la seguridad informática implementa una variedad de mecanismos de protección para prevenir ataques y brechas indeseadas.

TRÍADA CID

La tríada de **C**onfidencialidad, **I**ntegridad y **D**isponibilidad **(CID** ó CIA en inglés**)** La tríada de la CID es un modelo común que constituye la base para el desarrollo de sistemas de seguridad. Se utilizan para encontrar vulnerabilidades y métodos para crear soluciones.

TRÍADA CID II

- La **confidencialidad** trata de garantizar que la información permanezca protegida y solo se divulgue a las personas que necesitan conocerla. Por ejemplo, las directivas de los usuarios en un sistema operativo delimitan el acceso a datos.

- La **integridad** se basa en la idea de que no se realiza ningún cambio no autorizado en la información, los sistemas ni las redes para proteger la confianza en la precisión de la información y otros sistemas de IT. Por ejemplo, el uso de hash de archivos para comprobar su integridad.

- **Disponibilidad**. La información, los sistemas, las redes y otros recursos permanecen disponibles ante ataques cibernéticos, desastres naturales y otros eventos imprevistos. Por ejemplo, los clústeres.

PRECEDENTES I

El campo de la seguridad está en constante **evolución**, pero muchos ataques actuales no son completamente nuevos, a menudo se alteran o mejoran métodos previos. Comprender ataques pasados ayudará a cómo manejar o prevenir incidentes futuros.

Un **virus** informático es un código dañino que interrumpe las operaciones de la computadora y daña datos y software. Se adhiere a programas o documentos y se propaga a través de la red. Actualmente, estos virus se denominan comúnmente **malware**, software diseñado para dañar dispositivos o redes.

PRECEDENTES II

Brain, lanzado en 1986, es considerado el primer virus para MS-DOS, creado por los hermanos Alvi en Pakistán para combatir la piratería de su software. Infectaba el sector de arranque de los discos floppy y se ocultaba en el sistema. Los hermanos incluyeron sus datos de contacto en el código para que los usuarios infectados pudieran comunicarse para eliminar el virus. No anticiparon que el virus se propagaría globalmente. La primera llamada que recibieron fue de Miami. **Entrevista a hermanos Alvi.**

El Gusano **Morris**, lanzado en 1988, fue uno de los primeros malwares autorreplicables que afectó a ARPANET (precursora de internet), infectando aproximadamente 6.000 de los 60.000 equipos conectados a la red. Fue creado por Robert Tappan Morris, un estudiante de 23 años, como un experimento para medir el tamaño de Internet. Aunque no fue diseñado para causar daño, un error en su programación provocó una propagación masiva que ralentizó y colapsó sistemas. **Reportaje de RTVE de la época.**

PRECEDENTES III

Con la expansión de Internet de alta velocidad, el número de equipos conectados a Internet aumentó drásticamente. Debido a que el malware podía propagarse a través de Internet, ya no era necesario usar ningún disco físico.

El gusano "**ILOVEYOU**", creado por el filipino Onel de Guzmán en 2000, se propagaba a través de un correo electrónico y un archivo adjunto. Al abrir el archivo, el virus infectaba el equipo y se autoenviaba a todos los contactos de Outlook.

Causó estragos a nivel mundial. Infectó aproximadamente al menos a 50 millones de equipos, lo que representaba el 10% de las equipos conectados a Internet en ese momento, y causó daños estimados en más de 5.000 millones de dólares. Incluso llegó a dar problemas al Parlamento Británico y al Pentágono.

PRECEDENTES IV

Tras el caos causado por el gusano “ILOVEYOU”, la ciberseguridad se convirtió en una preocupación aún mayor. Sin embargo, la amenaza no terminó ahí. El ransomware, que podía propagarse a través de Internet, emergió como una nueva forma de ataque cibernético.

El ransomware **“WannaCry”**, que apareció por primera vez en 2017, se propagaba a través de una vulnerabilidad en el protocolo de red SMB de Microsoft. Al explotar esta vulnerabilidad, el ransomware infectaba el equipo, pidiendo un rescate y se propagaba a otros sistemas vulnerables en la misma red.

Causó un caos global. Infectó aproximadamente a más de 230.000 equipos en más de 150 países, lo que representaba una pequeña pero significativa fracción de los equipos conectados a Internet en ese momento, y causó daños estimados en más de 4.000 millones de dólares. Incluso llegó a afectar al Servicio Nacional de Salud del Reino Unido y a empresas multinacionales como Telefónica o FedEx.

ATAQUES COMUNES I

PHISHING

Es el uso de las comunicaciones digitales para engañar a las personas con el fin de que revelen datos sensibles o implementen software malicioso. Podemos distinguir entre varios tipos:

- **BEC**: Se dirige a empresas, donde los atacantes se hacen pasar por ejecutivos o empleados de confianza para engañar a otros empleados y obtener una ventaja financiera.
- **Spear Phishing**: Este ataque es más personalizado y se dirige a un individuo o grupo específico, utilizando información detallada sobre el objetivo para hacer que el correo electrónico parezca más convincente. Si se dirige específicamente a altos ejecutivos podemos hablar de **Whaling**.

ATAQUES COMUNES II

- **Vishing:** Basado en la voz para obtener información sensible o hacerse pasar por una fuente conocida.
- **Smishing :** El uso de mensajes de texto para engañar a los usuarios, con el fin de obtener información sensible o hacerse pasar por una fuente conocida.

SOFTWARE MALICIOSO

Es un software diseñado para dañar dispositivos o redes. Existen muchos tipos de software malicioso. El objetivo principal del software malicioso es obtener dinero o, en algunos casos, una ventaja de inteligencia que pueda utilizarse contra una persona, una organización o un territorio.

ATAQUES COMUNES III

- **Virus**: Un virus es un código malicioso que interfiere con las operaciones del equipo y daña datos y software. Se transmite a través de archivos adjuntos maliciosos o descargas, y se oculta en otros archivos del sistema infectado, donde puede dañar o destruir datos.
- **Gusano:** es un software malicioso que se duplica y se propaga por sí mismo. A diferencia de un virus, no necesita ser descargado por un usuario, sino que se autorreplica y se propaga desde un sistema infectado a otros en la misma red.
- **Ransomware:** Ataque en el que los ciberdelincuentes encriptan los datos de una organización y exigen un rescate para restaurar el acceso.
- **Software espía:** Software malicioso que se utiliza para recopilar y vender Información sin consentimiento

ATAQUES COMUNES IV

INGENIERÍA SOCIAL

Técnica de manipulación que explota el error humano para obtener información privada, accesibilidad u objetos de valor.

- **Uso de RRSS**: Se recopila información detallada sobre un objetivo en las redes sociales.
- **Ataque de "agujero de agua":** Consiste en la creación de un sitio web falso o en la “infección” de uno real con el objetivo de estafar a los usuarios visitantes.
- **USB baiting**: Consiste en dejar estratégicamente una memoria USB con software malicioso para que un empleado la encuentre e instale, con el fin de infectar una red sin saberlo.
- **Ingeniería social física:** Consiste en hacerse pasar por un empleado, cliente o proveedor para obtener acceso no autorizado a un lugar físico.

ATAQUES COMUNES V

PRINCIPIOS DE INGENIERÍA SOCIAL

La ingeniería social es increíblemente eficaz. Esto se debe a que la gente suele ser confiada y está condicionada a respetar la autoridad. El número de ataques de ingeniería social aumenta con cada nueva aplicación de Redes sociales que permite el acceso público a los datos de las personas. Aunque compartir datos personales -como su ubicación o sus fotos- puede resultar cómodo, también supone un riesgo. Principales razones por las que son eficaces:

- **Autoridad:** Se hacen pasar por figuras o instituciones de autoridad.
- **Intimidación**: Incluye persuadir e intimidar a las víctimas para que hagan lo que se les dice.
- **Consenso/Prueba social:** Dado que la gente a veces hace cosas que cree que muchos otros están haciendo, utilizar la confianza de los demás para fingir que son legítimos. Por ejemplo, intentar obtener acceso a datos privados diciéndole a un empleado que otros le han dado acceso en el pasado.

ATAQUES COMUNES VI

- **Escasez:** Táctica utilizada para dar a entender que la oferta de bienes o servicios es limitada.
- **Familiaridad/Confianza:** Falsa conexión emocional con los usuarios que puede ser explotada. Utilizan esta relación para desarrollar la confianza y obtener información personal.
- **Urgencia:** Busca persuadir a los demás para que respondan rápidamente y sin hacer preguntas.