**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | *Hacking* ético en sistemas y redes |
| --- | --- |

| COMPETENCIA | 220501111 - Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-02 - Aplicar procesos y procedimientos de seguridad informática en sistemas y redes de acuerdo con métodos y técnicas. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF002 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Levantamiento de huellas y herramientas de hacking ético |
| BREVE DESCRIPCIÓN | Con el estudio de este componente, el aprendiz estará mejor capacitado para realizar procesos de seguridad informática, aspecto fundamental de las organizaciones y el medio digital. Podrá aplicar diferentes herramientas digitales de ciberseguridad, hacer recolección de huellas, mejorar controles de datos, proteger sistemas y activos de información, de posibles ataques cibernéticos. |
| PALABRAS CLAVE | *Doxing*, *footprinting*, *hacking*, huella, redes. |

| ÁREA OCUPACIONAL | 2 - Ciencias naturales, aplicadas y relacionadas |
| --- | --- |
| IDIOMA | Español |

1. **TABLA DE CONTENIDOS**
2. ***Footprinting* y reconocimiento**
   1. Concepto y generalidades
   2. Herramientas y Google Hacking
   3. Contramedidas
3. **Escaneo de redes y dispositivos**
   1. Metodología de exploración CEH
   2. Herramientas de escaneo
   3. *Fingerprinting*, aparcamiento y OS
   4. Uso de *proxy* y anonimizadores
4. **Enumeración de activos**
   1. Conceptos y generalidades
   2. Técnicas de enumeración
   3. Contramedidas
5. **Introducción**

En el mundo digital de hoy, hay una gran cantidad de información al alcance de casi cualquier persona, lo cual se ha convertido en uno de los activos más importantes para las organizaciones. Con el uso de las tecnologías de información y comunicación y su avance tan vertiginoso, aparecen agentes internos y externos que pueden poner en riesgo los sistemas de información, los datos almacenados y hasta la infraestructura tecnológica. Es así como el *hacking* ético se ha convertido en una herramienta de gestión para la seguridad.



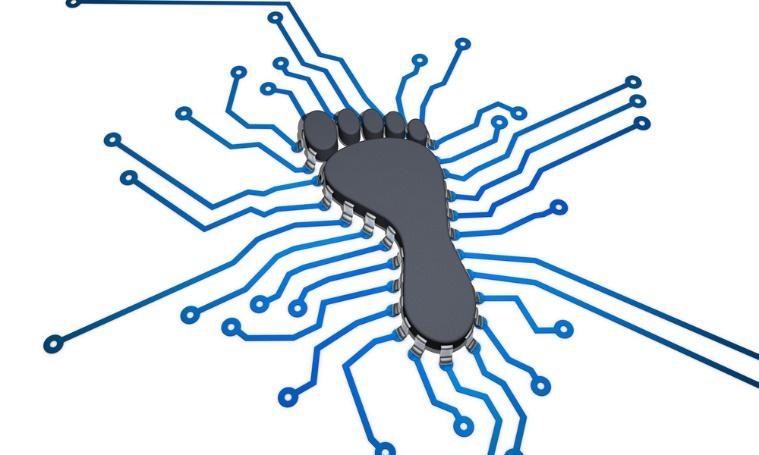
<https://cdn.pixabay.com/photo/2020/05/25/08/54/banner-5217681__340.jpg>

Es así, como para comenzar con el estudio de este componente, se invita a explorar el recurso que a continuación se propone. Le deseamos todos los éxitos en esta experiencia de formación:



1. **DESARROLLO DE CONTENIDOS**
   * + 1. ***Footprinting* y reconocimiento**

El *footprinting* se define como el proceso de creación de un plano o mapa de la red y los sistemas de una organización; igualmente, a la recopilación de información también se le conoce como “*footprinting*” (huella) de una organización. Este se comienza por determinar el sistema, la aplicación o la ubicación física del objetivo y, una vez que se conoce esta información, se reúne información específica sobre la organización utilizando métodos no intrusivos.



<https://cyberdemonzs.files.wordpress.com/2019/08/footprinting.jpg>

Se puede tomar como ejemplo, la propia página web de la organización que puede proporcionar un directorio de personal o una lista de las biografías de los empleados, lo que resulta útil si el pirata informático necesita utilizar un ataque de ingeniería social para alcanzar el objetivo.



Estos son algunos de los datos que se deben reunir, sobre un objetivo, durante el *footprinting*:

* Nombre de dominio.
* Bloques de red.
* Servicios y aplicaciones de red.
* Arquitectura del sistema.
* Sistema de detección de intrusos.
* Mecanismos de autenticación.
* Direcciones IP específicas.
* Mecanismos de control de acceso.
* Números de teléfono.
* Direcciones de contacto.

Una vez que esta información es compilada, puede dar a un hacker una mejor visión de la organización, donde se almacena la información valiosa y cómo se puede acceder a ella.

* 1. **Concepto y generalidades**

El *footprinting* es el proceso de reunir la mayor cantidad de información posible sobre un sistema/red objetivo para identificar diferentes formas de intrusión en la red de una organización.



<https://freelearningtech.in/wp-content/uploads/2020/01/Footprinting_-Advanced-Learning-Course.jpg>

Dentro de los procesos más comunes de esta técnica están:

* Recoger información básica.
* Encuentra la versión del sistema operativo, la edición del servidor web, etc.
* Obtener información de DNS usando Whois, etc.
* Busca vulnerabilidades y explota para lanzar ataques.

El *footprinting* es el primer paso en el hacking ético e implica la recolección de información sobre el objetivo y su entorno. En esta etapa se puede recopilar información importante que luego es útil en las etapas posteriores del *hacking* ético.

El *footprinting* se puede llevar a cabo de diferentes formas, entre las que se destacan:



* 1. **Herramientas y Google Hacking**

Dentro del *hacking* ético, existen diferentes herramientas para poder realizar un reconocimiento de huellas o *footprinting*. Este proceso busca información pública o privada que pueda ser objeto de un ataque.



<https://cdn.pixabay.com/photo/2017/05/17/14/03/ransomware-2320941__340.jpg>

Para ello, se pueden realizar diferentes actividades, como las que se describen a continuación:





* 1. **Contramedidas**

Dentro del *footprinting* o huellas, se debe tener en cuenta que las contramedidas que se pueden realizar son múltiples, dependiendo del trato que se les pueda dar, según el caso que se presente.



<https://cdn.pixabay.com/photo/2016/08/13/16/49/computer-1591018__340.jpg>

Para una mejor comprensión del proceso de mitigación de ellas, se presentan a continuación algunas consideraciones importantes:

* Configurar *routers* para restringir las respuestas a la solicitud de *footprinting.*
* Configurar servidores de internet para evitar la fuga de información y desactivar los protocolos no deseados.
* Bloquear los puertos con la configuración adecuada del *firewall.*
* Utilizar un IDS que se pueda configurar para rechazar el tráfico sospechoso y recoger los patrones de *footprinting.*
* Evaluar la información antes de publicarla en el sitio web / internet.
* Realizar técnicas de *footprinting* y eliminar cualquier información sensible encontrada.
* Evitar que los motores de búsqueda almacenen caché de una página web y el uso de registro de servicios anónimos.
* Desactivar la lista de directorios y utilizar *Split DNS.*

***Pentesting* de *footprinting***

El *pentest* de *footprinting* se utiliza para determinar la información de la organización, a disposición del público en Internet: arquitectura de red, sistemas operativos, aplicaciones y usuarios. El *pentester* intenta reunir la mayor cantidad de información posible acerca de la organización destino en internet y otras fuentes accesibles al público.



<https://esgeeks.com/wp-content/uploads/2017/08/Footprinting-de-Sitios-Web-Guia.jpg>

El *footprinting* es el primer paso por realizar dentro de la prueba de penetración; se deben tener presentes los siguientes aspectos:

Los doce pasos principales a seguir en la prueba de penetración de *footprinting* son:



* + - 1. **Escaneo de redes y dispositivos**

El escaneo en redes y dispositivos dentro de un sistema busca encontrar todo tipo de vulnerabilidades para identificar fallas en la seguridad, es el segundo paso a realizarse después de un levantamiento de huellas. Es de suma importancia apropiar conocimientos básicos y esenciales para aplicar herramientas que ayuden a determinar este tipo de acciones, orientadas a la seguridad e integridad de la información e infraestructura de una organización.



<https://media.istockphoto.com/photos/automation-industrial-business-process-workflow-optimisation-picture-id1280048451?s=2048x2048>

Sabiendo lo anterior, se invita a profundizar a través del siguiente video en los principales conceptos y generalidades del escaneo de redes y dispositivos. Se sugiere llevar registro de los aspectos más relevantes en una libreta personal de apuntes:



* 1. **Metodología de exploración CEH**

Para que un *hacker* ético pueda realizar exploraciones a los sistemas y redes, debe determinar las metodologías de escaneo, las cuales se pueden resumir en: comprobación de sistemas vivos, comprobación de puertos abiertos, captura de banderas, análisis de búsqueda de vulnerabilidades, dibujo de diagramas de red, preparación de *proxies*.



<https://consejosi.org/images/logotipo-ec-council-ceh.svg>

Tenga en cuenta las siguientes particularidades de las exploraciones y escaneos que puede realizar el *hacker* ético:



**Proceso de apretón de manos**

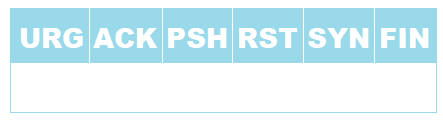
El proceso de apretón de manos de tres vías está diseñado de tal manera que ambos extremos ayudan a iniciar, negociar y separar las conexiones de *sockets* TCP al mismo tiempo. También permite transferir múltiples conexiones de *sockets* TCP, en ambas direcciones, al mismo tiempo.

He aquí los tres pasos:



**Banderas de comunicación TCP**

Las banderas de TCP tienen la misma función de mostrar cambios, situaciones o condiciones de la información; podrían compararse con un semáforo, ya que alertan sobre cuándo se debe parar, seguir o tener precaución. Estas banderas informan el estado de la información, de extremo a extremo, para que los datos lleguen íntegros (tal cual como son).



<https://caminosdigitales.es/wp-content/uploads/2018/06/banderas-tcp.png>



* 1. **Herramientas de escaneo**

Hablar de estas para identificar diferentes vulnerabilidades en un sistema, consiste tanto en permanecer en el anonimato como en falsificar la identidad de un dispositivo que era confiable por los sistemas defensivos; todo con el fin de realizar intrusiones y analizar qué fallas existen en las redes y solventarlas.



<https://techdator.net/wp-content/uploads/2020/05/Best-Vulnerability-Scanning-Tools-min.png>

Entre las herramientas más comunes, se pueden mencionar:



****

* 1. ***Fingerprinting*, aparcamiento y OS**

OS *fingerprinting* se refiere a la detección del sistema operativo de un *host* final, mediante el análisis de paquetes, que se originan en ese sistema. Es utilizada por los profesionales de la seguridad y los piratas informáticos para trazar mapas de redes remotas y determinar qué vulnerabilidades podrían estar presentes para ser explotadas.



<https://aphaia.co.uk/wp-content/uploads/2019/03/Fingerprint-tracking-02.jpg>

OS *fingerprinting* funciona solo para paquetes que contienen una conexión TCP completa; es decir, la conexión TCP debe tener una conexión SYN, SYN/ACK y ACK.



Algunas de las áreas que pueden ser examinadas para determinar el sistema operativo son:

* TTL.
* El tamaño de la ventana.
* Tamaño del paquete.
* DF bitl.
* TOSl.
* ***Fingerprinting* activo del sistema operativo**

Implica determinar activamente el SO de un PC objetivo, enviando paquetes cuidadosamente elaborados y examinando el comportamiento TCP/IP de las respuestas recibidas.

* ***Fingerprinting* pasivo del sistema operativo**

La huella del sistema operativo pasivo es el examen de una muestra de paquetes recolectada pasivamente de un *host*. Se basa en rastros del sistema remoto. En lugar de consultar activamente el sistema remoto, puede capturar los paquetes enviados desde el sistema remoto.

* 1. **Uso de *proxy* y anonimizadores**

Un servidor *proxy* actúa como una puerta de enlace entre un usuario e internet. Es un servidor intermediario que separa a los usuarios finales de los sitios web que navegan. Los servidores *proxy* proporcionan diferentes niveles de funcionalidad, seguridad y privacidad, dependiendo de su caso de uso, necesidades o política de la empresa.



<https://dircomfidencial.com/wp-content/uploads/2018/06/proxy-web.jpg>

Si se utiliza un servidor *proxy*, el tráfico de internet fluye a través del servidor *proxy* en su camino hacia la dirección que se solicitó; la solicitud vuelve, entonces, a través de ese mismo servidor *proxy* (hay excepciones a esta regla) y luego el servidor *proxy* reenvía los datos recibidos del sitio web al usuario.



En el siguiente recurso se puede conocer, profundizar y asimilar las razones técnicas, por las cuales se hace útil y necesario el uso de un servidor *proxy*:



**Anonimizadores**

Los sitios anonimizadores acceden a Internet a su nombre, protegiendo la información personal del usuario; Un anonimizador protege toda la información de identificación de una computadora, mientras navega en lugar de la persona, permitiendo permanecer, al menos, un paso alejada de los sitios que visita.



<https://mundo-hackers.weebly.com/uploads/9/8/5/0/98506118/published/160115192610-anonymous-2-780x439.jpg?1485190345>

Estas son las particularidades de los tipos de anonimizadores:



* + - 1. **Enumeración de activos**

El inventario de activos o llamada enumeración, es una actividad que se debe de realizar en primera instancia para poder llevar a cabo un proceso de gestión de la seguridad de un sistema; es de vital importancia conocer sus recursos físicos, infraestructura, personas, *software*, entre otros, que son parte de la cadena de valor de la organización y estos, a su vez, sean protegidos para evitar ataques de ciberdelincuentes. Las amenazas a las cuales se encuentran expuestos, cada vez, son mayores y de gran tecnología.



<https://cdn.pixabay.com/photo/2017/01/29/13/20/mobile-devices-2017978__340.png>

* 1. **Conceptos y generalidades**

La enumeración se define como el proceso de extracción de nombres de usuario, nombres de máquinas, recursos de red, recursos compartidos y servicios de un sistema. En esta fase, el atacante crea una conexión activa con el sistema y realiza consultas dirigidas para obtener más información sobre el objetivo.



<https://cdn.pixabay.com/photo/2020/02/11/10/13/hacking-4839031__340.jpg>

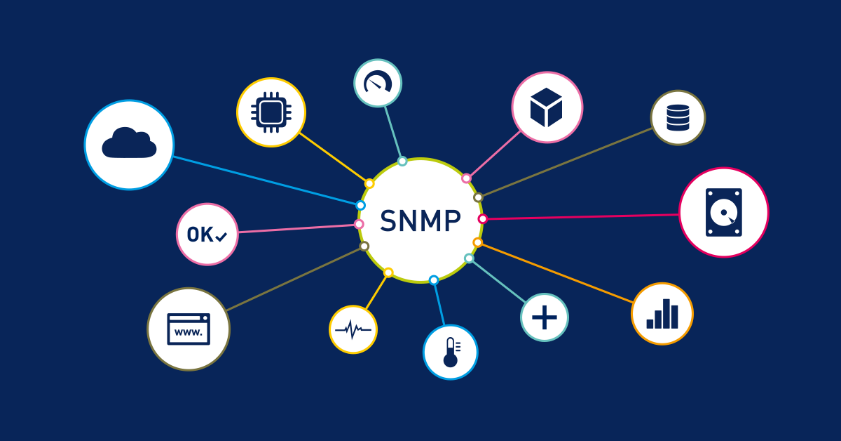
La información reunida se utiliza para identificar las vulnerabilidades o los puntos débiles de la seguridad del sistema y trata de explotarlos en la fase de obtención del sistema.

Estos son los tipos de información enumerados por los intrusos:



* 1. **Técnicas de enumeración**

Existen muchas formas de recopilar datos, como los usuarios de la red, las tablas de enrutamiento y la información del protocolo simple de gestión de redes (SNMP).



<https://hlassets.paessler.com/common/files/blog/2017/snmp-1-fb.png>

A continuación, se analizan las posibles formas en que un atacante podría enumerar una red objetivo:



* 1. **Contramedidas**

Durante la enumeración se recoge, sistemáticamente, información y se identifican los sistemas individuales, los *pentesters* examinan los sistemas en su totalidad; esto permite evaluar las debilidades de seguridad que no necesariamente se derivan de un problema técnico.

Una protección con contraseña, técnicamente segura, puede, por ejemplo, resultar inútil si los atacantes pueden ver la entrada de la contraseña de un usuario a través de una ventana; durante la enumeración, los *pentesters* recogen información sobre posibles debilidades que se verifican o refutan durante la fase de explotación.

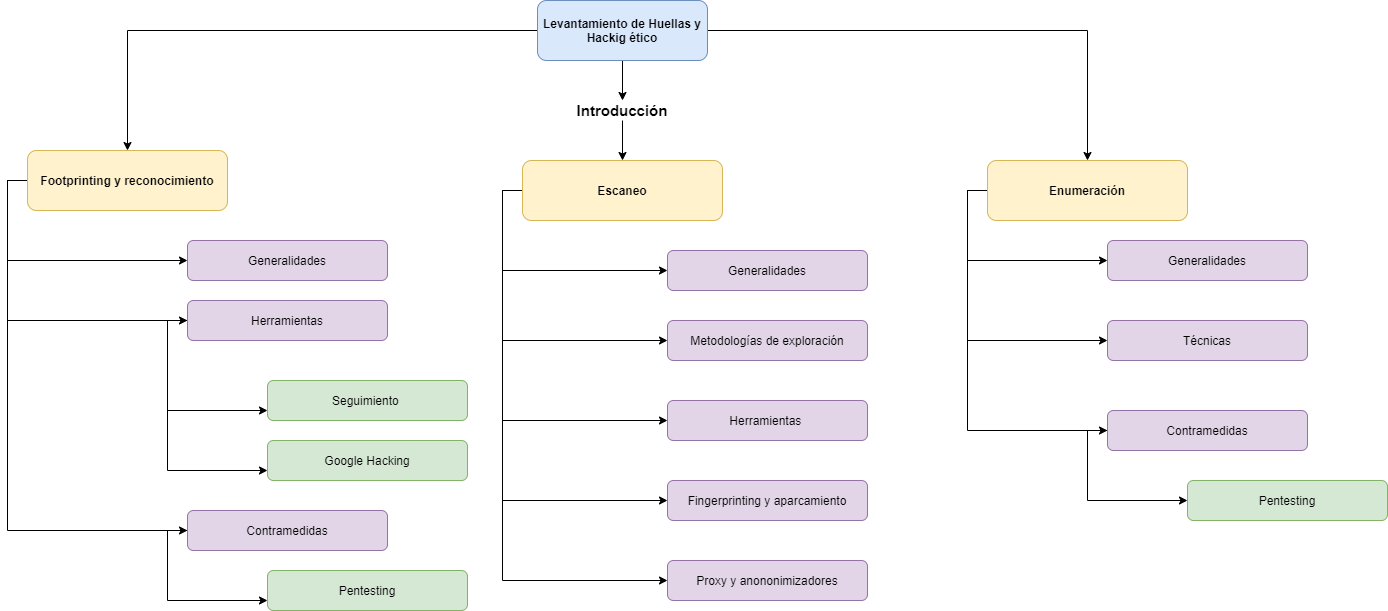


<https://cdn.pixabay.com/photo/2017/02/18/12/36/hacker-2077138_960_720.jpg>

*Pentesting* de enumeración:

* Encontrar el rango de red (utilizar herramientas como Whols Lookup y Graphical DNS Zones).
* Calcular la máscara de subred (utilizar herramientas como Subnet Mask Calculator).
* Realizar descubrimiento (utilizar herramientas como Nmap (nmap sP <network range>)).
* Realizar enumeración NetBIOS.
* Realizar enumeración DNS (utilizar herramientas como nslookup y The men y Mice Suite).
* Realizar análisis de puertos (utilizar herramientas como Nmap (mmap sS <network range>)).
* Utilizar herramientas como SuperScan, NetBIOS Enumerator y PsTools suite.

1. **SÍNTESIS**

****

1. **ACTIVIDADES DIDÁCTICAS**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Levantamiento de huellas y herramientas de *hacking* ético. |
| Objetivo de la actividad | Identificar los objetivos del *footprinting* y qué datos se pueden recoger las huellas según el tipo, para poder conocer vulnerabilidades de una organización. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | 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. Footprinting y reconocimiento | Wild IT Academy. (2021). *Footprinting.* [Video]. YouTube. <https://www.youtube.com/watch?v=ain4yOlpf3I> | Video - Clase | <https://www.youtube.com/watch?v=ain4yOlpf3I> |
| 2. Escaneo de redes y dispositivos | Ciberseguridad comprensible. (2020). *Maltego: ¿Qué es?, ¿para qué sirve y cómo usarlo?* [Video]. YouTube. <https://www.youtube.com/watch?v=cBjQt2EPFUs> | Video – Tutorial | <https://www.youtube.com/watch?v=cBjQt2EPFUs> |

1. **GLOSARIO**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Cifrado | esconder información, la cual se utiliza para proteger la estructura de los datos e información de una empresa o persona. |
| *Footprinting* | proceso de creación de un plano o mapa de la red y los sistemas de una organización. |
| Nmap | herramienta informática *opensource* (programa de código abierto) que se utiliza para escanear puertos de un sistema. |
| OSINT | (Open Source INTelligence, significa inteligencia de código abierto) se refiere a cualquier información que pueda ser legalmente obtenida de fuentes públicas y gratuitas. |
| *Pentesting* | pruebas de penetración, que consiste en atacar un sistema para encontrar vulnerabilidades y poder contrarrestarlas, las hay de caja blanca, negra y gris. |
| *Proxy* | programa que hace de intermediario entre los servicios y recursos de la red, trabaja bajo peticiones. |

1. **REFERENCIAS BIBLIOGRÁFICAS**

Borges, E. (2019). *Servidor FTP.* [Web log post]*.* <https://blog.infranetworking.com/servidor-ftp/>

Borges, S. (2019). *Servidor Web*. [Web log post]*.* <https://blog.infranetworking.com/servidor-web/>

Caballero, A. (2015). *Introducción a OSSTMM*. [Web log post]. Reydes*.* <http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual>

Castillo, J. (2018). *Active Directory qué es y para qué sirve*. [Web log post]. Profesionalreview*.* <https://www.profesionalreview.com/2018/12/15/active-directory/>

Echeverry, J. (2009). *Metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada.* Semanticscholar. <https://pdfs.semanticscholar.org/60c7/dbe2abab31a25422c92ead74085fd7093715.pdf>

Gaviria, R. (2015). *Guía práctica para pruebas de pentest basada en la metodología OSSTMM V2.1 y la guía OWASP V3.0.* Unilibrepereira.

Instituto Nacional de Ciberseguridad (2017). *Amenaza vs. vulnerabilidad, ¿sabes en qué se diferencia?* Incibe. <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>

Martínez, E. (2018*). Las diferentes amenazas de seguridad informática*. Sites.google. <https://sites.google.com/site/lasamenazaslainformatica/>

Zuluaga, A. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia.* Unad. <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Pedro Javier Lozada Villota | Experto Temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Diciembre de 2021 |
| Alix Cecilia Chinchilla Rueda | Diseñadora Instruccional | Regional Distrito Capital - Centro de Gestión Industrial | Diciembre de 2021 |
| Fabián Leonardo Correa Díaz | Diseñador Instruccional | Regional Tolima - Centro agropecuario La Granja | Diciembre de 2021 |
| Andrés Felipe Velandia Espitia | Revisor Metodológico y Pedagógico | Regional Distrito Capital – Centro de Diseño y Metrología | Diciembre de 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor Pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura | Diciembre de 2021 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica. | Diciembre del 2021. |

1. **CONTROL DE CAMBIOS**

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