**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

|  |  |
| --- | --- |
| **PROGRAMA DE FORMACIÓN** | Tecnología en gestión de redes de datos. |

|  |  |  |  |
| --- | --- | --- | --- |
| **COMPETENCIA** | 220501106. Configurar dispositivos de cómputo de acuerdo con especificaciones del diseño y protocolos técnicos. | **RESULTADOS DE APRENDIZAJE** | 220501106-03. Verificar el funcionamiento de dispositivos de cómputo y servicios de red de acuerdo **a** políticas de la organización. |

|  |  |
| --- | --- |
| **NÚMERO DEL COMPONENTE FORMATIVO** | 10 |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Verificación de acuerdo con políticas de la organización |
| **BREVE DESCRIPCIÓN** | Este componente formativo aborda elementos generales y claves del proceso de verificación de dispositivos y servicios de red, según las políticas y criterios de la organización. Con su estudio responsable, el aprendiz podrá apropiarse de inspección física y lógica de la red, parámetros, comandos, monitoreos de rendimiento, protocolos de prueba y demás acciones propias del proceso. |
| **PALABRAS CLAVE** | Inspección, monitoreo, administración, intrusión. |

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

1. **TABLA DE CONTENIDOS:**
2. **Verificación de conectividad**
   1. Inspección física de la red
   2. Inspección lógica de la red
3. **Verificación de dispositivos de cómputo**
4. **Verificación de red**
   1. Monitoreo de rendimiento
   2. Monitoreo de red
   3. Protocolos de prueba
5. **INTRODUCCIÓN:**

Reciba una gran bienvenida al estudio del componente formativo “**Verificación de acuerdo con políticas de la organización**”. Comience consultando el siguiente video, donde se ofrece un primer acercamiento y contextualización con los temas por desarrollar. ¡**Adelante**!

|  |
| --- |
| **DI\_CF10\_0\_Video\_Introduccion** |

1. **DESARROLLO DE CONTENIDOS:**
2. **Verificación de conectividad**

A partir del desarrollo de las infraestructuras tecnológicas, el personal encargado de la administración de la red realiza una verificación inicial antes del despliegue; esto para comprobar la instalación de los dispositivos periféricos y que su configuración cumpla con los requerimientos de la organización. Así mismo, se verifica la red de datos.



Para realizar esa actividad los administradores cuentan con un conjunto de herramientas e instrumentos que pueden ser tanto físicos (cableado, dispositivos, conexiones, módems, etc,) como en *software* (configuraciones, comando, etc.), dicha comprobación debe ser documentada a fin de realizar futuras revisiones. La siguiente figura ilustra las características de cada tipo de inspección:

Figura 1

*Inspección física e inspección lógica*



* 1. **Inspección física de la red**

La primera comprobación consiste en la revisión física de la red mediante un recorrido donde se inspecciona el estado de los cables, los conectores, los paneles y los adaptadores de red.



Donde se requiera la inspección de la operatividad del cableado, se usan herramientas físicas para el testeo de la red; estos son:

|  |
| --- |
| **DI\_CF10\_1-1\_Slide\_HerramientasFisicasParaTesteoRed** |

Por otro lado, al realizar la verificación física de los dispositivos de red como *switch*, *router*, servidores, entre otros, se suele realizar una inspección rápida de los indicadores luminosos, comúnmente conocidos como LED que proporcionan una vista rápida del estado de conexión del equipo.



Algunos identificadores LED que se encuentran en estos dispositivos son:

**Tabla 1**

*Indicadores LED*

|  |  |
| --- | --- |
| LED | FUNCIÓN |
| Sistema o Power | Indica si el equipo está encendido y conectado a la red eléctrica. |
| Estado del enlace del puerto | Se asocia a la conexión del dispositivo en la red. |
| Modo del puerto | Indica el modo de operación del puerto. |
| Velocidad de transmisión | Indica la velocidad de transmisión a la que opera el puerto. |

Nota: tomado de Castaño (2013).

* 1. **Inspección lógica de la red**

Es aquella que se implementa mediante *software*; permite verificar la conectividad lógica de la red. Esta inspección del sistema consta de comprobar que los parámetros de los dispositivos de dicha red estén correctamente configurados. Así, se puede revisar la comunicación interna y externa de los equipos en red.

Dentro de las inspecciones lógicas de red se encuentran:

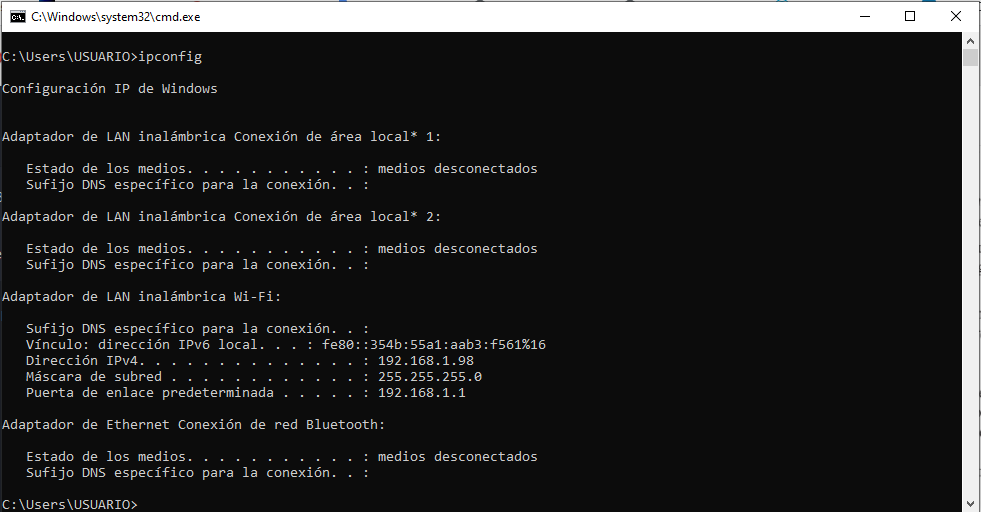
* Parámetros de red
* Comando ping
* Comando tracert y traceroute
* Comando ARP
* Comando Route
* Comando Nslookup

**Parámetros de red**

Para realizar dicha verificación se hace uso de los comandos del sistema *ipconfig* en sistemas operativos Windows, o ***ifconfig*** en sistemas operativos derivados de UNIX como Linux o MAC OS. Esta operación se realiza en el intérprete de comando conocido como **cmd.exe** o símbolo del sistema, su invocación muestra los parámetros básicos de la configuración TCP/IP de las interfaces de red habilitadas en los equipos de cómputo o estaciones de trabajo:

**Figura 2**

*Comando ipconfig*



Dentro de los parámetros de red a visualizar se tienen la dirección IP, la máscara de subred y la puerta de enlace predeterminada o *Gateway*.

Cuando se desee conocer mayor información de la configuración TCP/IP del equipo se puede recurrir a los siguientes comandos del sistema:

**Tabla 2**

*Comandos del sistema*

|  |  |
| --- | --- |
| Windows | UNIX |
| ipconfig/all: Muestra la información detallada de las interfaces del equipo | ifconfig-a: Muestra la información detallada de las interfaces del equipo  ifconfig *interfaz*: Informar sobre una interfaz determinada |
| ipconfig/release: Permite borrar la configuración actual del adaptador de red | ifconfig *interfaz address* *dirección\_IP* netmask *máscara*: Permite modificar los parámetros de acceso a la red de una interfaz según las especificaciones de dirección\_IP y máscara configurados |
| Ipconfig/renew: Permite volver a cargar la configuración del adaptador de red | Ifconfig *interfaz* up: Habilita la interfaz indicada  Ifconfig *interfaz* down*:* Deshabilita la interfaz indicada. |

Nota: adaptada de Castaño (2013).

**Comando ping**

Ping (*Packet Internet Groper*) está presente tanto en sistemas operativos Windows como en UNIX y en los sistemas operativos de red de algunos *routers*. El comando *ping*emplea el protocolo ICMP (Protocolo de control y notificación de errores) que está implementado por el modelo TCP/IP.



Para verificar la conectividad de los dispositivos en red se especifica la dirección IP del dispositivo destino con el que se quiere establecer la conexión; si el comando ping no recibe respuesta, esto indica un problema de conectividad que se encuentra ubicado en algún elemento del nivel físico o de red, o en la misma configuración de red del equipo origen o destino.

**Figura 3**

*Comando ping a dirección IP*

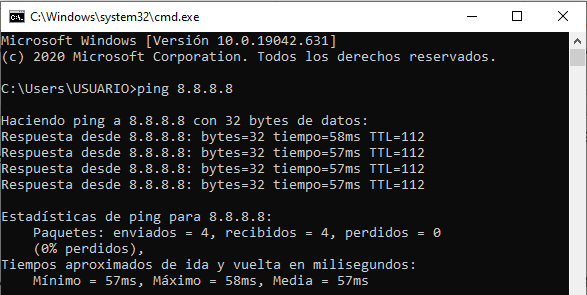
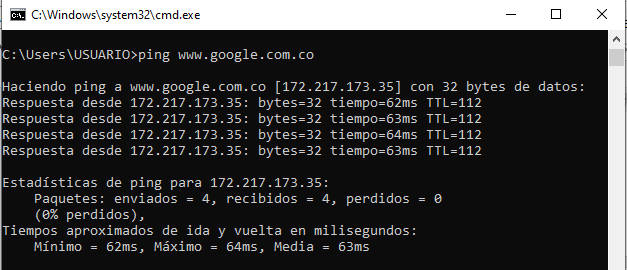


Figura 4

Ejecución del comando ping a URL



Al usar el comando ping, este envía un mensaje ICMP con una solicitud de ***echo*** al equipo destino. Los resultados emitidos están conformados por el número de paquetes que se envían de origen a destino, los paquetes recibidos y los paquetes perdidos, incluyendo el tiempo de ida y vuelta de los paquetes medido en milisegundos. Si la conexión a internet es la correcta se obtiene una respuesta donde los paquetes perdidos representan el 0 %.

**Comando tracert y traceroute**

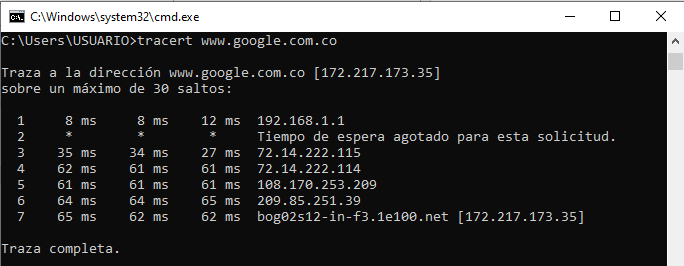
El comando **tracert** para sistemas operativos Windows y **traceroute** para sistemas operativos UNIX como MAC OS o Linux y para sistemas operativos de red de algunos *routers*, es una herramienta de diagnóstico que permite rastrear el recorrido de los paquetes y los tiempos de retardo que se producen. Al aplicar el comando, este muestra los datos de los dispositivos de red y los nodos por los que pasa y el tiempo que toma cada salto hasta conseguir llegar al destino.



En sistemas Windows, para ejecutar este comando, se abre una ventana del sistema **cmd.exe** o símbolo del sistema. Allí, digitar la siguiente línea: **tracert** *URL\_pagina\_web.*

**Figura 5**

*Comando tracert*



La figura siguiente, detalla más y mejor la ejecución del comando tracert y traceroute:

**Figura 6**

*Comando tracert y traceroute*



A



**Switch**

**Switch**



**Router A**



**Router B**



**Router C**



B



C



D

10.1.0.254/24

10.0.0.254/24



**NIC**

Rastreo:

RouterA#traceroute 10.1.0.2

Rastreo:

c:\>tracert 10.1.0.2

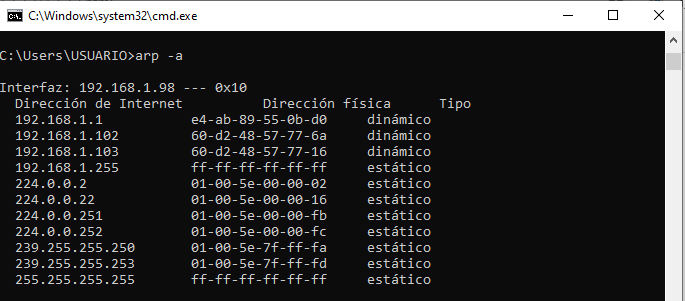
Las columnas con la información que se muestra en la pantalla después de la ejecución del comando Tracert indica, respectivamente: primera columna el número de salto, las siguientes tres columnas el tiempo de respuesta de los paquetes que son enviados, donde el símbolo del asterisco (\*) indica que no se obtuvo respuesta, y la última columna indica la dirección IP del nodo por el que pasa el paquete.

**Comando ARP**

El comando ARP, (Protocolo de resolución de direcciones) permite obtener la información de la tabla ARP del dispositivo en red.

**Figura 7**

*Comando ARP*



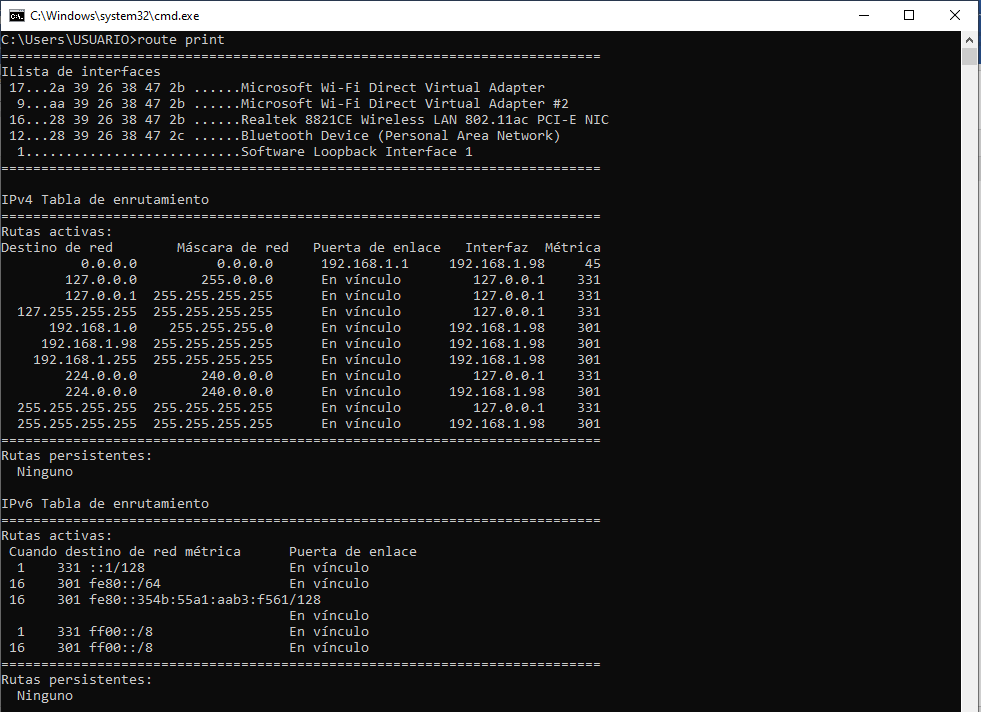
Como sugiere la imagen del comando ARP, la tabla contiene una asociación de dirección IPv4 con su correspondiente dirección MAC o dirección física, incluido el tipo de direccionamiento IP (estático o dinámico). Para la ejecución del comando ARP se usa la ventana cmd.exe digitando la siguiente línea: arp -a

**Comando Route**

Este comando es una herramienta del sistema que permite la consulta de las tablas de enrutamiento del equipo en red.

**Figura 8**

*Comando Route print*



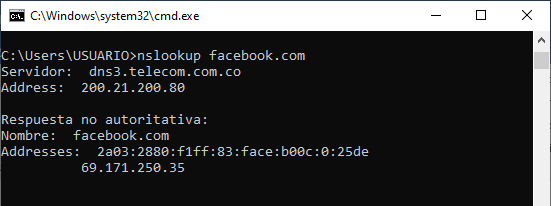
Para consultar la información en sistemas operativos Windows en la ventana cmd.exe digitar la siguiente línea: *route print,* para sistemas derivados de UNIX digitar la línea: *route -n.*

**Comando** N**slookup**

Este comando es una herramienta del sistema que permite la comprobación del correcto funcionamiento del servidor DNS. La información asocia el nombre de dominio consultado a su respectiva dirección IPv4 o IPv6 según sea el caso.

**Figura 9**

*Comando nslookup*



La ejecución del comando se puede realizar de dos formas una interactiva donde en sistemas operativos Windows en la consola cmd.exe se digita: *nslookup***,** al presionar la tecla enter se realizará una conexión con el servidor DNS y aquí se puede realizar la consulta digitando la URL. De otra forma no interactiva se digita el comando directamente en la consola cmd.exe, por ejemplo: *nslookup**facebook.com.*

En el siguiente video se explican algunos de los comandos de red en Windows que pueden ser usados para verificar la conectividad de la red:

|  |
| --- |
| **DI\_CF10\_1-2\_Video\_ComandosDeRedEnWindows** |

1. **Verificación de dispositivos de cómputo**

Dentro de los sistemas informáticos, el uso de sistemas computacionales es constante. De tal modo, realizar una verificación de estos dispositivos dentro de una red es muy importante.

Dentro de las actividades de comprobación se encuentran:

|  |
| --- |
| **DI\_CF10\_2\_Pestanas\_VerificacionDispositivosDeComputo** |

1. **Verificación de red**

Para abordar la gestión de redes en sí, hay que considerar primero algunos escenarios a manera de ejemplo, en el cual componentes complejos del sistema interactúan y son inspeccionados, gestionados y monitoreados por un supervisor.



|  |  |  |
| --- | --- | --- |
| El primer escenario a estudiar es el caso del panel de control de un avión, el cual le permite al piloto monitorear las variables operativas y analizar los datos para asegurar que los dispositivos estén operando dentro de los límites. | Como segundo escenario, se tiene una planta de generación de energía eléctrica, esta tiene una sala de control donde los diales, medidores y luces monitorean el estado de las variables a verificar (presión, flujo, temperatura, entre otros) en las tuberías, válvulas, contenedores y otros componentes del sistema. Estos dispositivos de monitoreo le permiten al operador tomar acciones en caso de presentarse problemas inminentes. | En una forma similar, el administrador de la red supervisará, gestionará y controlará prontamente el sistema que se le confía. La verificación de la red incluye un monitoreo de red en un sentido más amplio indica la forma de supervisar de forma constante la funcionalidad de la red a fin de garantizar que los parámetros cumplen con las especificaciones del diseño de la organización. |

Cuando un administrador encuentra un problema de red, puede ejecutar algunas verificaciones del sistema realizando inspección física o lógica, a fin de localizar el origen del problema y ajustar la configuración del sistema. Se puede optar por un reinicio del *hardware* o *software* o acceder de forma remota.

Las redes privadas y públicas han crecido de pequeñas redes a una gran infraestructura global, la necesidad de administrar la gran cantidad de componentes de *hardware* y *software* dentro de estas redes, de manera más sistemática, también se ha vuelto una tarea más importante. Además, en los sistemas informáticos se pueden configurar a fin de monitorear la red con avisos y alarmas que se envíen de forma automática al administrador de la red.

* 1. **Monitoreo de rendimiento**

Los monitoreos de rendimiento permiten analizar el rendimiento de la red. Son útiles a la hora de verificar las funciones de los dispositivos que se monitoreen.

Dentro de los parámetros de rendimiento de la red, usualmente monitoreados, se encuentran:

|  |
| --- |
| **DI\_CF10\_3-1\_Slide\_ParametrosDeRendimientoDeLaRed** |

* 1. **Monitoreo de red**

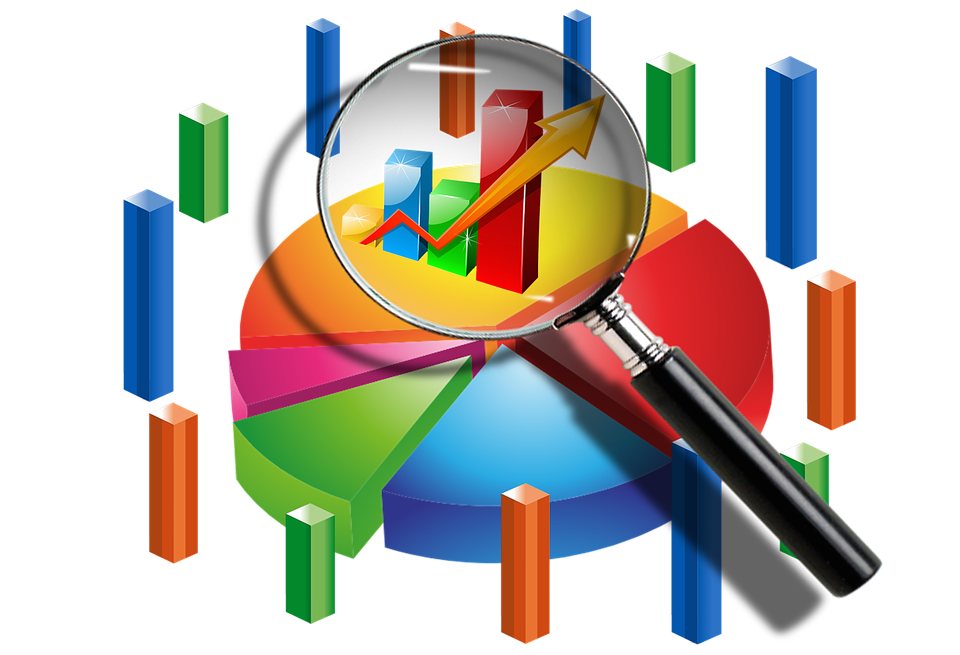
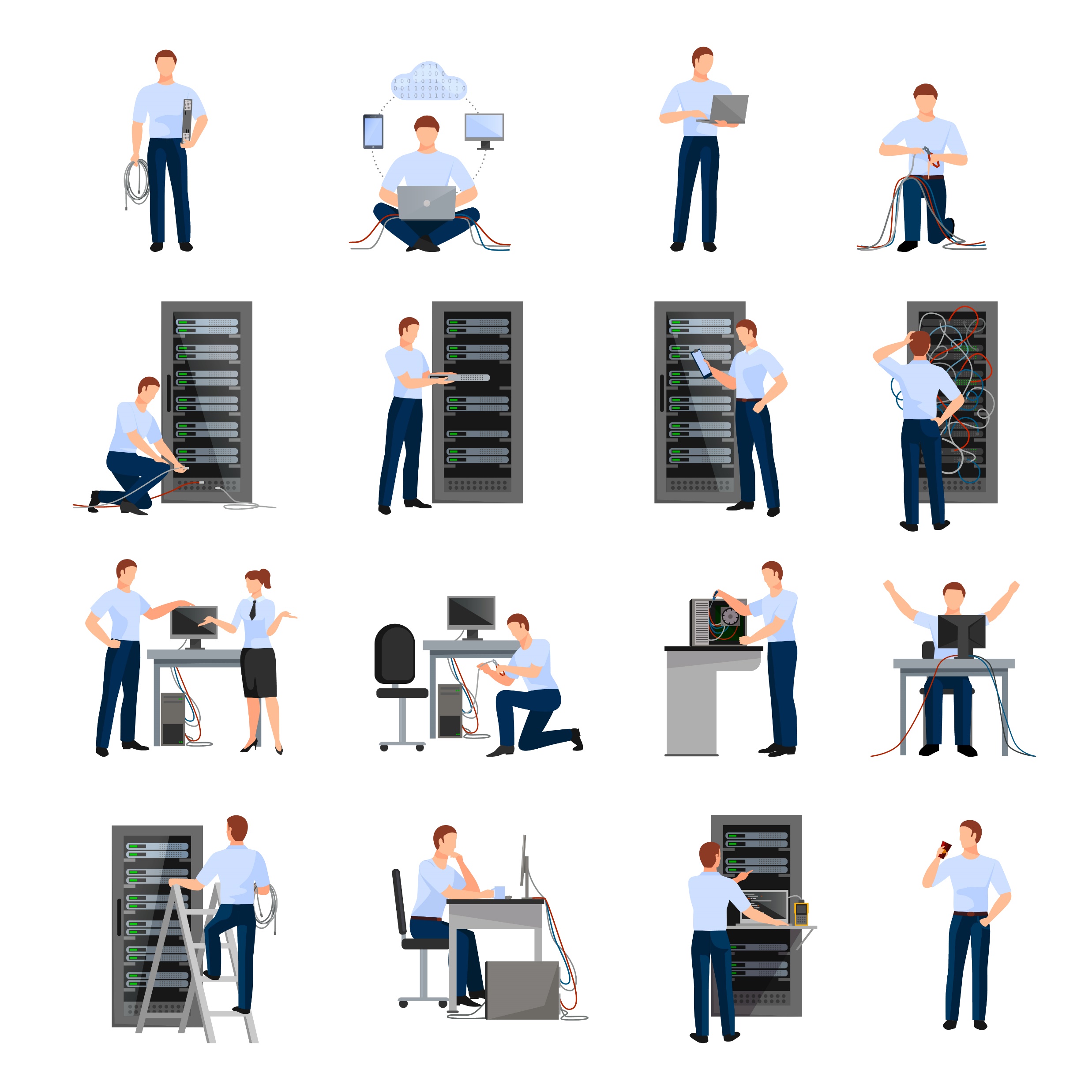
Dentro de las fases más largas de la ejecución y puesta en marcha de sistemas informáticos, está la monitorización de la red, la cual permite la supervisión a fin de detectar posibles fallas en la red y verificar su correcto funcionamiento.



El monitoreo de red no es exclusivo para organizaciones con infraestructuras de red extensas; también es necesario y conveniente realizar una supervisión en redes con pocos dispositivos a fin de detectar problemas que afecten los servicios prestados por la empresa.

**Figura 10**

*Elementos a monitorear en red*



Dispositivos de red

Monitor de red

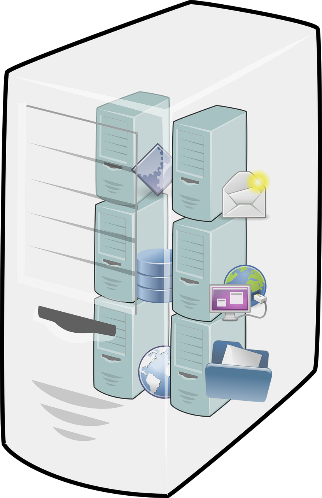


Router/Switch/Firewall



SAI (Sistema de Alimentación

Ininterrumpida)



Impresora en red



Servidor

Nota: adaptado de Castaño (2013).

Entre las herramientas de monitorización de la red se puede mencionar:

|  |  |  |
| --- | --- | --- |
| **Analizadores de protocolos**  También conocidos como *sniffers.* Estos analizan el tráfico de la red y proporcionan datos como cantidad y tipo de tráfico. Lo principal, al examinar las tramas de red, es detectar los tipos de protocolos que se están usando, para prevenir posibles ataques del exterior de la red. | **Algunos ejemplos de analizadores**  Tcpdump para sistemas UNIX, pertenece a software libre.  Wireshark esta herramienta está disponible para sistemas UNIX y Windows.  Ntop herramienta de *software* libre. | **Monitorización remota**  Son herramientas en las que un dispositivo de red recopila y analiza los datos resultantes del monitoreo de los dispositivos de red y los centraliza en un único dispositivo que facilita la consulta por parte del administrador de red. |

* 1. **Protocolos de prueba**

Se trata de protocolos incorporados al modelo TCP/IP que permiten una administración y gestión de la red. Dichos protocolos conforman un conjunto de lineamientos que son reglas e instrucciones que permiten a los dispositivos compartir información en la red; los sistemas de monitoreo de red aplican estos protocolos para identificar fallas y notificar al administrador de la red.



Según Valdivia (2020) hay dos protocolos importantes, que son usados para testear redes de datos:

* **Internet Control Message Protocol (ICMP)**: es el Protocolo de mensajes de control de Internet.
* **Simple Network Management Protocol (SNMP)**: es el Protocolo simple de administración de redes.

**Protocolo ICMP**

Es un protocolo ubicado en la capa de red del modelo TCP/IP. Los dispositivos que trabajan en esta capa como los *routers* y servidores, usan este protocolo para enviar información sobre incidencias en la red. Este protocolo permite el envío de mensajes ICMP que se transmiten como datagramas IP a través de la red.



Dentro de las funcionalidades de los mensajes ICMP, está la de confirmar si un destino se encuentra activo y es alcanzable; también, informar problemas de parámetros en una cabecera de datagrama, la sincronización de reloj y las estimaciones de tiempo de tránsito, además, obtiene direcciones de Internet y máscaras de subred.

La figura siguiente muestra el formato del mensaje ICMP

**Figura 11**

*Formato del mensaje ICMP*

*Tipo*

*Código*

*Checksum*

Cabecera

Cabecera IP

Datos del datagrama IP

Datos ICMP

Mensaje ICMP

Datagrama IP

Nota: adaptado de Valdivia (2020).

**Protocolo SNMP**

Este protocolo se ubica en la capa de aplicación del modelo TCP/IP. Fue desarrollado para administrar servidores, estaciones de trabajo, *Switches*, *Routers*, *Access points*, entre otros. En una red de datos, el protocolo SNMP facilita el intercambio de información mediante el modelo cliente/servidor, proporcionando funciones de monitoreo de red que permita la supervisión de dispositivos de red.

**Figura 12**

*Esquema SNMP*



NMS

IP Network



Agente

Agente

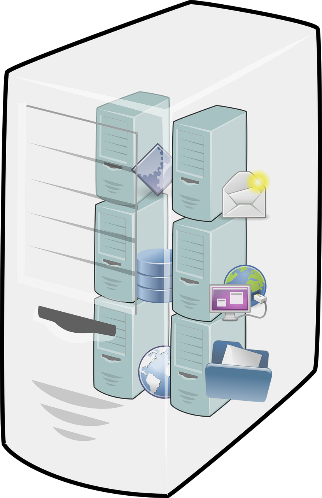
Agente

SNMP

SNMP

SNMP

SNMP



Los elementos claves a la hora de monitorizar una red basados en el protocolo SNMP son:

|  |  |
| --- | --- |
| **Agente de gestión**  Representa el *software* que se encuentra instalado en los equipos que se desean gestionar/monitorear. Estos mismos proporcionan la información que solicite el NMS, además este protocolo permite la gestión de forma remota. | **NMS (Network Management Station)**  Representa la estación de gestión de la red, requiere de Ia instalación de *software* específico, que permita gestionar/monitorizar la red.  Dentro del *software* de gestión de SNMP se encuentra la suite Net-SNMP que integra diversas aplicaciones de gestión de red, basadas en el protocolo SNMP. |

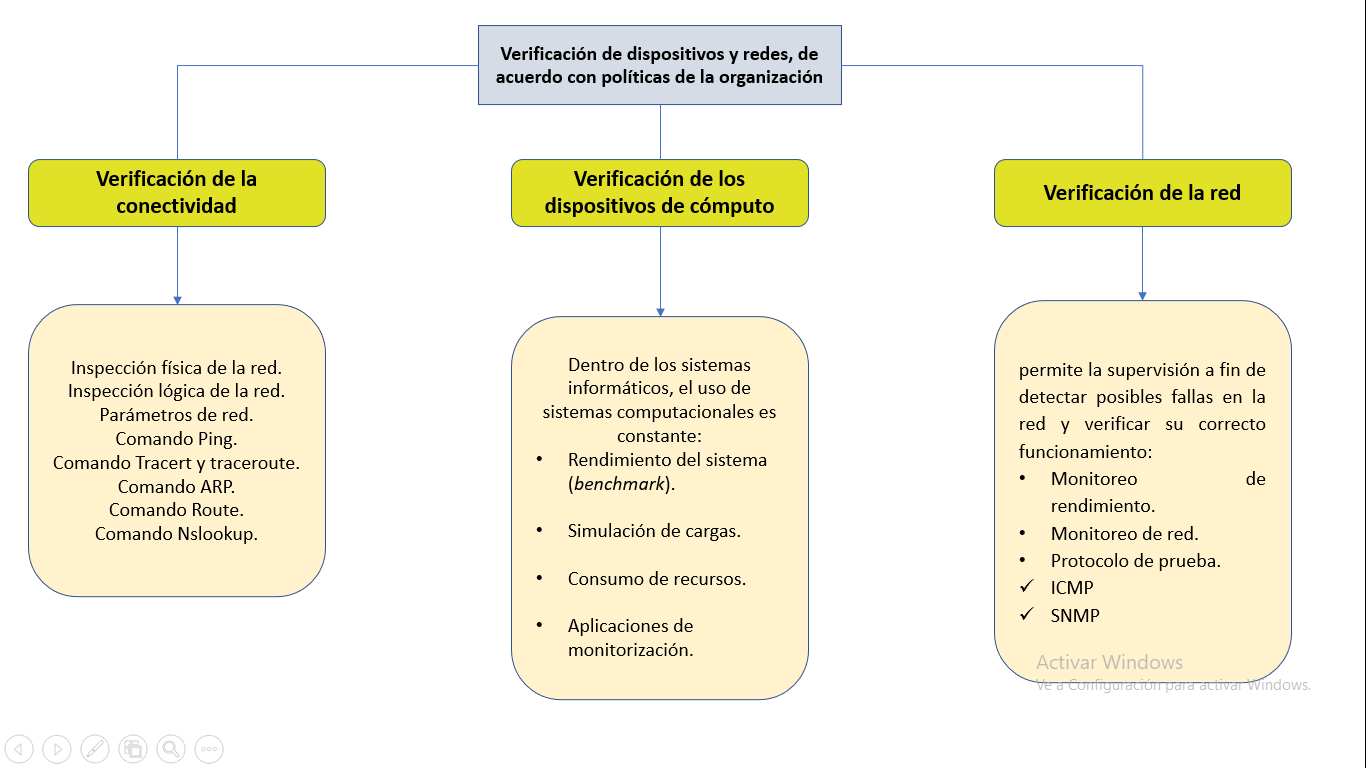
El funcionamiento de los elementos del protocolo SNMP se basa en la estructura de datos normalizada, denominada MIB (*Management information base*).

Simplemente, es una base de información con los datos que se reciben de los dispositivos gestionados, llamados agentes. El intercambio de información entre el NMS y el agente de gestión se realiza a través del protocolo UDP en el nivel de transporte.

Son tres las versiones del protocolo SNMP: SNMPv1, SNMPv2, y SNMPv3. Las versiones 1 y 2 no poseen mecanismo de cifrado de los mensajes SNMP. Si se desea proteger la información que se intercambia a fin de evitar posibles ataques, se debe usar la versión 3.

1. **SÍNTESIS:**

Ha llegado al final de los contenidos de este componente formativo. En este punto, haga un análisis del mapa que se muestra enseguida y realice su propia síntesis de los temas, conceptos y elementos desarrollados. ¡**Adelante**!



1. **ACTIVIDAD DIDÁCTICA**

|  |  |
| --- | --- |
| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| Nombre de la Actividad | **Verificando dispositivos de cómputo y servicios de red** |
| Objetivo de la actividad | Reforzar los conceptos, acciones y procedimientos de la verificación de dispositivos y servicios de red, con base en los temas desarrollados en el componente formativo. |
| Tipo de actividad sugerida | Relacionar términos (arrastrar – soltar). |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Carpeta Formatos\_DI:  **Actividad\_didáctica\_1** |

1. **MATERIAL COMPLEMENTARIO**

|  |  |  |  |
| --- | --- | --- | --- |
| Tema | Referencia APA del Material | Tipo de material | Enlace del Recurso o  Archivo del documento o material |
| Inspección lógica de la red | Instituto Tecnológico de Roque (2021). Introducción a redes. *Itroque* | Sitio web | <http://itroque.edu.mx/cisco/cisco1/course/module8/#8.3.2.1> |
| ICMP | Instituto Tecnológico de Roque (2021). Introducción a redes. *Itroque* | Sitio web | <http://itroque.edu.mx/cisco/cisco1/course/module8/#8.3.1.1> |
| SNMP | Network Direction (2020). *How SNMP Works | Network Fundamentals Part 24*. [Video] YouTube | Video | <https://www.youtube.com/watch?v=vWZefoGNk5g> |

1. **GLOSARIO:**

**Checksum:** detecta cambios inesperados en una cadena de datos, verificando su integridad.

**CPU:** siglas que indican Unidad de Procesamiento Central, aquí se encuentran los componentes que permiten a los equipos electrónicos realizar el procesamiento de datos.

**SAI:** sistema de alimentación ininterrumpida o también conocido como UPS son dispositivos que sirven para proporcionar una protección eléctrica.

**UDP:** es el protocolo de datagramas de usuario, permite la transmisión de datagramas en red.

**UNIX: s**istema operativo multitarea y multiusuario. Los posteriores desarrollos de este sistema son Linux, MAC OS X, Android, iOS, entre otros.

**URL:** localizador de recursos uniforme, es un identificador que se le asigna a los recursos disponibles en internet como páginas WEB, textos, fotos, videos, entre otros. La URL tiene su correspondencia con una dirección IP.

1. **Referencias bibliográficas**

Ariganello, E. (2020). Redes cisco - Guía de estudio para la certificación CCNA 200-301. *alphaeditorialcloud*. <https://www-alphaeditorialcloud-com.bdigital.sena.edu.co/auth/ip?intended_url=https://www-alphaeditorialcloud-com.bdigital.sena.edu.co/library/publication/redes-cisco-guia-de-estudio-para-la-certificacion-ccna-200-301>

Castaño Ribes, R. J. (2013). Redes locales. Macmillan Iberia S.A.

<https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/43257?page=298>

Valdivia, C. (2020). *Sistemas informáticos y redes locales*. Ediciones Paraninfo S.A.

1. **Control del documento**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Nombre | Cargo | Dependencia | Fecha |
| Autor (es) | Carlos Mauricio Tovar Artunduaga | Experto temático | Centro de Servicios y Gestión Empresarial.  Regional Antioquia. | Agosto 2021 |
| Jorge Eliécer Loaiza Muñoz | Experto temático | Centro de Diseño e innovación tecnológica industrial.  Regional Antioquia. | Agosto 2021 |
| Cinthia Rocío Trejos Chacón | Experta temática | Centro de la Industria, la empresa y los servicios. Regional Norte de Santander. | Agosto 2021 |
| Deivis Eduard Ramírez Martínez | Diseñador instruccional | Centro para la Industria de la Comunicación Gráfica. Regional Distrito Capital. | Agosto 2021 |
| Silvia Milena Sequeda Cárdenas | Evaluadora instruccional | Centro de la gestión industrial. Regional Distrito Capital. | Agosto 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Centro industrial del Diseño y la Manufactura. Regional Santander. | Agosto 2021 |
| Jhon Jairo Rodríguez Pérez | Diseñador y evaluador instruccional | Centro para la Industria de la Comunicación Gráfica. Regional Distrito Capital. | Septiembre 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Santander – Centro Industrial del Diseño y la Manufactura | Octubre 2023 |
| Rafael Neftalí Lizcano Reyes | Responsable desarrollo curricular Ecosistema RED Santander | Centro industrial del Diseño y la Manufactura. Regional Santander. | Octubre 2023 |

1. **CONTROL DE CAMBIOS**

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