



TIC



▶ TALENTO TECH

REGIÓN 3

CAUCA - NARIÑO

UNIDAD 2





TIC



MÓDULO 1 NIVEL EXPLORADOR

Introducción



Debido a la expansión de la cobertura de servicios de internet y las tecnologías de la información y comunicaciones, nuestras interacciones con nuestro entorno cada vez más dependen de conexión constante a internet. Actividades como pagar un recibo, agendar una cita médica, revisar la cartelera de cine, hablar con un amigo y muchas otras, dependen de un dispositivo, generalmente un celular, conectado a internet.

Cada interacción que tenemos genera información personal que se almacena tanto en los dispositivos que utilizamos para conectarnos a internet como en los servidores a los que accedemos. ¿Has pensado alguna vez cómo se maneja la información recopilada?

Por ese motivo es importante tener en cuenta cómo las entidades a cargo de manejar este tipo de información gestionan los datos.

En este módulo se aprenderán los fundamentos de seguridad en la información y las generalidades de la seguridad digital.

Unidad 2: Datos en internet

Tiempo de ejecución: 20 horas

PLANTEAMIENTO DE LA SESIÓN

Materiales

Se sugiere repartir el contenido de la presente unidad en 5 sesiones de 2 horas cada una o 2 sesiones de 2 y 3 horas cada una. La metodología sugerida para las sesiones es de aula invertida, en la que, se dejan como tarea antes de la sesión lecturas al estudiante. Se inicia la sesión con una práctica y se acompaña al estudiante como un guía para que construya el desarrollo teórico luego de haber realizado la práctica. Esto con el fin de que el conocimiento adquirido sea deductivo a partir de la experiencia de las actividades.

- https://www.youtube.com/watch?v=zV2sfyvfqik&ab_channel=INCIBE

Datos e internet



TIC



Desde la adopción de los computadores en los entornos de trabajo y hogares, internet se convirtió en una herramienta indispensable para cualquier labor o consulta. Con el crecimiento de internet, se hizo necesario ampliar la infraestructura que permitía conectar las redes de datos físicamente. En el año 2011 se descubrió que la tecnología que permitía asignar una dirección única a cada dispositivo en internet era insuficiente para la creciente demanda de equipos conectados.

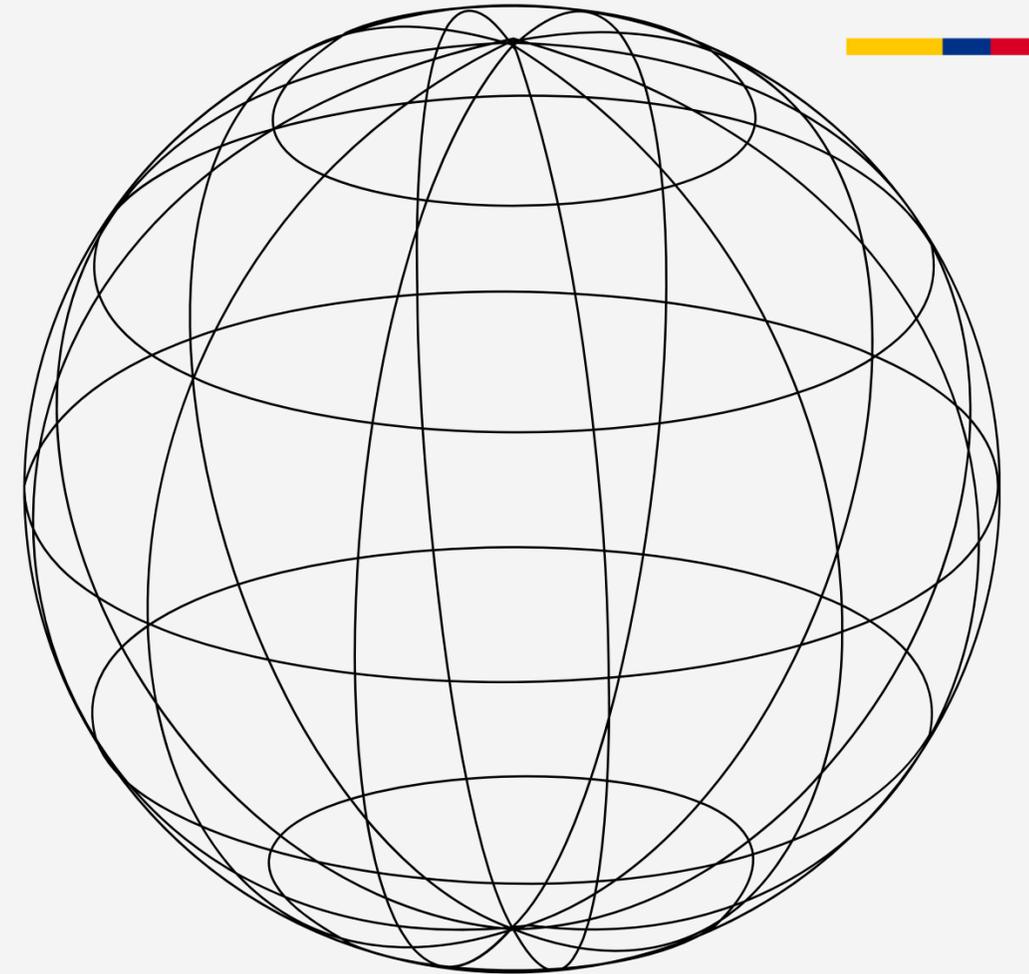
Como solución al problema del direccionamiento se crearon nuevas reglas y protocolos de red que permiten dividir una red global en subredes. Cada subred cuenta con muchos equipos encargados de la comunicación de paquetes de una red a otra y equipos encargados de leer paquetes y enrutarlos adecuadamente. Estos protocolos y reglas siguen vigentes actualmente. Cuando contratamos un servicio ya sea de datos en el hogar o datos móviles, hay muchos equipos encargados de la dirección de la información a su destino.

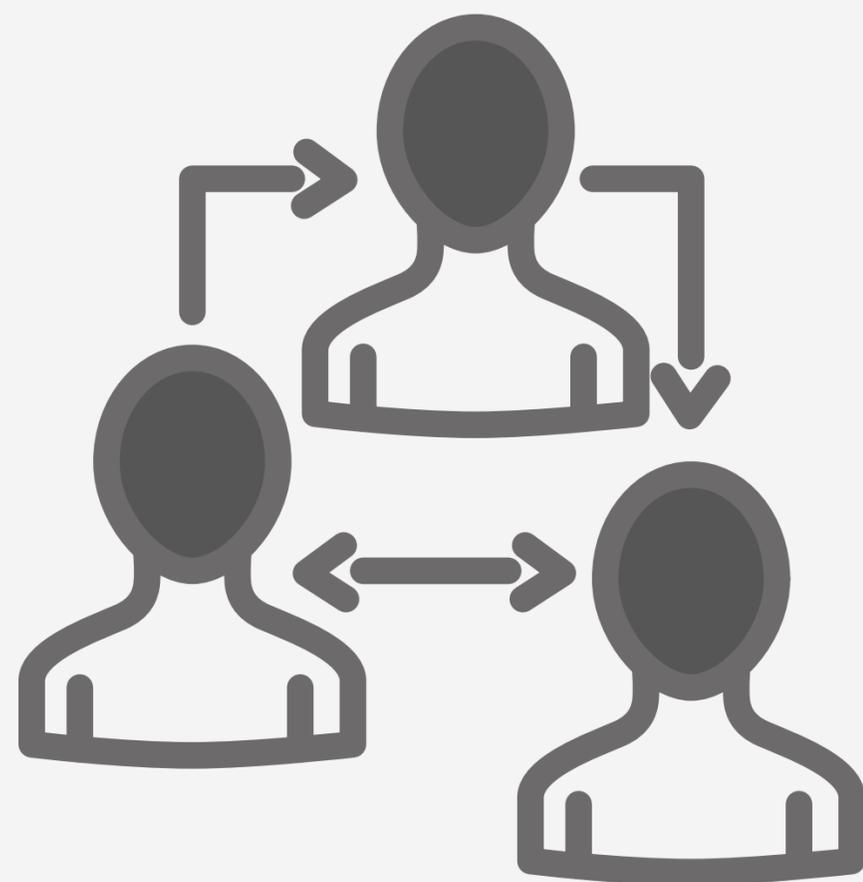
Cada equipo con la capacidad de redireccionar información la puede leer para saber cuál es el equipo de origen y de destino. Por ejemplo, para el envío de un correo, el texto se separa en tramas de datos como pueden ser oraciones en el correo agrupadas y cada trama viaja desde el computador en donde se escribe el correo hasta un enrutador, luego el operador que provee internet por ese enrutador debe tener muchos equipos de intercambio de datos por varias redes.

El protocolo que se usa para el intercambio de datos está diseñado para que los equipos puedan leer todos los paquetes de información que viajan en la red y decidan si esos paquetes les pertenecen o no. Esto quiere decir que, cualquier computador puede leer todos los datos que están circulando en una red. Una persona malintencionada puede crear o utilizar programas existentes que habilitan a un computador para que no solo reciba los paquetes que le pertenecen sino paquetes que van para otros dispositivos, interceptando las comunicaciones.



TIC





Esto quiere decir que toda la información que se envía por internet está expuesta ya que no viaja directamente al equipo de destino, sino que va pasando por una serie de puntos intermedios con capacidad de ver la información. Por lo tanto, basta con tener conocimientos del protocolo de comunicaciones, un equipo de cómputo y programas que permitan reconstruir la información para ver mensajes, correos, imágenes, y muchos datos de otros usuarios sin permiso, violando la privacidad.

Con el desarrollo de sistemas de cómputo modernos con más capacidad de procesamiento, también crecieron las brechas de seguridad en la información. Un computador moderno es capaz de interceptar millones de datos por segundo y agruparlos reconstruyendo información legible.



TIC



Es allí donde nacen las brechas en la información y la necesidad de protegerse. Así como sucedía con los griegos antiguos, hoy en día pasa lo mismo. Como internet es ese mensajero que puede filtrar la información, es necesario codificarla para que otra persona, a pesar de ver los paquetes (equivalentes a las cintas de la escitala) no tengan la capacidad de entender el contenido pese a que lo pueden leer y manipular.

La seguridad en la información en internet consiste en todas las técnicas tanto de criptografía como de comportamientos que evitan que la información se filtre. Tanto desde el lado del desarrollo de programas que manipulan datos, como desde el lado de los usuarios, quienes tienen la responsabilidad de tener buenas prácticas a la hora de manipular información, tanto personal como corporativa.



TIC





TIC



Por citar algunos ejemplos de la gravedad de no tener cuidado en cómo se maneja la información, existen casos que sirven para estudiar las consecuencias de no tener buenas prácticas a la hora del manejo de la información. Por ejemplo, ¿Qué pasa si un hospital falla al proteger los registros médicos e historias clínicas de todos sus pacientes? ¿Qué puede suceder si una tienda en línea, por algún error, filtra información sobre todos sus usuarios con nombres, números de identificación, números de tarjeta de crédito y claves?

En estos casos, no solo la empresa en el ejemplo está en riesgo, sino muchas personas, dañando irreparablemente el buen nombre de todos los implicados.

Las víctimas de una filtración pueden interponer acciones legales, llevando a multas y sanciones por parte de gobiernos de diferentes países.

Si bien, son ejemplos ficticios, existen casos reales de filtraciones que han afectado empresas.