Verificación / transmisión de datos

Breve descripción:

Este componente formativo, aborda generalidades y aspectos clave del proceso de verificación / transmisión de datos, la comprobación del flujo de información sobre la infraestructura inalámbrica y otras acciones conexas. Con su estudio responsable, el aprendiz se afianzará en la gestión de medios inalámbricos, estándares de transmisión, seguridad en la red, medios y métodos de funcionamiento, entre otros.

Octubre 2023

Tabla de contenido

Introducción

Reciba una cordial bienvenida al estudio del componente formativo “Verificación / transmisión de datos”; comience consultando el video que se propone enseguida con el cual usted podrá familiarizarse con el enfoque y temas que aquí se desarrollarán. ¡Adelante!

Video 1. Verificación/ transmisión de información

Enlace de reproducción del video

Síntesis del video: Verificación/ transmisión de información
Verificación y transmisión de información. En la actualidad, las comunicaciones inalámbricas son muy atractivas para la conformación de redes de datos y, en general, para la comunicación. Debido a que se puede prescindir de medios de transmisión alámbricos. Estas nuevas maneras de gestión de información han favorecido la agilidad, exactitud y credibilidad de los datos, ayudando además a una inclusión de más y más personas en la dinámica de la información y la comunicación. Sin embargo, este tipo de comunicación presenta varias desventajas, como, por ejemplo, las interferencias e intercepciones, robos de información, entre otras. De ahí de la importancia de realizar verificaciones periódicamente del flujo de información por medio de la infraestructura inalámbrica. Con ello se favorecerá la identificación, valoración y resolución de potenciales fallos que puedan poner en riesgo la integridad de la información y de la red en sí misma.

1. Medios inalámbricos

Dicho en términos de expertos y pioneros en la materia, los medios inalámbricos se pueden definir como:

"Aquellos espacios libres, por donde se propaga un tipo particular de ondas electromagnéticas: ondas de radiofrecuencia que son portadoras de señales de datos." Durán et al. (2008).

En otras palabras:

- **Canales de transmisión**. Son todos aquellos medios por los cuales se puede transmitir información sin la presencia de cableado.
- **Medios prácticos y accesibles.** Este tipo de medio de comunicación es muy práctico para aquellos puntos donde se hace difícil el tendido de cables por la ubicación geográfica.
- **Medios susceptibles**. Su naturaleza la hace susceptible a interferencias e interceptaciones, lo que puede significar una principal desventaja en su implementación.
- **Medios electromagnéticos.** Este tipo de comunicación se vale del espectro electromagnético, el cual Prieto (2011) define como el rango de frecuencias de todas las ondas electromagnéticas que se pueden propagar a través del espacio libre, ordenadas según su longitud de onda y su frecuencia.

Los rangos de frecuencias más utilizados en las comunicaciones inalámbricas son:

- **Infrarrojos (IR).** Se utilizan en comunicaciones punto a punto de corto alcance, son muy direccionales y no pueden atravesar obstáculos. Este medio se utiliza habitualmente en el mando a distancia de la televisión y, hasta hace unos años, era también un sistema de comunicación que se utilizaba a menudo para conectar dispositivos situados el uno al lado del otro. Es el rango de frecuencia más alto para comunicaciones inalámbricas.
- **Microondas (MW).** Este rango de frecuencias es adecuado para transmisiones de largo recorrido (comunicaciones por satélite, comunicaciones terrestres punto a punto como alternativa al cable coaxial o la fibra óptica y, también, la mayoría de las tecnologías inalámbricas más habituales que existen en la actualidad, como UMTS, "Bluetooth" o WLAN). Las microondas suelen ser direccionales y utilizan una parte del espectro con frecuencias más pequeñas que los infrarrojos.
- **Radiofrecuencias (RF).** Es el rango que utilizan las transmisiones de radio (FM, AM) y televisión digital terrestre (TDT). Las radiofrecuencias son omnidireccionales y pueden atravesar obstáculos sin ningún problema.

1.1. Estándares de transmisión inalámbrica

Los estándares en la comunicación inalámbrica permiten una versatilidad en todos los servicios y productos que ofrece esta tecnología. Esto se traduce en una interoperabilidad, es decir, que puede alternar entre diferentes proveedores de esta tecnología, como:

- El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés) es una organización dedicada a la implementación de estándares de comunicación en el área de las tecnologías de la comunicación y la información.
- Está constituido por una serie de profesionales, ingenieros eléctricos, electrónicos, de sistemas y afines, los cuales aportan sus conocimientos para determinar los mejores canales y mecanismos a la hora de establecer sistemas de comunicaciones.

El conjunto de estándares para redes de área local LAN son definidos por el Instituto de Ingenieros Eléctricos y Electrónicos IEEE. Este organismo define los estándares de obligatorio cumplimiento, en este caso, en el desarrollo de productos de red. Uno de estos estándares es el 802. Existen muchos estándares individuales dentro del paraguas del 802, incluyendo los 802.3 (redes basadas en cable) y los 802.11 (redes inalámbricas).

Estos son, algunos estándares de transmisión inalámbrica más comunes y usados:

- **IEEE802.3**. Estándar para redes basadas en cable: se originó a finales de los años setenta y es mundialmente conocido como el estándar "Ethernet". Inicialmente, definió redes a velocidad de 10Mbps (Megabits por segundo) sobre cable de tipo coaxial o también de par trenzado.
- **IEEE 802.11.** Estándar creado en 1997 que define y gobierna las redes de área local inalámbricas WLAN que operan en el espectro de los 2,4 GHz

(Gigahercios). El estándar original especificaba la operación a 1 y 2 Mbps, usando tres tecnologías diferentes:

  - "Frequency Hopping Spread Spectrum" FHSS.
  - "Direct Sequence Spread Spectrum" DSSS.
  - Infrarrojos IR.

- **IEEE 802.11b.** Definido en 1999. Permite velocidades de 5,5 y 11 Mbps en el espectro de los 2,4GHz. Compatible con el estándar original de 1 y 2 Mbps (sólo con los sistemas DSSS, no con los FHSS o sistemas infrarrojos), incluye una nueva técnica de modulación llamada "Complementary Code Keying" (CCK), que permite el incremento de velocidad. El estándar 802.11b define una única técnica de modulación para las velocidades superiores - CCK - al contrario que el estándar original 802.11, que permitía tres técnicas diferentes (DSSS, FHSS e infrarrojos).
- **IEEE 802.11b+.** Variación del IEEE 802.11b, opera a 22Mbps contra los 11Mbps de la versión 11b; sin embargo, no es un estándar. Aunque aparece en la mayoría de las documentaciones como IEEE 802.11b+, IEEE nunca lo ha certificado como estándar. Fue diseñado por Texas Instruments y adoptado por algunos fabricantes de dispositivos inalámbricos, como D-Link y Global Sun, que utilizan estos "chipsets".
- **IEEE 802.11g**. Ofrece 54Mbps en la banda de 2,4GHz, compatible con los equipos wifi preexistentes. Para dispositivos inalámbricos de tipo wifi 802.11g, proporciona una forma sencilla de migración a alta velocidad, extendiendo el período de vida de los dispositivos de 11Mbps.
- **IEEE 802.15.** Define las redes de área personal WPAN. Estas redes también se conocen como redes inalámbricas de corta distancia y se usan

principalmente en PDAs, periféricos, teléfonos móviles y electrónica de consumo. El objetivo de este grupo de trabajo es publicar estándares WPAN para el mercado doméstico y de consumo que, además, sean compatibles con otras soluciones inalámbricas "Bluetooth" y basadas en cable. Aún no tienen estándares operativos definidos.

- **IEEE 802.16**. Acceso inalámbrico a banda ancha WiMAX. La misión del grupo de trabajo 802.16 es desarrollar sistemas Inalámbricos de Área Metropolitana. Durante el año pasado, WiMAX se ha promocionado como el estándar inalámbrico de banda ancha del futuro.

¿Qué sucede cuando un fabricante o proveedor no desea compartir sus secretos comerciales?

- Puede definir un estándar cerrado.
- En caso contrario, lo puede definir como abierto.
- Definir un estándar como cerrado trae consigo muchos beneficios al fabricante o vendedor, pues no podrá ser objeto de plagios que pongan en riesgo su actividad.
- El estándar cerrado suele aumentar los ingresos económicos del proveedor.

La anterior determinación influye negativamente en el constante proceso de evolución de la tecnología, pues muchos de los conocimientos adquiridos en cierto sistema de comunicación quedan limitados a su fabricante. En contraste, un estándar definido como abierto, está dispuesto para toda la comunidad científica y de ingenieros, los cuales pueden realizar mejoras, aportes al estándar y, así mismo, contribuir al desarrollo de dicha tecnología.

1.2. Seguridad en la red

La seguridad en la red de datos, sea alámbrica o no, es un factor fundamental en el libre desarrollo del desempeño de cualquier organización, pues es por la red por donde circula uno de los activos más importantes con los que cuenta dicha organización.

La seguridad en la red, entonces, consiste en mantener alejados a los diferentes entes maliciosos que desean obtener la información sin previa autorización.

Sobre el concepto de seguridad en la red, es clave tener presente aspectos como:

- **¿Qué es, realmente la seguridad en la red?.** De acuerdo con Soriano (2014), el concepto de seguridad de la información no se limita a eliminar virus, evitar que hackers puedan acceder a la red y suprimir el spam en el correo electrónico.
- **Procedimientos de la seguridad.** La seguridad de la información también abarca los procedimientos que deben seguir los empleados y la dirección de una compañía para garantizar la protección de los datos confidenciales y de los sistemas de información frente a las amenazas actuales.
- **Implicaciones organizacionales.** La seguridad de la información se convierte en una política obligatoria, que toda empresa debe implementar para proteger su activo más preciado.
- **Elementos de garantía de la seguridad.** Son cinco los elementos necesarios para garantizar la seguridad de la información:
    - Confidencialidad
    - Autenticación
    - Integridad

- Disponibilidad
- No repudiación (rendición de cuentas)

Estas son algunas especificaciones que usted debe tener en cuenta, en relación con los cinco elementos de garantía de la seguridad de la información:

- **Confidencialidad**. Hay que asegurar que la información no es divulgada a personas no autorizadas, procesos o dispositivos. (Protección contra divulgación no autorizada).
- **Autenticación.** Medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información (verificación de emisor).
- **Integridad.** La calidad de un sistema de información refleja el correcto funcionamiento y confiabilidad del sistema operativo, la coherencia del hardware y el software que implementan los sistemas de protección y la consistencia de las estructuras de datos de la información almacenada.
- **Disponibilidad.** Acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.
- **No repudiación (rendición de cuentas).** Hay que asegurar que el remitente de información está provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes pueda negar el proceso de dicha información.

Confidencialidad en WLAN.

La confidencialidad en las LAN inalámbricas hace referencia a la integridad de la información que se transmite por ella. Es decir, que ningún ente sin autorización pueda acceder a dicha información. Esta confidencialidad, en otras palabras, debe garantizar que la conexión entre uno o varios puntos de la red no sea susceptible a interceptaciones.

Protocolos de seguridad (WEP, WPA, WPA2).

Dado el auge de las conexiones inalámbricas, se hizo necesario desarrollar una serie de protocolos que garanticen la integridad de la información en dicha tecnología. Algunos de ellos se detallan a continuación:

- **WEP**. El cifrado WEP o "Wired Equivalent Privacy" (desde 1999) tenía como finalidad proteger la privacidad de la información enviada a través de la conexión wifi. Sin embargo, se demostró que este estándar tenía muchas debilidades y permitía a los atacantes leer la información cifrada que se transportaba en la red. Tuvo algunas mejoras, llegando a la versión WEP2, pero no fueron suficientes para tratar todas las debilidades que se presentaban.
- **WPA**. La poca seguridad ofrecida por el estándar WEP dio origen, en 2003, a la incorporación del WPA ("Wifi Protected Access"). Este estándar se caracterizó por incorporar algoritmos de cifrado más robustos para el intercambio de información, que, junto al uso de claves de mayor tamaño, permitió reforzar en gran medida la seguridad de las comunicaciones wifi.

- **WPA2**. Se crea como una actualización de los protocolos WEP y WPA. Incluía todos los requisitos del estándar IEEE 802.11i, ofreciendo un control de acceso más seguro y mayor protección de los datos. En julio de 2004, se publicó el WPA2, basado en el mecanismo "Robust Security Network" (RSN), soportando mecanismos disponibles en su predecesor y las siguientes mejoras:
  a) Prestación de un mayor apoyo tanto a la infraestructura como a las redes "ad-hoc", en términos de cifrado y autenticación. El WPA se limitaba únicamente a las redes de infraestructura.
  b) Provisión de caché de claves oportunista, reduciendo costes de itinerancia entre los puntos de acceso.

Autenticación en redes inalámbricas

Por tratarse de una tecnología que transmite información, es de suma importancia establecer políticas de autenticación para el ingreso a una WLAN. Es decir, se deben instaurar o determinar una serie de requisitos que deben cumplir los interesados en unirse a una red inalámbrica y así adquirir el derecho a transmitir por dicha red.

Tal como sucede con un celular a la hora de conectarse a una red inalámbrica, el proceso de autenticación inicia con una sesión de comunicación entre un nodo (celular) y un punto de acceso. A este proceso se le conoce como "asociación".

Cuando el estándar IEEE 802.11b fue diseñado, se introdujeron dos mecanismos de “asociación”:

- **Autenticación abierta.** Implica que no hay seguridad y cualquiera puede hablarle al punto de acceso.
- **Autenticación con llave compartida.** Se comparte una contraseña entre el punto de acceso y la estación cliente. Un mecanismo de reto/respuesta le permite al punto de acceso verificar que el cliente conoce la llave compartida y, entonces, concede el acceso.

Evitar difundir la SSID

De acuerdo con Salvetti (2011), el término SSID (“Service Set Identifier”) se refiere al nombre asignado a la red inalámbrica y sirve para diferenciarla de otras, pues hoy en día son demasiadas las que se encuentran en un rango determinado. El objetivo principal de este identificador es informar a los potenciales nodos que pueden unirse a una red específica con el objetivo de adquirir los derechos de transmisión de dicha red.

Evitar difundir la SSID puede verse como una medida de seguridad, pero no necesariamente evitará que alguna aplicación maliciosa detecte la conexión o petición de conexión por parte de otro potencial nodo.

Filtrar direcciones MAC

Es una opción en el esfuerzo de mejorar la seguridad en las redes inalámbricas. Díaz (2012) plantea que cada tarjeta de red tiene una dirección única de 6 “bytes”, denominada MAC.

Sobre las direcciones MAC, se destacan aspectos como:

- En el filtrado MAC, se autentican las estaciones clientes en el AP, el cual tiene una tabla de direcciones aprobadas.
- Este planteamiento tiene una ventaja y es que los usuarios involuntarios no pueden conectarse a la red.
- Mientras que una debilidad es que un usuario malintencionado corre una aplicación, lee los paquetes y detecta una o más MAC validadas en la tabla y, mediante "software", cambia la MAC de su tarjeta, pudiendo acceder al AP.
- Claramente, el filtrado de las direcciones MAC no es una solución definitiva a los problemas referentes a la seguridad en las redes tipo "wireless".

Integridad de datos en WLAN

De acuerdo con Baño y Bosques (2015), la integridad de datos es la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas.

Estos son algunos datos que usted debe conocer sobre la integridad de datos en WLAN:

a) En 1999, el protocolo WEP también buscó proveer integridad de tráfico de datos, pero desafortunadamente el mecanismo de integridad, o CRC (código de redundancia cíclica), resultó inseguro.

b) El diseño fallido de WEP permite la alteración del código CRC del tráfico, sin la necesidad de saber la llave WEP, es decir, que el tráfico puede alterarse sin que se note.

c) Los protocolos WPA y WPA2 resolvieron el problema de la integridad de datos en WEP, mediante la inclusión de un mensaje de código de autenticación más seguro y la inclusión de un contador de segmentos (“frames”), que previene los “ataques por repetición” (“replay attack”).

d) En un ataque de repetición, el atacante registra la conversación entre un cliente y un punto de acceso, para obtener un acceso no autorizado.

e) Al responder una conversación “antigua”, el atacante no necesita saber la llave secreta WEP.

2. Implementación

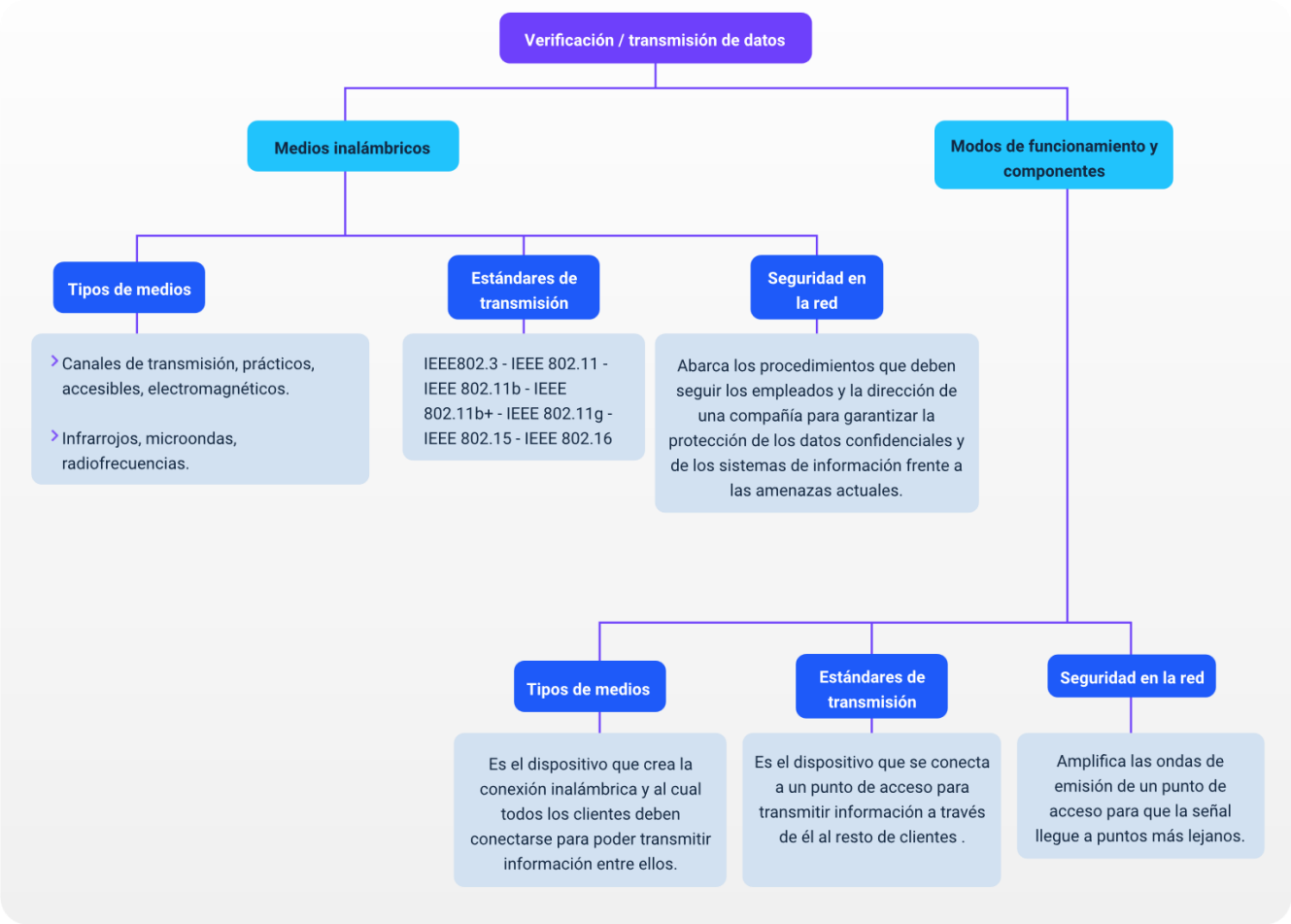
El modo de funcionamiento de la Infraestructura se basa en que todos los dispositivos se tienen que comunicar entre ellos a través de un dispositivo central y nunca directamente uno con otro.

Sus componentes son:

- **Punto de acceso.** Es el dispositivo que crea la conexión inalámbrica y al cual todos los clientes deben conectarse para poder transmitir información entre ellos. Este dispositivo define las características de la red inalámbrica, como su identificador SSID ("Service Set Identifier"), la velocidad de transmisión, la banda de frecuencia, la codificación de la información, etc. Normalmente, este dispositivo, a su vez, se conecta a una red Ethernet para dar acceso al resto de equipos.
- **Cliente.** Es el dispositivo que se conecta a un punto de acceso para transmitir información a través de él al resto de clientes o a la red Ethernet si existiera. Dispositivo que se comunica directamente con otro cliente.
- **Repetidor.** Dispositivo opcional que se encarga de amplificar las ondas de emisión de un punto de acceso para que la señal llegue a puntos más lejanos. El modo de funcionamiento "ad-hoc" (punto a punto) se basa en que los dispositivos se comunican entre sí, directamente, sin necesitar un dispositivo central que los relacione.

Síntesis

Usted ha finalizado el recorrido por los temas de este componente formativo. A continuación, haga un análisis del mapa que se muestra y realice su propia síntesis de lo estudiado.



Este mapa muestra cómo el componente formativo abordó generalidades y aspectos clave sobre el proceso de verificación / transmisión de datos, la comprobación del flujo de información sobre la infraestructura inalámbrica y otras acciones o procesos conexos: medios inalámbricos, estándares de transmisión, seguridad en la red, medios y métodos de funcionamiento, entre otros.

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1.3. Seguridad en la red	Castro, R. (2005). Avanzando en la seguridad de las redes WIFI. ENFOQUES, 73, p. 23-33.	Artículo	https://www.rediris.es/difusion/publicaciones/boletin/73/ENFOQUE1.pdf

Glosario

“Ad-hoc”: configuración del equipo cliente que ofrece conectividad independiente entre dispositivos dentro de una red LAN inalámbrica (Nafria, 2018).

Confidencialidad en las LAN: integridad de la información que se transmite por ella. Es decir, que ningún ente sin autorización pueda acceder a dicha información.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés) es una organización dedicada a la implementación de estándares de comunicación en el área de las tecnologías de la comunicación y la información.

Integridad de datos: es la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas.

Medios inalámbricos: espacios libres, por donde se propaga un tipo particular de ondas electromagnéticas: ondas de radiofrecuencia que son portadoras de señales de datos (Durán et al, 2008).

Referencias bibliográficas

Baño, F. y Bosques, V. (2015). *Mecanismos de seguridad en redes inalámbricas aplicado a la Universidad Estatal de Bolívar Centro Académico Las Naves*. Universidad Regional Autónoma de Los Andes. https://dspace.uniandes.edu.ec/handle/123456789/413

Díaz, M. (2012). *Conexiones inalámbricas ¿Una puerta abierta para los hackers?* ITCA Editores.

Durán, F., Mondragón, N. y Sánchez, M. (2008). *Redes cableadas e inalámbricas para transmisión de datos. Científica,* 12(3), p. 113-118. https://www.redalyc.org/pdf/614/61411377003.pdf

Nafria, F. (2018). *Redes wifi, ¿realmente se pueden proteger?.* UOC. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81269/3/fbnafriaTFM0618memoria.pdf

Prieto, J. (2011). *Introducción a los sistemas de comunicación inalámbricos*. UOC. https://www.exabyteinformatica.com/uoc/Informatica/Tecnologia_y_desarrollo_en_dispositivos_moviles/Tecnologia_y_desarrollo_en_dispositivos_moviles_(Modulo_1).pdf

Salvetti, D. (2011). *Redes wireless*. Fox Andina.

Soriano, M. (2014). *Seguridad en redes y seguridad de la información.* IMPROVET. https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n

Créditos

Nombre	Cargo	Centro de Formación y Regional
Claudia Patricia Aristizábal	Líder del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Jorge Eliécer Loaiza Muñoz	Experto Temático	Centro de Servicios y Gestión Empresarial - Regional Antioquia
Carlos Mauricio Tovar Artunduaga	Experto Temático	Centro de Servicios y Gestión Empresarial - Regional Antioquia
Fabián Leonardo Correa Díaz	Diseñador Instruccional	Centro Industrial del Diseño y la Manufactura - Regional Santander
Blanca Flor Tinoco Torres	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Francisco José Lizcano	Desarrollador Fullstack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Actividad Didáctica	Centro Industrial del Diseño y la Manufactura - Regional Santander
Carmen Alicia Martinez Torres	Animador y Productor Multimedia	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniela Muñoz Bedoya	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruiz Torres	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Luis Gabriel Urueta Alvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis Gómez	Evaluador para Contenidos Inclusivos y Accesibles	Centro Industrial del Diseño y la Manufactura - Regional Santander