**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| PROGRAMA DE FORMACIÓN | Tecnólogo en gestión de redes de datos |

|  |  |  |  |
| --- | --- | --- | --- |
| COMPETENCIA | 220501107. Implementar red inalámbrica local según especificaciones del diseño y estándares técnicos | RESULTADOS DE APRENDIZAJE | 220501107-03. Verificar la transmisión de datos en la infraestructura inalámbrica bajo criterios y procedimientos técnicos establecidos. |

|  |  |
| --- | --- |
| NÚMERO DEL COMPONENTE FORMATIVO | 007 |
| NOMBRE DEL COMPONENTE FORMATIVO | Verificación / transmisión de datos |
| BREVE DESCRIPCIÓN | Este componente formativo, aborda 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 conexas. Co su estudio responsable, el aprendiz estará se afianzará en: medios inalámbricos, estándares de transmisión, seguridad en la red, medios y métodos de funcionamiento, entre otros. |
| PALABRAS CLAVE | Dispositivos, información, servicios, redes, transmisión. |

|  |  |
| --- | --- |
| ÁREA OCUPACIONAL | Ciencias naturales, aplicadas y relacionadas. |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS:**

**Introducción**

**1. Medios inalámbricos**

1.1. Estándares de transmisión inalámbrica

1.2. Seguridad en la red

**2. Modos de funcionamiento y componentes**

1. **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**!

|  |
| --- |
| **DI\_CF07\_0\_Video\_Introduccion** |

1. **DESARROLLO DE CONTENIDOS**:

**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:

|  |
| --- |
| **DI\_CF07\_1\_Slide\_MediosInalambricos** |

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

|  |
| --- |
| **DI\_CF07\_1\_Acordeón\_RangosDeFrecuencias** |

**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:

|  |
| --- |
| **DI\_CF07\_1-1\_LienaDeTiempo\_EstandaresDeTransmision** |

¿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:

|  |
| --- |
| **DI\_CF07\_1-2\_Pestañas\_GeneralidadesSeguridadEnLaRed** |

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

|  |
| --- |
| **DI\_CF07\_1-2\_Slide\_CincoElementosGarantiaDeSeguridad** |

**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:

|  |
| --- |
| **DI\_CF07\_1-2\_Slide\_ProtocolosDeSeguridadWEP-WPA-WPA2** |

**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:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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. | 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. | 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*). | En un ataque de repetición, el atacante registra la conversación entre un cliente y un punto de acceso, para obtener un acceso no autorizado. | Al responder una conversación “antigua”, el atacante no necesita saber la llave secreta WEP. |

**2. Modos de funcionamiento y componentes**

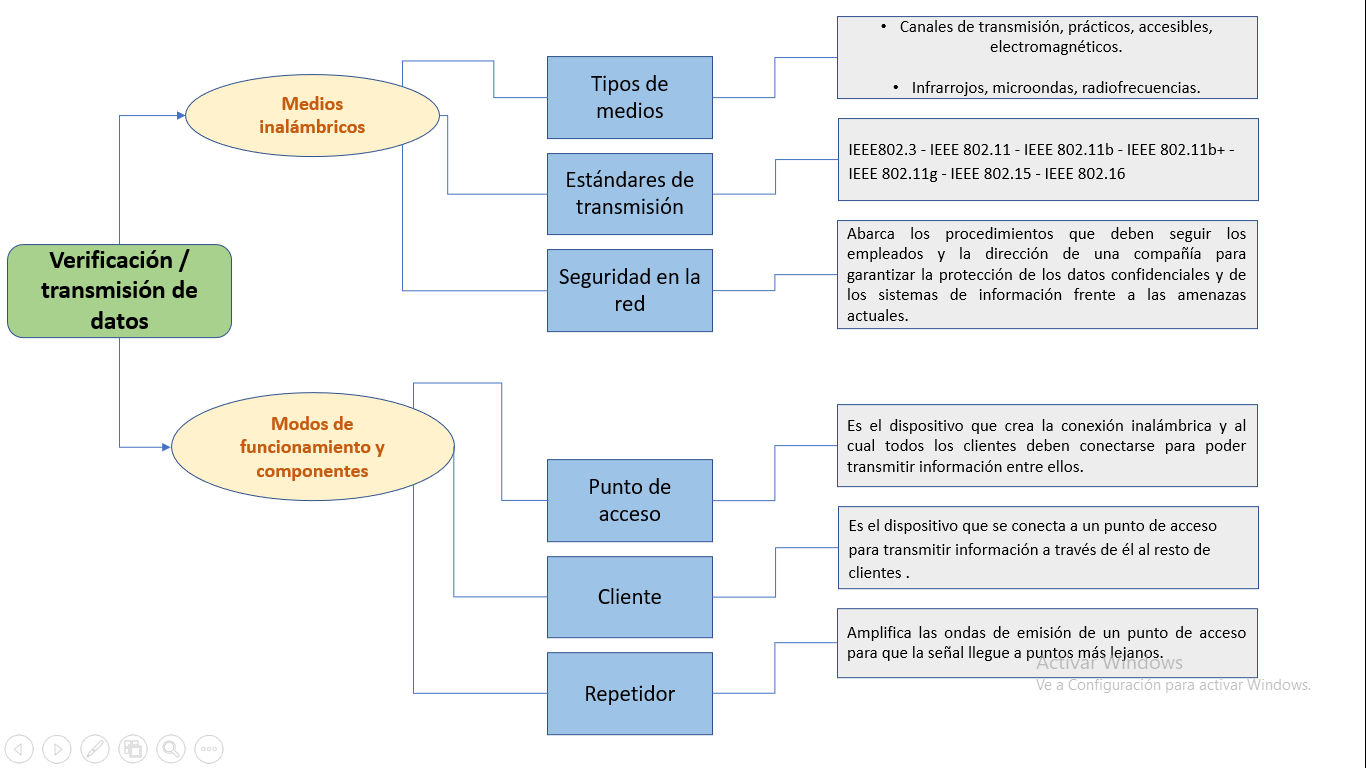
El modo de funcionamiento de la Infraestructura se basa en que todos los dispositivos se tienen que comunicar entre ellos a través de un dispositivo central y nunca directamente uno con otro.

Sus componentes son:

|  |
| --- |
| **DI\_CF07\_2\_Pestañas\_ModosDeFuncionamientoYComponentes** |

1. **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.



1. **ACTIVIDAD DIDÁCTICA**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | Verificando y transfiriendo datos |
| Objetivo de la actividad | Profundizar en los conceptos, acciones y gestión del proceso de verificación y transmisión de datos, con base en los temas desarrollados en el componente formativo. |
| Tipo de actividad sugerida | Falso o verdadero. |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Carpeta Formatos\_DI:  **Actividad\_Didactica\_1** |

1. **MATERIAL COMPLEMENTARIO**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| 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> |

1. **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).

1. **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. <http://hdl.handle.net/10972/487>

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>

1. **CONTROL DEL DOCUMENTO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha |
| Autor(es) | Jorge Eliécer Loaiza Muñoz | Experto temático | Centros de Servicios y Gestión Empresarial - Antioquia. | Agosto de 2021 |
| Carlos Mauricio Tovar Artunduaga | Experto temático | Centros de Servicios y Gestión Empresarial - Antioquia. | Agosto de 2021 |
| Luz Mila Pacheco Fuentes | Diseñadora instruccional | Centro de Diseño y Metrología  Regional distrito Capital | Agosto de 2021 |
| Deivis Eduard Ramírez Martinez | Diseñador  Instruccional | Centro para la Industria de la Comunicación Gráfica - Distrito capital | Agosto de 2021 |
| Silvia Milena Sequeda Cárdenas | Evaluadora instruccional | Centro de gestión industrial - Distrito Capital | Agosto de 2021 |
| Rafael Neftalí  Lizcano Reyes. | Asesor pedagógico | Centro Industrial de Diseño y la Manufactura | Agosto de 2021 |
| Darío González | Corrección de estilo | Regional Tolima – Centro Agropecuario La Granja | Agosto 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Santander – Centro Industrial del diseño y la Manufactura | Septiembre 2023 |
| Rafael Neftalí  Lizcano Reyes. | Responsable desarrollo curricular Ecosistema RED Santander | Centro Industrial de Diseño y la Manufactura | Septiembre 2023 |

1. **CONTROL DE CAMBIOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| Autor (es) |  |  |  |  |  |