UNIVERSIDAD HISPANOAMERICANA

INGENIERÍA INFORMÁTICA

PROYECTO DE INVESTIGACIÓN PARA OPTAR POR EL GRADO DE BACHILLERATO EN LA CARRERA DE INGENIERÍA INFORMÁTICA

PROPUESTA PARA EL MEJORAMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL CECI DE SAN JUAN DE SANTA BÁRBARA DE HEREDIA

SUSTENTANTE:

EDGAR VARGAS ALPÍZAR

DIRECTOR:

ROBERTO ROMERO POVEDA

MARZO, 2019

Índice de contenido

Índice de tablas

Índice de ilustraciones

Declaración jurada

DECLARACIÓN JURADA

Yo Edgar Alfonso Vargas Alpízar, mayor de edad, portador de la cédula de identidad número 1-1285-0374 egresado de la carrera de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Bachiller en Ingeniería Informática, juro solemnemente que mi trabajo de investigación titulado: Propuesta para el mejoramiento de la Infraestructura Informática del CECI de San Juan de Santa Bárbara de Heredia, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior, firmo en la ciudad de San José, a los 18 días del mes de marzo del año 2019.

Firma del estudiante
Cédula 1-1285-0374

Carta de aprobación del Tutor

San José, 17 de marzo de 2019

Ing. Marylin Arias Soto

Ingeniería Informática

Universidad Hispanoamericana

Estimada Señora:

El estudiante Edgar Vargas Alpízar, cédula 1-1285-0374, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado Propuesta para el mejoramiento de la Infraestructura Tecnológica del CECI de San Juan de Santa Bárbara de Heredia, el cual ha elaborado para optar por el grado académico de Bachillerato en Ingeniería Informática.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

Rubro	Valor	Puntaje obtenido
a. Originalidad del tema	10%	10%
b. Cumplimiento en la entrega de avances.	20%	20%
c. Coherencia entre los objetivos, los instrumentos aplicados y los resultados de la investigación	30%	30%
d. Relevancia de las conclusiones y recomendaciones	20%	20%
e. Calidad, detalle del marco teórico.	20%	20%
Total	100 %	100%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

MSc. Roberto Romero Poveda

Máster en Proyectos

Cédula 1-0996-0505

Carta de aprobación del lector

CARTA DE LECTOR

Universidad Hispanoamericana
Sede Heredia
Carrera Ingeniería Informática

Estimada Jessica

El estudiante Edgar Vargas Alpízar, cédula de identidad: 1-1285-0374, me ha presentado la Tesina para efectos de revisión y aprobación, denominada "**PROPUESTA PARA EL MEJORAMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL CECI DE SAN JUAN DE SANTA BÁRBARA DE HEREDIA** ", el cual ha elaborado para obtener su grado de Bachillerato en Ingeniería Informática.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. Así mismo, se realizaron las modificaciones solicitadas a nivel de contenido y forma.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.
Atte.

Firma

Nombre Ing. Luis Navarro S

Cédula 2-0484-0537

Constancia de revisión filológica

Constancia de revisión filológica

Heredia, 18 de mayo de 2019

Señores:
Universidad Hispanoamericana
Ingeniería Informática

Estimados señores:

Se han revisado y corregido errores gramaticales, de puntuación, ortográficos y de estilo, que se manifiestan en el documento escrito de un proyecto de graduación. Se ha verificado que estos fueron corregidos por el autor.

Título del proyecto: *PROPUESTA PARA EL MEJORAMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA DEL CECI DE SAN JUAN DE SANTA BÁRBARA DE HEREDIA*

Sustentante: Edgar Vargas Alpízar

Título académico por el que se opta: Bachillerato en Ingeniería Informática

Este Trabajo Final de Graduación cumple con los requisitos formales exigidos por la Universidad.

Atentamente,

Sandra M. Aguilar M.

Bachiller Sandra María Aguilar Molina
Cédula. 401350928
Carné de Colegio de Licenciados y Profesores en Letras, Filosofía, Ciencias y Arte # 9605
Asociación Costarricense de Filólogos # 246
Correo: sandraaguilar2009@gmail.com
Teléfonos: 22380346/ 70674854

Carta de autorización para licencia

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 24 de Julio 2019

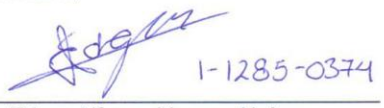
Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Edgar Alfonso Vargas Alpízar con número de identificación 1-1285-0374 autor (a) del trabajo de graduación titulado: **Propuesta para el mejoramiento de la infraestructura tecnológica del CECI de San Juan de Santa Bárbara de Heredia** presentado y aprobado en el año 2019 como requisito para optar por el título de Bachillerato en Ingeniería Informática; SI autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,



Edgar Alfonso Vargas Alpízar

Dedicatoria

Primero que todo a Dios, quien siempre me dio la fuerza y esperanza de que realizar este escrito era posible, a mi esposa Andrea Vázquez quién estuvo conmigo a cada segundo de este proceso. Y por último a mis papás y familia, de quienes siempre tuve el apoyo y palabras de aliento para seguir adelante.

Agradecimientos

A Dios, porque a pesar de nuestros errores, nunca nos abandona y siempre nos sorprende con sus bendiciones.

A mi esposa Andrea Vásquez Saénz, por demostrarme su amor de tantas maneras distintas, por no dejarme caer en los momentos de desesperanza, y ser un ejemplo de lucha, trabajo y perseverancia.

A mis papás y hermanos, gracias por su amor, palabras de apoyo y hacer de mi vida, una mejor vida.

Al resto de mi familia y amigos, quienes siempre tuvieron palabras de apoyo; siempre que necesité ayuda, ahí estuvieron.

A mis compañeros de ASECCSS, por brindarme su colaboración y apoyo durante el proceso el desarrollo y culminación de este proyecto.

Abreviaturas

ADI: Asociación de Desarrollo Integral.

ADSL: Asymmetric Digital Subscriber Line

ASECCSS: Asociación Solidarista de Empleados de la Caja Costarricese del Seguro Social.

CECI: Centro Comunitario Inteligente.

DHCP: Dynamic Host Configuration Protocol.

DINADECO: Dirección Nacional de Desarrollo de la Comunidad.

DNS: Domine Name Server.

GB: Gigabyte

GUI: Graphical User Interface

ICE: Instituto Costarricense de Electricidad.

IDI: Índice de Desarrollo TIC.

ISO: International Organización of Standardization.

LAN: Local Area Network.

LCD: Liquid Cristal Display

MAN: Metropolitan Area Network.

MICITT: Ministerio de Ciencia, Tecnología y Telecomunicaciones.

MIDEPLAN: Ministerio de Planificación Nacional y Política Económica.

MTSS: Ministerio de Trabajo y Seguridad Social.

NUC: Next Unite of Computing

OEA: Organización de los Estados Americanos.

ONG: Organización No Gubernamental

PNDT: Plan Nacional de Desarrollo de las Telecomunicaciones.

PROSIC: Programa sociedad de la información y el conocimiento.

RAM: Random Access Memory

SINABI: Sistema Nacional de Bibliotecas.

SUTEL: Superintendencia de Telecomunicaciones.

TB: Terabyte

TCU: Trabajo Comunal Universitario.

TIC: Tecnologías de la información y la comunicación.

UNED: Universidad Estatal a Distancia.

UNESCO: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

UPS: Uninterruptible Power Supply

USB: Universal Serial Bus

WAN: Wide Area Network.

WLAN: Wireless Local Area Network.

Resumen

El presente documento es el informe del trabajo final de graduación para optar por el grado de bachillerato en Ingeniería Informática, el cual plantea una propuesta para el mejoramiento de la infraestructura tecnológica del Centro Comunitario Inteligente (CECI) de San Juan de Santa Bárbara de Heredia.

Los CECI son un proyecto del Departamento de Promoción Social de la Ciencia, Tecnología e Innovación del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), el cual se desarrolla en articulación con actores locales como lo son las asociaciones de desarrollo. Constituyen laboratorios ubicados en distintos puntos del país equipados con computadoras de última tecnología, ofreciendo así diversos servicios a la comunidad, en este caso la de San Juan de Santa Bárbara de Heredia.

El acercamiento al CECI de San Juan de Santa Bárbara de Heredia, así como el diagnóstico administrativo y técnico develaron que dicho laboratorio cuenta con equipo de cómputo, pero el mismo no tiene una configuración de red que los mantenga unidos a un dominio común. Esto se asocia a la ausencia de un servidor y ocasiona debilidades en la seguridad informática del centro.

Por lo tanto, se plantea como objetivo general del trabajo final de graduación: Fortalecer el CECI de San Juan de Santa Bárbara de Heredia mediante la propuesta de un plan de infraestructura y seguridad informática con el fin de mejorar el control, acceso y seguridad digital de los usuarios.

Para ello se propone la configuración de la red alámbrica (área de cobertura, configuración y topología). Además, se plantea una propuesta para la implementación y configuración de un servidor que mejore la administración de los permisos y accesos de los usuarios.

También se describen los requerimientos básicos de seguridad informática para la red y se brindan lineamientos de seguridad informática (control, acceso y registro) para el uso de los equipos del CECI.

Se considera que la propuesta significa un mejoramiento en el funcionamiento del laboratorio, ya que se mejora la comunicación entre los equipos, se aumenta la seguridad informática y se garantiza el desarrollo de las mejores prácticas.

CAPÍTULO I: PROBLEMA DEL PROYECTO

CAPÍTULO I: PROBLEMA DEL PROYECTO

1.1 ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

1.1.1 Antecedentes del contexto de la organización

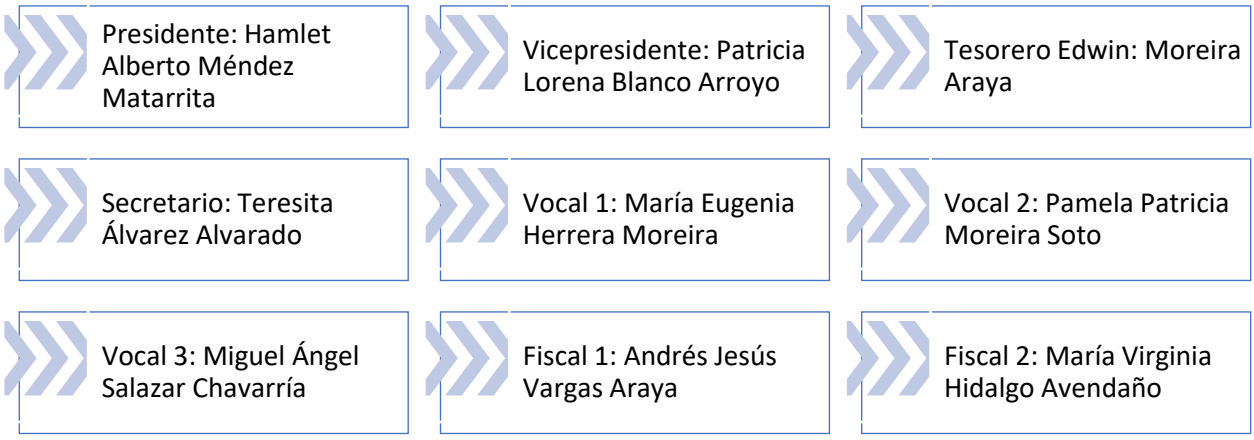
Este apartado hace referencia a la contextualización del Centro Comunitario Inteligente (CECI) de San Juan de Santa Bárbara de Heredia, así como el proyecto que se desarrolló como parte del Trabajo Final de Graduación.

El Centro Inteligente de San Juan de Santa Bárbara de Heredia se encuentra al Costado Oeste de la Plaza de Deportes, Edificio Color Beige. Actualmente, este Centro Inteligente está a cargo de la Asociación de Desarrollo Integral de San Juan de Santa Bárbara (ADI) (MICITT, 2019).

La ADI de San Juan de Santa Bárbara de Heredia fue constituida el 23 de noviembre de 1975. Según registros de DINADECO (2019), tiene vigente su personería jurídica hasta el día 6 de marzo de 2020.

Actualmente su Junta Directiva está conformada por:

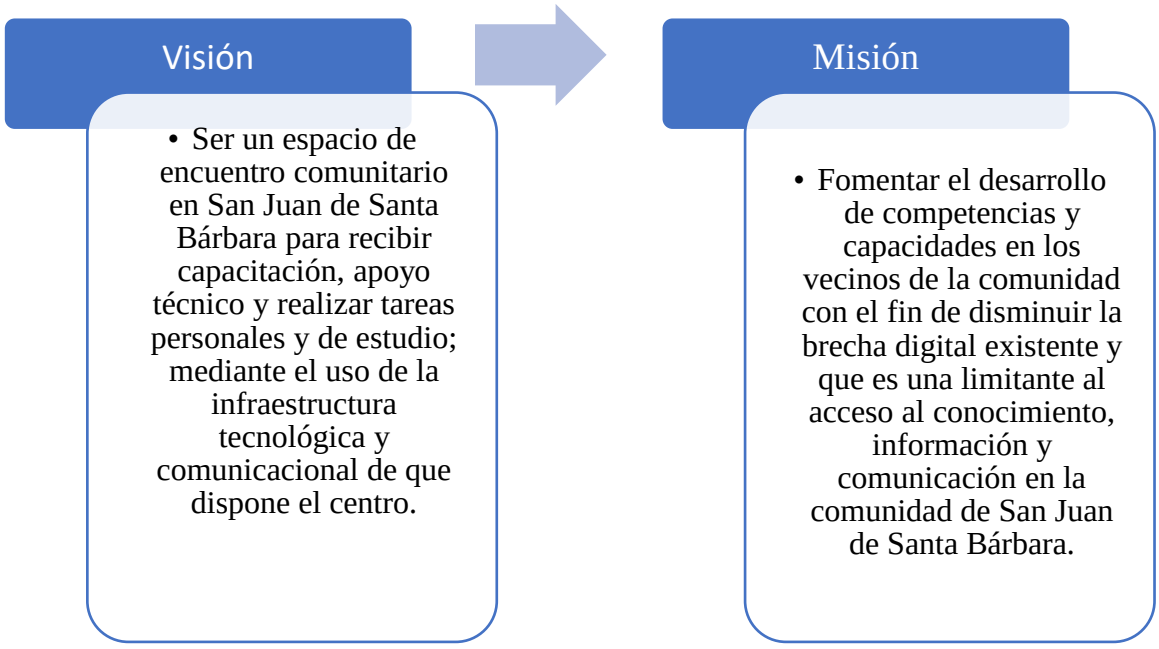
Figura 1: Conformación de la Junta Directiva de la ADI de San Juan de Santa Bárbara de Heredia.



Fuente: elaboración propia.

La misión y la visión de la institución se detallan a continuación:

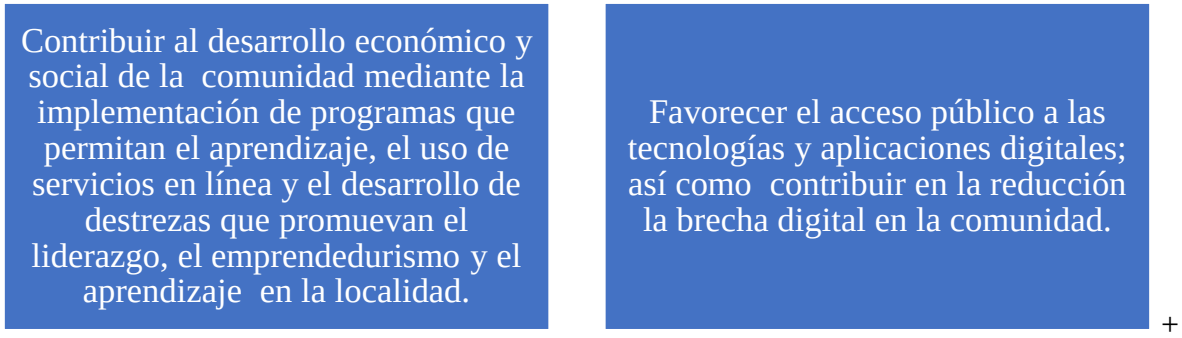
Figura 2: Visión y Misión de la ADI San Juan de Santa Bárbara de Heredia.



Fuente: elaboración propia.

A partir de estos principios orientadores plantean como objetivos los siguientes:

Figura 3: Objetivos ADI San Juan de Santa Bárbara de Heredia.



Fuente: elaboración propia

Las ADI tienen su fundamento en el artículo 16 de la Ley No.3859; el cual indica que las asociaciones constituyen un grupo de personas cuyo interés será el de promover, mediante el esfuerzo conjunto y organizado, el desarrollo económico y el progreso social y cultural de un área determinada del país.

De igual manera, en el artículo 18 de la misma Ley, indica que las asociaciones de desarrollo están obligadas a coordinar sus actividades con las que realice la municipalidad del cantón respectivo, a fin de contribuir con su acción al buen éxito de las labores del organismo municipal y obtener su apoyo.

Lo anterior nos permite afirmar que las ADI deben de articular sus esfuerzos y proyectos a las actividades de desarrollo comunitario que planté la municipalidad de la zona en la cual se encuentra; en el caso de la ADI de San Juan de Santa Bárbara de Heredia debe contribuir al Plan de Desarrollo Humano Local 2010-2020 de la municipalidad (Municipalidad Santa Bárbara, 2009).

Los objetivos estratégicos de dicho plan son los siguientes:

- Desarrollo económico sostenible

- Desarrollo social
- Seguridad Humana
- Educación
- Servicios Públicos
- Gestión Ambiental y ordenamiento territorial
- Infraestructura

Algunos de los objetivos específicos directamente relacionados con el interés de la ADI de Santa Barbara de tener un CECI son los siguientes:

- **Desarrollo económico sostenible**:

  Promover la capacitación de las personas, especialmente jóvenes y mujeres, para participar de la diversificación y mejoramiento de las actividades productivas y de servicios en el cantón. Algunas de las líneas de acción de este objetivo son las siguientes:

  - Capacitar a mujeres jefas de hogar, y jóvenes para su adecuada inserción en las actividades productivas del cantón.
  - Capacitar a la comunidad sobre la creación de microempresas de acuerdo con tecnologías actuales.
  - Apoyar la capacitación en la creación de agroindustria pequeña y mediana escala.

- **Desarrollo Social:**

  Promover el liderazgo comunitario en los adultos mayores para elevar la calidad de vida de sus habitantes.

Los CECI contribuyen a estos objetivos debido a que están pensados para promover el desarrollo socioeconómico de todas las regiones del territorio nacional mediante la alfabetización digital de

sus usuarios, además de que buscan el “empoderamiento” tecnológico de las comunidades por medio del acceso al conocimiento, la información, la creatividad y la capacidad para asumir nuevos retos.

Los CECI dan prioridad a la capacitación básica en el uso de Internet, aplicaciones, correo electrónico, inglés, video conferencias, temario para pymes, entre otros.

Actualmente el CECI de San Juan de Santa Bárbara de Heredia cuenta con 16 equipos de cómputo funcionales y un servicio de internet inalámbrico. Además de equipos de red y un servidor que no están siendo utilizados.

De modo que se requiere optimizar el uso de los equipos para los cursos y capacitaciones que ahí se imparten, mediante la organización y configuración de las computadoras, servidor y equipos de red disponibles.

1.1.2 Justificación del proyecto

Regueyra (2001) indica que: el avance de la sociedad ha sido producto del conocimiento del ser humano, de ahí que, para lograr el desarrollo económico y social de un país, se debe socializar el conocimiento generado, promover la investigación científica y la innovación, así como el uso de tecnologías de punta, lo que le permitirá no solo alcanzar niveles de desarrollo económico, sino también el bienestar de su población.

Por lo tanto, con la propuesta de este proyecto se espera mejorar los servicios tecnológicos que brinda el CECI a los miembros de su comunidad, tanto en materia de seguridad de sus datos e

información mientras utilizan los equipos; como en la disponibilidad de los recursos y servicios disponibles, facilitando así que más personas puedan ser capacitadas en diferentes áreas de la tecnología, lo cual aumentará en gran medida las posibilidades de empleo en las personas capacitadas o que puedan comenzar su propio proyecto de emprendedurismo.

De igual manera, al rediseñar la infraestructura tecnológica con procesos, políticas y mejores prácticas con respecto al manejo que se le da al laboratorio mejorarán, el registro y control de ingreso a las computadoras, seguridad de los datos e información de los usuarios, control y filtrado web, seguridad y optimización de la red.

Otro problema que se subsanará con el presente proyecto es el riesgo de robo de información confidencial. El robo de información confidencial puede afectar a cualquier persona, no sólo a grandes empresas o corporaciones; se han dado varios casos a nivel mundial de acceso a la información personal de manera ilícita, como, por ejemplo: hackeo de cuentas de correo, cuentas de almacenamiento en la nube o redes sociales, lo que provoca en muchos casos, chantajes, extorsión o el simple hecho de borrar información importante para el usuario.

Es importante señalar que mediante el Plan Nacional de Desarrollo y de Inversión Pública 2019 – 2022 (MIDEPLAN, 2018), se evidencia el interés del gobierno de fortalecer la oferta en formación y capacitación para reducir la brecha digital de acceso, uso y apropiación de las tecnologías de la información y la comunicación (TIC), así como promover la formación de jóvenes en la alfabetización digital mediante la creación de espacios de acercamiento como los CECI.

Por otro lado, el PROSIC coloca como uno de los principales desafíos: “impulsar y desarrollar la ciencia y a tecnología, y elevar la calidad de la formación profesional, ya que en el país y en la región los indicadores muestran grandes diferencias respecto a los países desarrollados” (2007, pág. 200).

1.2 DEFINICIÓN DEL PROBLEMA

Los Centros Comunitarios (CECI) son un proyecto del Departamento de Promoción Social de la Ciencia, Tecnología e Innovación del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT).

Constituyen laboratorios ubicados en distintos puntos del país equipados con computadoras de última tecnología, ofreciendo así diversos servicios a la comunidad.

“Estos centros permiten promover el desarrollo socioeconómico de todas las regiones del territorio nacional mediante la alfabetización digital de sus usuarios. En esencia, los CECI buscan el "empoderamiento" tecnológico de las comunidades por medio del acceso al conocimiento, la información, la creatividad y la capacidad para asumir nuevos retos” (MICITT, 2019).

Según el MICITT, actualmente existen unos 200 CECI operando en el país, los cuales brindan una oferta variada de cursos y cuentan con un número disímil de computadoras. No obstante, su funcionamiento no ha sido optimo; desde 2007 que se inició con la implementación y el equipamiento de 136 CECI, tal número ha variado considerablemente, ya que para el 2014 se tenían 253, y durante el 2015 se preveía el cierre o reubicación de unos 40 centros.

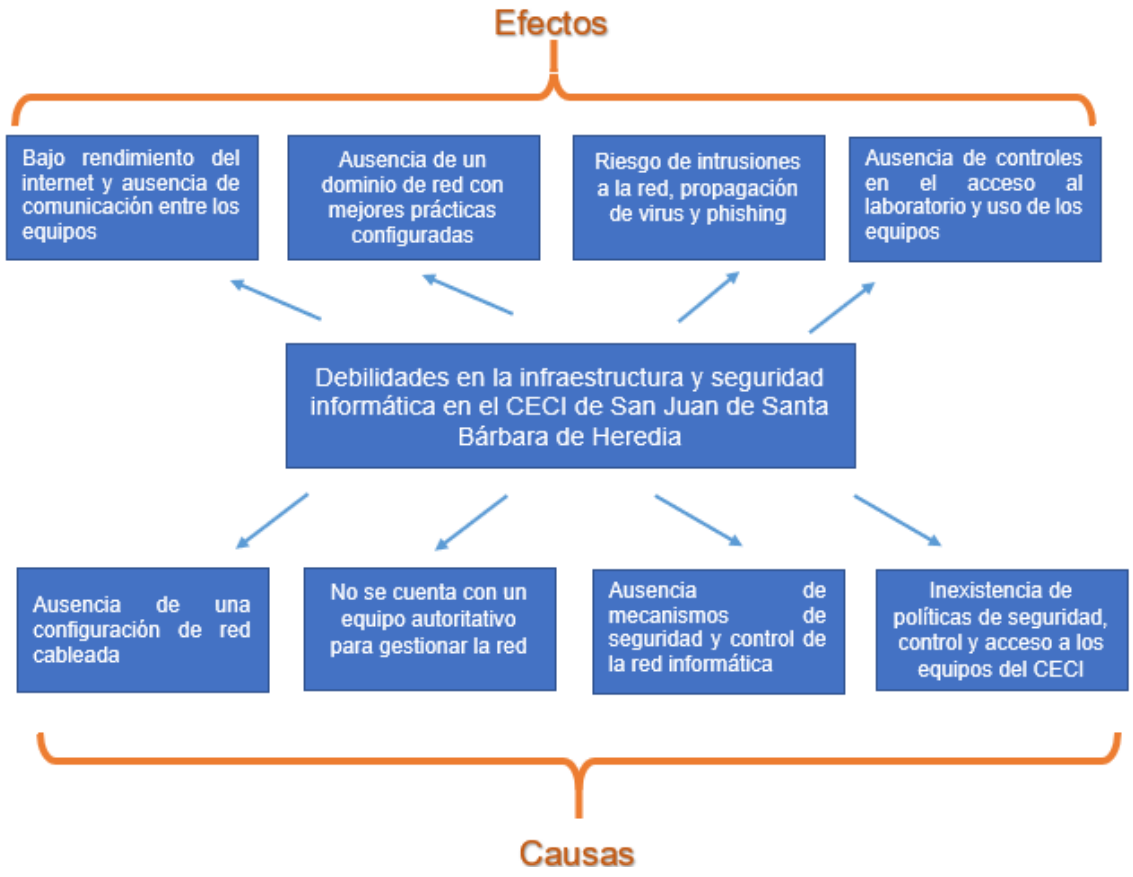
El presente proyecto final de graduación se va a desarrollar en el CECI de San Juan de Santa Bárbara de Heredia, el cual está a cargo de la Asociación de Desarrollo de la Comunidad.

Dicho CECI cuenta con equipo o terminales de cómputo, sin embargo, no cuenta con una red local que comunique los equipos entre sí o los mantenga unidos a un dominio común.

Además, se cuenta con un servidor donado por la UNESCO, al cual no se le está dando ningún uso actualmente, y se planea utilizar para brindar mayor seguridad a la red y alojamiento de archivos o sitios web. Por lo tanto, no se cuenta con protocolos o políticas de seguridad para el correcto uso y funcionamiento de los equipos.

Lo anterior, se configura en una situación problema que debe ser atendida por los efectos que puede ocasionar. La siguiente ejemplifica lo descrito:

Figura 4: Diagrama de causa y efectos



Fuente: Elaboración propia

Con ayuda del diagrama causa y efecto anterior se puede apreciar que el problema principal son las debilidades en la infraestructura y seguridad informática del CECI de San Juan de Santa Bárbara de Heredia.

Entre las causas de este problema se encuentran que: no se tienen establecidos los requerimientos de seguridad básicos para la red inalámbrica, no se cuenta con una arquitectura para el uso óptimo del equipo de cómputo y del servidor, ni tampoco con la configuración del servidor, ni con políticas de seguridad, control y acceso a los equipos del CECI.

Lo anterior ocasiona: riegos de intrusiones, debilidades en el control y seguridad del acceso, ausencia de un dominio de red con directiva configurada y posibles pérdidas de la información.

Todo esto permite que el presente proyecto se aboque al:

Fortalecimiento del CECI de San Juan de Santa Bárbara de Heredia mediante la propuesta de un plan de seguridad informática con el fin de mejorar el control, acceso y seguridad digital de los usuarios.

1.3 OBJETIVOS DEL PROYECTO

1.3.1 Objetivo general

Fortalecer el CECI de San Juan de Santa Bárbara de Heredia mediante la propuesta de un plan de infraestructura y seguridad informática con el fin de mejorar el control, acceso y seguridad digital de los usuarios.

1.3.2 Objetivos específicos

- Proponer la configuración de la red alámbrica (área de cobertura, configuración, y topología) del CECI San Juan de Santa Bárbara.
- Elaborar la propuesta para implementación y configuración de un servidor (grupos de usuarios, roles, dominio) que mejore la administración de los permisos y accesos a usuarios.
- Describir los requerimientos básicos de seguridad informática para la red y equipos del CECI.
- Plantear políticas de seguridad informática (control, acceso y registro) para el uso de los equipos del CECI.

1.4 ALCANCES Y LIMITACIONES

1.4.1 Alcances

- El primer entregable es un diseño de red donde se contempla cada uno de los computadores y equipos de red disponibles para un uso óptimo del laboratorio del CECI San Juan de Santa Bárbara.
- El segundo entregable es una propuesta para la implementación y configuración de un servidor, así como un dominio común que mejore la administración de permisos, roles y accesos.

- El tercer entregable son recomendaciones para la configuración, control, acceso y filtrado de la red, utilizando un software o dispositivos existentes en el mercado actual.
- El cuarto entregable es un documento con lineamientos y políticas de seguridad que incluyen: control, acceso y registro a los equipos del laboratorio e instalaciones del CECI.

1.4.2 Limitaciones

- Una limitación sería la capacidad presupuestaria del CECI, esto no solamente para la implementación de la infraestructura tecnológica sino también para la adquisición de las licencias de software y su mantenimiento, de allí que el proyecto debe ajustarse a estas limitaciones.
- Una segunda limitación serían las restricciones a nivel de modificaciones en el edificio o sus inmuebles, por ejemplo: agujeros en las paredes o muebles, clavos o tornillos en paredes, canaletas en techo, paredes o suelo.
- Una tercera limitación es la conexión a internet que tiene el CECI con su proveedor actual, específicamente en cuanto a velocidad, ancho de banda y latencia del servicio.

1.5 Cronograma de Actividades

A continuación, se presente el cronograma de actividades, según las diferentes etapas del proyecto.

Tabla 1: Cronograma de actividades

Actividad	Inicio	Fin
Etapa 1: Elaboración de la Propuesta	2/07/18	6/08/18
Capítulo I: Planteamiento del problema	2/07/18	8/07/18
Antecedentes y justificación del proyecto	9/07/18	15/07/18
Definición del problema	16/07/18	22/07/18
Objetivos generales y específicos	23/07/18	29/07/18
Alcances y limitaciones	30/07/18	5/08/18
Entrega de la propuesta	6/08/18	6/08/18
Etapa 2: Desarrollo del Proyecto	24/09/18	3/03/19
Capítulo II: Marco Teórico	24/09/18	7/10/18
Elaboración de marco teórico	8/10/18	21/10/18
Correcciones de marco teórico	22/10/18	4/11/18
Capítulo II: Marco metodológico	5/11/18	18/11/18
Elaboración de marco metodológico	19/11/18	2/12/18
Correcciones de marco metodológico	3/12/18	16/12/18
Capítulo IV: Diagnóstico de la situación actual	17/12/18	30/12/18
Desarrollo del diagnóstico de la situación actual	31/12/18	13/01/19
Análisis de la situación actual	14/01/19	20/01/19
Capítulo V: Propuesta del proyecto	21/01/19	3/02/19
Desarrollo de la propuesta de proyecto	4/02/19	3/03/19
Etapa 3: Elaboración de Conclusiones	4/03/19	18/03/19
Capítulo VI: Conclusiones y recomendaciones	4/03/19	10/03/19
Desarrollo de conclusiones y recomendaciones	11/03/19	17/03/19
Entrega del proyecto	18/03/19	18/03/19

Fuente: Elaboración propia

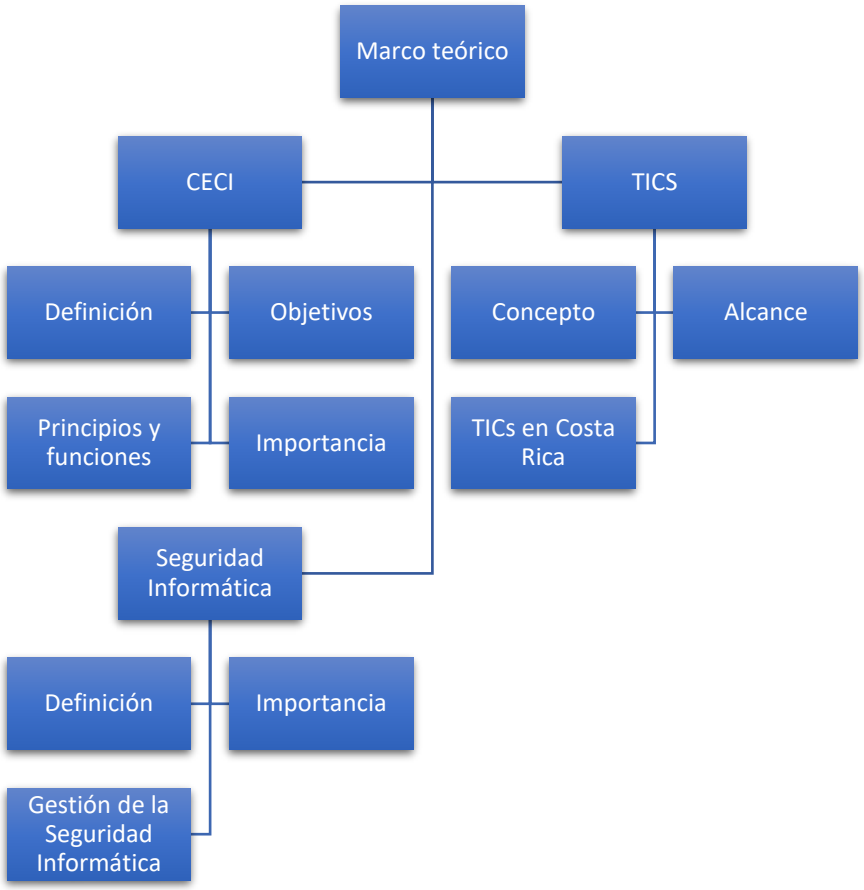
CAPÍTULO II: MARCO TEÓRICO

CAPÍTULO II: MARCO TEORICO

El marco teórico según Barrantes (2012) cumple la función fundamental de dar sustento teórico a la investigación ya que explica las relaciones entre las variables que componen el problema, tiene como objetivo ubicar el objeto de estudio dentro del conjunto de las teorías existentes.

El siguiente mapa conceptual ilustra las categorías teóricas y conceptuales que componen el presente apartado y que permitirán comprender el problema de estudio y su abordaje:

Figura 5: Esquema del marco teórico conceptual



Fuente: Elaboración propia.

Como se observa en la imagen el presente marco teórico está compuesto por tres conceptos centrales a saber: Centros Comunitarios Inteligentes (CECI), Tecnologías de la Comunicación y la Información (TIC) y Seguridad Informática. Estos conceptos están interrelacionados y son interdependientes; su comprensión permite construir cada una de las etapas del proyecto y alcanzar los objetivos.

El concepto central es el de Centro Comunitario Inteligente (CECI) por lo tanto se debe conocer su definición, objetivos, principios y funciones y la importancia de este.

El segundo concepto son las Tecnologías de la Comunicación y la Información (TIC) las cuales de una u otra forma son las que motivan el surgimiento de los CECI; su avance hace que se deba trabaja en la inclusión digital y el cierre de la brecha digital, objetivos para los cuales los CECI aportan. Sobre las TIC y relacionadas al problema del proyecto se debe conocer su definición, alcance y el estado actual de desarrollo en Costa Rica.

Finalmente, e interrelacionado a los conceptos anteriores, se encuentra la categoría de Seguridad Informática, en ella se analizará la definición, importancia y elementos para su gestión.

2.1 Centros Comunitarios Inteligentes (CECI)

El primer concepto que se abordará es el de Centros Comunitarios Inteligentes por la centralidad que tiene en el problema de estudio. El Ministerio de Ciencia, Tecnología y Telecomunicaciones, define los CECI como un centro dirigido a promover el desarrollo socioeconómico mediante la alfabetización digital de los usuarios a través del empoderamiento tecnológico.

Es un programa del estado costarricense que se inserta dentro del objetivo del milenio de inclusión y cierre de la brecha digital.

La inclusión digital se comprende como el acceso, uso y apropiación social de las tecnologías digitales para atender las necesidades de las comunidades. De esta manera, la inclusión digital contribuye a mejorar las condiciones económicas, sociales, políticas y personales de la población (Delgadillo, Gómez, & Sotll, 2002).

CECI es la nomenclatura que en el país se ha utilizado para caracterizar lo que en América Latina se conoce como Telecentros Comunitarios. Por lo anterior, se utilizan los contenidos teóricos de los telecentros para comprender mejor lo relacionado a los CECI en Costa Rica.

Existen diferentes definiciones para Telecentro o CECI una de ellas establece que:

Los telecentros son lugares de encuentro, aprendizaje y comunicación donde se ofrecen el uso de las nuevas tecnologías de información y comunicación, TIC, como medios para el fortalecimiento y la gestión de iniciativas encaminadas a mejorar las condiciones de vida de las comunidades (Carrión, 2014, pág. 289)

De este modo, se configuran como una herramienta para el empoderamiento de las personas que hacen uso de los servicios, a la vez que apoyan el desarrollo comunitario y la inclusión digital. Esto implica que puedan proveer servicios de información económicamente accesibles para la población, con contenidos pertinentes a la comunidad (Contreras, Varas, & Hojman, 1999).

Delgadillo, Gómez y Stoll (2002) explican que en América Latina y el Caribe existen diferentes tipos de telecentros, en los que se combinan diversas tecnologías digitales avanzadas con conectividad de banda ancha a los servicios de Internet. Algunos de ellos operan en escuelas, casas

de la cultura, u organizaciones comunitarias, como es el caso del CECI de San Juan de Santa Bárbara de Heredia.

Su énfasis es el uso social y la apropiación de las herramientas tecnológicas en función de un proyecto de transformación social para mejorar las condiciones de vida de las personas de la comunidad.

Los telecentros son lugares de encuentro e intercambio, espacios de aprendizaje, crecimiento personal, y movilización para resolver problemas y necesidades de la comunidad (Delgadillo, Gómez, Stoll 2002).

Con base a lo anterior, los autores mencionados destacan los siguientes principios básicos para los CECI:

Tabla 2: Principios básicos de los Centros Comunitarios Inteligentes

Participación de la comunidad
Consolidación de una visión social, de modo que se integren a otros espacios y actividades.
Gestión y utilización de tecnologías apropiadas
Formación y capacitación permanente

Fuente: Elaboración propia a partir de Delgadillo, Gómez, Stoll (2002)

Estos principios son los que determinan la importancia de los CECI, ya que garantizan su contribución al desarrollo personal y comunitario. Al respecto, Delgadillo, Gómez y Stoll (2002) destacan el aporte de dichos centros:

Tabla 3: Beneficios y aportes de los Centros Comunitarios Inteligentes

Empleo y microempresa	**Fortalece habilidades y conocimientos que abren nuevas puertas a empleo o a la generación de ingresos propios.**
Salud	Facilita el acceso a información sobre enfermedades y salud.
Educación	Apoya las actividades escolares y contribuye a la educación no formal.
Fortalecimiento de la autoestima	Ayuda a reconocer las capacidades propias, a visualizar un mejor futuro, a desarrollar la creatividad y a fortalecer el trabajo en equipo.
Organización comunitaria	Propicia la construcción de nuevas formas de organización, fortaleciendo las capacidades individuales y colectivas, promoviendo nuevos líderes y ayudando a solucionar problemas y necesidades concretas en la comunidad.
Descentralización e incidencia política	Dinamiza la participación comunitaria y la información para la incidencia política, facilita la comunicación con gobiernos locales, fortalece la descentralización administrativa y la realización de trámites.
Información y conocimiento	Ofrece acceso a nuevas y más diversas fuentes de conocimiento e información y
Comunicación y cultura	Facilita la creación de diferentes formas de expresión artística y cultural, con el uso de las tecnologías de comunicación de utilidad para la comunidad.

Elaboración propia a partir de Delgadillo, Goméz y Stoll (2002).

A partir de esto, se puede afirmar que los CECI son aceleradores del desarrollo por su potencial para que la población se apropie de las tecnologías de la información y por lo tanto impulsen el crecimiento económico.

Jensen y Esterhuysen (2001) explican que el acceso público brinda la comunidad la posibilidad de utilizar tecnologías de computación y comunicación para explorar áreas de interés y ampliar capacidades.

2.2 Tecnologías de la Información y Comunicación (TIC)

Durante los últimos años se ha dado un gran crecimiento y desarrollo tecnológico en el mundo, con tanta incidencia que muchos la llaman “la sociedad de la información”; haciendo referencia al hecho de que la sociedad se mueve entorno a la información, siendo así la materia prima que sirve para la creación de empleos, carreras profesionales, insumos y bienes; así como la adaptación de los ya existentes (Belloch, 2012)

Este contexto, de desarrollo científico y tecnológico, produce avances en los en los ámbitos de la informática y las telecomunicaciones; generando lo que se conoce como Tecnologías de la Información y la Comunicación (TIC).

Para Belloch (2012) las TIC son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido).

Se desarrollan en torno a la informática, la microelectrónica y las telecomunicaciones de forma articulada, interactiva e interconectada lo que permite conseguir nuevas realidades comunicativas (Belloch, 2012)

Las TIC permiten almacenar, recuperar, procesar y compartir la información utilizando dispositivos electrónicos. Existen múltiples instrumentos electrónicos que se encuadran dentro del concepto de TIC, como, por ejemplo: los televisores, los celulares y las computadoras. Esto hace que las TIC se conviertan en un medio de inclusión o de exclusión social.

Sin lugar a duda, los medios más representativos de la sociedad actual son los ordenadores que permiten utilizar diferentes aplicaciones informáticas (presentaciones, aplicaciones multimedia, programas ofimáticos) y más específicamente las redes de comunicación, en concreto la Internet (Belloch, 2012).

De este modo, las computadoras se constituyen en uno de los dispositivos más populares y democratizados, ya que los gobiernos han gestionado su acceso en centros educativos, bibliotecas o bien centros comunitarios inteligentes.

2.2.1 Alcances de las TIC

Las Tecnologías de la Información y de la Comunicación (TIC) han impactado diversos ámbitos de la vida en sociedad, sus alcances y su contribución al desarrollo de los países es incontable. A

continuación, se enumerarán algunos elementos que permiten dar cuenta de la trascendencia de las TIC[1]:

1. Permiten superar la distancia y el tiempo ya que hacen que la información se mueva de manera rápida sin importar la distancia.
2. Permiten realizar de forma virtual acciones comerciales, financieras y de servicios de muy diversa índole, que hace unos años solamente se podían realizar de manera presencial.
3. Permite a las personas mantenerse informadas de acontecimientos a nivel mundial en tiempo real a través de la televisión, celulares, tabletas y computadores.
4. Innova los procesos educativos mediante la incorporación de recursos audiovisuales, el uso de multimedia y la internet.
5. Permite el acceso virtual a bibiotecas, revistas y libros, lo que democratiza el conocimiento.
6. Promueve la investigación cientifica y la innovación, lo que favorece el desarrollo económico y el bienestar de la población.

Todo lo anterior ejemplifica la importancia de las TIC y la necesidad de cerrar la brecha digital, ya que este tipo de tecnologías están inmersas en todos los ámbitos de la vida diaria y su alcance es cada vez mayor.

[1] A partir de PROSIC (2006)

2.2.2 Las TIC en Costa Rica

El Programa Sociedad de la Información y el Conocimento (PROSIC) de la Universidad de Costa Rica, en sus diversos informes señala que el país es pionero mundialmente en el desarrollo de infraestructura en telecomunicaciones y en la implementación de políticas públicas asociadas a la educación, la salud, la modernización de la economía y la productividad.

En el informe del 2018 se indica que Costa Rica, según los índices internacionales se encuentra entre los países más avanzados en el tema de las TIC en Latinoamérica; no obstante, también señala un estancamiento de los avances logrados indicando que el país se encuentra en un periodo de inmovilización respecto a otras economías que avanzan en materia de tecnología.

En el mismo informe se señala que para el 2017 un 96% de los hogares costarricenses tienen teléfono celular y un 69% servicio de Internet (valores que al 2010 eran de 74% y 24% respectivamente).

Estos datos, junto con la amplia cobertura, la relativa accesibilidad de los precios y el nivel educativo, entre otros factores, hacen que el país se encuentre entre los mejores de América Latina en el tema TIC. Sin embargo, cuando tomamos en cuenta el resto del mundo, aún tenemos mucho trayecto que recorrer, especialmente cuando en los índices internacionales como el IDI se ve un estancamiento en la posición del país que, si bien pasó del puesto 80 al 57 entre el 2010 y el 2015, entre el 2015 y el 2017 el país descendió al puesto 60, señalando pérdidas en condiciones de acceso y en habilidades ((PROSIC, 2018, pág. 178).

Ante este estancamiento, el gobierno costarricense diseñó el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 “Costa Rica: Una Sociedad Conectada”; el cual propone como visión: Transformar a Costa Rica en una sociedad conectada a partir de un enfoque inclusivo del

acceso, uso, apropiación de las tecnologías de información y las comunicaciones; de forma segura, responsable y productiva ((PNDT, 2015, pág. 49).

Para ello define la siguiente hoja de ruta:

1. Concretizar proyectos de acceso universal, servicio universal y solidaridad de las Telecomunicaciones/TIC.
2. Crear un entorno habilitador que permita la innovación de la radiodifusión sonora y televisiva hacia su digitalización.
3. Construir participativamente las bases del Modelo de Ciudades Digitales a través de un gobierno electrónico cercano.

Este plan se encontraba en consonancia con el plan nacional del gobierno anterior y probablemente se mantenga esta línea. De modo que, los pilares fundamentales del PNDT que son: Inclusión Digital, Economía Digital y Gobierno Electrónico y Transparente, están dirigidos a contribuir con los objetivos de desarrollo de reducir la pobreza, impulsar el desarrollo económico, combatir la corrupción y fortalecer la transparencia.

Este plan establece dentro de las políticas a desarrollar la promoción de la accesibilidad de las TIC y dentro de ella como plan piloto la accesibilidad universal en los CECI.

2.3 Seguridad Informática

La Seguridad Informática se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso a usuarios autorizados al sistema (Gómez, 2017)

También puede ser comprendidad desde una perspectiva más amplia como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable (Aguilera, 2010).

De este modo se puede sintetizar que la seguridad informática permite aumentar la fiabilidad de la seguridad, bloqueando operaciones no autorizadas através de configuraciones en sistemas, regulaciones y la educación de los encargados y usuarios.

Aguilera (2010) explica que un sistema informático está constituido por un conjunto de elementos físicos, lógicos y humanos. Dentro de los elementos físicos se encuentran el hardware, dispositivos y periféricos; los elementos lógicos son aquellos que tienen que ver con el software y los humanos con el personal que se encarga del manejo de los elementos anteriores.

La seguridad informática se vuelve primordial en los diversos servicios de la sociedad, como lo son los financieros, los controles de producción, el suminstro eléctrico, los medios de transporte, la sanidad y la administración pública, entre otros; ya que todos funcionan, dependen o están montados sobre sistemas y redes informáticas.

Goméz (2017) señala que la gran cantidad de ataques informáticos, virus y códigos malignos, que se distribuyen todos los días en la internet han generado un gran interés en temas de ciberseguridad

a nivel mundial, de ahí la gran importancia de implementar medidas de seguridad informática en toda organización, sin importar su actividad o tamaño.

Es tal la relevancia de la seguridad de la información que en la actualidad, que se ha regulado mediante normas ISO. La norma ISO/IEC 17799, define la seguridad de la información como la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

Goméz (2017) menciona que la seguridad de un sistema informático dependerá de diversos factores, entre los que se podrían destacar los siguientes:

- El grado de sensiblización sobre la necesidad de destinar recursos a la seguridad informática por parte de las personas responsables de la organización o institución.
- Los conocimientos, capacidades e implicación de los responsables del sistema informático.
- La formación y la responsabilidad de las personas usuarias de los sistemas.
- La correcta instalación, configuración y mantenimiento de los equipos.
- La limitación en la asignación de los permisos y privilegios de los usuarios.
- El soporte y actualización de hardware y software. de los fabricantes de hardware y software.
- El análisis e intervención de las amenazas externas e internas a la organización.
- La adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades específicas de la organización.

Como se observa son múltiples los factores que podrían potenciar o debilitar la seguridad informática, de allí la importancia de que las personas en los niveles gerenciales o de decisión implementen una adecuada gestión de la seguridad informática.

En este sentido la seguridad informática tiene como objetivos[2]:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal.

Para cumplir con estos objetivos toda organización o institución debe contemplar medidas de seguridad en los siguientes ámbitos[3]:

- Medidas administrativas: Son establecidas por la dirección de cada entidad mediante regulaciones y su cumplimiento es obligatorio por todo el personal hacia el cuál están dirigidas.
- Medidas de seguridad física: Incluye medios físicos, medios técnicos de detección y alarma y el personal que forma parte de las fuerzas especializadas.
- Medidas técnicas y lógicas: Generalmente implementadas por medio del uso de software y dispositivos, que pueden trabajar de forma individual o conjunta.

[2] Tomado de Gómez (2017).
[3] Elaborado a partir de (Doina, 2019).

- Medidas de seguridad de operaciones: Son procedimientos definidos que garantizan el cumplimiento de las regulaciones establecidas por cada entidad y las instancias superiores.
- Medidas legales: Disposiciones jurídicas y administativas, en donde se encuentran los deberes, derechos, funciones, atribuciones y obligaciones, tipos de violaciones y responsabilidades administrativas, civiles, penales u otras.
- Medidas educativas: Educación sobre la existencia de un Sistema de Gestión de Seguridad Informática y la participación conciente para el éxito de los objetivos planteados.
- Medidas de recuperación: Se establecen una vez que se tienen identificados los posibles incidentes o fallos que puedan causar afectación de los procesos informáticos.

Estas medidas se aplican mediante procedimientos de prevención, de detección y de recperación, lo que permite garantizar su cumplimiento, debido a que describen la secuencia de acciones que deben implementarse.

Los procedimientos de prevención tienen como objetivo evitar que una amenaza se materialice; los de detección identifican los indicios de una posible materialización de la amenaza o vulnerabilidad en el sistema; y finalmente, los de recuperación son las aciones que se deben ejecutar cuando la amenaza se ha materializado y hay una afectación total o parcial de los activos informáticos.

Cuando las amenzas se han materializado los impactos pueden resultar difíciles de evaluar, ya que además de los daños ocasionados a la información guardada en los equipos y dispositivos de red se deben considerar otras consecuencias como las siguientes:

- Horas de trabajo invertidas en las reparaciones y reconfiguración de los equipos y redes.
- Pérdidas ocasionadas por la indisponibilidad de diversas aplicaciones y servicios informáticos.
- Robo de información confidencial y su posible revelación a terceros no autorizados.
- Posible impacto en la imagen de la empresa ante terceros.
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que afrontar además responsabilidades legales y la imposición de sanciones administrativas.
- Utilización de los equipos y redes de una organización para llevar a cabo ataques contra las redes de otras empresas y organizaciones.
- Almacenamiento de contenidos ilegales en los equipos comprometidos.
- Utilización de los equipos de una organización para realizar envíos masivos de correo no solicitado.

La implantación de determinadas medidas de seguridad puede resultar incómoda para muchos usuarios del sistema o equipos, y por ello, resulta fundamental contemplar la adecuada formación y sensibilización de los usuarios para que estas medidas de seguridad se puedan implantar de forma efectiva (Gómez, 2017).

2.3.1 Gestión de la Seguridad de la Informática

Se define como la parte del sistema general de gestión que incluye la política, la estructura organizativa, los recursos necesarios, los procedimientos y procesos para implementar medidas de seguridad de la infromación en una organización (Gómez, 2017).

Es importante aclarar que aunque se cumplan con todas las tareas y procedimientos establecidos por la organización, los riesgos no pueden ser eliminados en su totalidad, pero sí pueden ser gestionados.

La gestión de la seguridad informática incluye un conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas, que determinan el modo en que se gestionan, se protejen y se distribuyen los activos y recursos, incluyendo la información que se maneja en la organización.

Es necesario tomar en consideración los siguientes aspectos[4]:

- Humanos: incluye la sensibilidad y formación, así como las obligaciones y responsabilidades del personal y usuarios. También considera acciones de control y supervisión.
- Tecnológicos: hace referencia a la selección, instalación, configuración y actualización de soluciones de Hardware y Software; así como la estandarización de productos.
- Organizacionales: se refiera a las políticas, normas y procedimientos; además, planes de contingencia y respuesta a incidentes.
- Legales: significa el cumplimiento de las políticas, normas y procedimientos.

[4] Elaborado a partir de Gómez (2017).

Aunado a lo anterior la norma ISO/IEC 17799 establece la importancia de identificar los requerimientos de seguridad en 3 fuentes principales:

a) Evaluación de los riesgos para la organización: se debe identificar amenazas para los activos y evaluar la vulnerabilidad y probabilidad de ocurrencia, calculando el impacto potencial.

b) Requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización.

c) Requeimientos particulares según principios y objetivos para el procesamiento de la información que la organización a desarrollado.

Dicha norma indica que posterior a la identificación de requerimientos y riesgos de seguridad, se deben seleccionar los controles apropiados he implementarlos para asegurar que los riesgos se reduzcan a un nivel aceptable.

Los controles considerados como escenciales por la norma ISO/IEC 17799 y que pueden implementarse en el los CECI son:

- Protección de data y privacidad de la información personal.
- Documento de la política de seguridad de la información.
- Asignación de responsabilidades de la seguridad de la información.
- Conocimiento, educación y capacitación en seguridad de la información.
- Gestión de los incidentes y mejoras de la seguridad de la información.
- Gestión de la vulnerabilidad técnica.

CAPÍTULO III: MARCO METODOLÓGICO

CAPÍTULO III: MARCO METODOLÓGICO

Barrantes (2012) indica que el marco metodológico es uno de los aspectos más importantes de cualquier investigación puesto que señala cómo y con qué se realiza la investigación. A continuación, se describirán los elementos que lo componen:

3.1 Tipo y Enfoque de la Investigación

El tipo de investigación que se utilizará es la de tipo aplicada y de campo, debido a que se busca el fortalecimiento del CECI de San Juan de Santa Bárbara de Heredia mediante la propuesta de un plan de seguridad informática con el fin de mejorar el control, acceso y seguridad digital de los usuarios.

De acuerdo con el Manual de Proyecto de Graduación de la Universidad Hispanoamericana (2018), es aplicada porque buscar "utilizar los conocimientos obtenidos en las investigaciones en la práctica, y con ello traer beneficios a la sociedad"; y es de campo porque persigue interpretar y solucionar alguna situación, problema o necesidad en un momento determinado.

Por su parte, el enfoque de investigación será el cualitativo ya que se busca describir el estado actual relacionado a la seguridad informática que se maneja actualmente en el CECI. La escogencia del enfoque cualitativo se debió a que este es flexible, ya que se mueve entre los eventos y su interpretación (Baptista, Fernández, & Hernández, 1991), con el fin de reconstruir la realidad.

Baptista, Fernández, & Hernández (1991) el enfoque cualitativo no utiliza la recolección de datos numéricos durante el proceso de investigación, sino que utiliza descripciones detalladas de situaciones o eventos.

3.2 Fuentes y sujetos de Información

3.2.1 Fuentes de información

Las fuentes de información son aquellas de donde se obtiene el sustento teórico y práctico, mediante el cual se podrá fundamentar la propuesta a desarrollar en el proyecto, sirven para validar los resultados del proyecto mediante la comparación con información fiable y de calidad (Universidad Hispanoamericana, 2018)

Para el presente proyecto se utilizaron las siguientes fuentes:

- Fuentes primarias: se revisaron artículos de investigación, entrevistas a informantes clave, trabajos finales de graduación, documentos oficiales del CECI, entre otros.
- Fuentes secundarias: se analizaron libros, artículos de revistas, normativas, planes y políticas relacionados con los centros comunitarios inteligentes y la seguridad informática.

3.2.2 Sujetos de información

Los sujetos de información son aquellas personas a quienes se contacta para la obtención de información valiosa para el proyecto (Universidad Hispanoamericana, 2018).

Tabla 4: Sujetos de información

Puesto Laboral	Profesión u Oficio	Experiencia	Relación con el tema
Encargado del CECI	Profesor	6 años	Encargado del CECI
Encargado Servidores ASECCSS	Técnico	4 años	Colaborador de ASECCSS, usuario interno.
Encargado de Redes	Ingeniero	8 años	Colaborador de ASECCSS, usuario interno.

Fuente: Elaboración propia.

3.3 Técnicas y herramientas de recolección de datos

Como se especificó, la investigación se realiza desde un enfoque cualitativo, lo cula permite que las técnicas e instrumentos a utilizar cuentes con flexibilidad a la hora de recolectar la información.

Por esta razón, es necesario mencionar las técnicas que se utilizaron , ya que su aplicación da respuesta a los objetivos establecidos. A continuación se exponen las técnicas de investigación que se utilizaron en el presente proyecto.

a) **Observación**: se utiliza esta técnica ya que permite la recolección de datos e información por medio del registro visual de las relaciones y de la realidad, permite crear una vinculación entre el investigador y el hecho a estudiar.

La observación se llevó a cabo en el escenario del CECI San Juan Santa Bárbara de Heredia, en dónde se imparten lecciones y capacitaciones a la comunidad utilizando equipos y redes informáticas.

Se utilizó una guía de observación previamente elaborada que buscó la recopilación de información acerca de la medidas de seguridad informática que se utilizan en el lugar.

Es importante especificar que hay varios tipos de observación, en el caso del presente proyecto se realizaron dos tipos:

- Observación no participante: Campos y Lule (2012) señalan que se trata de una observación realizada por agentes externos que no tienen intervención alguna dentro de los hechos; por lo tanto no existe una relación con los sujetos del escenario; tan sólo se es espectador de lo que ocurre, y el investigador se limita a tomar nota de lo que sucede para conseguir sus fines" (p. 53). Esta observación en dos ocasiones, durante la realización de dichas clases.

- Observación participante: Campos y Lule (2012) mencionan lo siguiente es una observación donde el investigador se involucra dentro de los procesos a quienes observa, y éste es plenamente aceptado, por lo tanto, se estima que lo observado no se ve afectado por la acción del observador" (p.53). Se utiliza esta técnica ya que permite la recolección de datos siendo partícipe de los procesos. La observación participante se llevó a cabo en el CECI San Juan Santa Bárbara de Heredia, lugar dónde se impartieron lecciones y capacitaciones a la comunidad utilizando los equipos y redes informáticas del lugar. Esta observación se realizó de manera participante en varias ocasiones como parte del trabajo comunal universitario.

b) **Entrevista semiestructurada**: permite obtener información sobre un determinado problema en la investigación mediante la formulación de preguntas, la recolección y registro de las respuestas. Se utilizó una guía de entrevista semi estruicturada para la recopilación de la información.

c) **Revisión Bibliográfica**: esta es una técnica fundamental ya que permite la recopilación de insumos teóricos para la comprensión, interpretación y desarrollo de alternativas de solución del proyecto. Esta técnica posibilitará la recuperación de información primordial para puntualizar, sintetizar y orientar científicamente la investigación.

La siguiente tabla permite comprender mejor las técnicas utilizadas:

Tabla 5: Técnicas de recolección de información

Técnica	Objetivo	Descripción
Observación	Observar la arquitectura e infraestructura del equipo del cómputo del CECI, así como el uso que se le dan los distintos usuarios a los equipos, con la finalidad de identificar riesgos y vacíos en el área de seguridad informática.	Se implementarán dos tipos de observación, la no participante a través de la cual se analizar la dinámica de los usuarios en el uso del equipo, mediante visitas al CECI; y la participante como tutor de cursos en el marco de trabajo comunal universitario. Para la observación se utilizaron lista de verificación.
Entrevista semiestructurada	Obtener información de los sujetos de investigación, información que es clave para todas las etapas del proyecto.	Se realizará por medio de un compendio de preguntas abiertas y cerradas con el fin de profundizar los elementos esenciales del CECI y su plan de seguridad informática. Al ser una

		entrevista no estructurada el sustentante puede realizar preguntas que no estén dentro de lo previamente diseñado.
Revisión Bibliográfica	Recopilar de insumos teóricos para la comprensión, interpretación y desarrollo de alternativas de solución del proyecto	Por medio de artículos, tesis, tesinas y todas aquellas fuentes secundarias que relacionadas directamente a los conceptos del marco teórico e indirectamente al tema de investigación definido.

Fuente: Elaboración propia.

3.4 Variables de investigación

La variable de investigación son aquellos elementos que describen y explican las variaciones en el problema de investigación; por lo tanto son las unidades básicas de información que se estudian e interpretan en una investigación (Universidad Hispanoamerica, 2018). Por lo anterior, es necesario comprenderlas, analizarlas e interpretarlas para entender cómo se relacionan en el proyecto a realizar.

De acuerdo a lo establecido en el Manual de Proyectos de la Universidad Hispanoamericana, para los proyectos cualitativos se establecen categorías de análisis en lugar de variables; las mismas se establecen en función de los objetivos determinados para el mismo, de esta manera se hace entendible la relación de cada variable con cada objetivo planteado para el proyecto.

Tabla 6: Ejemplo de definición de variables

Objetivo Específicos	Categorías de análisis	Descripción
Proponer la configuración (área de cobertura, acceso y privacidad, relación funcional y topología) de la red informática del CECI San Juan de Santa Bárbara.	Configuración de red	Red: una red es un conjunto de ordenadores conectados entre sí que pueden compartir información, (documentos, imágenes,), recursos (impresoras, discos duros) y servicios. Una red puede estar formada por dos ordenadores o llegar incluso a tener conectados miles de ordenadores repartidos por todo el mundo (como Internet) (IES VALLE INCLÁN, 2019). Por lo que se describirá el tamaño o cobertura, el acceso y privacidad, la relación funcional y la topología, entendiendo esta última como la disposición física en la que se conecta una red de ordenadores (Molina, 2019). De modo que se presentará un esquema de tipología para el CECI.
Elaborar la propuesta para la implementación y configuración de un servidor (grupos de usuarios, roles, dominio) que mejore la administración de los permisos y accesos a usuarios.	Servidor	Un servidor es una computadora utilizada para gestionar el sistema de archivos de la red, da servicio a las impresoras, controla las comunicaciones y realiza otras funciones (Molina, 2019). De modo que se elaborará una propuesta de grupos de usuarios, roles, seguridad, dominio.
Describir los requerimientos básicos de seguridad Informática para la red del CECI.	Requerimientos básicos de seguridad	Los requerimientos básicos de seguridad son disponibilidad, integridad, confidencialidad o privacidad y autenticidad. La disponibilidad es la garantía de que la información será accesible por los usuarios a los servicios de la red según su "perfil" en el momento requerido y sin "degradaciones". (perfil: depende de que requieren para su desempeño laboral en la empresa). La tiene que ver con la protección que se da a los activos informáticos para que solo puedan ser

		modificados por las personas autorizadas: Escritura, Cambio de información, cambio de estatus, borrado y creación. Es diferente para c/empresa. La confidencialidad o privacidad: "Propiedad o requerimiento de la seguridad que exige que la información sea accedida por cada usuario en base a lo que debe ver en razón a su área del negocio". La autenticidad es la propiedad fundamental de la información de ser confrontada en cualquier momento de su ciclo de vida contra su origen real (Verdadero/falso). Especialmente importante en sistemas económicos (banca, comercio electrónico, bolsa de valores, apuestas, etc.). (Comisión Interamericana de Telecomunicaciones, 2005)
Plantear políticas de seguridad informática (control, acceso y registro) para el uso de los equipos del CECI.	Política de seguridad informática	Una política de seguridad son un conjunto de directrices, normas, procedimientos instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico (Dussan, 2006).

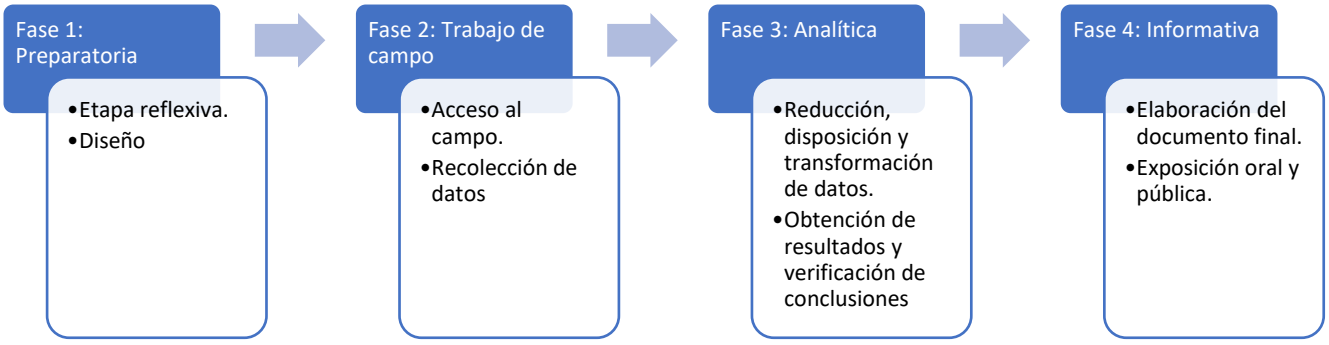
Fuente: Elaboración propia.

3.5 Diseño de investigación

En este apartado se detalla el diseño utilizado para llevar a cabo el proyecto final de graduación; es decir, las distintas fases y etapas, así como las técnicas y herramientas utilizadas e cada una de estas.

Barrantes (2010) define las siguientes fases para el enfoque cualitativo: fase preparatoria, trabajo de campo, fase analítica y la fase informativa:

Figura 6: Fases de la investigación



Fuente: elaboración propia a partir de Barrantes (2010).

A partir de la figura anterior, se describirán cada una de las fases:

1. **Fase preparatoria:** esta fase según Barrantes (2010) se subdivide en la etapa reflexiva y el diseño, y su producto final es la propuesta de proyecto de (p.147).

   Durante la etapa reflexiva se desarrollan los aspectos estructurales de la investigación tales como: problema, objetivos, sujeto de investigación, marco teórico, entre otros.

   Asimismo, durante la etapa de diseño se define el marco metodológico donde se incluye la estrategia metodológica de la investigación, el tipo de investigación, el enfoque, las

técnicas de recolección de información, entre otras. Las técnicas utilizadas en esta etapa son la revisión de bibliografía, el análisis de contenido y las reuniones con el director del proyecto de graduación.

2. **Fase de Trabajo de Campo:** para Barrantes (2010) esta fase se compone de dos etapas el acceso al campo y la recolección de datos; el producto final de esta fase son los datos acumulados (p.147).

   En la etapa de acceso al campo, se utilizaron las técnicas de entrevista y observación en sus dos modalidades; con la persona encargada del CECI y las personas usuarias de los servicios que allí se prestan. La técnica de la entrevista se aplica también con personas expertas de infraestructura y redes.

3. **Fase Analítica:** según Barrantes (2010) esta fase se compone de dos etapas reducción, disposición y transformación de datos; y obtención de resultados y verificación de conclusiones. Su producto final son los resultados (p.147).

   Durante la fase analítica se utiliza la técnica de análisis de contenido y la triangulación, de forma que se integra la teoría y la realidad. Asimismo, en esta fase se sistematizan los resultados de las entrevistas y observación de manera que se visualizan los resultados con las variables previamente definidas.

   Para finalizar esta etapa se desarrollan las conclusiones y recomendaciones obtenidas a través del análisis de variables establecidas.

4. **Fase Informativa:** esta fase se compone de una etapa la elaboración del informe y entrega del documento final a la Universidad Hispanoamericana para su libre acceso, así como la defensa pública y oral (Barrantes, 2010).

Tabla 7: Matriz de Coherencia.

Objetivo	Entregable	Fase, parte o etapa de la metodología del proyecto que posibilita la realización del entregable	Técnicas/métodos de recolección de la información	Instrumentos	Temas relacionados para marco teórico
Proponer la configuración (área de cobertura, acceso y privacidad, relación funcional y topología) de la red informática del CECI San Juan de Santa Bárbara.	Diseño de red donde se contempla cada uno de los computadores y equipos de red disponibles para un uso óptimo del laboratorio del CECI San Juan de Santa Bárbara.	• Fase de Trabajo de Campo. • Fase Analítica.	• Observación. • Entrevista semiestructurada. • Revisión Bibliográfica.	• Guía de observación. • Guía de entrevista.	• Tecnologías de la Información y Comunicación. • CECI. • Seguridad Informática.
Elaborar la propuesta para la implementación y configuración de un servidor (grupos de usuarios, roles, dominio) que mejore la administración de los permisos y accesos a usuarios.	Propuesta para la implementación y configuración de un servidor, así como un dominio común que mejore la administración de permisos, roles y accesos.	• Fase de Trabajo de Campo. • Fase Analítica.	• Observación. • Entrevista semiestructurada. • Revisión Bibliográfica.	• Guía de observación. • Guía de entrevista.	• Tecnologías de la Información y Comunicación. • Seguridad Informática.

Describir los requerimientos básicos de seguridad Informática para la red del CECI.	Recomendaciones para la configuración, control, acceso y filtrado de la red, utilizando un software o dispositivos existentes en el mercado actual.	• Fase Analítica.	• Observación. • Revisión Bibliográfica.	• Guía de observación.	• Tecnologías de la Información y Comunicación. • CECI. • Seguridad Informática.
Plantear políticas de seguridad informática (control, acceso y registro) para el uso de los equipos del CECI.	Documento con lineamientos y políticas de seguridad que incluyen: control, acceso y registro a los equipos del laboratorio e instalaciones del CECI.	• Fase Analítica.	• Revisión Bibliográfica.	• Resúmenes. • Esquemas.	• Tecnologías de la Información y Comunicación. • CECI. • Seguridad Informática.

Fuente: elaboración propia.

CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

En un diagnóstico de la situación actual, la adecuada definición de las estrategias y la movilización de recursos hacia el logro de objetivos planteados está en función del conocimiento de la realidad que se pretende modificar y de la identificación de los factores que explican la problemática a enfrentar; en este caso las debilidades en la infraestructura tecnológica y seguridad informática del CECI.

La OEA (2018) establece que conocer la realidad es uno de los aspectos imprescindibles previos al desarrollo de una intervención, cuyo propósito es poder disponer de los insumos necesarios para dialogar y negociar la definición de una ruta de acción.

En esta línea, una de las técnicas más utilizadas es el diagnóstico por su sencillez, bajo costo, rapidez de aplicación y efectividad. El diagnóstico se comprende así, como un conjunto de procedimientos ordenados y sistemáticos orientados al conocimiento de la realidad con el objeto de desarrollar un programa, proyecto o plan de actividades para su transformación. OEA (2018).

Algunos de los objetivos del diagnóstico son los siguientes:

- Evaluar en qué medida la organización de la empresa es compatible con las necesidades para un efectivo control de su gestión al nivel actual y esperado de operaciones.
- Identificar las áreas a desarrollar, las necesidades de información y control no satisfechas y las oportunidades de mejoras.
- Formular recomendaciones que permitan introducir cambios y mejoras en la organización.

En síntesis, el diagnóstico situacional refleja como indica su nombre la situación actual de una empresa u organización.

A partir de lo anterior y siguiendo el manual de proyectos de graduación de la Universidad Hispanoamericana, se realizará un diagnóstico administrativo y uno técnico.

4.1 Diagnóstico Administrativo

Herrera (2007) señala que un diagnóstico administrativo es un estudio sistemático integral y periódico que tiene como propósito fundamental conocer la organización administrativa. Este tipo de diagnóstico puede aplicarse a todo nivel y dentro de cualquier área.

Comprende el análisis de los siguientes aspectos:

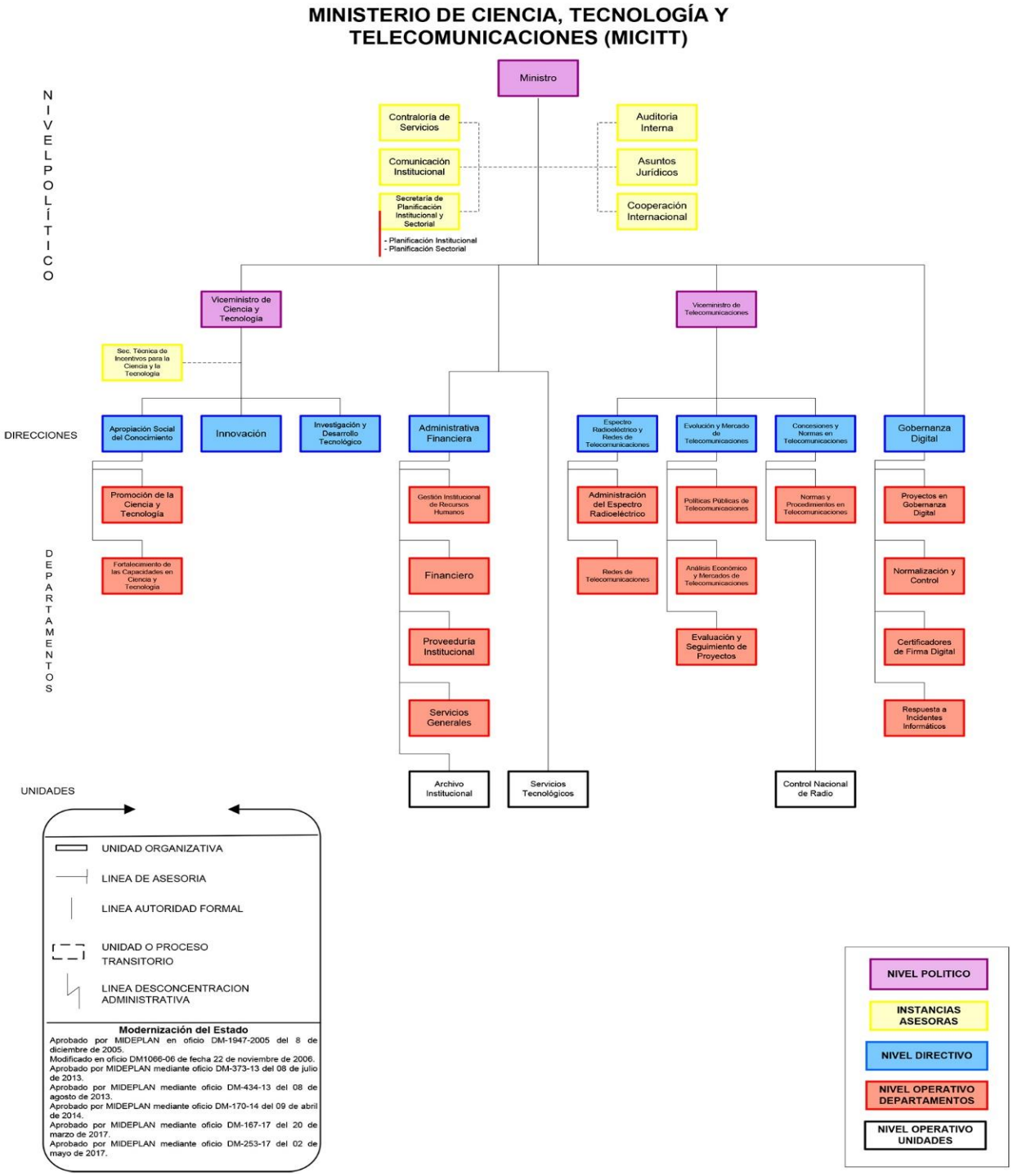
- Análisis de la estructura: comprende el estudio de la estructura organizacional para determinar si la forma en que se encuentra organizado ayuda a cumplir con la misión, visión y objetivos. Para ello se debe evaluar: organigrama, niveles jerárquicos, tipos y líneas de autoridad, recursos existentes y dependencia y relación con otras áreas.
- Análisis de Funciones: refiere al estudio de las funciones asignadas al área objeto de estudio, así como a las atribuciones y obligaciones que tienen que cumplir para el desempeño del trabajo.
- Análisis de Procesos: se estudian los procesos que se desarrollan dentro del área de estudio en función de la secuencia de cada una de las actividades que ahí se desarrolla.

4.1.1 Análisis de la estructura

El CECI es un proyecto del Departamento de Fortalecimiento de las Capacidades, que a su vez pertenece a la Dirección de Apropiación del Fortalecimiento Social del Conocimiento, la cual está adscrita al Viceministerio de Ciencia y Tecnología del MICITT. La línea de autoridad es formal y jerarquizada, el CECI se encuentra en el nivel operativo de la institución.

A continuación, se presenta el organigrama con el fin de ubicar a los CECI dentro de la estructura del MICITT:

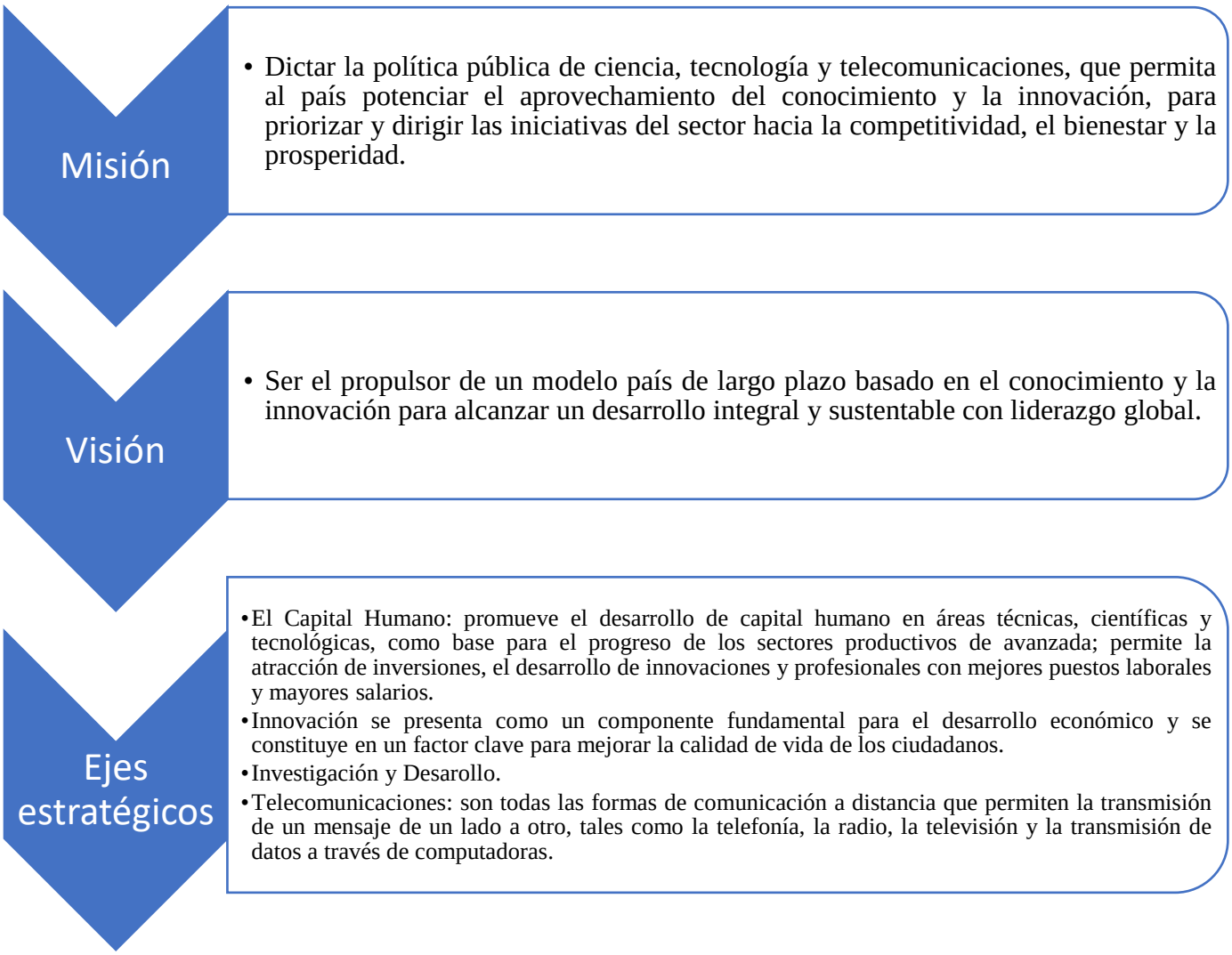
Figura 7: Organigrama MICITT



Fuente: Tomado de MICITT (2019).

Los CECI responden a la misión, visión y ejes estratégicos del MICITT los cuáles se transcriben a continuación:

Figura 8: Misión, visión y ejes estratégicos del MICITT



Fuente: Elaboración propia a partir de MICITT (2019).

Para su funcionamiento, los CECI cuentan con la colaboración de aliados estratégicos como, por ejemplo:

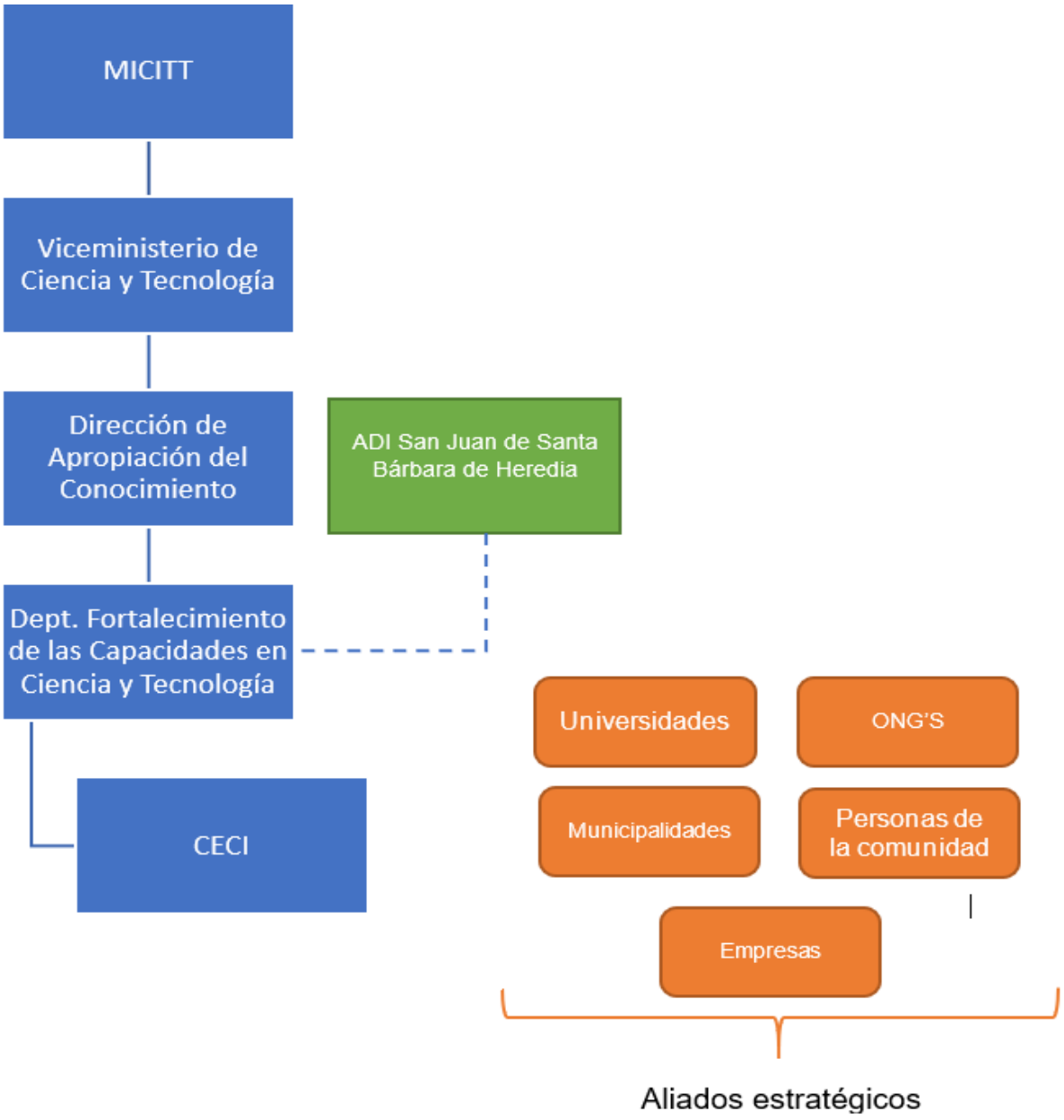
- SINABI: Sistema Nacional de Bibliotecas, según datos del MICITT se tienen más de 30 CECIS en bibliotecas públicas y municipales.

- UNED: Universidad Estatal a Distancia, se tienen laboratorios en más de 30 sedes.
- SUTEL: Superintendencia de Telecomunicaciones, es la encargada del Fondo Nacional de Telecomunicaciones que permitirá renovar los CECI actuales, instalar nuevos y brindar conectividad a los ubicados en las zonas más alejadas del país.
- MTSS: Ministerio de Trabajo y Seguridad Social, se desarrollan proyectos para la formación de personas y su inserción en el mercado laboral.
- Asociaciones de Desarrollo, más de 100 CECI están ubicados en asociaciones de desarrollo, que son las encargadas de brindar la infraestructura, el resguardo y el acceso del laboratorio a la comunidad.
- CISCO: mediante un convenio con el MICITT se da acceso a una variedad de cursos para los usuarios de los CECI.

Para ello utilizan funcionarios, estudiantes universitarios en su programa de TCU, voluntarios y miembros de la comunidad. A continuación, se presenta un diagrama que permite contextualizar el CECI a partir de la información anterior.

En el diagrama se observa la dependencia del CECI del MICITT, pero también a la ADI de San Juan de Santa Bárbara de Heredia y el acercamiento que debe tener a aliados estratégicos, tal es el caso de la Universidad Hispanoamericana, la cual envía estudiantes de diferentes carreras a realizar su TCU y aportar a la oferta de cursos y capacitaciones.

Figura 9: Contextualización del CECI



Fuente: Elaboración propia.

El CECI es un proyecto del MICITT que pertenece a la Dirección de Apropiación Social del Conocimiento, que tiene como objetivo promover la democratización y apropiación de la ciencia

y tecnología en el marco de los derechos humanos, que hagan del conocimiento un instrumento para el desarrollo de las comunidades del país.

Así mismo, fomenta la generación de capacidades en ciencia y tecnología en la población en general y con mayor énfasis en poblaciones vulnerables a través del uso de los CECI.

4.1.2 Análisis de Funciones

A partir de la revisión bibliográfica realizada se identifica que no están establecidas las funciones de los CECI, sin embargo; éstas se pueden inferir de los objetivos específicos del proyecto que son los siguientes[5]:

- Promover la inserción de las TIC en puntos estratégicos mediante la creación de Centros Comunitarios Inteligentes como una plataforma estable y sostenible que ofrece información y servicios interactivos de valor agregado.
- Integrar esfuerzos de varias instituciones del Estado para dotar a centros de población con plataformas de acceso a Internet y correo electrónico dinámicas, estables y accesibles.
- Promover el acceso de los ciudadanos a numerosas fuentes de información nacional e internacional, así como a servicios relacionados con las tecnologías de información que faciliten su labor cotidiana y disminuyan la brecha digital.
- Agilizar los procesos de los servicios que prestan las distintas instituciones reduciendo los tiempos, errores y demoras presentes, en la transmisión de información tradicional.

[5] Tomado de MICITT (2019).

- Incrementar las oportunidades de la población mediante servicios de comunicación más eficientes.
- Aumentar las habilidades de los estudiantes -futuros trabajadores- en el buen y sano uso de las computadoras, Internet y correo electrónico.
- Producir contenidos de interés local que fomenten actividades como el turismo, la agricultura y la inversión empresarial, entre otras.
- Construir instancias de promoción local que fomenten el desarrollo de comunidades virtuales.

Según la evaluación realizada por MIDEPLAN (2018) el marco estratégico del CECI se encuentra desactualizado en relación a objetivos, metas, acciones, actividades y resultados, existiendo una carencia de procedimientos estratégicos.

Por otra parte, a partir de la observación, la entrevista a la persona encargada del CECI y de los resultados del estudio de Chen (2016) se identifica que:

- La administración del CECI la tiene el líder comunal el Sr. José Ramírez Alfaro quien es responsable de la administración, seguridad y condiciones de infraestructura para el buen funcionamiento del centro.
- El mantenimiento del equipo lo realiza el MICITT. Cuando se daña alguna de las computadoras, el encargado coordina directamente con el MICITT para que envíe a algún técnico a repararla, o enviar la computadora al ministerio. Después de que es reparada se coordina la devolución del equipo al CECI.
- Las personas encargadas de los CECI llenan informes con datos de su uso y participantes, a través de una plataforma informática creada por el MICITT.

- Cada persona usuaria que llega a un CECI debe llenar un formulario en línea que actualiza automáticamente la información del sistema informático.
- El MICITT delega la responsabilidad de la divulgación y promoción de los cursos a ofrecer a quien está a cargo del CECI, no obstante, también se divulgan a través de la página web del MICITT y por las redes sociales del centro comunitario.

4.1.3 Análisis de Proceso

El análisis de proceso, como su nombre lo indica, comprende el estudio de los procesos que se desarrollan dentro del CECI, así como el aporte que ofrece a la organización. Incluye el análisis de los procesos principales, subprocesos, procesos contingentes, actividades que se llevan a cabo que corresponden a procesos de otras áreas (Herrera, 2007).

Una forma de hacer este análisis es revisando el manual de normas y procedimientos que se desarrollan dentro del área. En este sentido, se encuentra que los procesos de trabajo del CECI no están sistematizados.

A partir de la observación y entrevistas se pueden resumir las siguientes actividades y funciones que se ejecutan en el CECI:

- Facilitar el acceso a internet: el acceso a internet permite que jóvenes y adultos adquieran diferentes capacidades y desarrollo de competencias digitales. En el CECI el encargado asigna a una o más personas para brinden acompañamiento a los usuarios del laboratorio, ya sea como parte de su trabajo comunal universitario (TCU) o ad honorem. Usualmente se habilitan horarios determinados al menos 3 veces por semana, en espacios de 2 horas

por día para que los miembros de la comunidad puedan utilizar los equipos de cómputo y el servicio de internet, ya sea para realizar labores de índole estudiantil o laboral. De igual manera muchas personas utilizan los laboratorios para practicar o investigar sobre los cursos que el mismo CECI imparte en días diferentes.

- Capacitación en materia de tecnologías: se brindan capacitaciones en materia de ofimática (Word, Excel, PowerPoint), introducción a la computación, mantenimiento y reparación de computadoras, así como de redes CISCO. En un futuro se espera poder impartir cursos de programación y diseño gráfico.

- Desarrollo del aprendizaje y educación de manera presencial y virtual: en coordinación y con el convenio antes mencionado de los CECI con las Universidades. En el convenio los estudiantes que deben de completar su TCU brindan capacitaciones en diferentes áreas y temas, como lo son tecnología, inglés, emprendedurismo, agricultura, entre otros. También tienen la posibilidad de estudiar de manera "online", en los diferentes sitios web existentes para capacitarse de forma gratuita. El encargado del CECI de San Juan de Santa Bárbara de Heredia indica que en un futuro planean tener su propia plataforma de enseñanza en línea para el acceso de toda la comunidad.

En el sitio web del MICCIT se establecen las siguientes reglas para el uso de los CECI:

- En el Centro Comunitario está terminantemente prohibido, buscar, visitar o difundir material de índole pornográfico, racista o satánico.

- Todo usuario tiene la obligación de llenar los formularios o registros para uso de los CECIS.

- No se permite grabar música ni videos.

- Se prohíbe el uso de los equipos con propósitos fraudulentos que suponga la violación de cualquiera de las leyes vigentes (nacionales y extranjeras).
- Los encargados de la administración del Centro darán prioridad a los adultos mayores, personas con discapacidad y personas que no tienen conocimientos en el uso de las computadoras. Siempre tendrán prioridad aquellas personas que estén llevando algún curso de capacitación o fines investigativos académicos.
- En caso de daño de una microcomputadora, solo el personal del MICIT está autorizado para realizar las reparaciones correspondientes.
- Los usuarios no podrán realizar modificaciones en la configuración de equipos, archivos o programas propios del sistema.
- Queda prohibida la reproducción o distribución no autorizada de aquellos materiales y programas protegidos por el derecho de propiedad intelectual.
- Solo se permite una persona por computadora.
- No se pueden ingerir alimentos o bebidas mientras se permanezca en el Centro Comunitario.
- Ningún usuario está autorizado para instalar programas de cualquier tipo.
- Cada persona puede utilizar el servicio de los Centros Comunitarios Inteligentes por un periodo máximo de UNA HORA diaria, salvo en caso de capacitación cuyo horario lo establecerá el programa del curso. Queda a juicio de las personas que brindan la asistencia a los CECIS extender las horas establecidas por persona.

- El acceso a Internet para niños y niñas no es restringido, siempre y cuando se demuestre que se encuentran fuera del horario lectivo o presenten la autorización escrita de padre, madre o tutor.
- La denegación de uso podrá ser inmediata previo apercibimiento durante el transcurso de la sesión en caso de que sea infringido estas reglas, los lineamientos para el uso del servicio de Internet o cuando se determine la evidencia de que durante la sesión se accede a contenidos no permitidos para su visualización en lugar público.

Con base en estas reglas y la observación realizada se puede indicar:

- No existen dispositivos o programas de seguridad que eviten buscar, visitar o difundir material de índole pornográfico, racista o satánico.
- Hay debilidades en el llenado de los formularios o registros para uso de los CECIS.
- No hay medidas que restrinjan grabar música o videos desde las computadoras del CECI, ni tampoco la reproducción o distribución no autorizada de aquellos materiales y programas protegidos por el derecho de propiedad intelectual que se encuentran en los equipos.
- No existen protocolos de seguridad para evitar el uso de los equipos con fines fraudulentos.
- Existen debilidades de seguridad en lo que respecta a un posible acceso que permita realizar modificaciones en las computadoras.
- No hay rotulación ni regulaciones con respecto a ingerir alimentos en el CECI.

4.2 Diagnóstico Técnico

El diagnóstico técnico es la revisión de la infraestructura tecnológica a nivel físico y lógico del lugar que se encuentra en estudio.

En este orden el inventario del laboratorio del CECI, cuenta con los siguientes equipos disponibles:

- 18 minicomputadoras Intel, modelo NUC 8 NUC8I3CYSN, con las siguientes características:
    - Procesador Core I3.
    - Disco duro con 1TB de almacenamiento.
    - Memoria RAM de 4GB DDR4.
    - Video, sonido, puertos USB, de red LAN e inalámbrica y video integrados a la tarjeta madre.
- 18 monitores LCD de la marca AOC de 19 pulgadas.
- 18 cámaras web Logitech.
- 18 teclados USB Logitech en español.
- 18 Mouse o “Ratón” Logitech USB.
- 18 sistemas de alimentación ininterrumpida APC, más conocidos como UPS por sus siglas en inglés.
- 1 impresora de inyección de tinta USB, EPSON T22.
- 1 Switch marca CISCO Catalyst 2960-x de 24 puertos.

- 1 conexión a internet tipo ADSL de 10mb/2mb, mediante un dispositivo Huawei, que además de conexión LAN, también brinda conexión inalámbrica.

A nivel de software se cuenta con los siguientes recursos:

- 18 licencias de Microsoft Windows 10 Home.
- 18 licencias de Microsoft Office 365 Home & Student.
- Antivirus Windows Defender.

La observación, las entrevistas y el trabajo realizado durante el TCU permiten afirmar que el CECI cuenta con equipo de cómputo básico acorde a sus funciones y a las posibles necesidades de los usuarios.

No obstante, se identifica que hay licencias de software vencidas, no se cuenta con un antivirus de calidad, no existen dispositivos de red que controlen el tráfico web, las computadoras se encuentran conectadas por medio de una red inalámbrica, lo cual representa una desmejora de rendimiento, además cuenta con seguridad básica de contraseña de acceso, no existe un dominio común entre las máquinas que permita una mejor administración de permisos y accesos a nivel local.

4.3 Brechas o conclusiones del diagnóstico

En este apartado se definen las brechas que existen entre el estado actual del CECI y la propuesta de fortalecimiento de este.

El diagnostico administrativo permite concluir que el CECI de San Juan de Santa Bárbara de Heredia:

- Se encuentra en el nivel operativo de la estructura administrativa del MICCIT, la línea de autoridad es formal y jerarquizada.
- Responde a la misión, visión y ejes estratégicos del MICITT.
- Cuentan con la colaboración de la Asociación de Desarrollo de San Juan de Santa Bárbara de Heredia, de las Universidades Hispanoamericana, Estatal a Distancia, Internacional de las América, Autónoma de Centroamérica entre otras. Además de empresas privadas como CISCO.
- El marco estratégico del CECI se encuentra desactualizado existiendo una carencia de procedimientos estratégicos.
- No tiene funciones establecidas formalmente, no obstante, las que se pueden identificar se desprenden de los objetivos específicos del proyecto, los cuales se pueden resumir en: democratización, apropiación y generación de capacidades en ciencia y tecnología.
- Los procesos del trabajo del CECI no están sistematizados y no se cuenta con protocolos de seguridad que sigan las mejores prácticas en la materia.

Por su parte el diagnóstico técnico revela que:

- Los equipos informáticos tienen configuraciones de hardware y software básicos, lo cual limita su uso y configuración.
- No se cuenta con la configuración de una red estructurada que mejore el rendimiento del uso del internet.

- No se cuenta con servidor para administrar los permisos y accesos a usuarios.
- No se cumple con los requerimientos básicos de seguridad informática en la red.
- No existen políticas que regulen el control acceso y registro en los equipos del CECI.

CAPÍTULO V: PROPUESTA DE PROYECTO

CAPÍTULO V: PROPUESTA DE PROYECTO

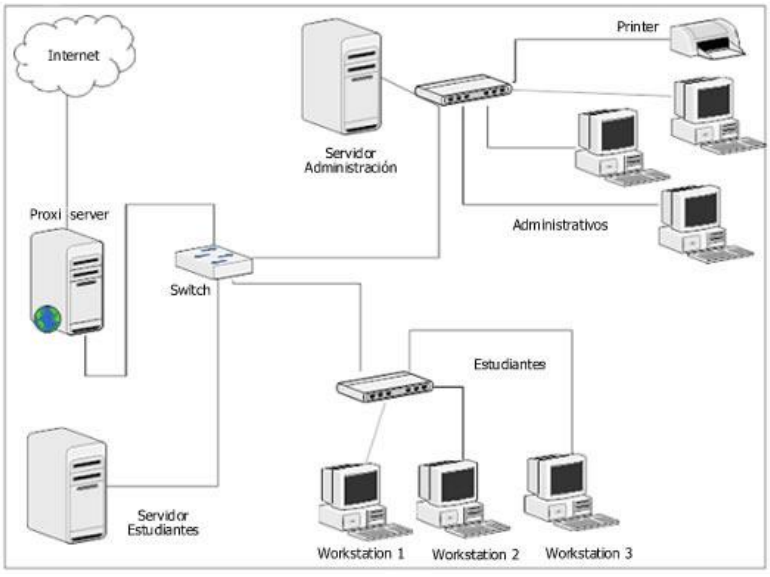
El presente capitulo desarrolla la propuesta de mejoramiento de la infraestructura tecnológica del CECI, a saber, su diseño de red, configuración del servidor y seguridad informática, lo anterior a partir del diagnóstico realizado.

5.1 Propuesta de diseño de red para el CECI

En el presente apartado se presenta la propuesta de diseño de red donde se contempla cada uno de los computadores y equipos de red disponibles en el CECI para un uso óptimo del laboratorio.

La red se conforma de equipos físicos y aplicaciones conectadas entre sí, que comparten recursos e información. En la figura 10, se muestra un ejemplo de lo que se refiere a una red de datos:

Figura 10: Ejemplo de red de datos



Fuente: Tomado de López & Figueroa (2018).

La propuesta de red de datos para el CECI es similar a la figura 10, ya que se tienen varios computadores que van a estar unidos a una misma red. En ella un equipo de red controlará el tráfico

de datos y un servidor que va a administrar los grupos y acceso de usuarios, junto con conexión a internet mediante un servicio ADSL facilitado por el ICE.

Lo anterior, mejorará el rendimiento de la red y la posibilidad de compartir recursos y dispositivos entre las computadoras.

Para el proyecto se propone a utilizar la topología de red jerárquica, por las siguientes razones[6]:

- La falla de un nodo[7] no implica que falle la comunicación de los demás nodos.
- Es una red escalable, lo que significa que el administrador puede añadir, reemplazar y eliminar elementos en la red con funciones similares y definidas sin mayores complicaciones.
- Al ser una red diseñada en capas, se pueden identificar diferentes problemas a nivel de hardware y software dependiendo del nivel donde se presente.
- El equipo de comunicación central amplifica e incrementa la distancia a la que puede viajar la señal.
- Es soportado por varios vendedores de software y hardware.

La figura 11 muestra un ejemplo de Topología de Red Jerárquica.

[6] A partir de Espinoza (2015).
[7] Un nodo es una computadora que forma parte de una red.

Figura 11: Ejemplo de red tipo Jerárquica

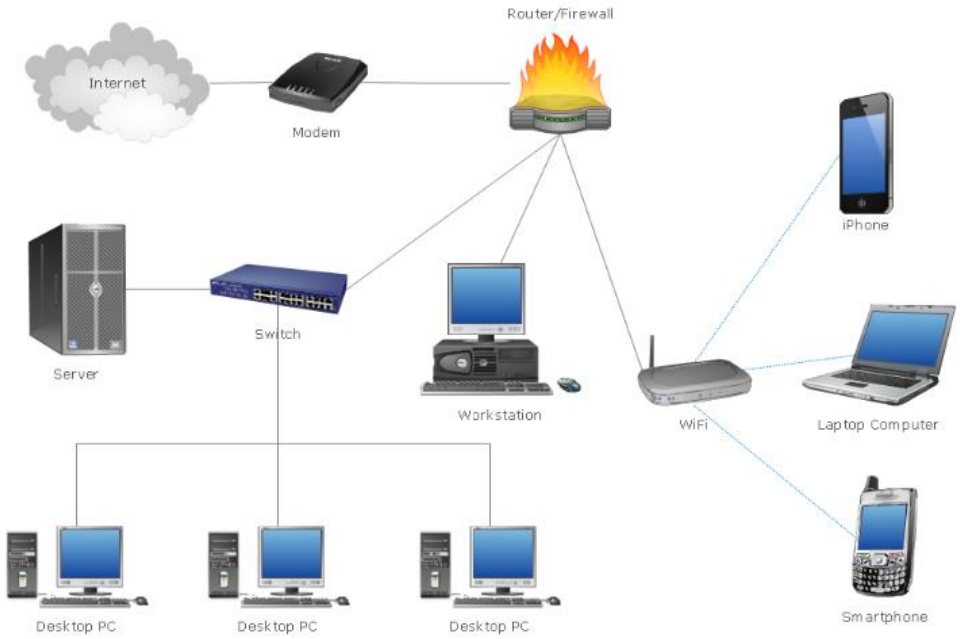
Tomado de Moreno (2019)

Las redes de datos también se califican de acuerdo con su alcance geográfico como redes WAN, LAN, MAN y WLAN.

- WAN (Wide Area Network): Permite la interconexión de equipos localizados en diferentes zonas geográficas.
- LAN (Local Area Network): Es una red que cubre un área pequeña y limitada, por ejemplo, en un edificio u oficina.
- MAN (Metropolitan Area Network): Conecta redes LAN que se encuentran cerca, en un rango de alrededor de 50km.
- WLAN (Wireless Local Area Network): Tipo de red de área local utiliza ondas de radio para transmitir los datos, en lugar de medios alámbricos.

Para este proyecto se utilizará una red LAN, debido a su tamaño, las limitaciones de presupuesto y los pocos equipos con que se cuenta actualmente.

Figura 12: Ejemplo de red LAN



Tomado de ConceptDraw (2019).

Como se puede observar en la figura 12 la Red de Área Local (LAN) conecta los dispositivos de red en una misma área; a la vez que permite acceso a dispositivos desde diferentes usuarios por medio de un administrador local.

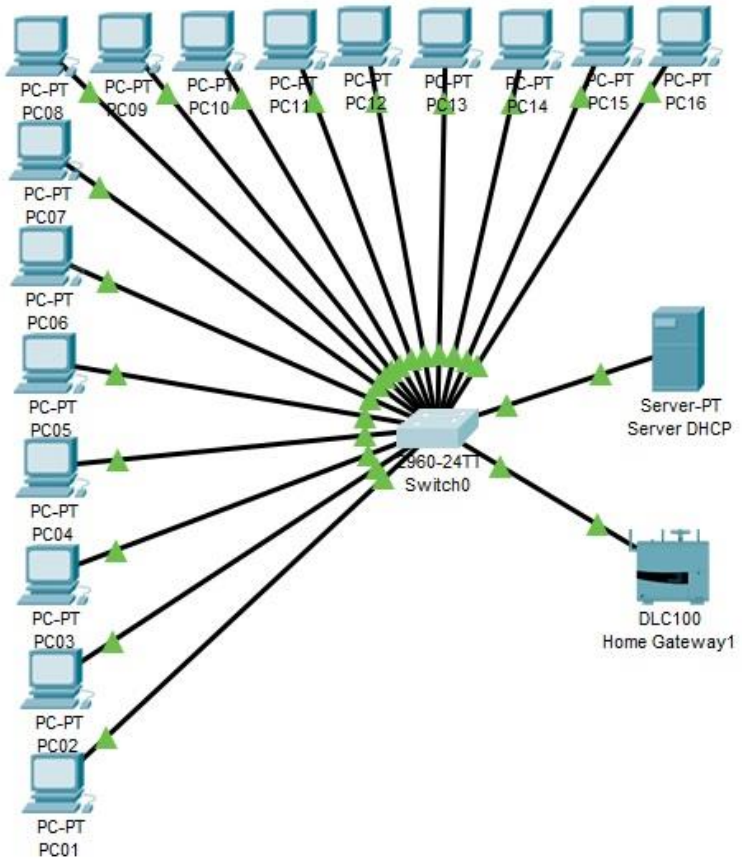
Además, maneja altas tasas en la transmisión de datos ya que estos viajan por medios alámbricos. La red LAN está conformada por diferentes dispositivos que se clasifican como: activos y pasivos.

Los componentes Activos: suele llamarse así a los componentes que utilizan electricidad para poder funcionar, tales como servidores, estaciones de trabajo y equipos de Red (Switch, Router).

Los componentes pasivos no utilizan electricidad para su funcionamiento, ya que solamente se utilizan para el paso de los datos, ejemplo de estos son: rack, diferentes tipos de cable: UTP, Fibra Óptica y panel de conexiones (Espinoza, 2015).

Todo lo descrito permite generar la siguiente propuesta de diseño de red para el CECI.

Figura 13: Topología de red propuesta

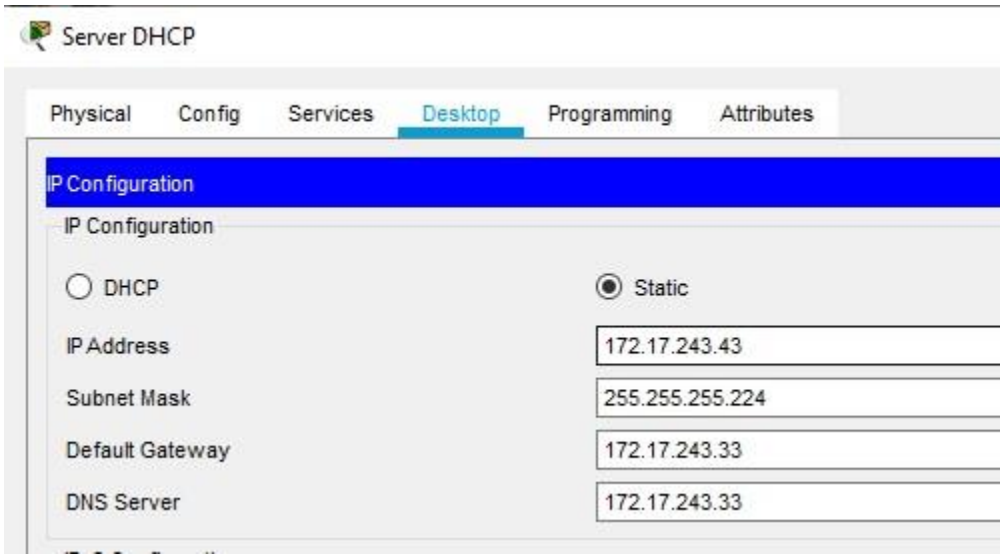


Fuente: elaboración propia con Packet Tracer.

La red LAN se conforma de los 18 computadores conectados a un Switch (2960-24), que a su vez se conecta con un servidor (Server-PT) y el equipo ADSL (Home Gateway) proveedor del servicio de internet.

A continuación, se muestra la configuración del Switch, la figura 14 inicia con la configuración de la dirección estática.

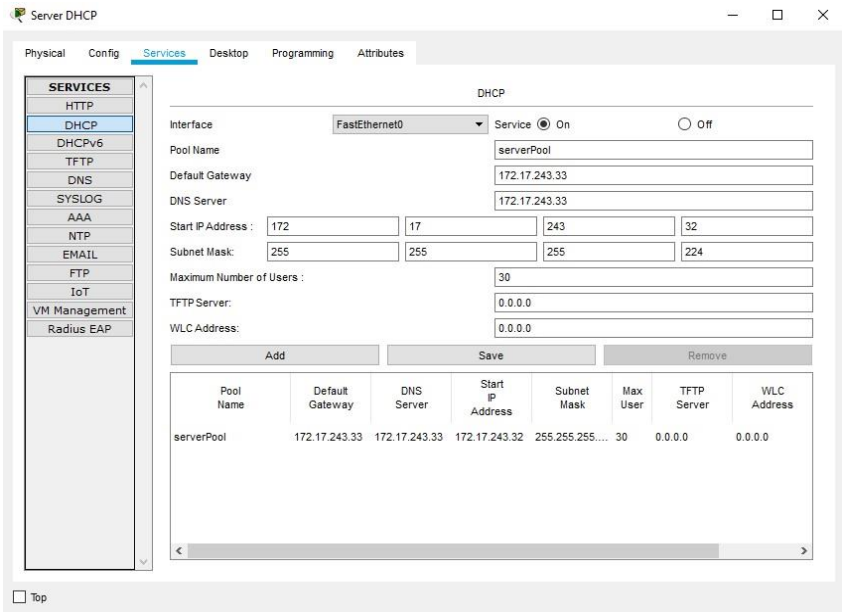
Figura 14: Configuración de dirección estática



Fuente: elaboración propia.

Seguidamente, se continúa con la configuración del pool de direcciones IP a entregar por el DHCP. La figura 15 ilustra lo anterior:

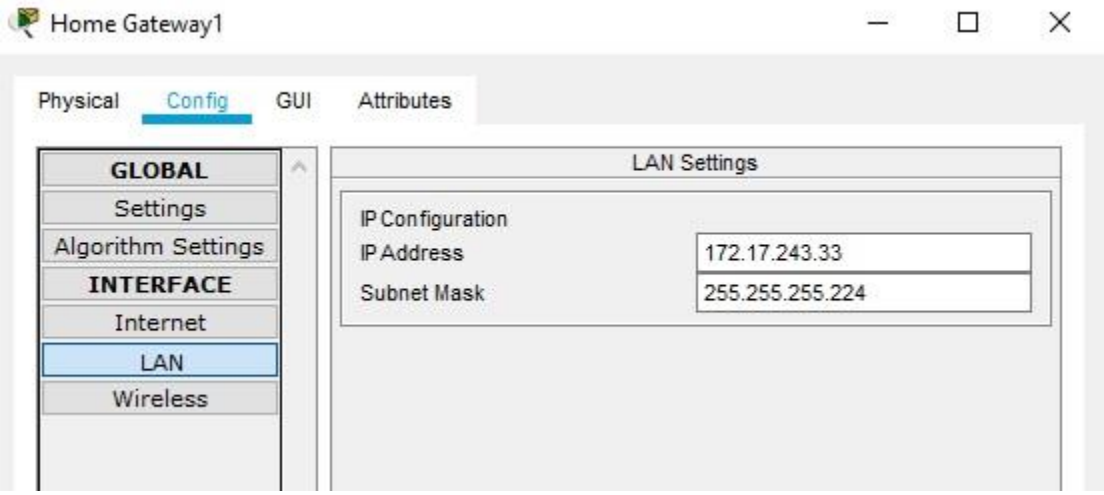
Figura 15: Configuración pool de direcciones



Fuente: elaboración propia.

El siguiente paso refiere a la configuración del Gateway. La figura 16 muestra cómo se realiza:

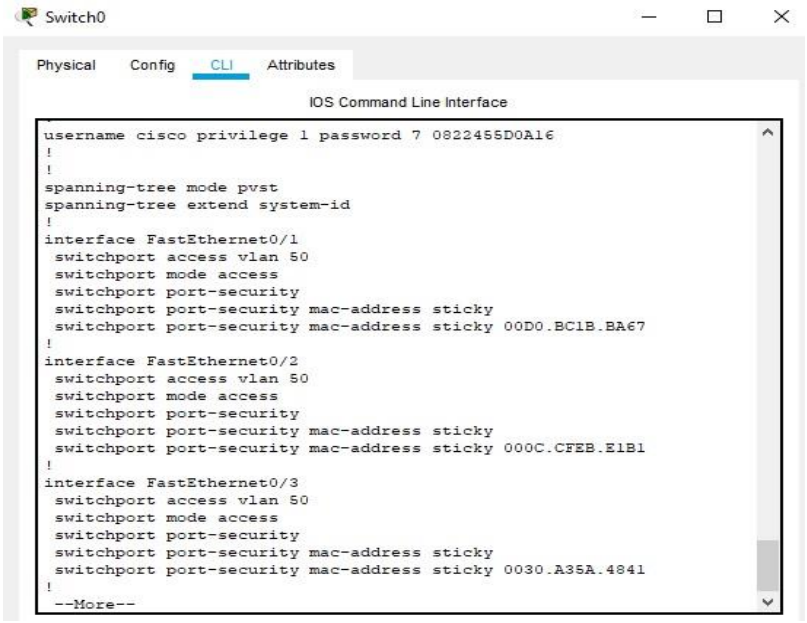
Figura 16: Configuración del gateway



Fuente: elaboración propia.

La figura 17 muestra la configuración de la contraseña con encriptación para el acceso a Switch, además de tres equipos propiamente identificados con sus direcciones físicas.

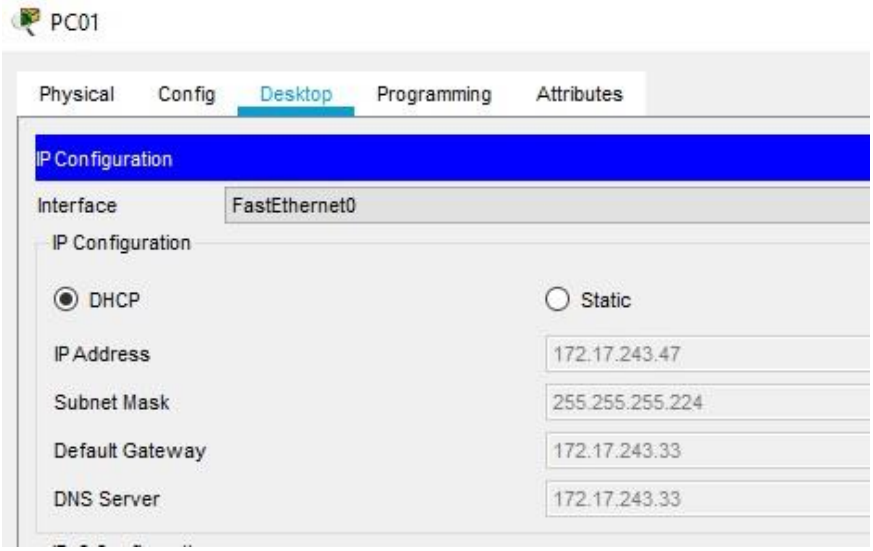
Figura 17: Equipos reconocidos en la red



Fuente: elaboración propia.

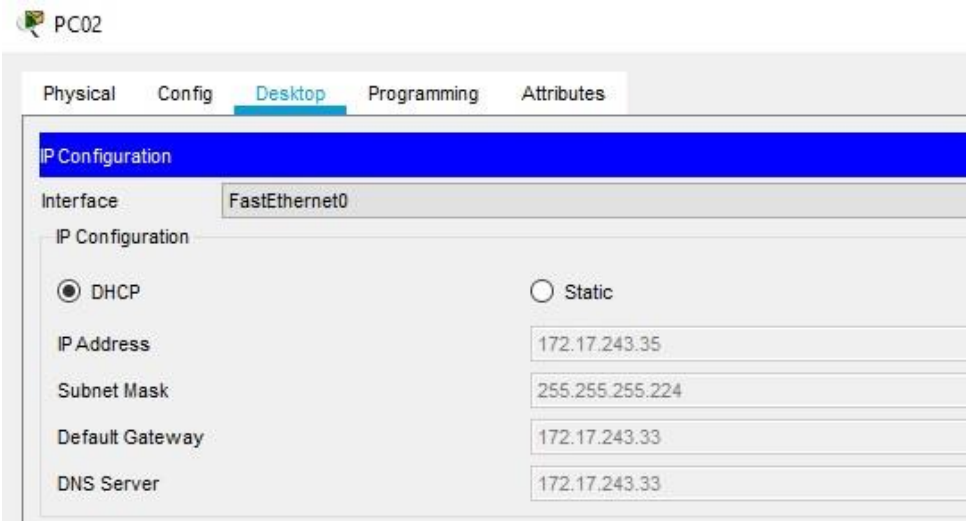
Finalmente, las figuras 18, 19 y 20 muestran a los equipos de la red obteniendo su respectiva dirección por DHCP:

Figura 18: PC01



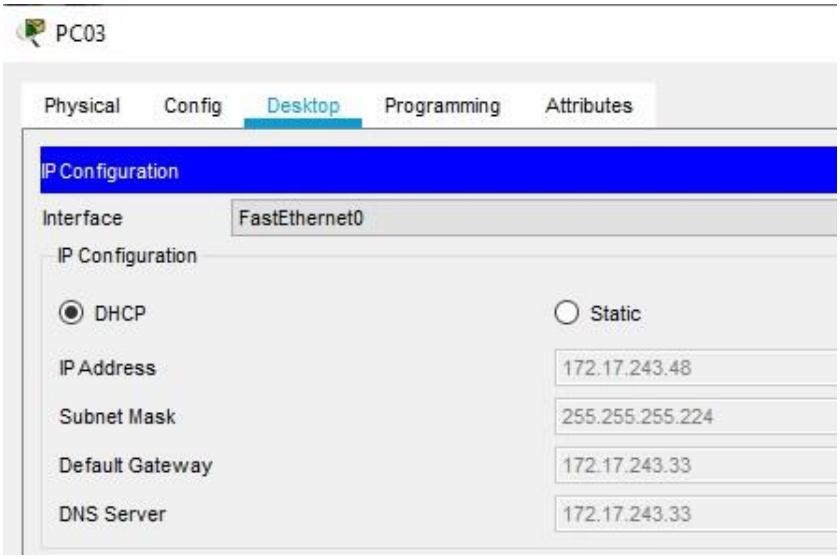
Fuente: elaboración propia.

Figura 19: PC02



Fuente: elaboración propia.

Figura 20: PC03



Fuente: elaboración propia.

Con base en esta propuesta de diseño de red, se elaborará la configuración de un servidor de Dominio, DNS y DHCP, con la implementación de mejores prácticas.

5.2 Implementación y configuración del servidor del CECI

Un servidor es un computador que tiene componentes con mayor capacidad de procesamiento, memoria y espacio de almacenamiento que un computador normal. Otros equipos de la red le solicitan datos o información y se configuran de diferentes maneras dependiendo de su aplicación.

Existen diferentes tipos de servidores, a continuación, algunos ejemplos:

- Servidor de Archivos: almacenan y administran datos, como archivos, imágenes y videos que pueden ser compartidos con otros equipos dentro de la red, sin necesidad de usar dispositivos de almacenamiento o el correo electrónico.
- Servidor de Correo: realizan todos los procedimientos relacionados con correos electrónicos para los clientes de la red: enviar, almacenar, recibir, entre otros.
- Servidor DNS: se encarga de traducir las direcciones IP a nombres de dominio y viceversa, además guarda estos registros en una base de datos para cuando vuelvan a ser consultados.
- Servidor DHCP: contiene una lista de direcciones IP para asignar a los equipos que se conecten a la red, con la finalidad de evitar conflictos entre los equipos en caso de que existiera una dirección IP duplicada.
- Servidor Proxy: funciona como un intermediario entre un dispositivo y la internet, de modo que toda solicitud de información desde un computador configurado con un servidor proxy será filtrada y analizada antes de salir o entrar en la red, esto para bloquear contenido prohibido o aumentos de velocidad para sitios almacenados en la memoria caché.

Según la información descrita, para el caso del CECI se propone configurar un servidor que funcione como DNS y DHCP, así como configuración de un directorio activo, para lo cual se recomienda adquirir un servidor que tenga los siguientes requerimientos mínimos de hardware:

- Procesador: 4 núcleos, 1.7GHz
- Memoria Caché del procesador: 15MB
- Memoria RAM: 8GB DDR4
- Almacenamiento: 1TB

A su vez se propone adquirir el siguiente requerimiento de software para la administración del servidor:

- Sistema Operativo: Windows Server Standard 2016.

Con base en lo anterior, se presenta la forma en que se instala el software de administración para el servidor, en este caso Windows Server 2012 R2 en su versión Standard.

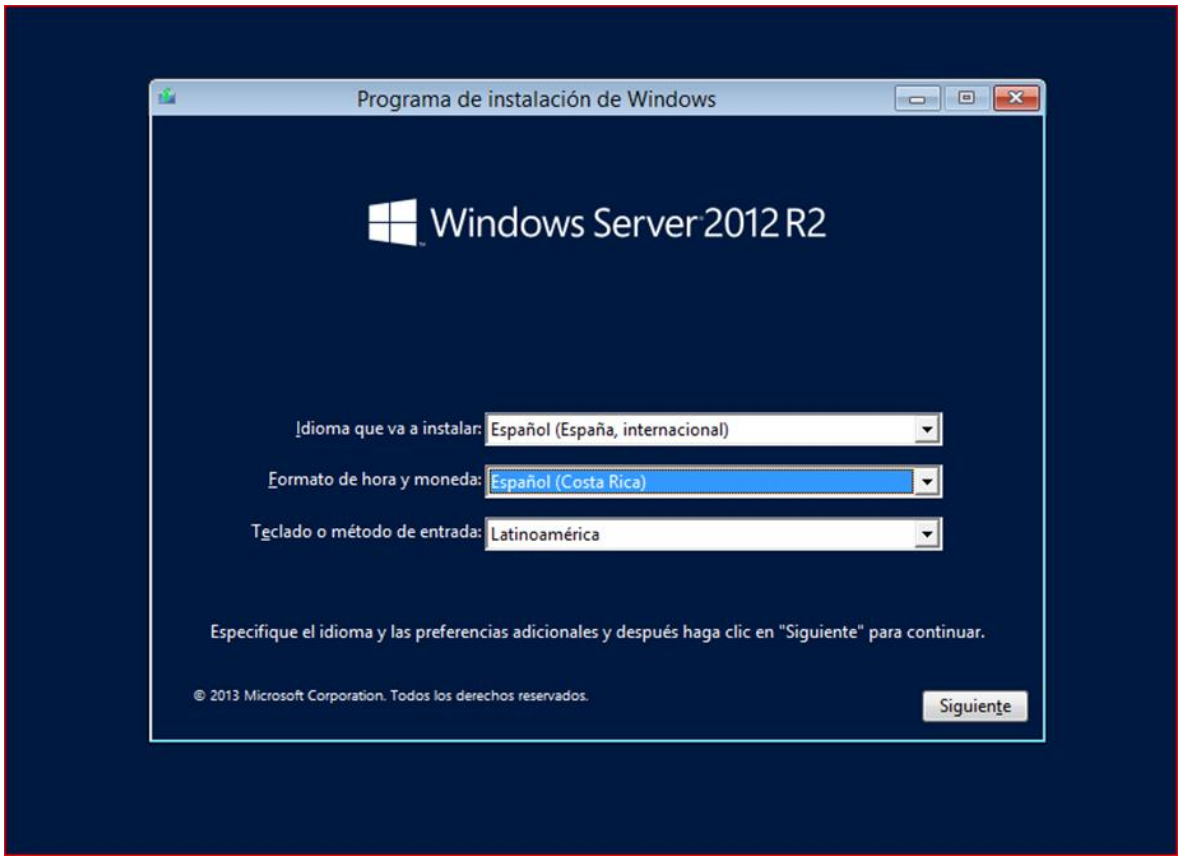
Para iniciar la figura 21 muestra la pantalla de configuración del idioma, en ella se permite elegir el idioma en que se va a instalar, el formato de hora y moneda, así como el método de entrada o teclado.

Existen variedad de idiomas a instalar, dependiendo de los requerimientos o preferencias del administrador o encargado del servidor. Se recomienda instalar en el idioma nativo para no tener problemas al momento de realizar las configuraciones.

En la parte de formato de hora y moneda de igual manera se recomienda instalar dependiendo de los requerimientos o necesidades de la empresa o usuarios.

El método de entrada básicamente significa el idioma del teclado. Si por ejemplo se escoge el idioma inglés, pero el teclado está en español, se pueden presentar problemas con los símbolos al momento de escribir.

Figura 21: Pantalla configuración de idioma



Fuente: Elaboración propia.

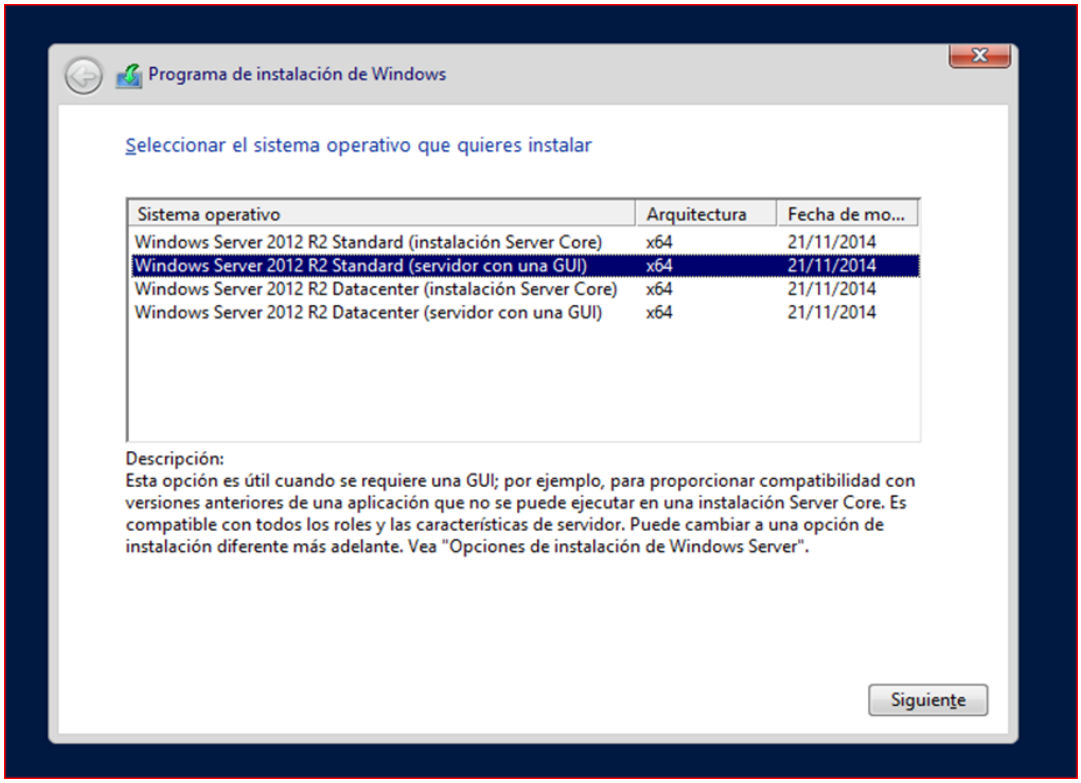
En el siguiente paso se debe seleccionar la versión que se va a utilizar, para el caso de la figura 22 que se tiene como ejemplo, se muestran dos versiones distintas, Standard y Datacenter, cada versión puede ser instalada como servidor con GUI o Server Core.

- Servidor Standard Core: no posee interfaz gráfica, toda la administración debe hacerse por línea de comandos o PowerShell.
- Servidor Standard GUI: posee una interfaz gráfica, lo cual hace que la administración de este sea más amigable e intuitiva para el usuario.

- Servidor Datacenter Core: no posee interfaz gráfica, toda la administración debe hacerse por línea de comandos o PowerShell, y esta versión de sistema posee características avanzadas para virtualización.
- Servidor Datacenter GUI: posee una interfaz gráfica, lo cual hace que la administración de este sea más amigable e intuitiva para el usuario e incluye características avanzadas para virtualización.

Para el CECI se va a utilizar una versión Standard con GUI, para que la configuración y administración sean más amigables para el encargado del servidor. Según los requerimientos actuales del CECI no se necesitan las características de virtualización y además esta versión tiene menor costo de licenciamiento, lo cual beneficia el corto nivel presupuestario del CECI.

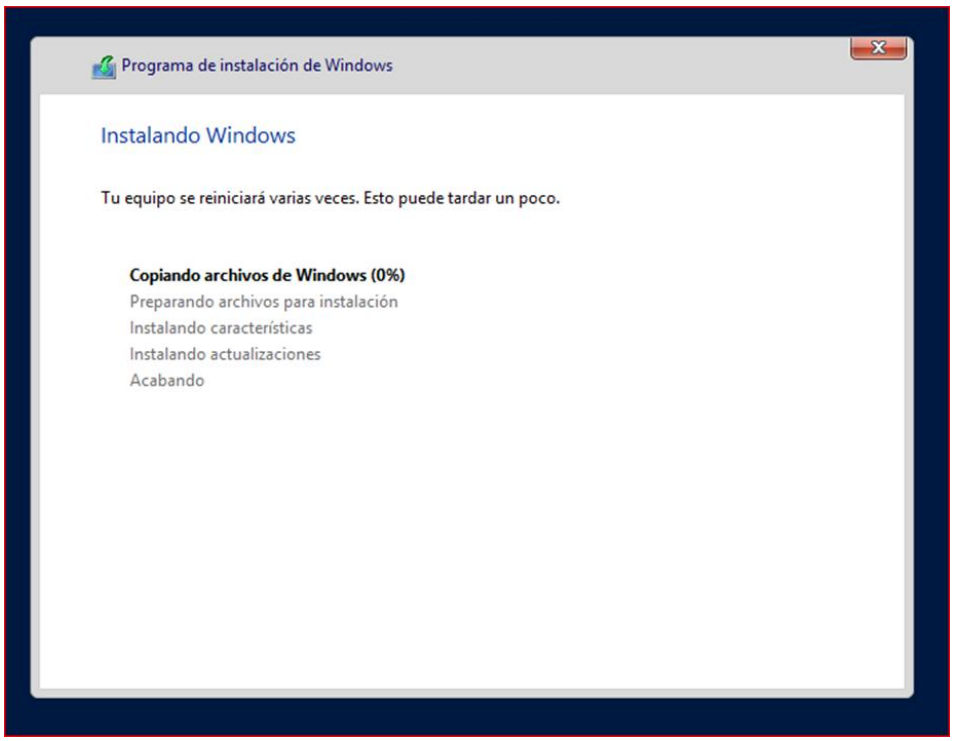
Figura 22: Selección de sistema operativo



Fuente: Elaboración propia.

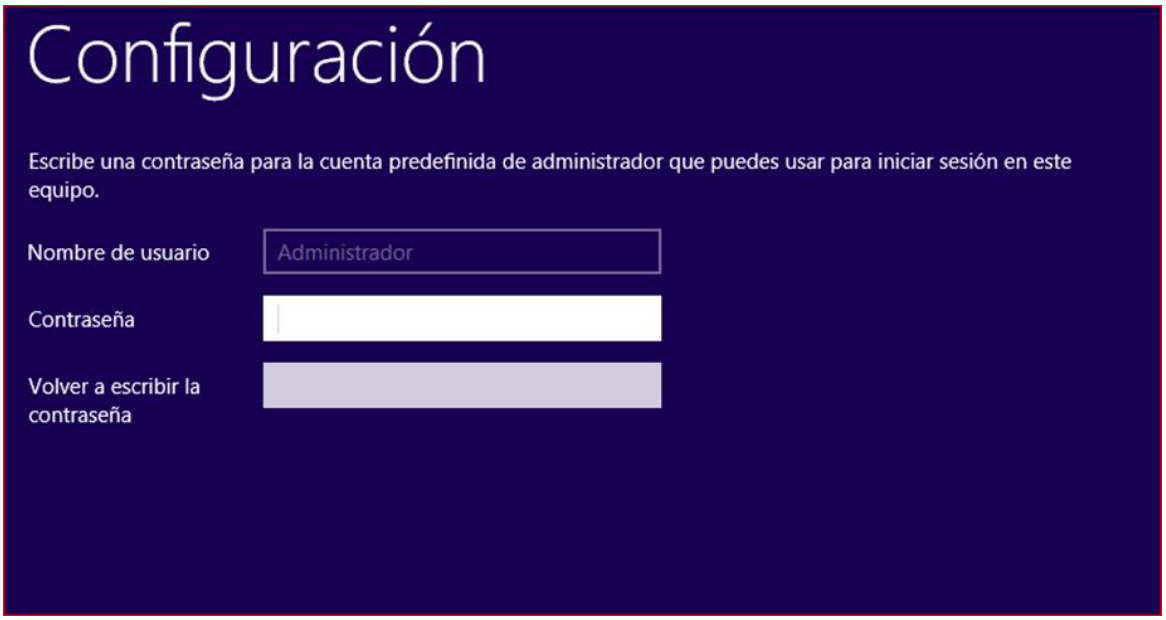
Las figuras 23 y 24 muestran el proceso de instalación del software y la creación de un usuario administrador con su respectiva contraseña.

Figura 23: Proceso de instalación del Sistema Operativo



Fuente: elaboración propia.

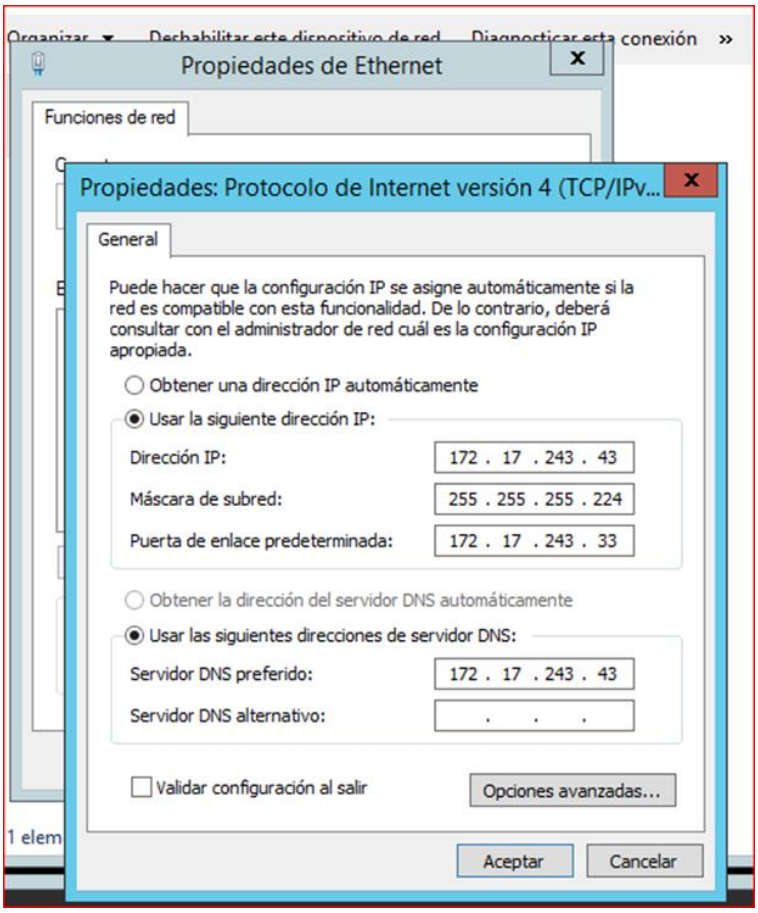
Figura 24: Configuración de usuario - administrador



Fuente: elaboración propia.

En la figura 25 siguiente se hace la configuración de una dirección IP fija para el servidor:

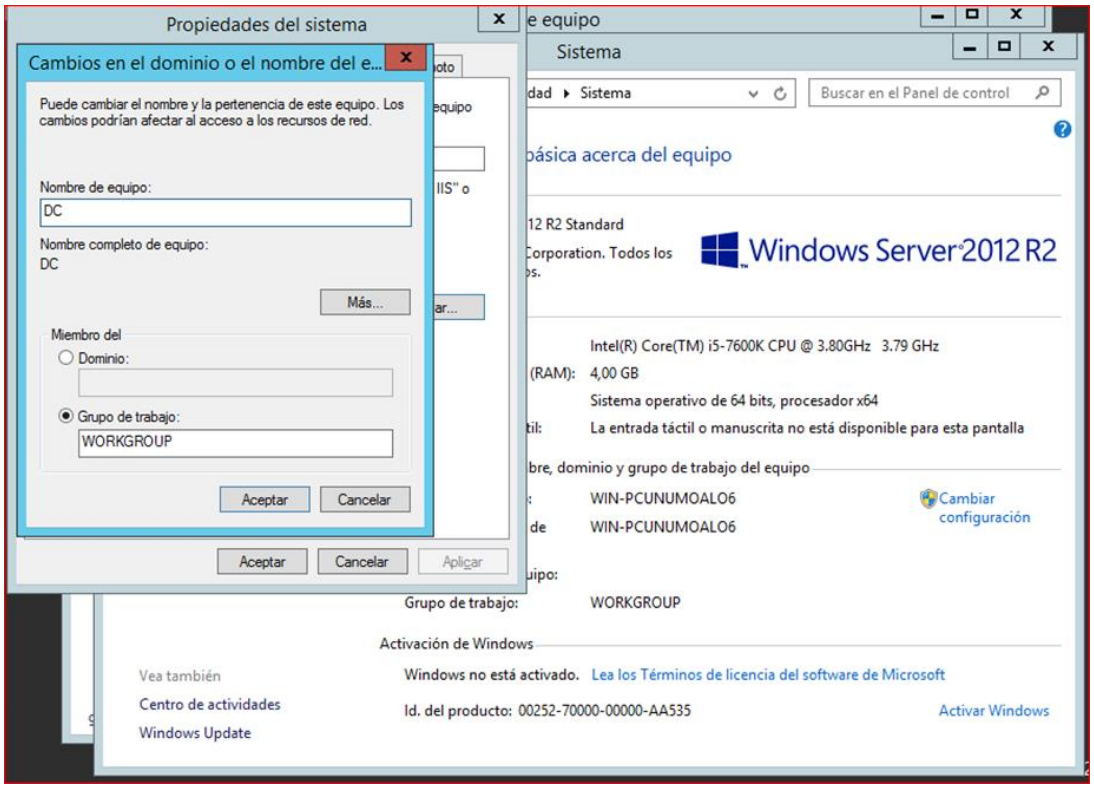
Figura 25: Configuración de IP fija en el servidor



Fuente: elaboración propia.

Seguidamente, se verifica y cambia el nombre del servidor a uno representativo, en este caso se utiliza DC, que significa Domain Controller o Controlador de Dominio en español. La figura 26 grafica lo descrito:

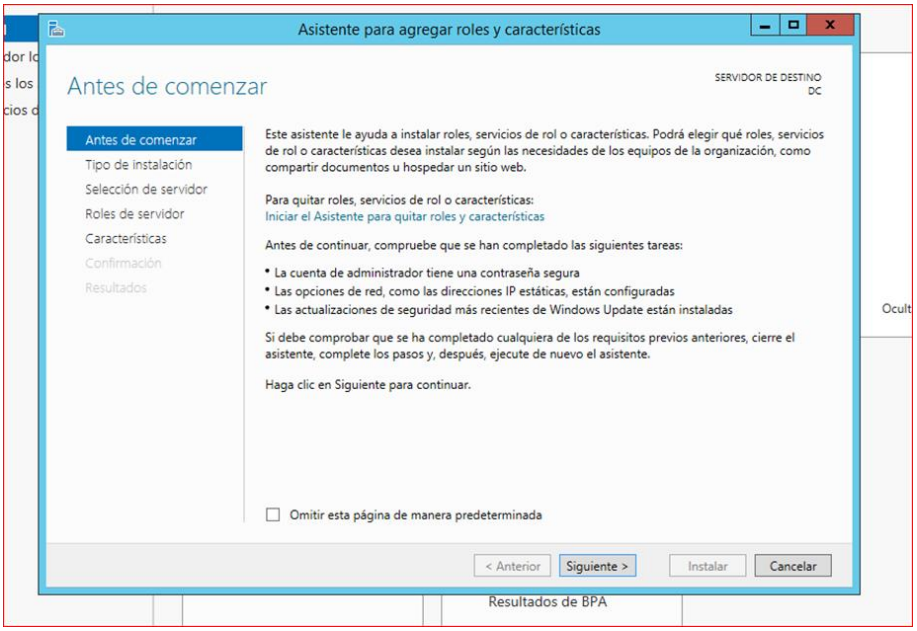
Figura 26: Cambio de nombre a servidor



Fuente: elaboración propia.

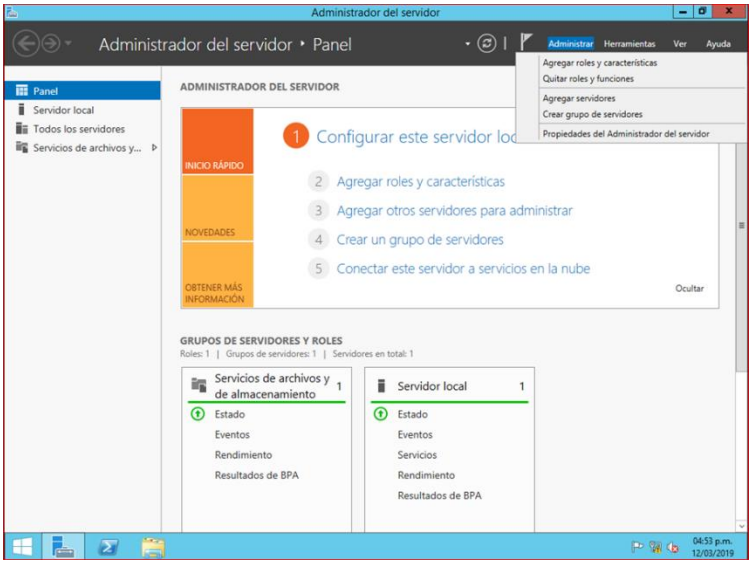
En el siguiente paso se realiza la instalación del rol de Active Directory desde la ventana principal de administración que utiliza Windows Server 2012 R2. Las figuras 27, 28, 29 y 30 describen el proceso de configuración.

Figura 27: Instalación del rol de Active Directory



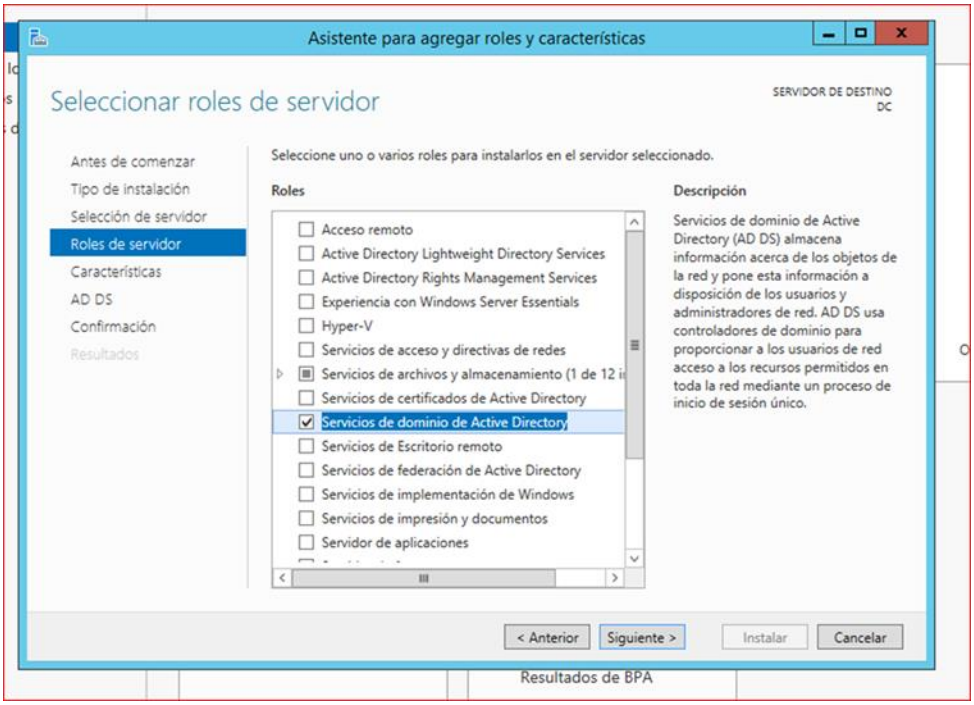
Fuente: elaboración propia.

Figura 28: Asistente para agregar roles y características 1



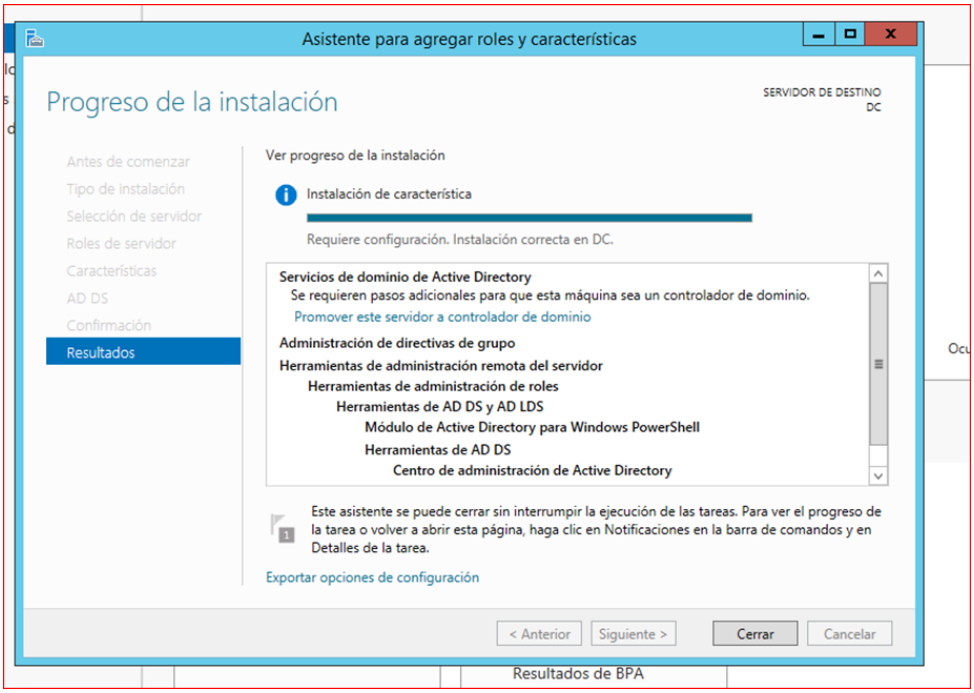
Fuente: elaboración propia.

Figura 29: Asistente para agregar roles y características 2



Fuente: elaboración propia.

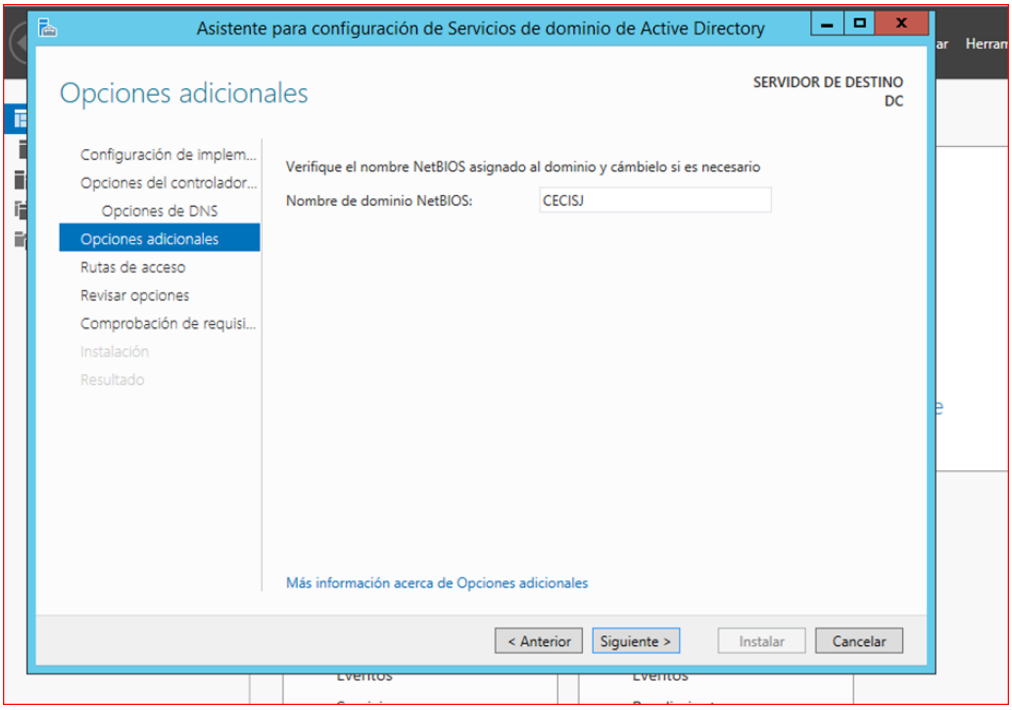
Figura 30: Asistente para agregar roles y características 3



Fuente: elaboración propia.

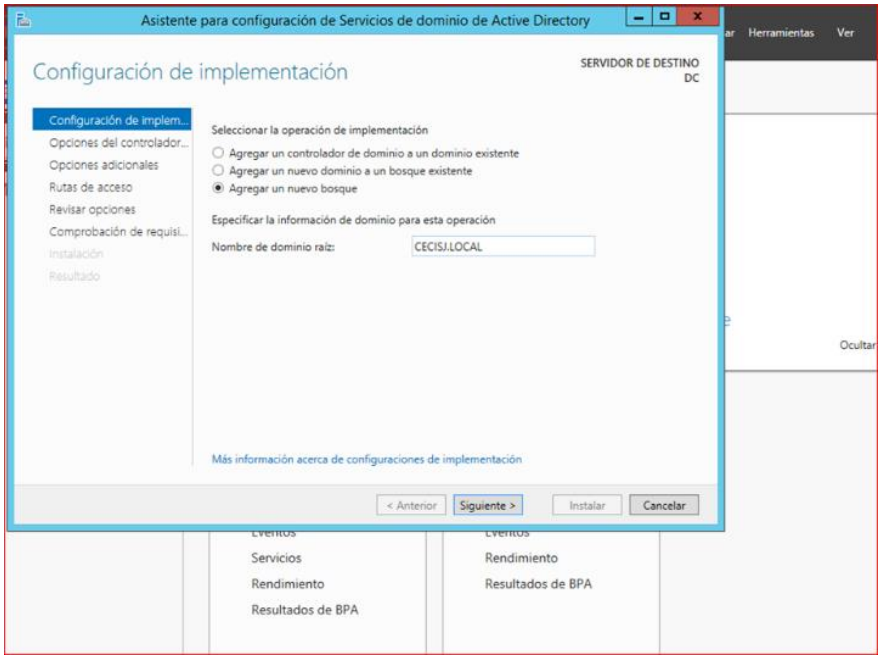
Posteriormente, se va a crear el dominio local con el nombre: CECISJ. Las figuras 31, 32 y 33 grafica el proceso:

Figura 31: Configuración de dominio local 1



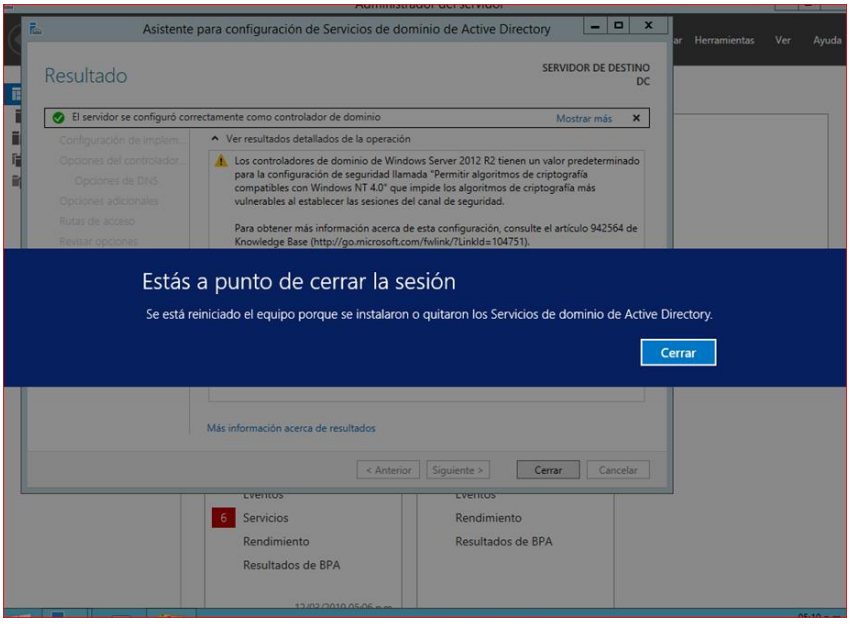
Fuente: elaboración propia.

Figura 32: Configuración de dominio local 2



Fuente: elaboración propia.

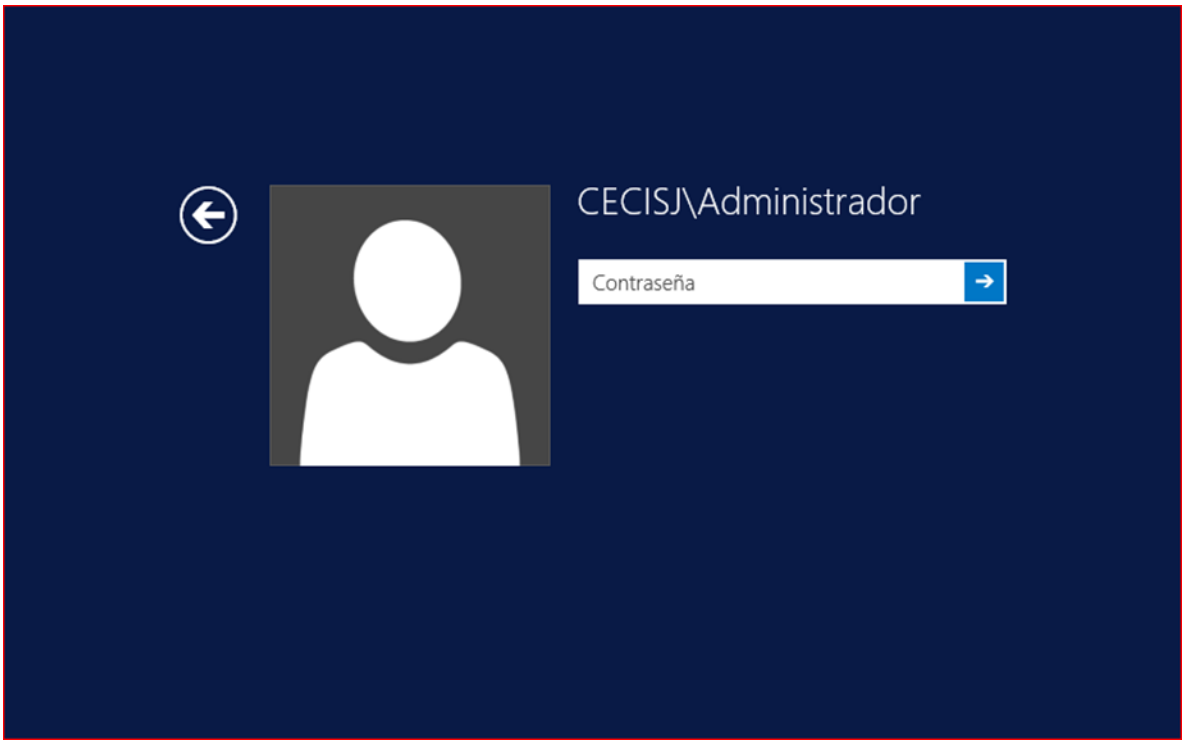
Figura 33: Configuración de dominio local 3



Fuente: elaboración propia.

Una vez reiniciado el servidor para completar la instalación, se puede observar en la figura 34 el dominio con la cuenta de administrador para su primer acceso:

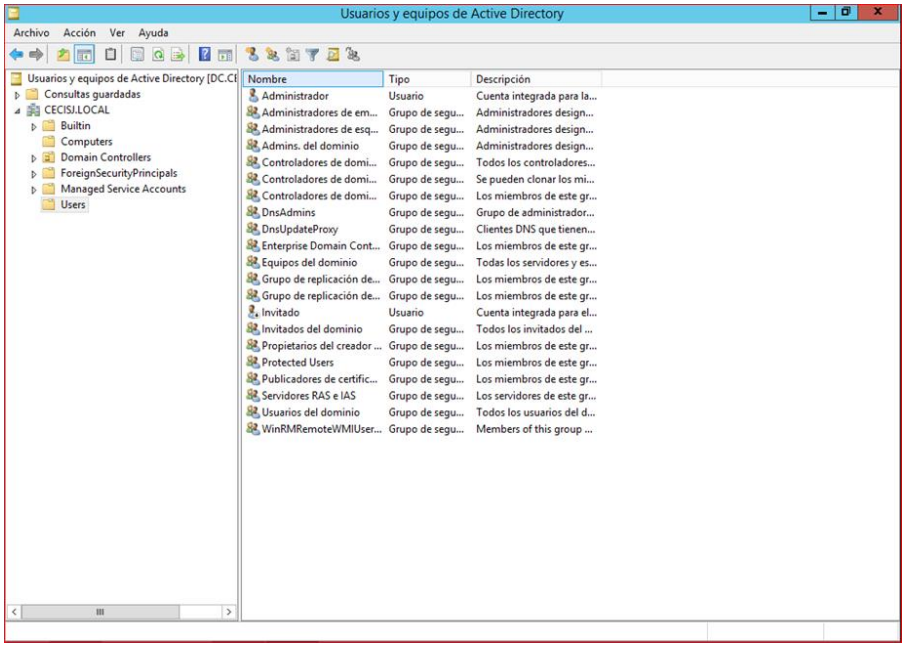
Figura 34: Cuenta de administrador configurada en dominio local



Fuente: elaboración propia.

Una vez que se ingresa, se puede verificar que el servicio de Active Directory ya se encuentra funcional para la creación de usuarios, equipos y grupos. La figura 35 muestra la visualización en pantalla:

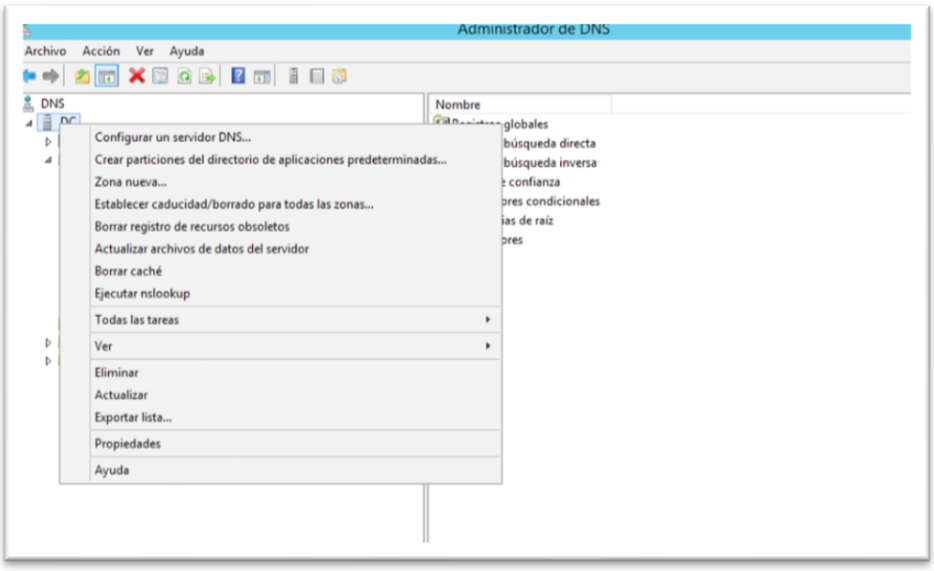
Figura 35: Verificación del servicio de Active Directory



Fuente: elaboración propia.

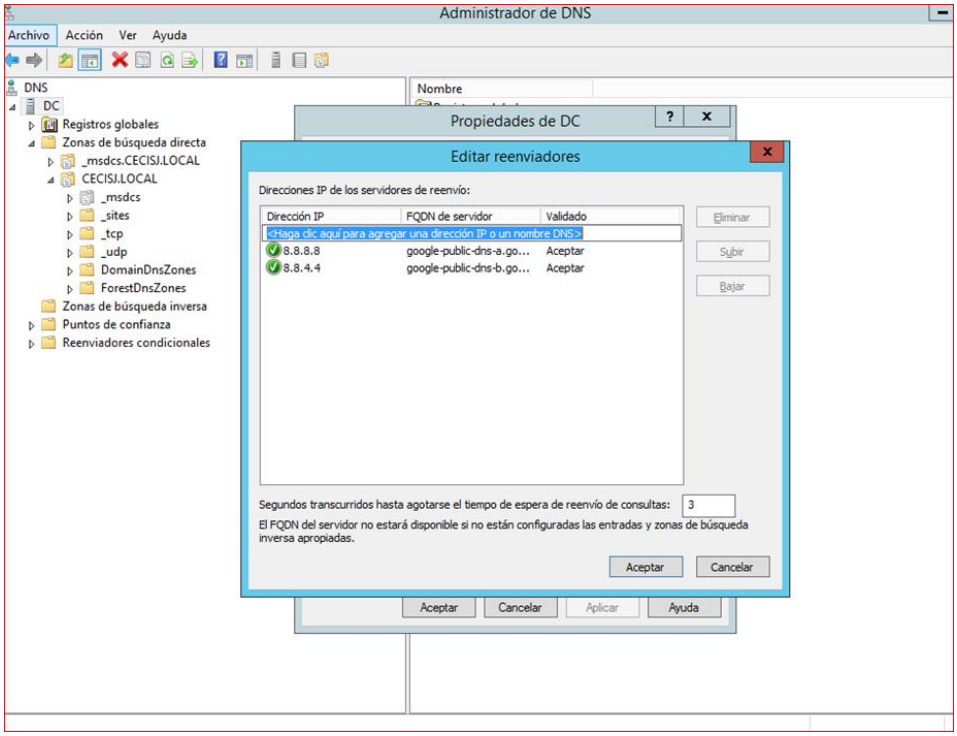
Otra configuración que es necesaria es la configuración de los reenviadores de internet para el servidor DNS, de manera que permita resolver consultas DNS para los clientes internos. Las figuras 36 y 37 muestra su configuración:

Figura 36: Configuración de los reenviadores de internet 1



Fuente: elaboración propia.

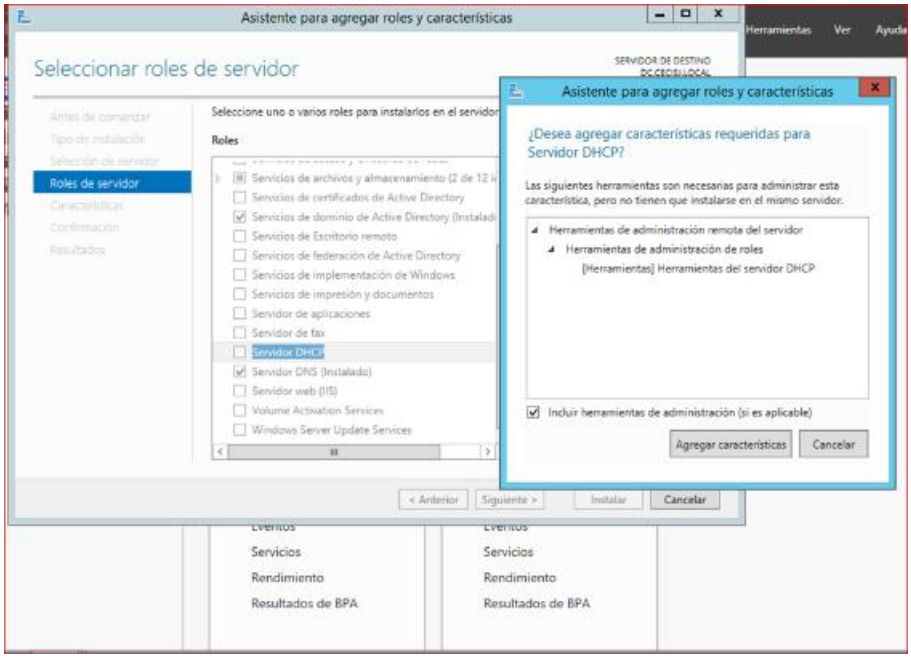
Figura 37: Configuración de los reenviadores de internet 2



Fuente: elaboración propia.

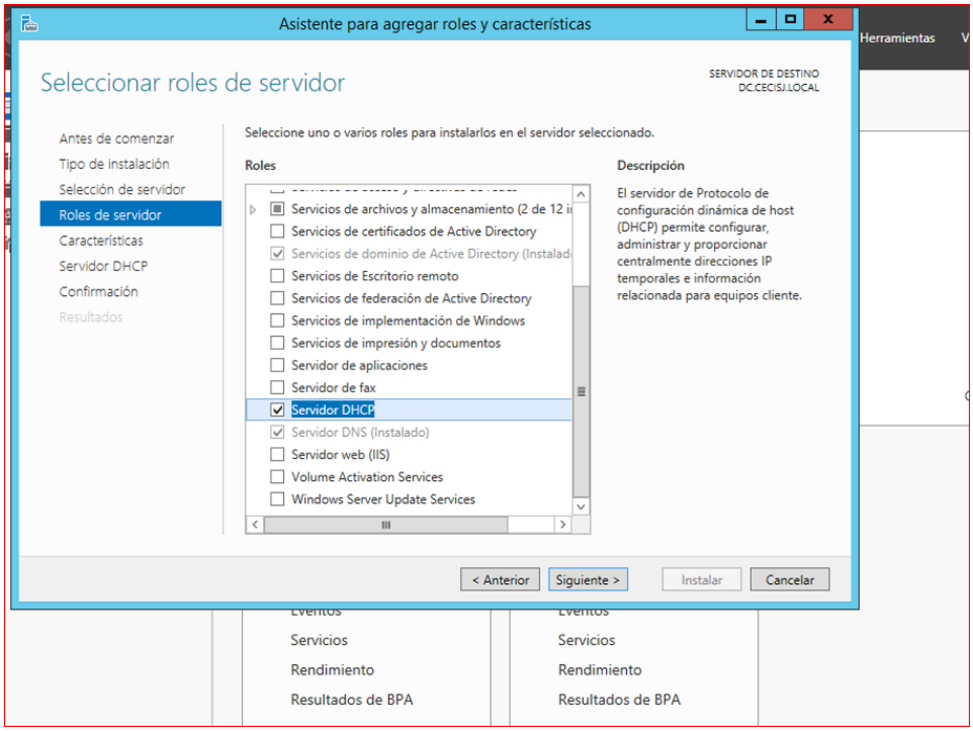
El siguiente paso es realizar la instalación del rol de DHCP que se encarga de entregar direcciones IP automáticamente a los clientes internos. Las figuras 38, 39, 40, 41, 42 y 43 muestran el proceso de instalación y activación.

Figura 38: Instalación DHCP 1



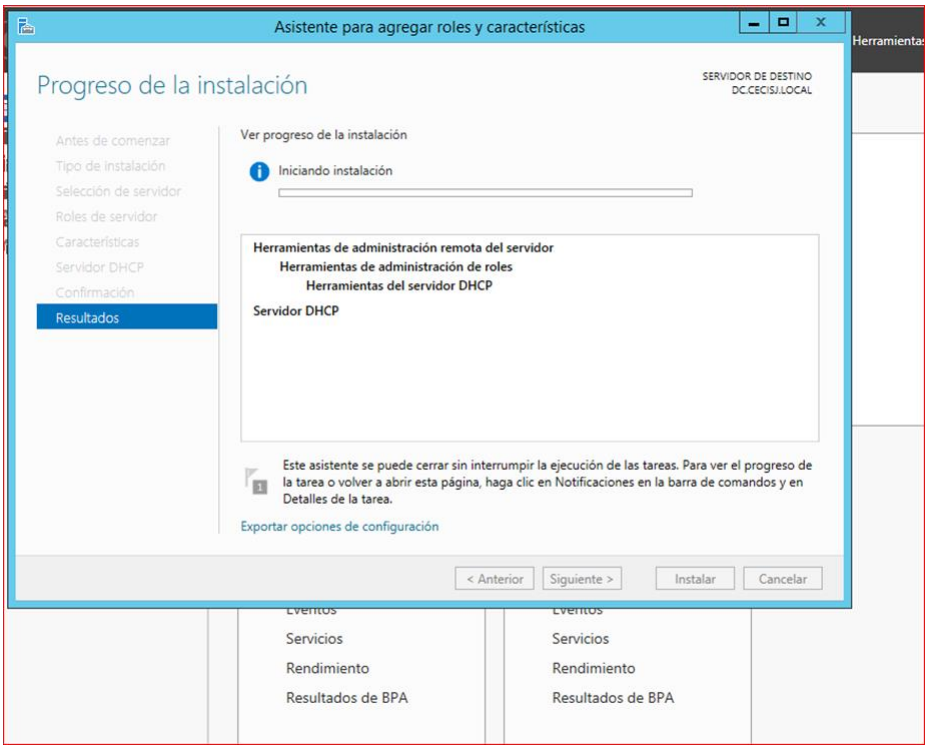
Fuente: elaboración propia.

Figura 39: Instalación DHCP 2



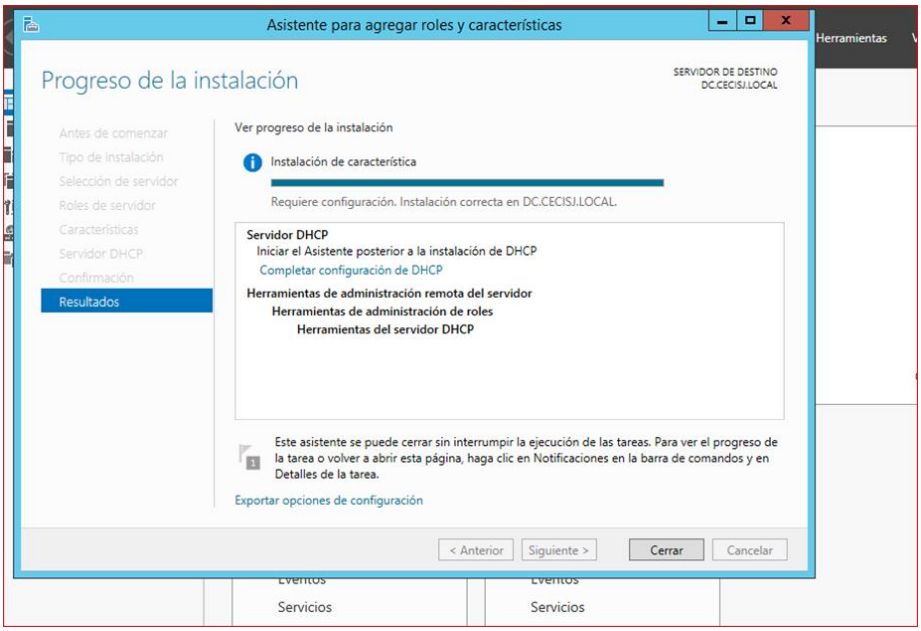
Fuente: elaboración propia.

Figura 40: Instalación DHCP 3



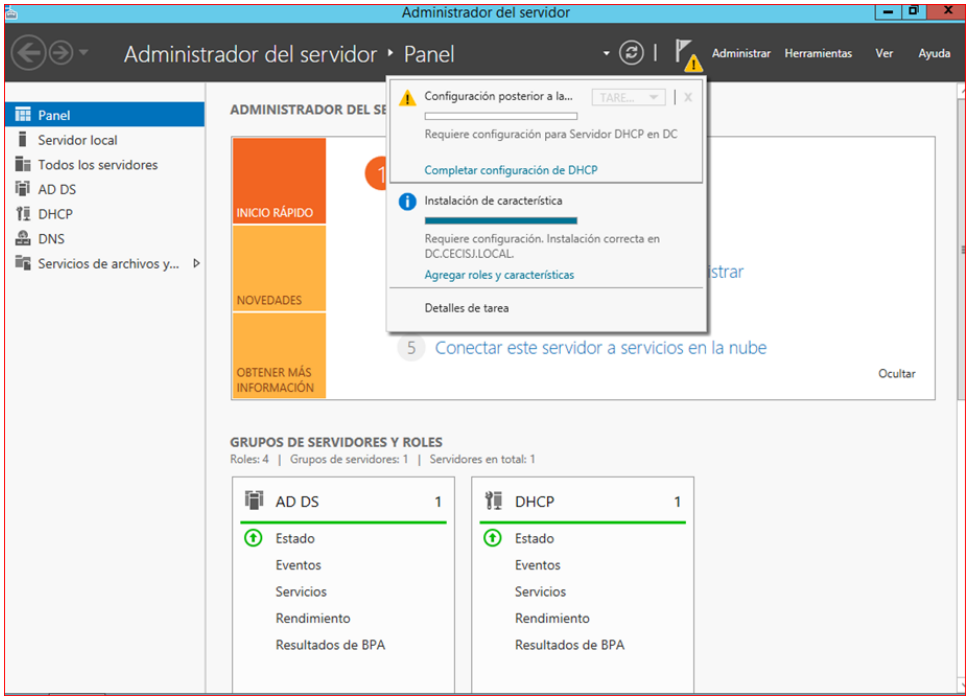
Fuente: elaboración propia.

Figura 41: Instalación DHCP 4



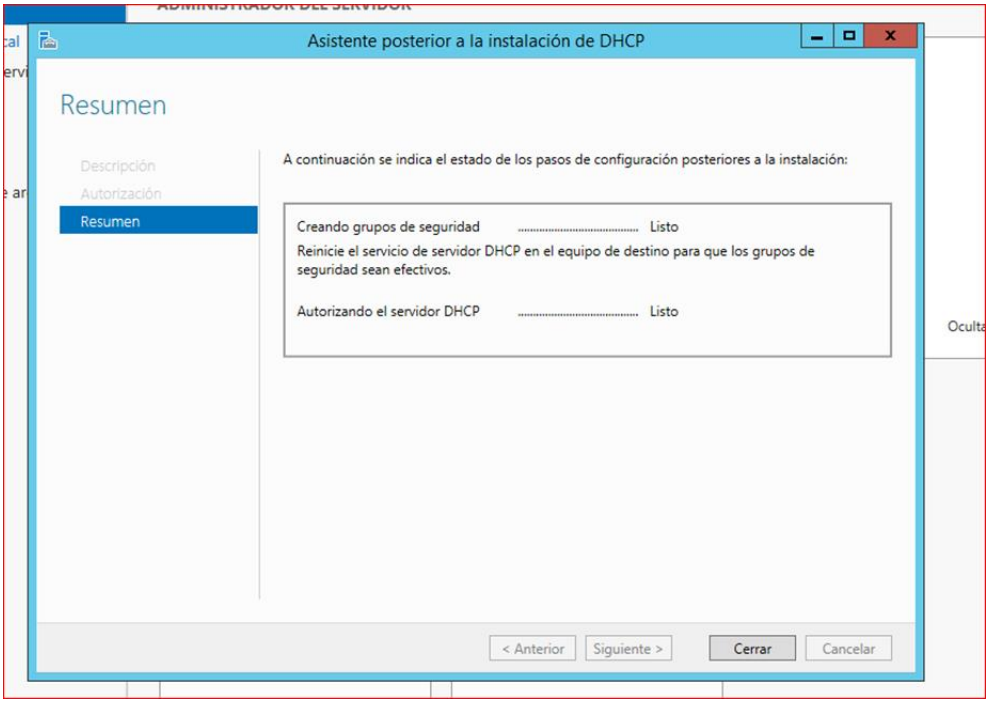
Fuente: elaboración propia.

Figura 42: Activación DHCP 1



Fuente: elaboración propia.

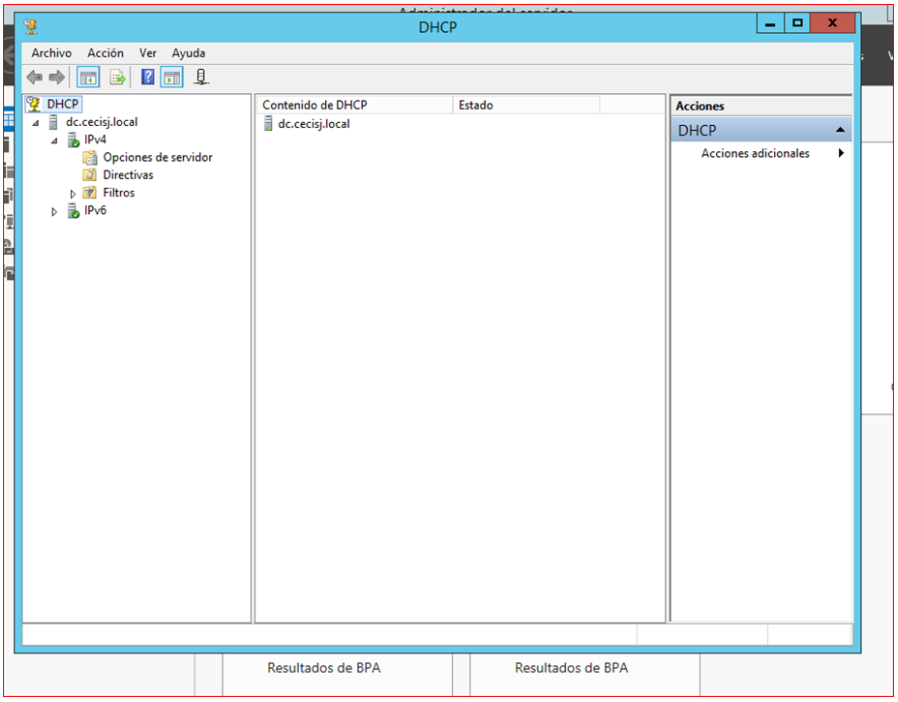
Figura 43: Activación DHCP 2



Fuente: elaboración propia.

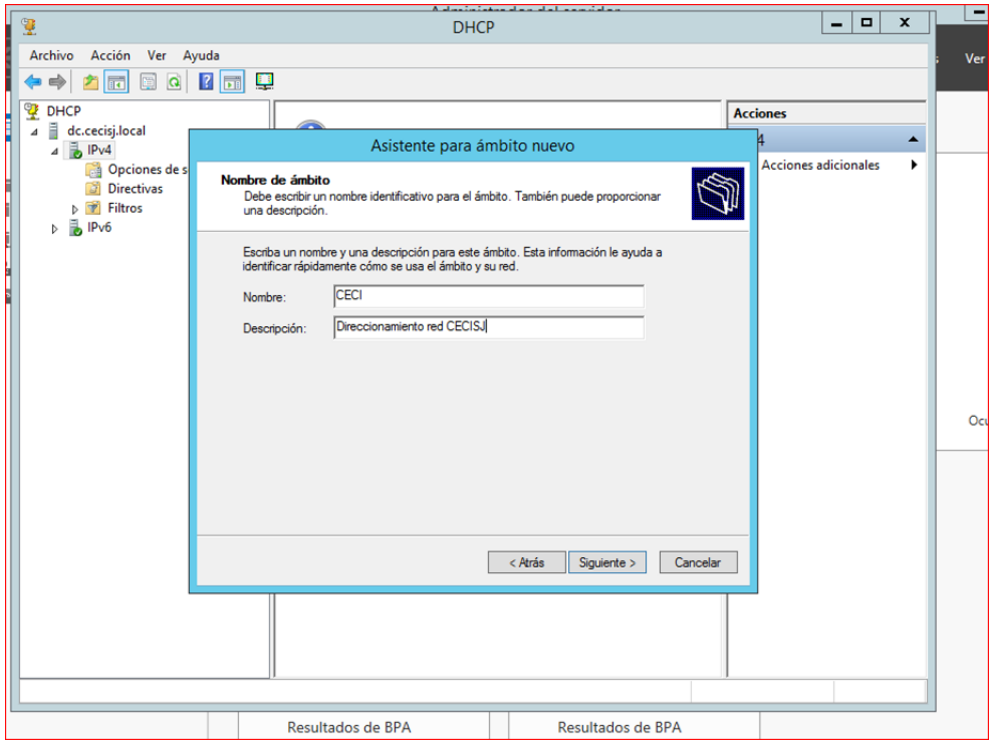
Después de realizar estos pasos, ya se tiene el servicio DHCP instalado y listo, por lo que se va a realizar la configuración del servicio indicando el rango de direcciones IP disponibles para ser entregadas a los clientes; las figuras 44, 45, 46, 47, 48 y 49 muestran el proceso.

Figura 44: DHCP listo para ser configurado



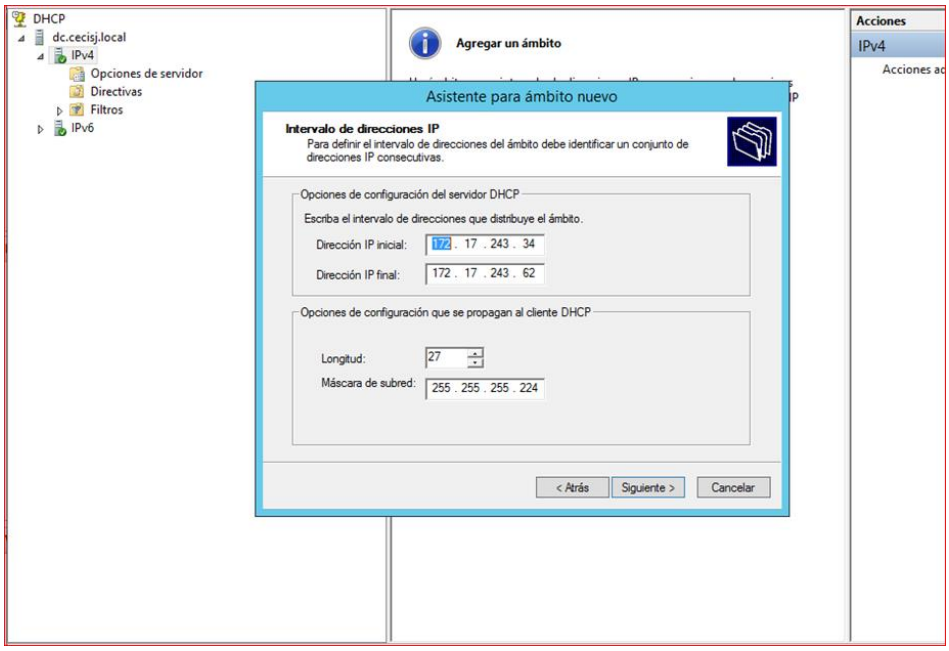
Fuente: elaboración propia.

Figura 45: Creación de nuevo ámbito



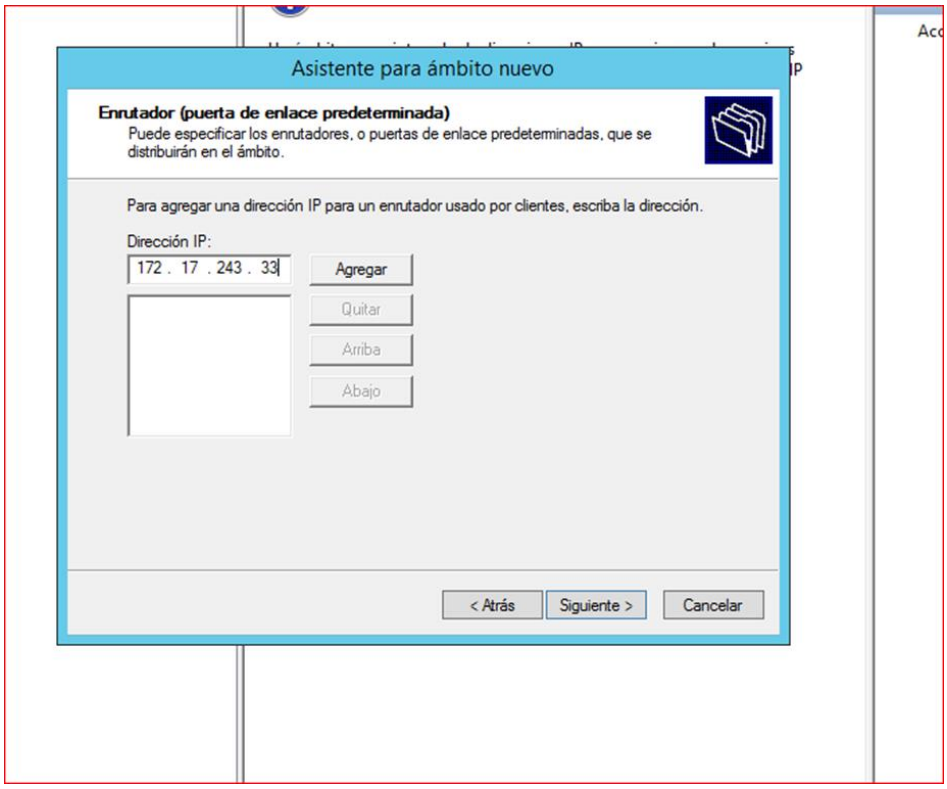
Fuente: elaboración propia.

Figura 46: Configuración del direccionamiento 1



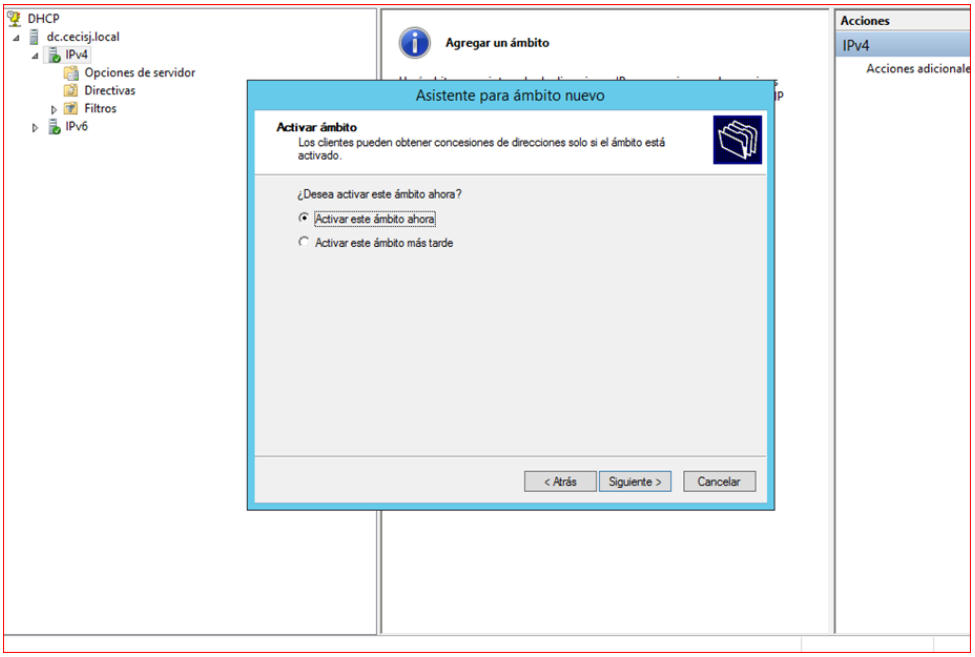
Fuente: elaboración propia.

Figura 47: Configuración del direccionamiento 2



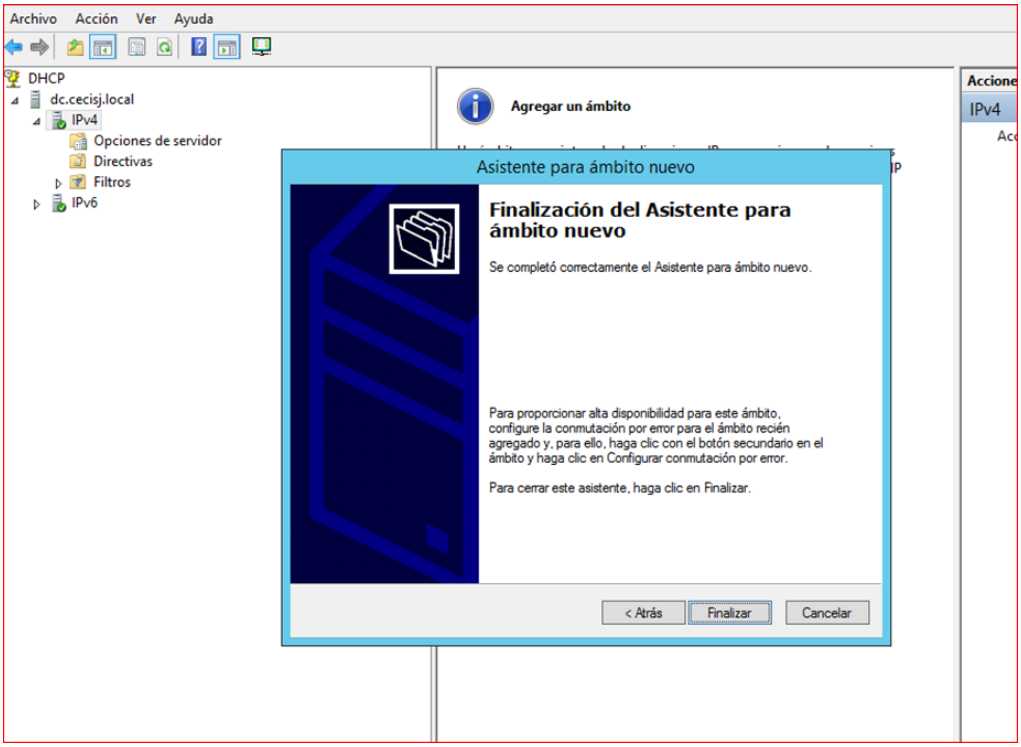
Fuente: elaboración propia.

Figura 48: Configuración del direccionamiento 3



Fuente: elaboración propia.

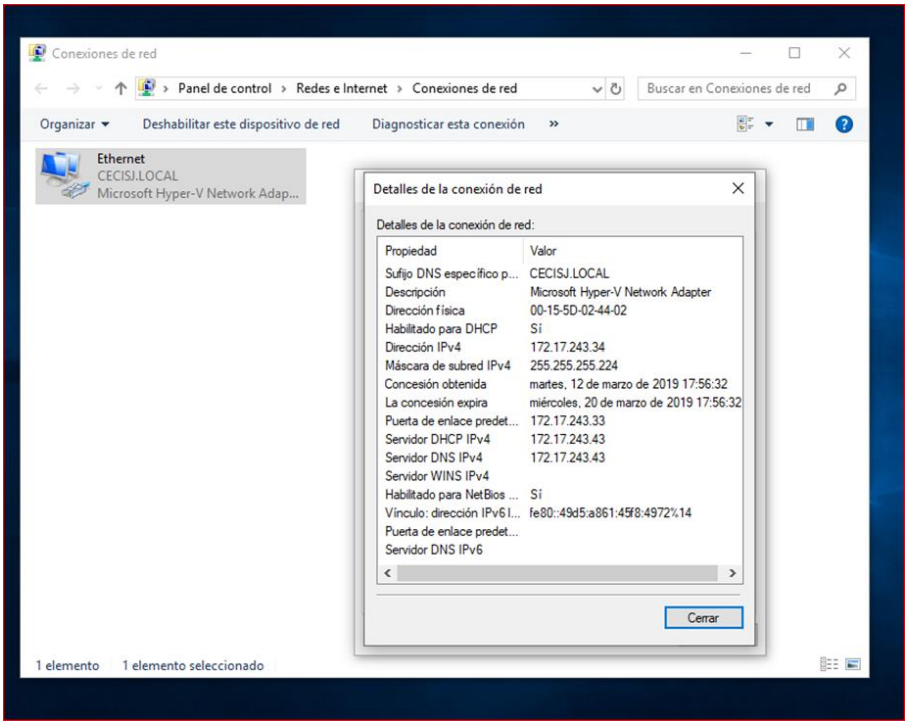
Figura 49: Configuración de direccionamiento 4



Fuente: elaboración propia.

El siguiente paso es ingresar a los equipos como usuario administrador para verificar que el DHCP esté asignando las direcciones correctamente; lo anterior se muestra en la figura 50.

Figura 50: Verificación de direccionamiento DHCP



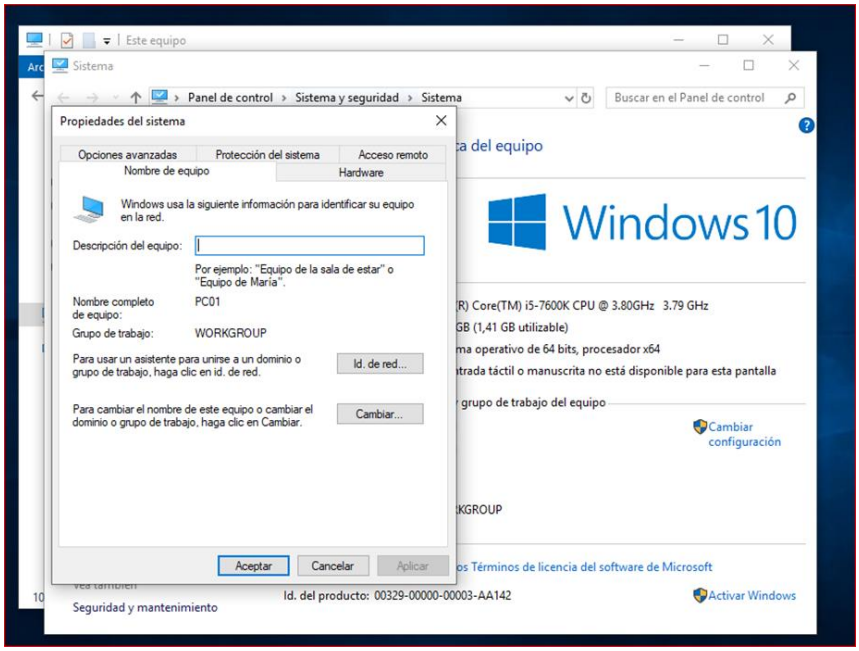
Fuente: elaboración propia.

Como segundo paso se debe agregar el equipo cliente al dominio local y asignarle un nombre de equipo, en este caso el nombre del equipo es PC01.

Sin embargo, se recomienda que para el CECI los equipos tengan un nombre con una nomenclatura similar a la siguiente: CECISJ-PC01, CECISJ-PC02. La nomenclatura CECISJ-SRV01 para el caso de un servidor y CECISJ-IMP01 en caso de que en el futuro puedan contar con una impresora en red.

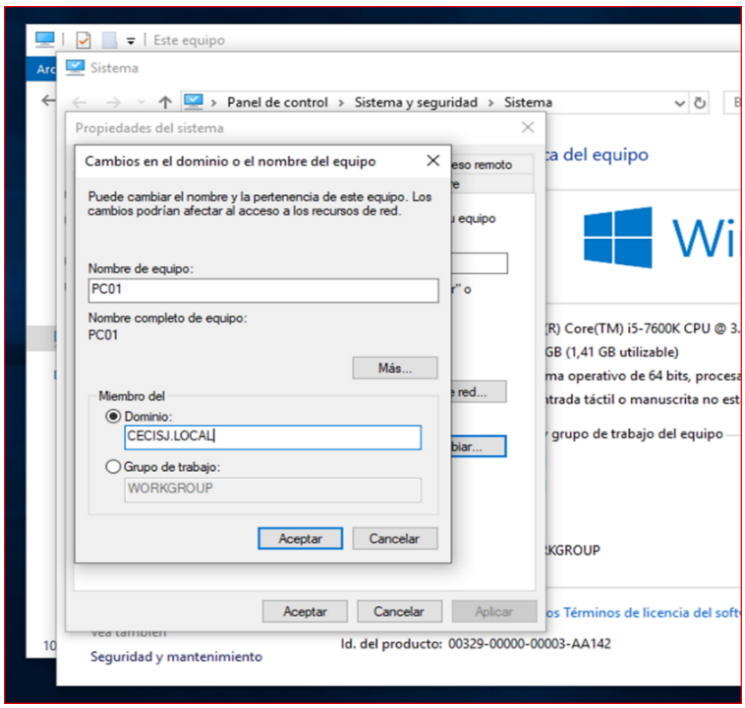
De esta manera, los primeros caracteres corresponderán al lugar donde pertenecen los equipos, seguidamente el tipo de dispositivo y número de equipo. Con esto se pretende mantener un registro de equipos mucho más ordenado y que facilite su reconocimiento en caso de falla u otros inconvenientes. Esto se puede apreciar en las figuras 51, 52, 53, 54, 55 y 56.

Figura 51: Inclusión del equipo cliente al dominio local 1



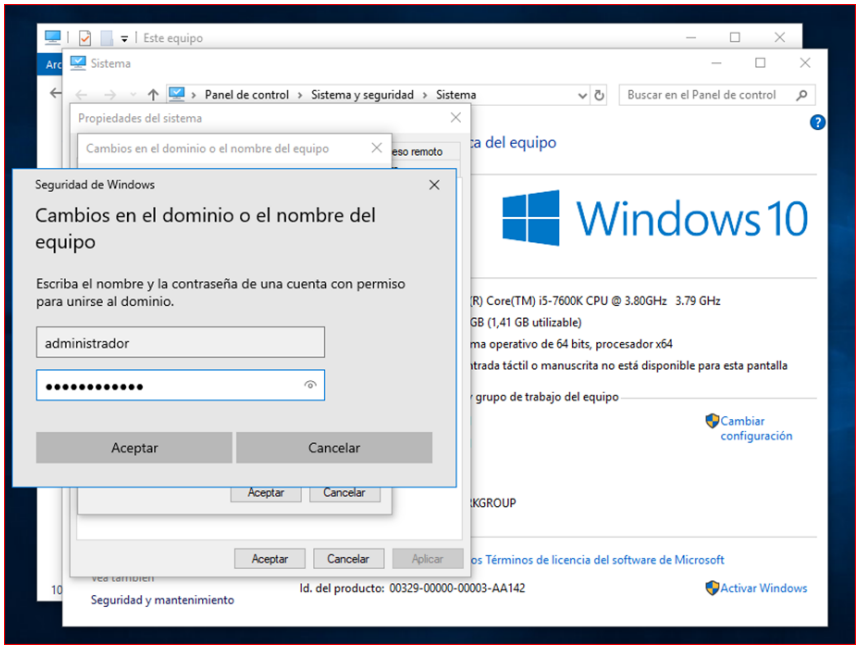
Fuente: elaboración propia.

Figura 52: Inclusión del equipo cliente al dominio local 2



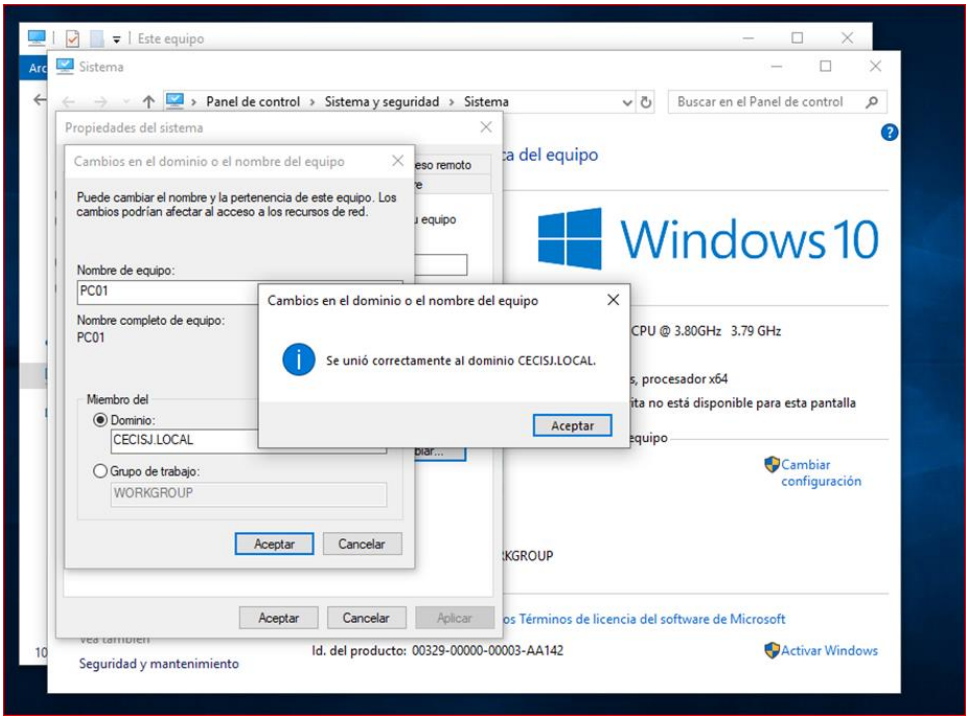
Fuente: elaboración propia.

Figura 53: Inclusión del equipo cliente al dominio local 3



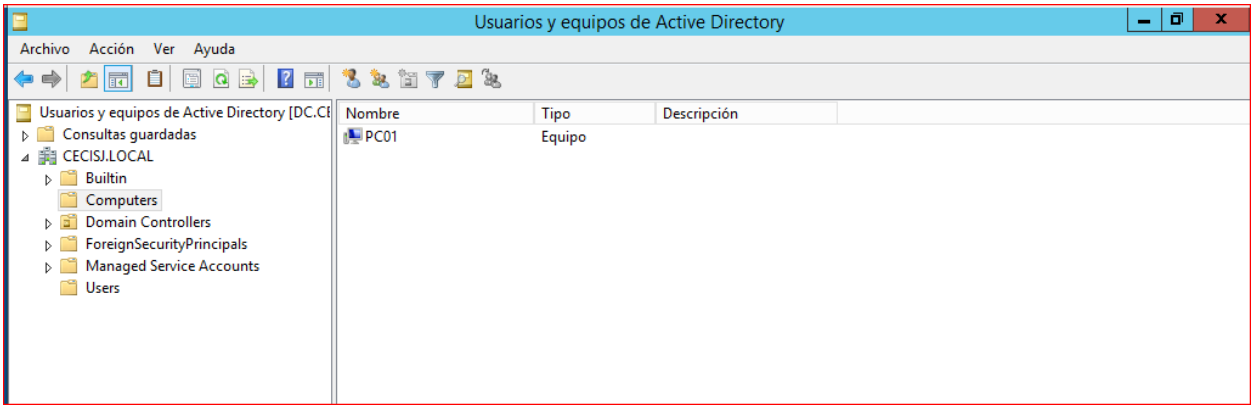
Fuente: elaboración propia.

Figura 54: Inclusión del equipo cliente al dominio local 4



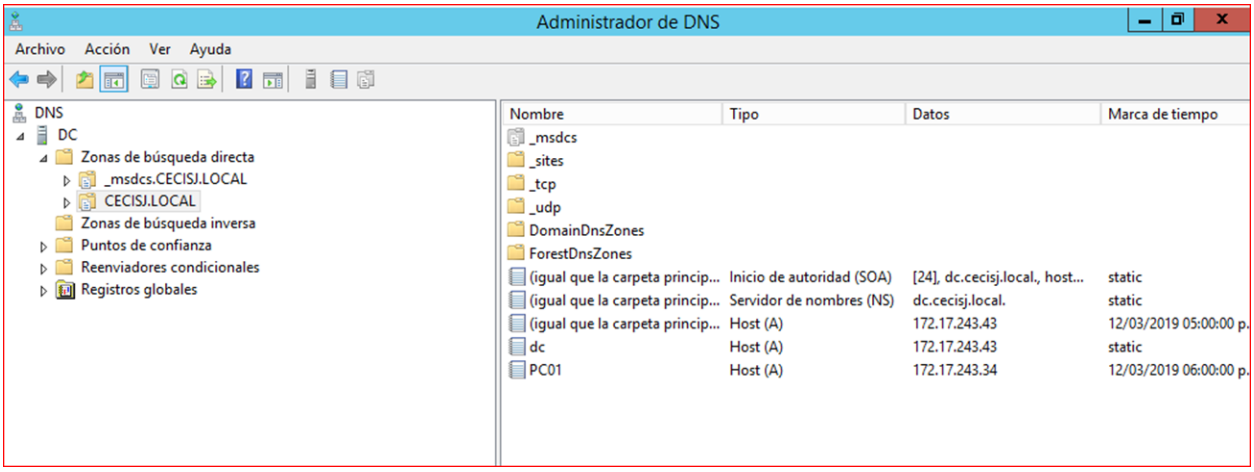
Fuente: elaboración propia.

Figura 55: Verificación del registro del cliente en el dominio



Fuente: elaboración propia.

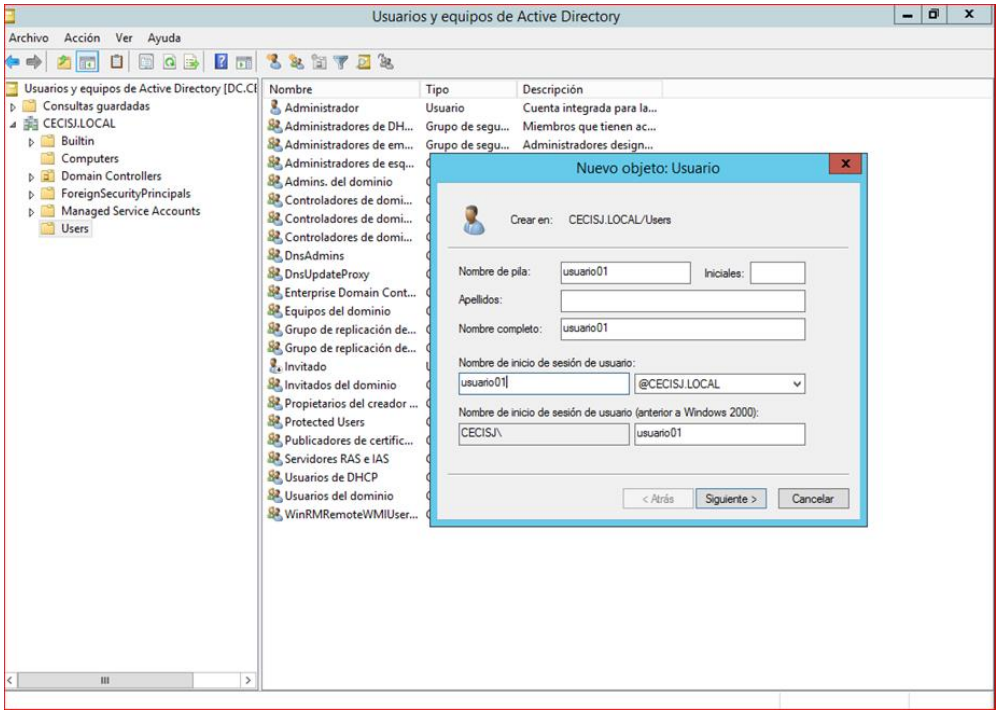
Figura 56: Verificación del cliente en el DNS



Fuente: elaboración propia.

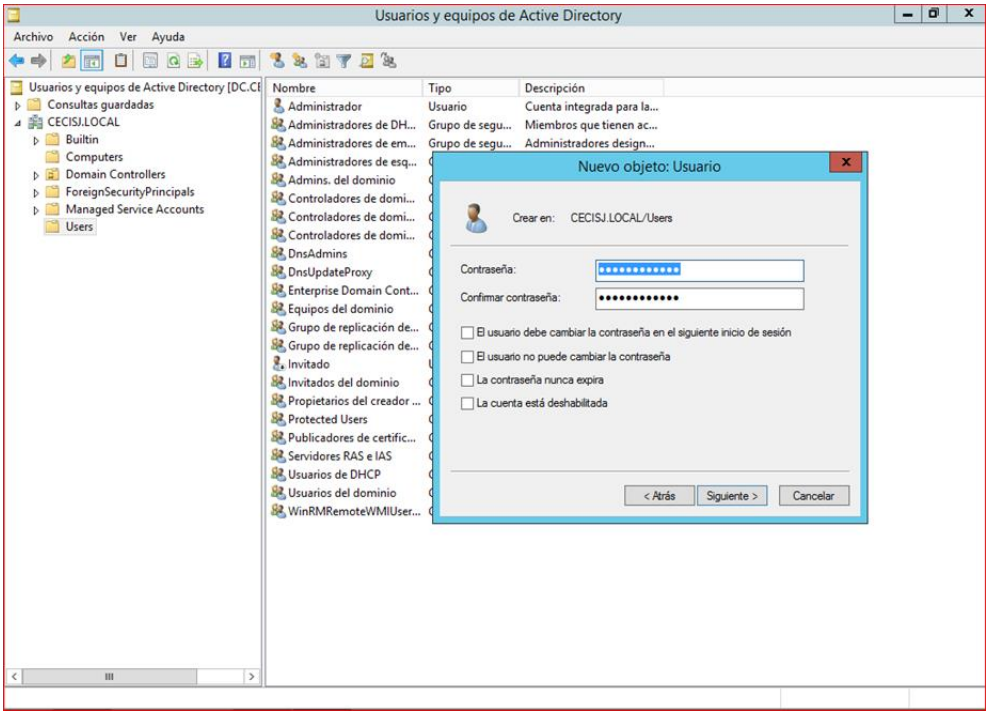
Acto seguido, en las figuras 57, 58 y 59 se puede observar la creación uno de los usuarios de red en el Active Directory. Para efectos del presente proyecto el nombre de este usuario va a ser: Usuario01. Sin embargo, para efectos del CECI se recomienda la siguiente nomenclatura: CECI01, CECI02 o CECI_Admin para los usuarios administradores. Es importante mencionar que en empresas o lugar donde las computadoras son asignadas a una sola persona, se suele utilizar la primera letra del nombre junto con el apellido, un ejemplo de usuario para alguien llamado Carlos Soto Alpízar sería: csoto y en caso de que ese usuario ya exista cambiaría a: csalpizar.

Figura 57: Creación de usuario de red



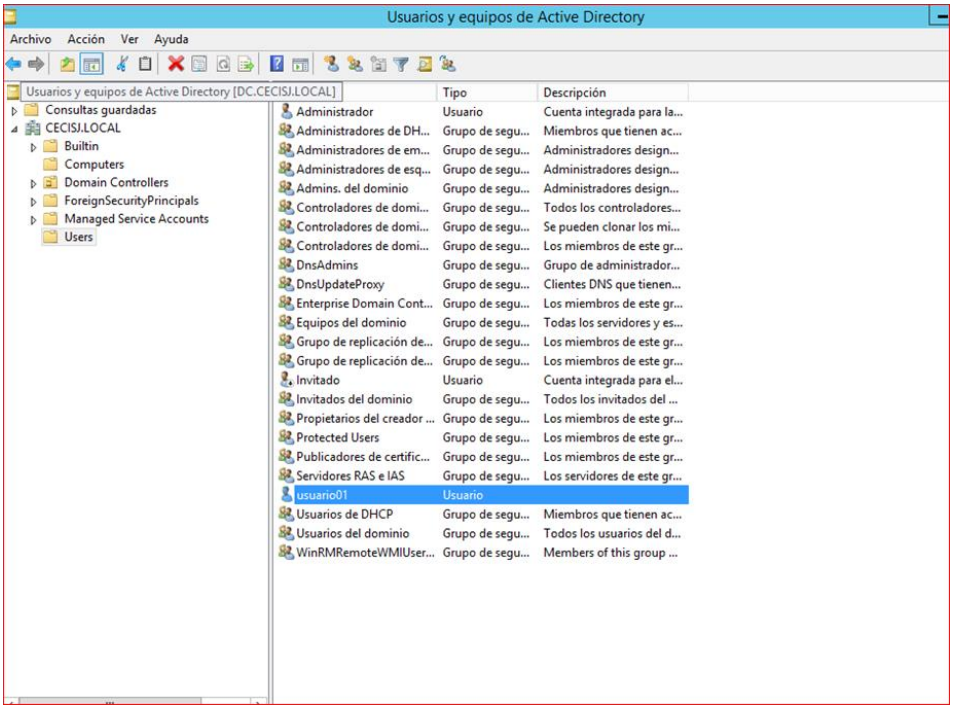
Fuente: elaboración propia.

Figura 58: Asignación de contraseña



Fuente: elaboración propia.

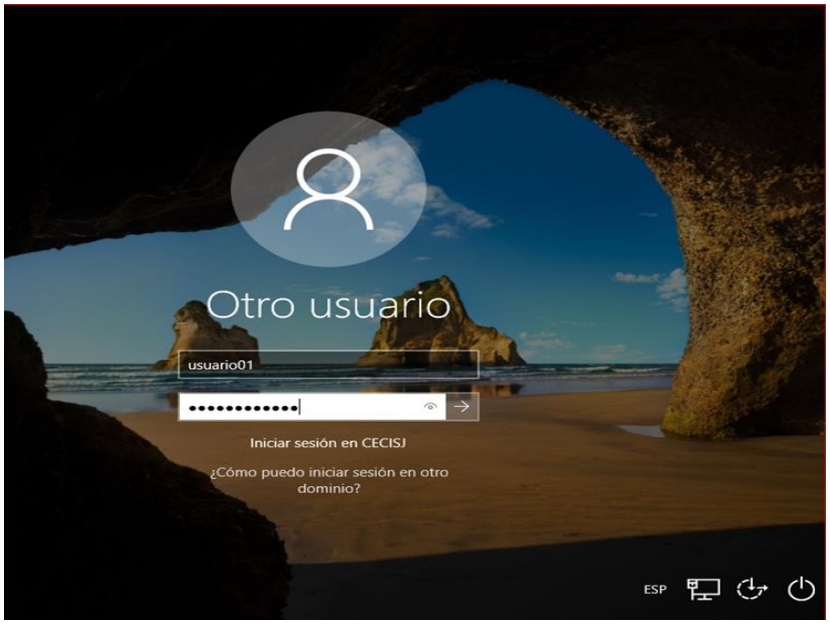
Figura 59: Usuario creado correctamente



Fuente: elaboración propia.

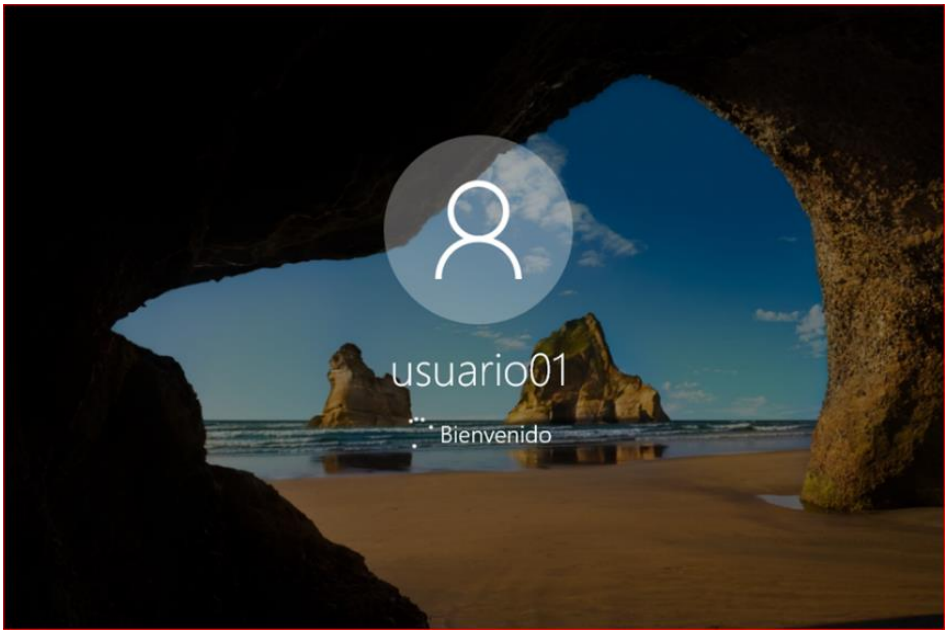
En el siguiente paso vamos a verificar que se pueda acceder a las máquinas con el usuario de red que se acaba de crear, este paso se muestra en las figuras 60, 61, 62 y 63.

Figura 60: Ingreso con usuario de red



Fuente: elaboración propia.

Figura 61: Carga de perfil de usuario de red

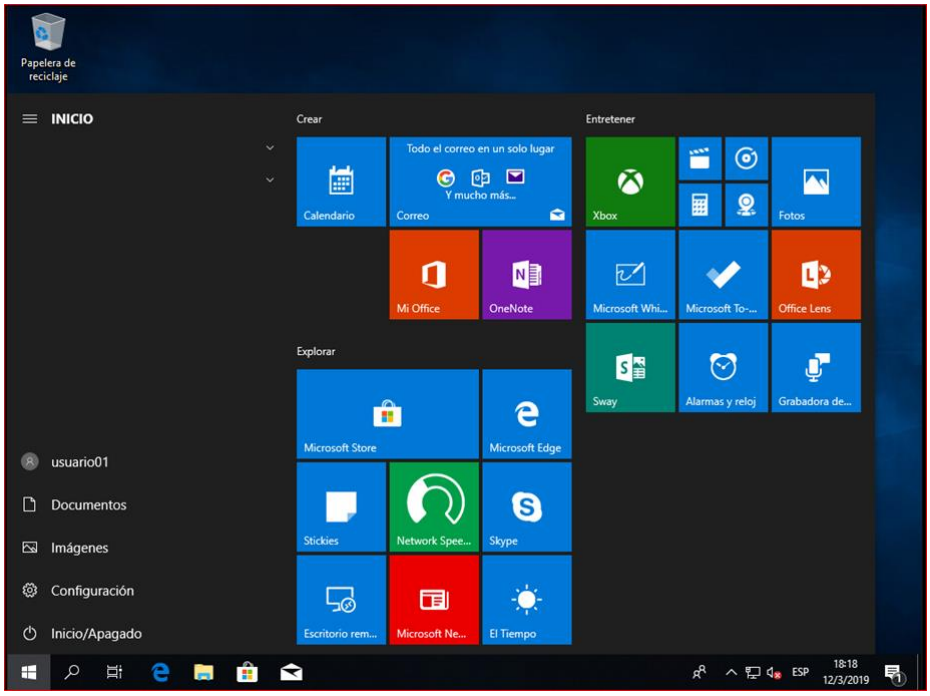


Fuente: elaboración propia.

Figura 62: Perfil completado para el usuario 1

Fuente: elaboración propia.

Figura 63: Perfil completado para el usuario 2

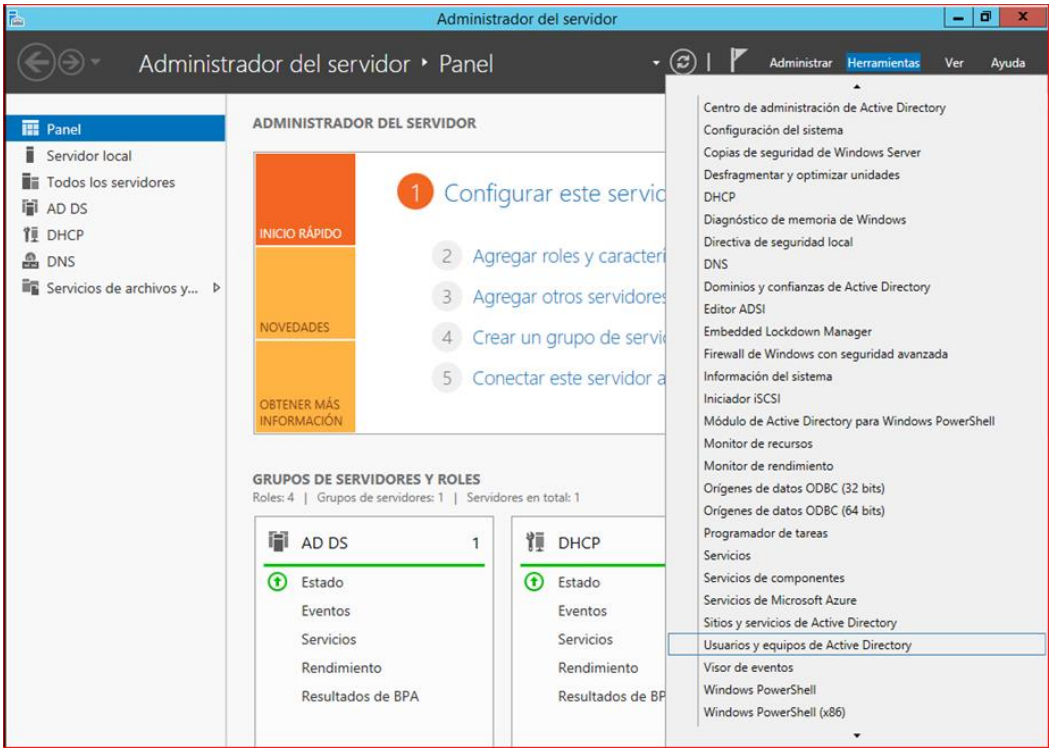


Fuente: elaboración propia.

En el siguiente paso se va a realizar la configuración de un grupo de usuarios en el Active Directory, lo cual simplifica la administración, ya que se pueden asignar permisos a un grupo de usuarios para que todos se vean afectados de una sola vez, y no tener que asignar los permisos uno por uno.

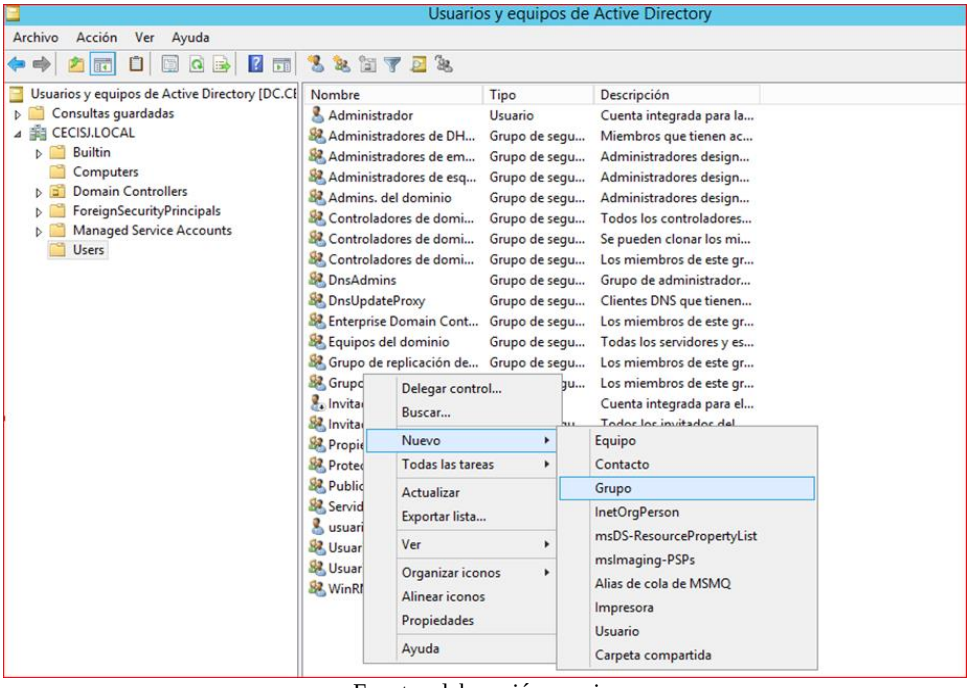
También es muy útil cuando se requiere asignar permisos temporales a uno o más usuarios, se pueden agregar a un grupo y después de cierto tiempo cambiarlos a su grupo original. Las figuras 64, 65, 66, 67, 68, 69 muestran la creación del grupo y la inclusión del usuario Usuario01 a este grupo.

Figura 64: Creación de grupo en Active Directory 1



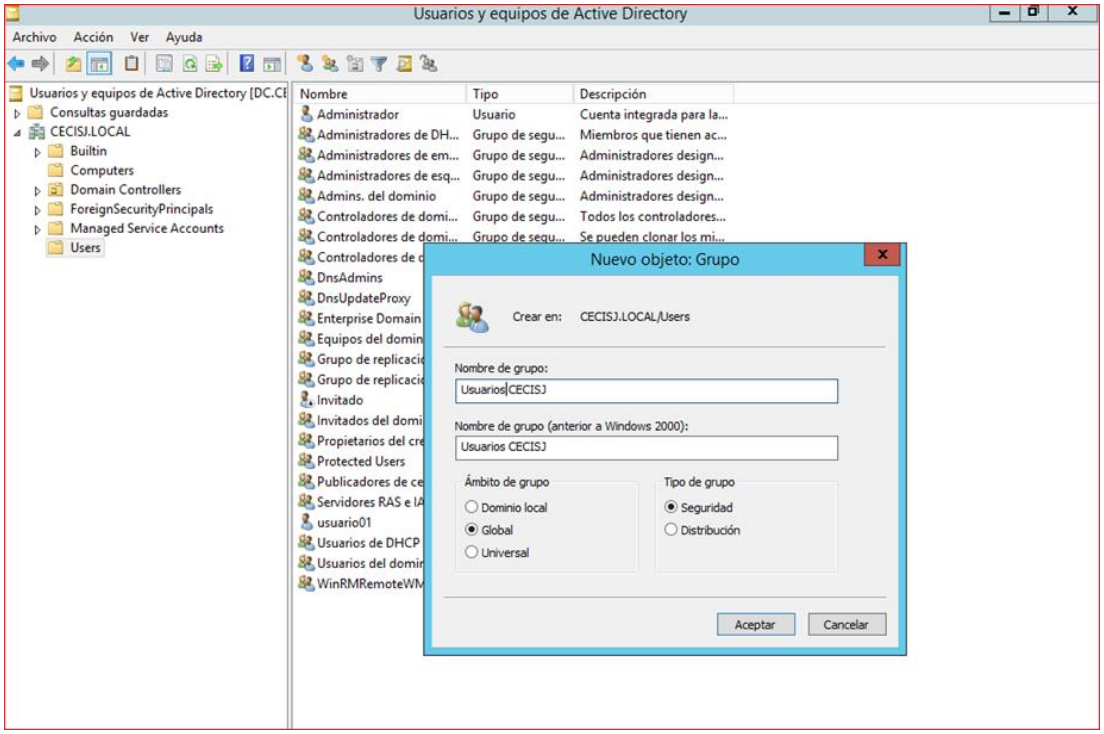
Fuente: elaboración propia.

Figura 65: Creación de grupo en Active Directory 2



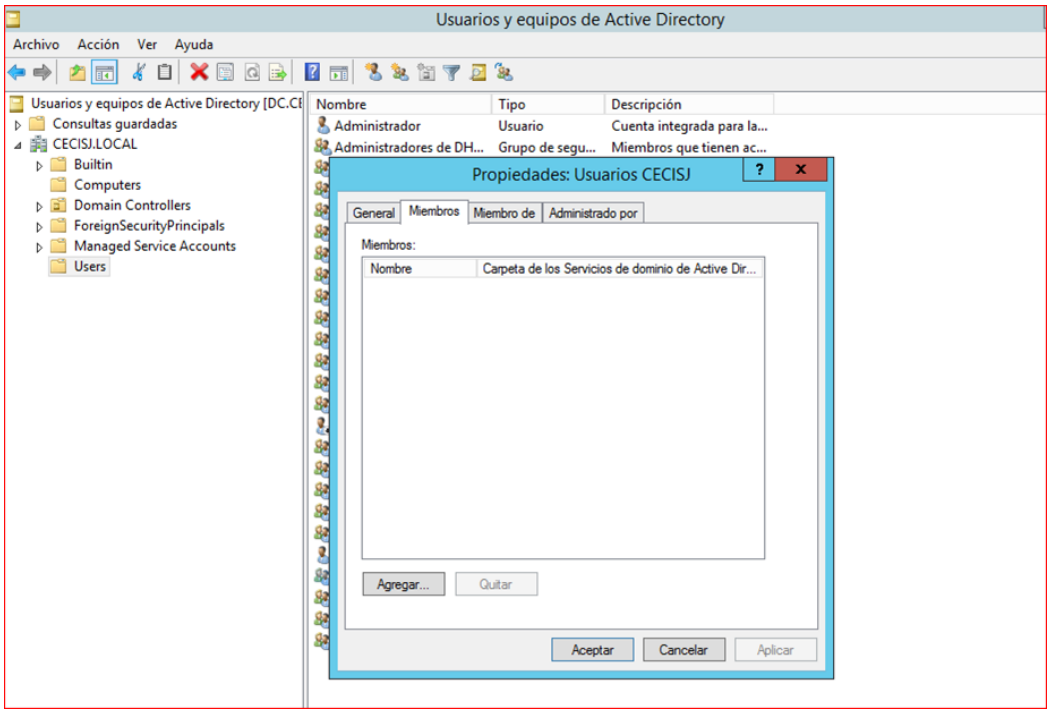
Fuente: elaboración propia.

Figura 66: Creación de grupo en Active Directory 3



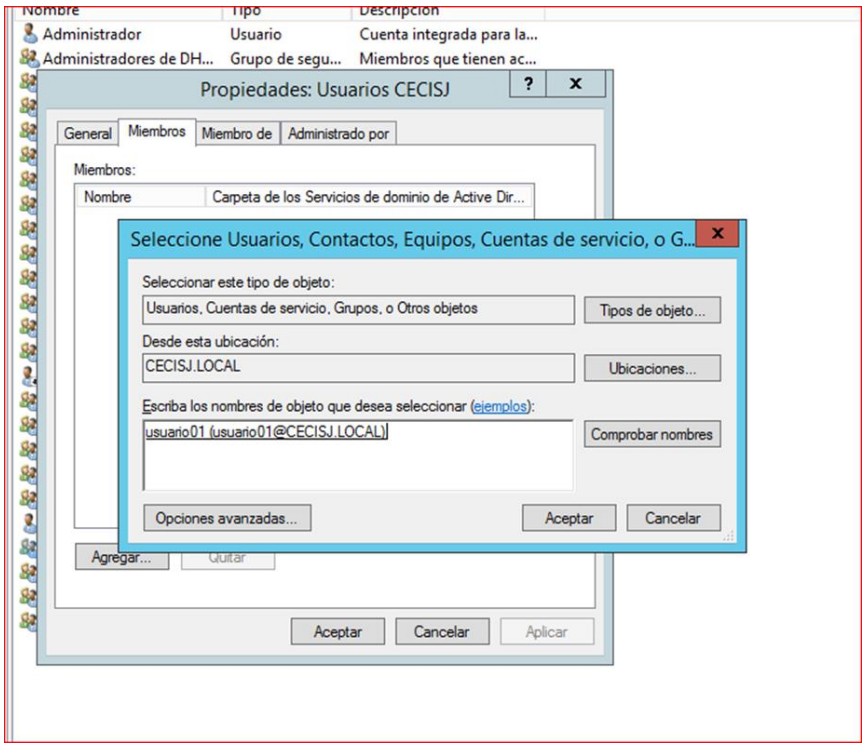
Fuente: elaboración propia.

Figura 67: Inclusión de usuario en grupo 1



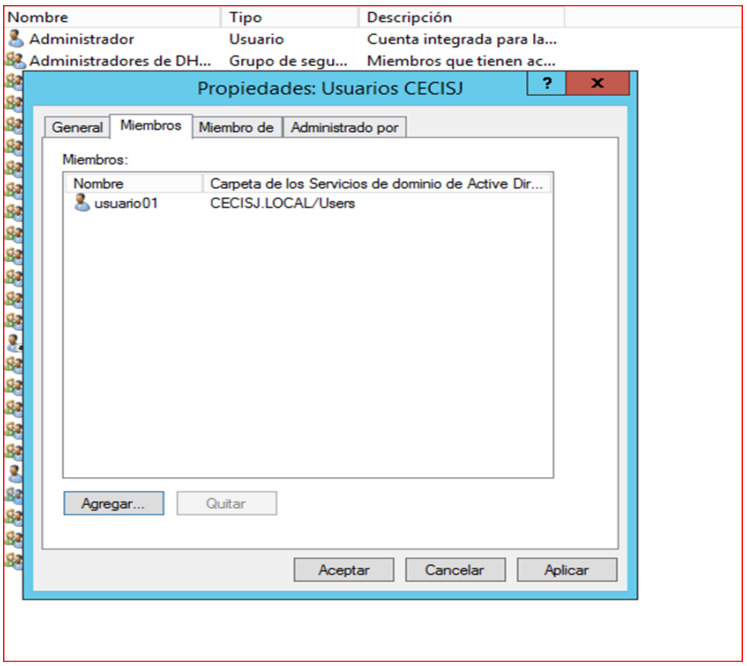
Fuente: elaboración propia.

Figura 68: Inclusión de usuario en grupo 2



Fuente: elaboración propia.

Figura 69: Inclusión de usuario en grupo 3

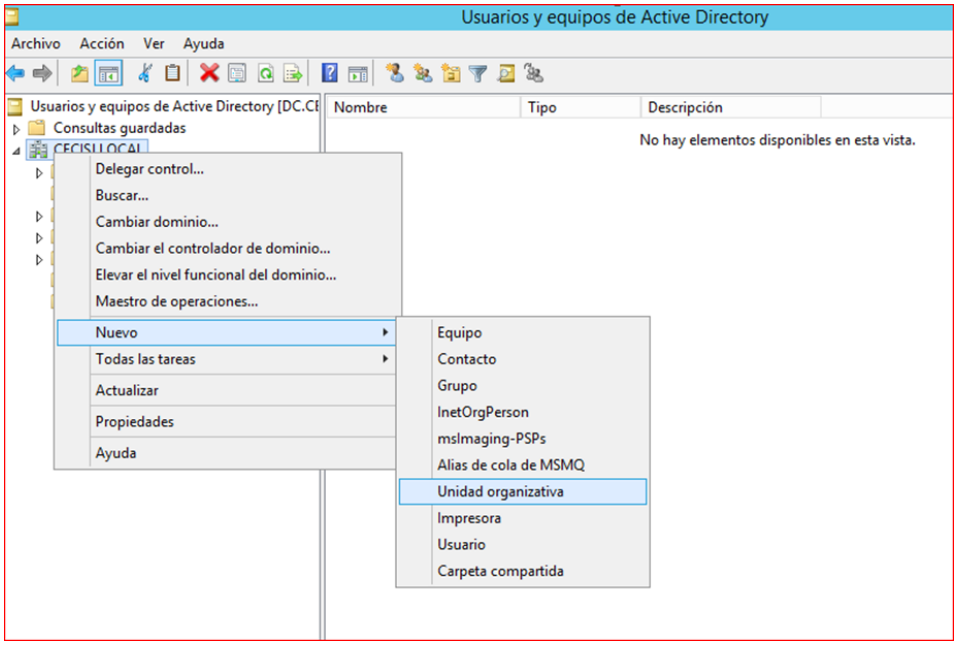


Fuente: elaboración propia.

El siguiente paso que se va a realizar es crear una Unidad Organizativa para los usuarios del CECI, esto permite administrar de mejor manera las cuentas de usuarios, equipos y grupos, también pueden agregar dispositivos compartidos para ser administrados, un ejemplo de esto son las impresoras en red.

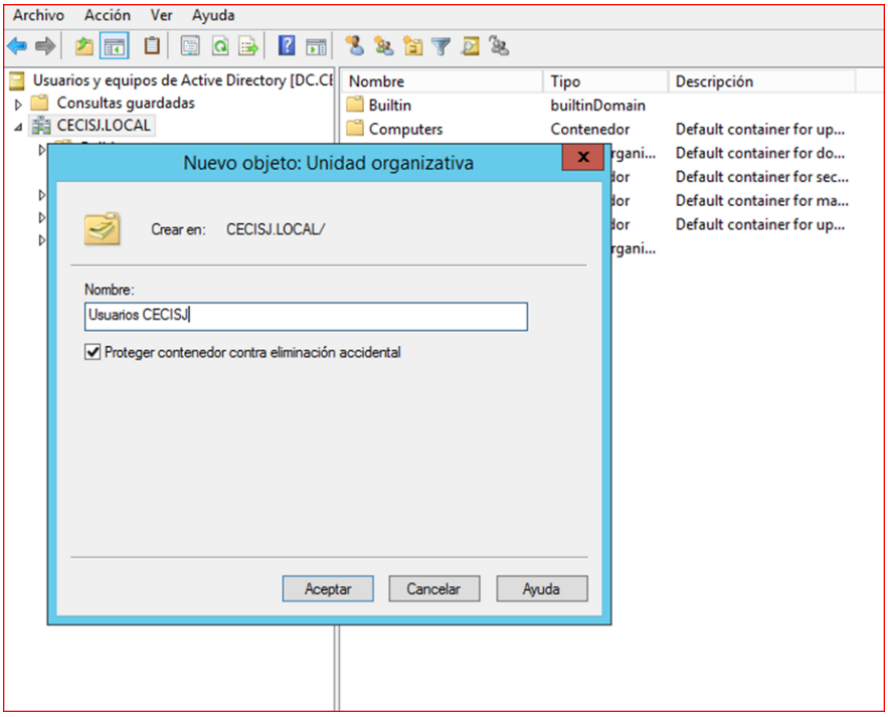
Las figuras 70, 71, 72, 73, 74 y 75 muestran los pasos para su creación.

Figura 70: Creación de Unidad Organizativa para usuarios 1



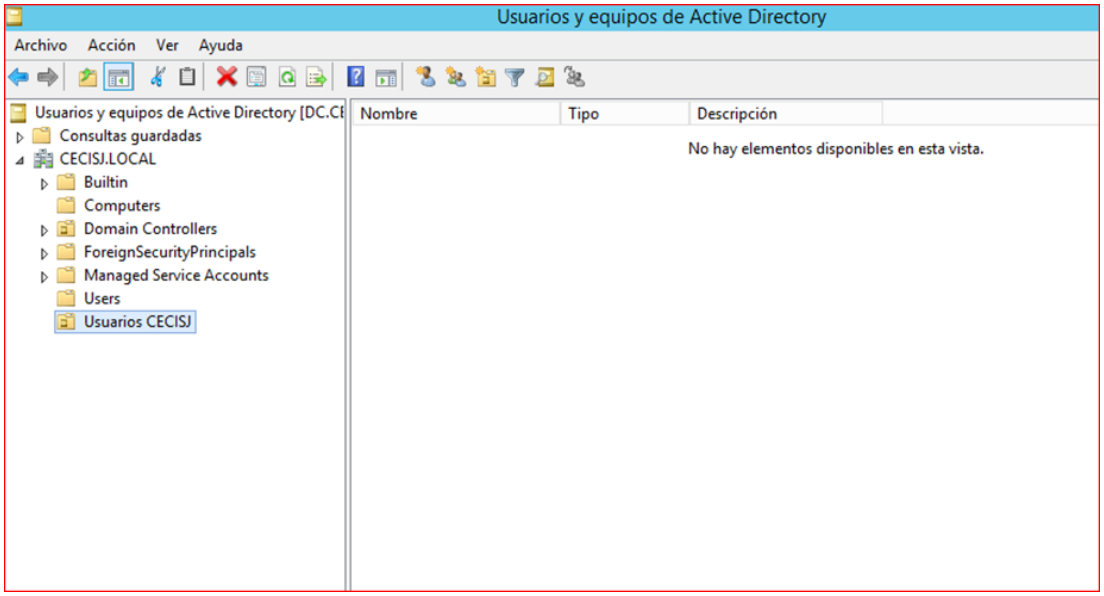
Fuente: elaboración propia.

Figura 71: Creación de Unidad Organizativa para usuarios 2



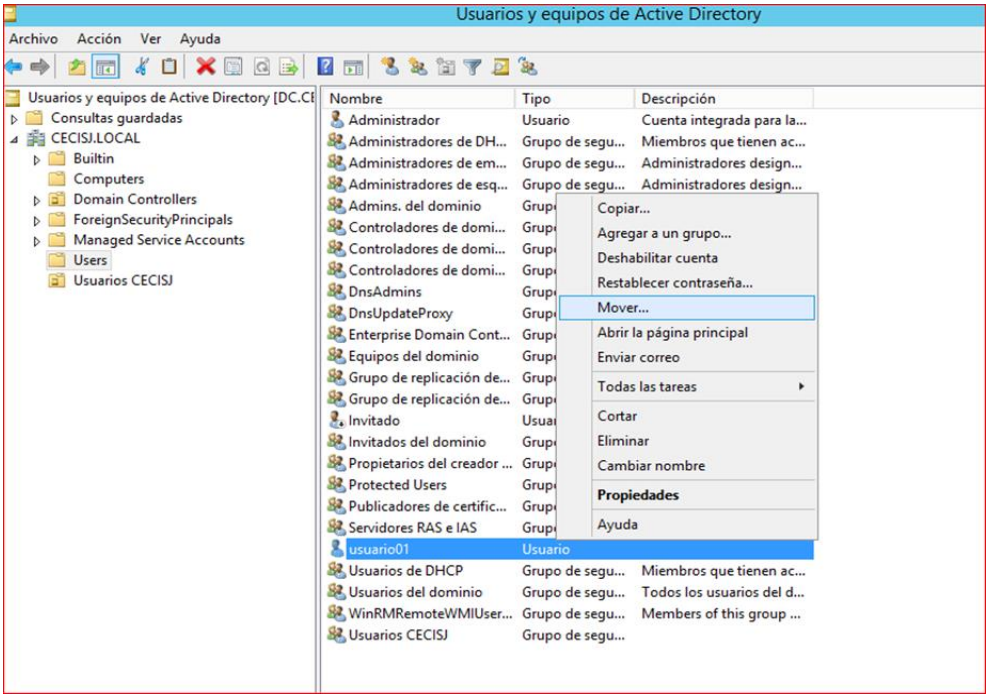
Fuente: elaboración propia.

Figura 72: Creación de Unidad Organizativa para usuarios 3



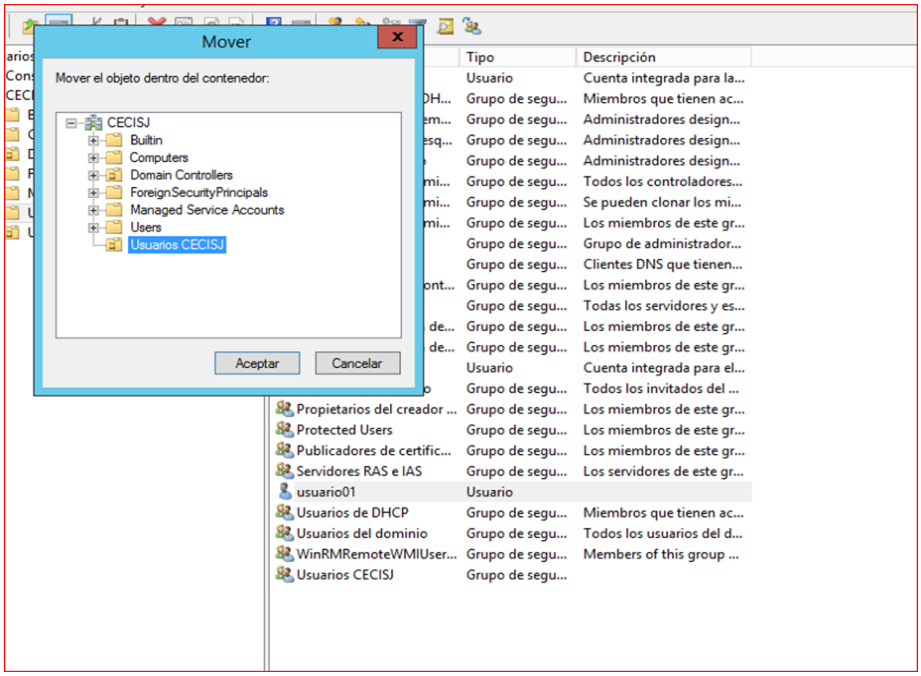
Fuente: elaboración propia.

Figura 73: Mover usuarios a la nueva Unidad Organizativa 1



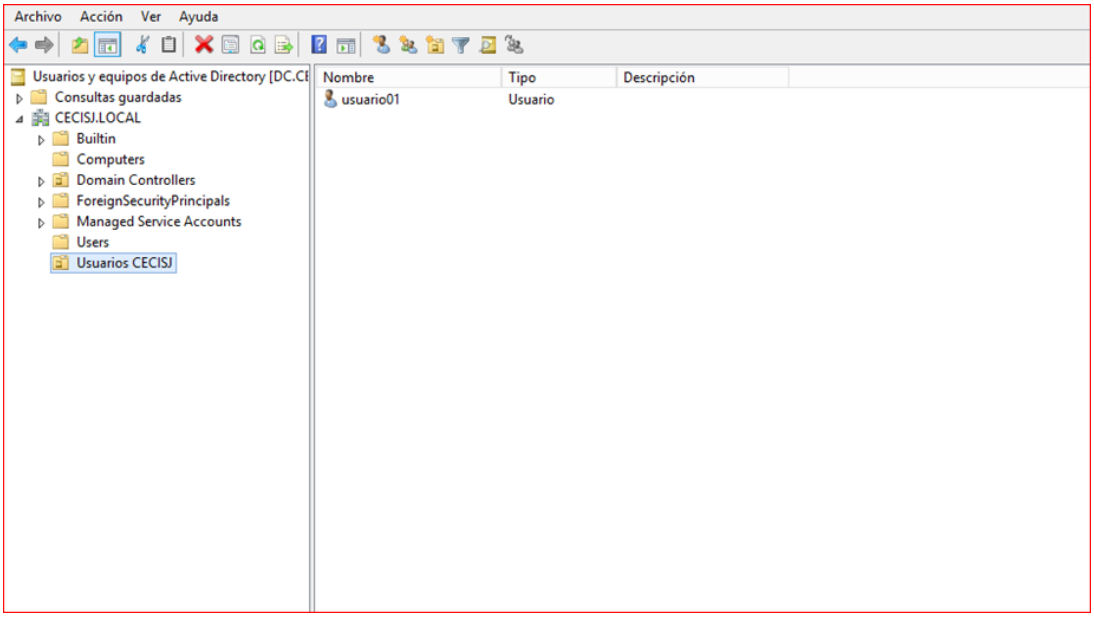
Fuente: elaboración propia.

Figura 74: Mover usuarios a la nueva Unidad Organizativa 2



Fuente: elaboración propia.

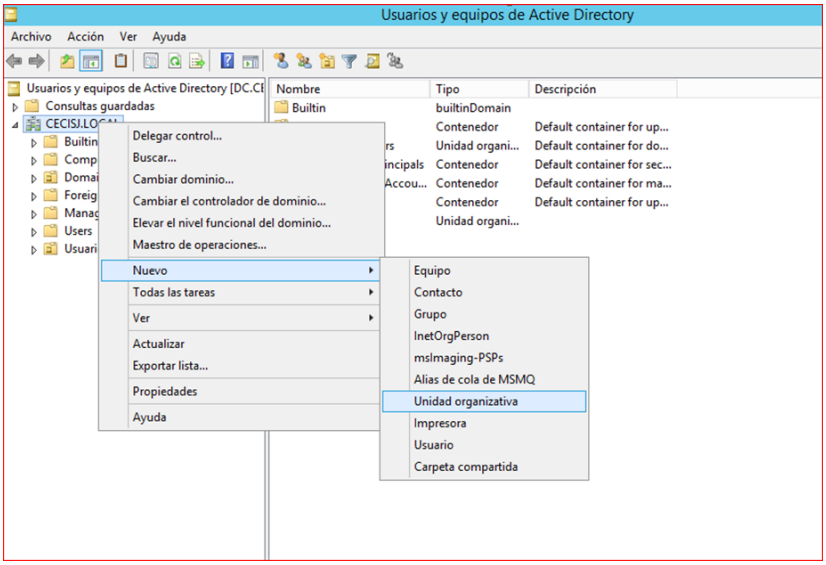
Figura 75: Usuario incluido en la Unidad Organizativa



Fuente: elaboración propia.

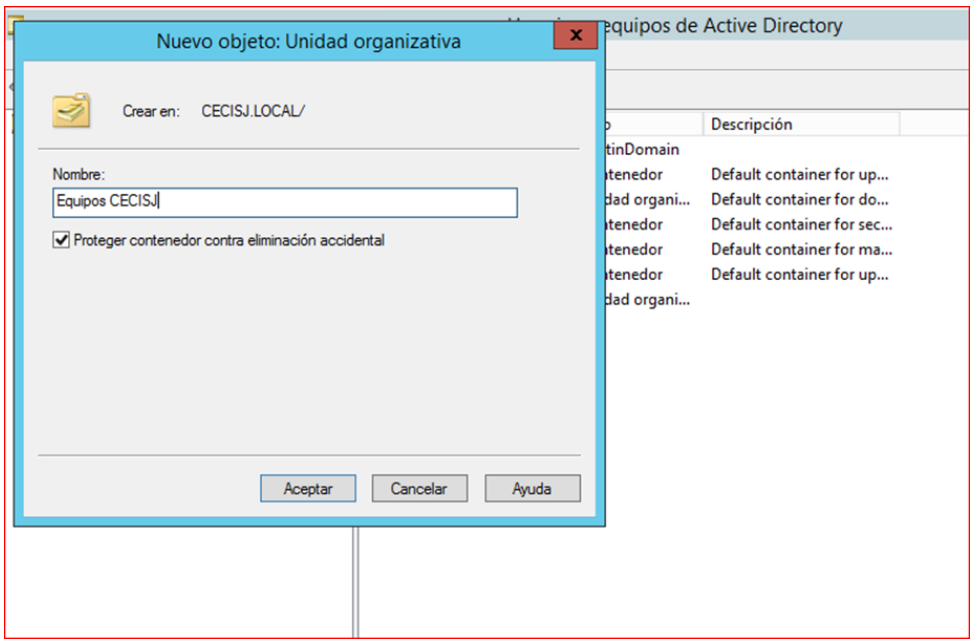
A continuación, se va a crear otra Unidad Organizativa, pero esta vez será para equipos. Los pasos para la configuración e inclusión de la PC01 en este grupo se pueden ver en las figuras 76, 77, 78, 79 y 80.

Figura 76: Creación de Unidad Organizativa para equipos 1



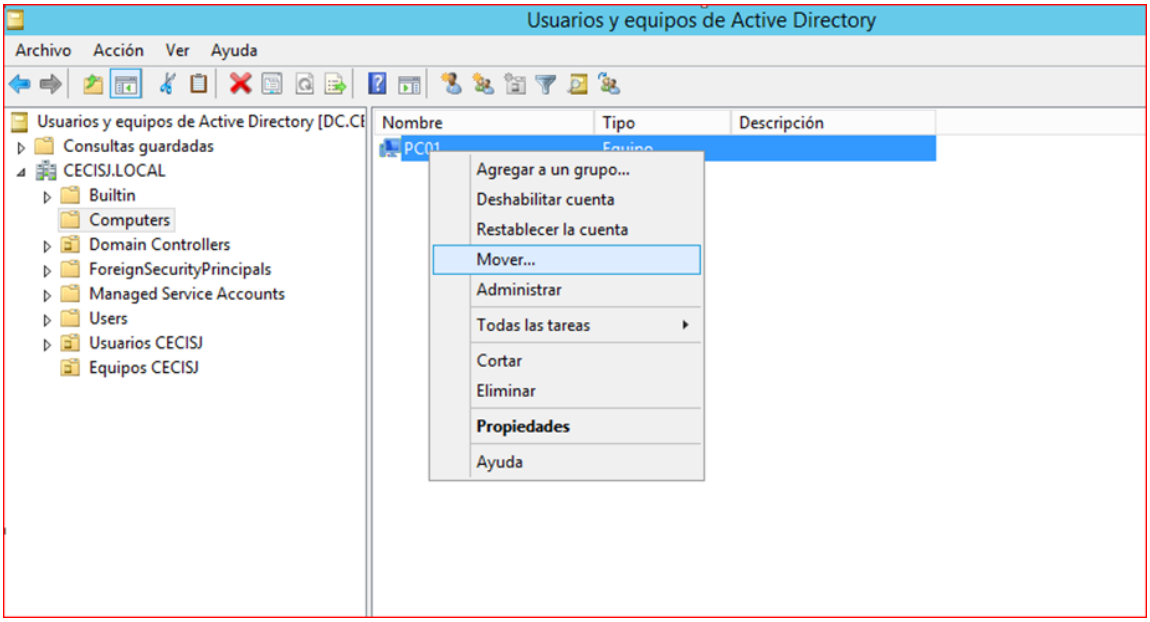
Fuente: elaboración propia.

Figura 77: Creación de Unidad Organizativa para equipos 2



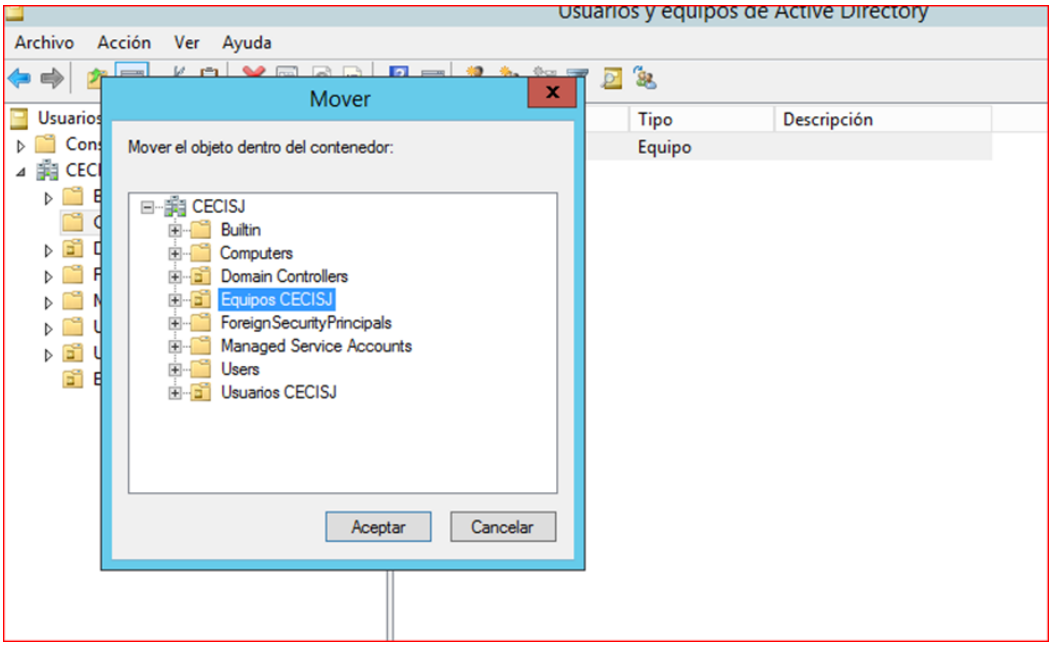
Fuente: elaboración propia.

Figura 78: Mover equipos a la nueva Unidad Organizativa 1



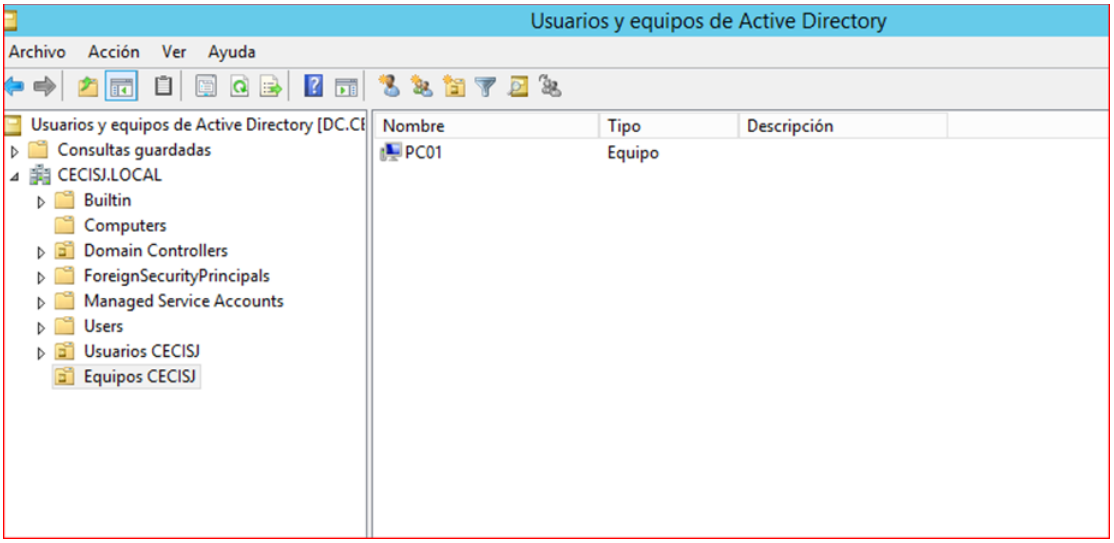
Fuente: elaboración propia.

Figura 79: Mover equipos a la nueva Unidad Organizativa 2



Fuente: elaboración propia.

Figura 80: Mover equipos a la nueva Unidad Organizativa 3

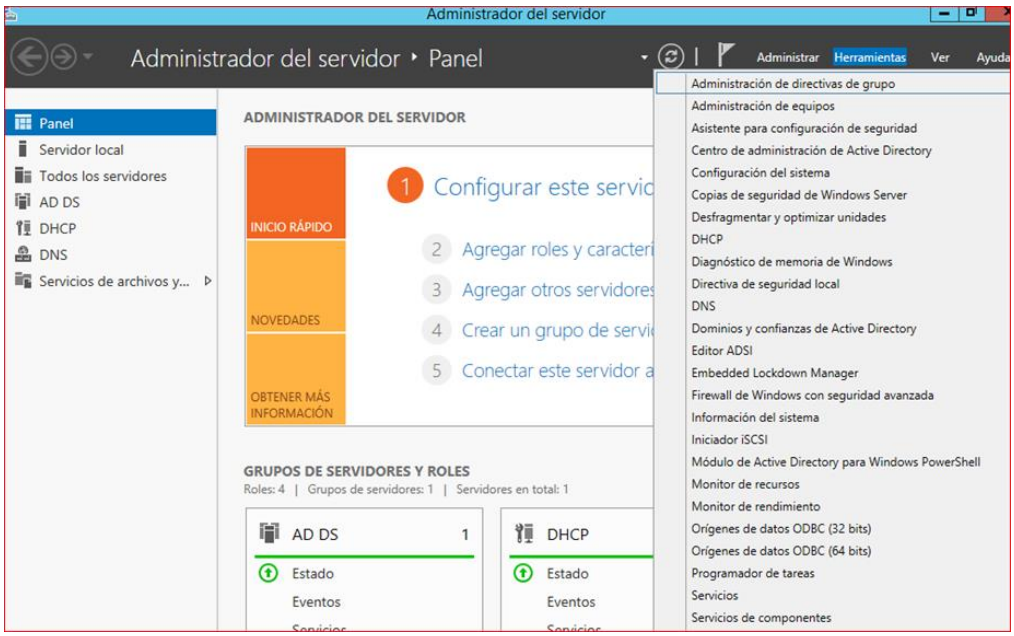


Fuente: elaboración propia.

En el siguiente apartado y siguiendo las buenas prácticas, se va a crear una política de seguridad para usuarios, que consiste en que los que tengan esa política activada no pueden hacer uso del editor de registro en ninguna máquina.

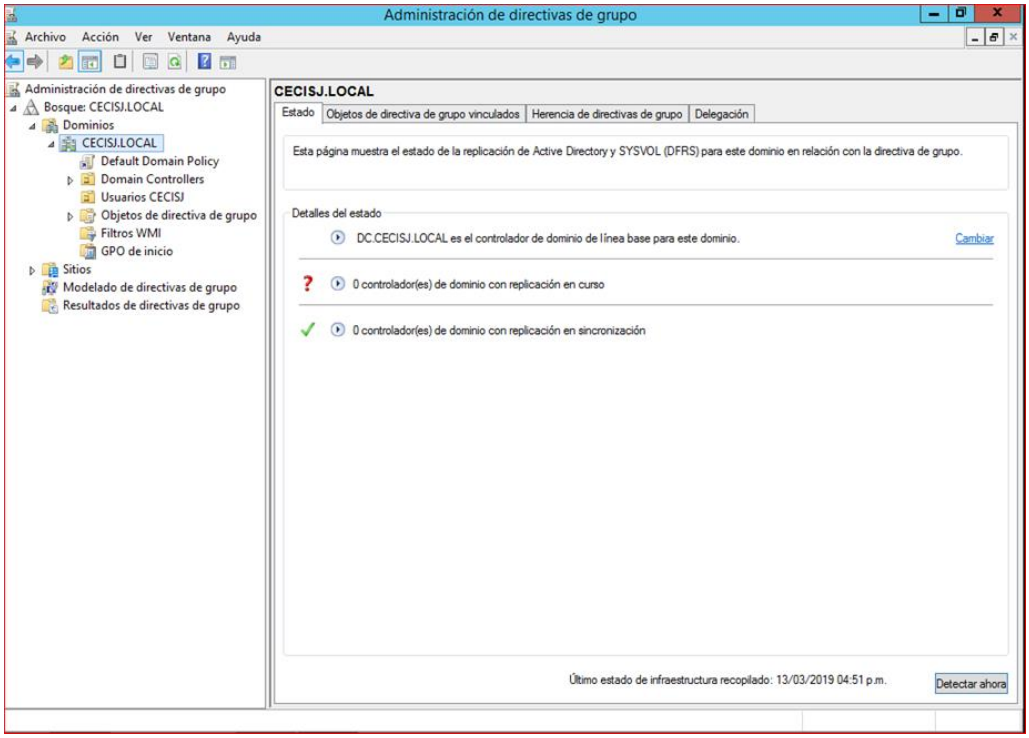
El editor de registro o más conocido como regedit, permite que se realicen modificaciones que pueden provocar un mal funcionamiento de los equipos si no se tienen los conocimientos necesarios para su utilización. Las figuras 81, 82, 83, 84, 85, 86, 87, 88, 89 y 90 muestran cómo se realiza la configuración y una prueba para comprobar que el acceso a esta herramienta ha sido bloqueado.

Figura 81: Creación de política de usuario 1



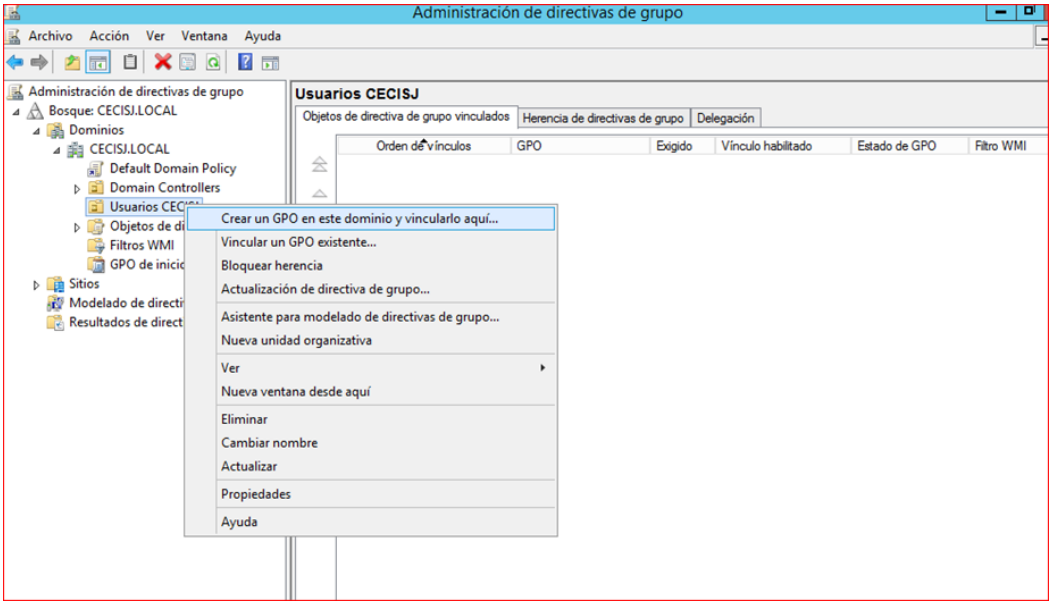
Fuente: elaboración propia.

Figura 82: Creación de política de usuario 2



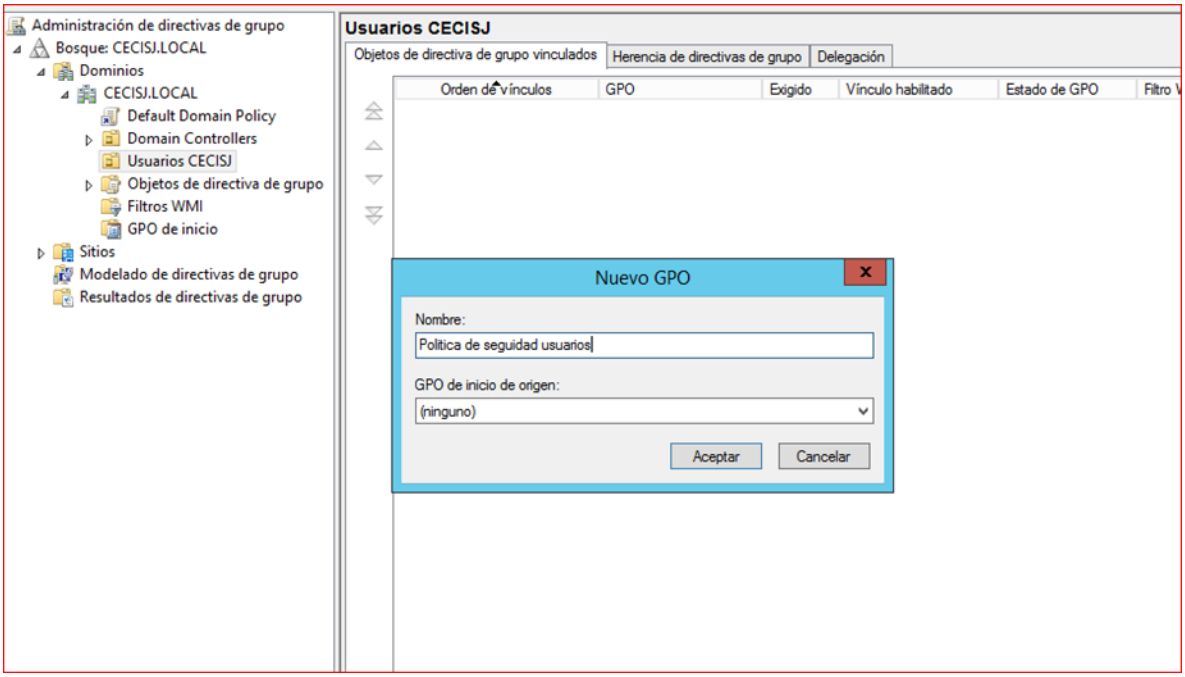
Fuente: elaboración propia.

Figura 83: Creación de política de usuario 3



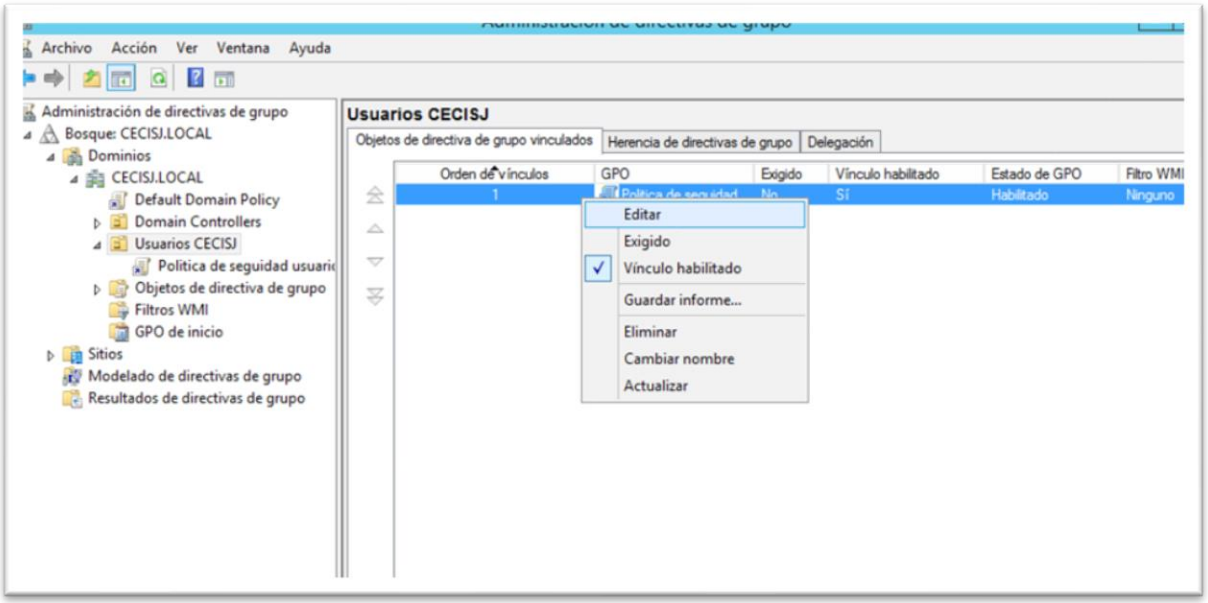
Fuente: elaboración propia.

Figura 84: Creación de política de usuario 4



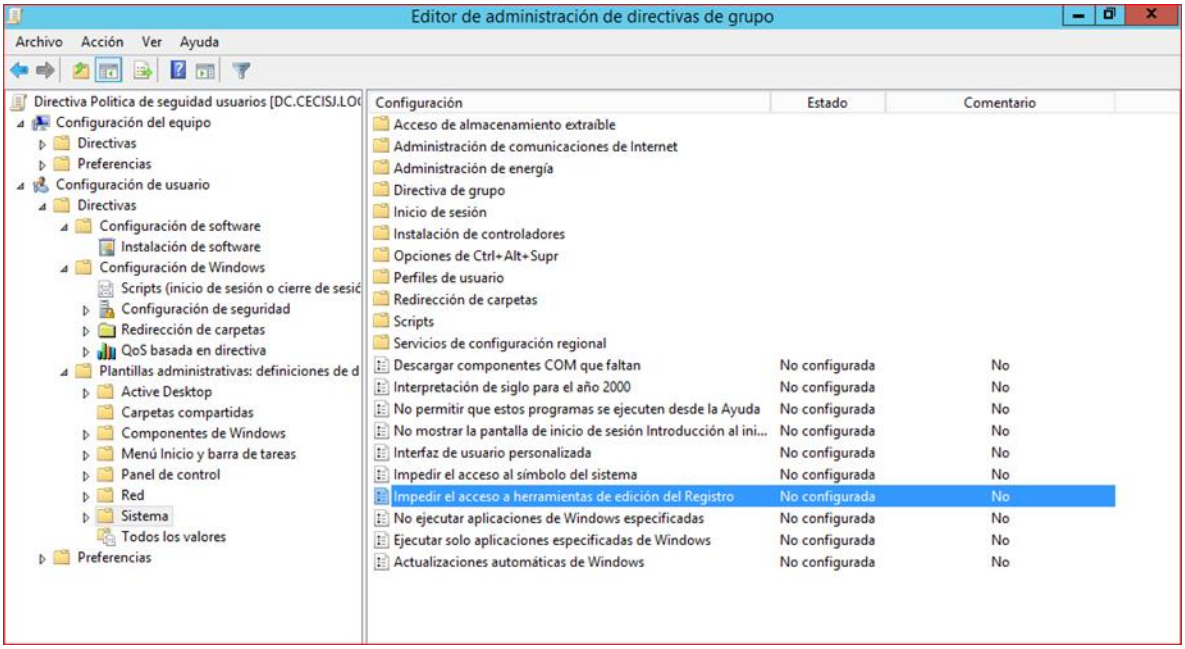
Fuente: elaboración propia.

Figura 85: Creación de política de usuario 5



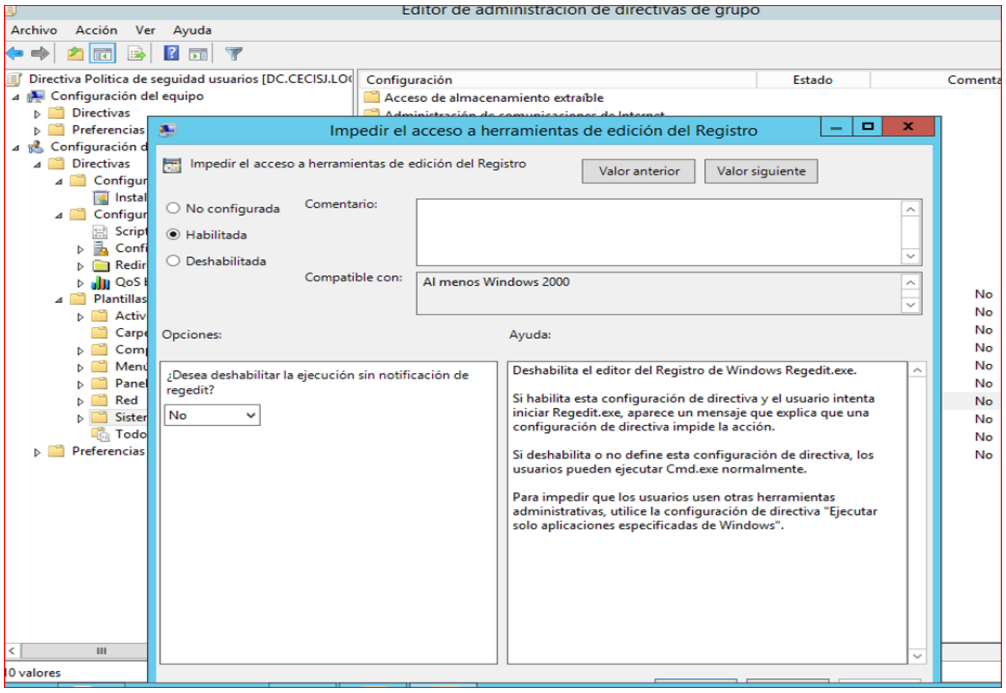
Fuente: elaboración propia.

Figura 86: Creación de política de usuario 6



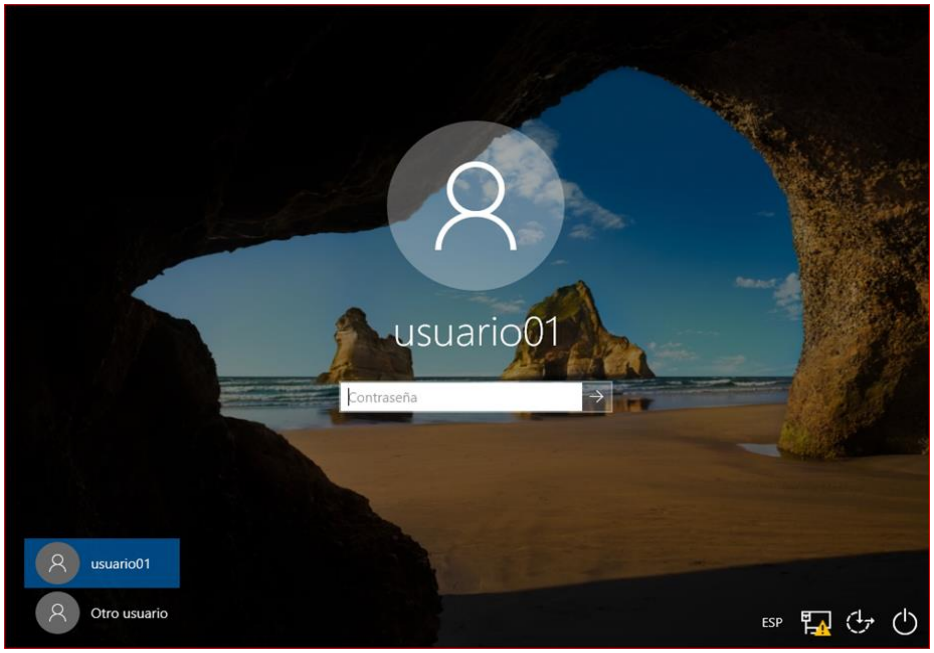
Fuente: elaboración propia.

Figura 87: Creación de política de usuario 7



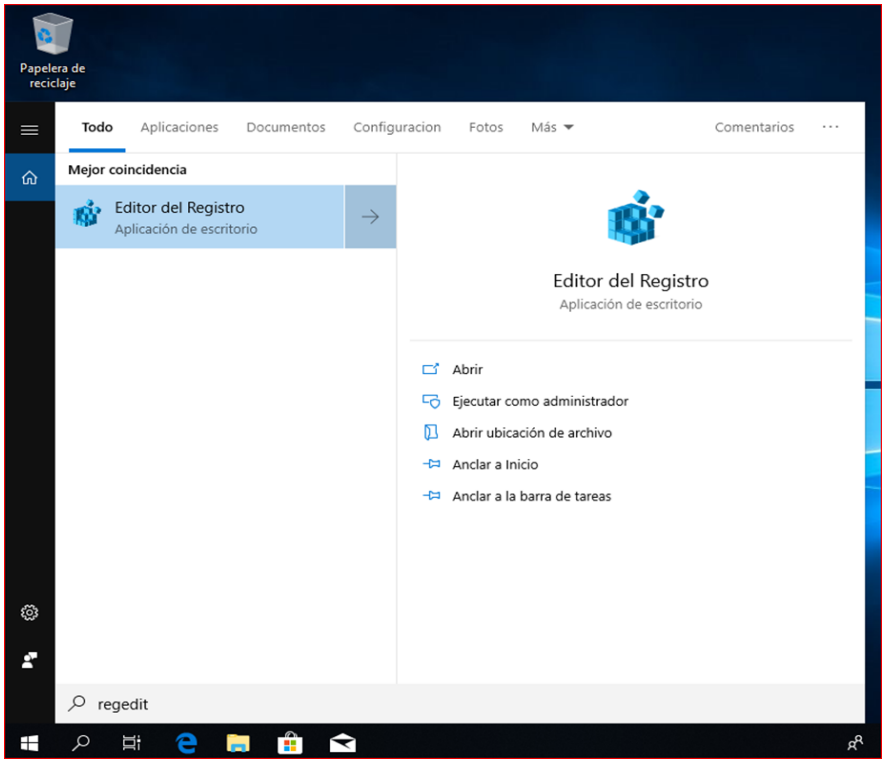
Fuente: elaboración propia.

Figura 88: Prueba política sin permiso a regedit 1



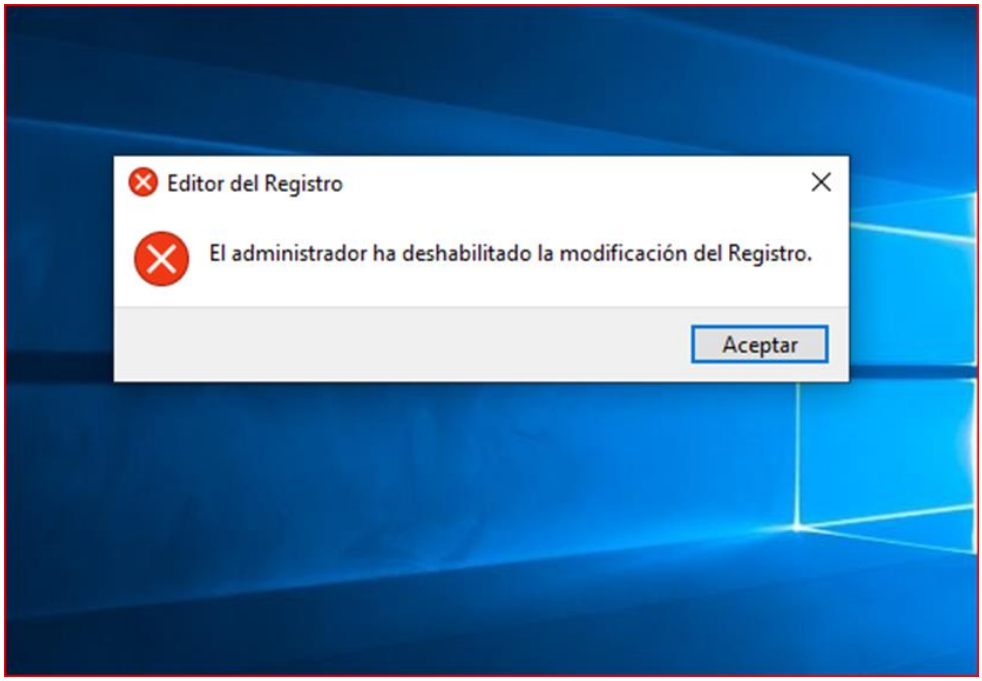
Fuente: elaboración propia.

Figura 89: Prueba política sin permiso a regedit 2



Fuente: elaboración propia.

Figura 90: Prueba política sin permiso a regedit 3



Fuente: elaboración propia.

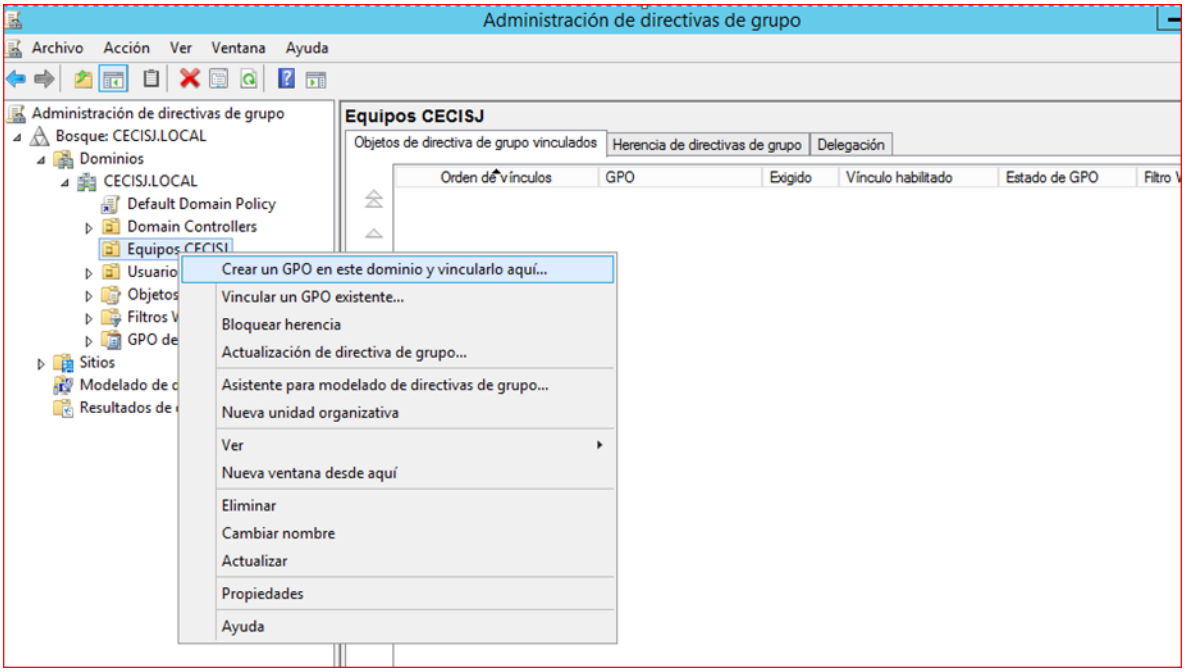
Como siguiente paso se va a configurar una política de equipo que evita la posibilidad de que algunos usuarios puedan acceder a los discos duros y datos de otros mediante el comando \\nombre_equipo\c$.

Las figuras 91, 92, 93, 94, 95, 96, 97, 98 y 99 describen como realizar el proceso y una verificación de que el recurso C$ fue eliminado.

Figura 91: Creación de política de equipo 1

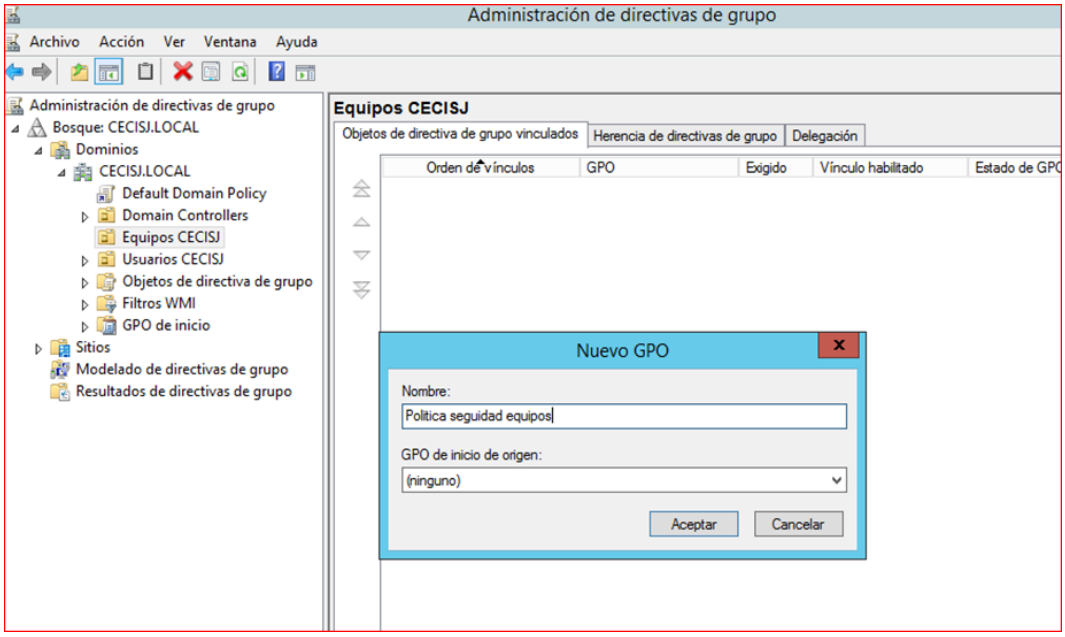
Fuente: elaboración propia.

Figura 92: Creación de política de equipo 2



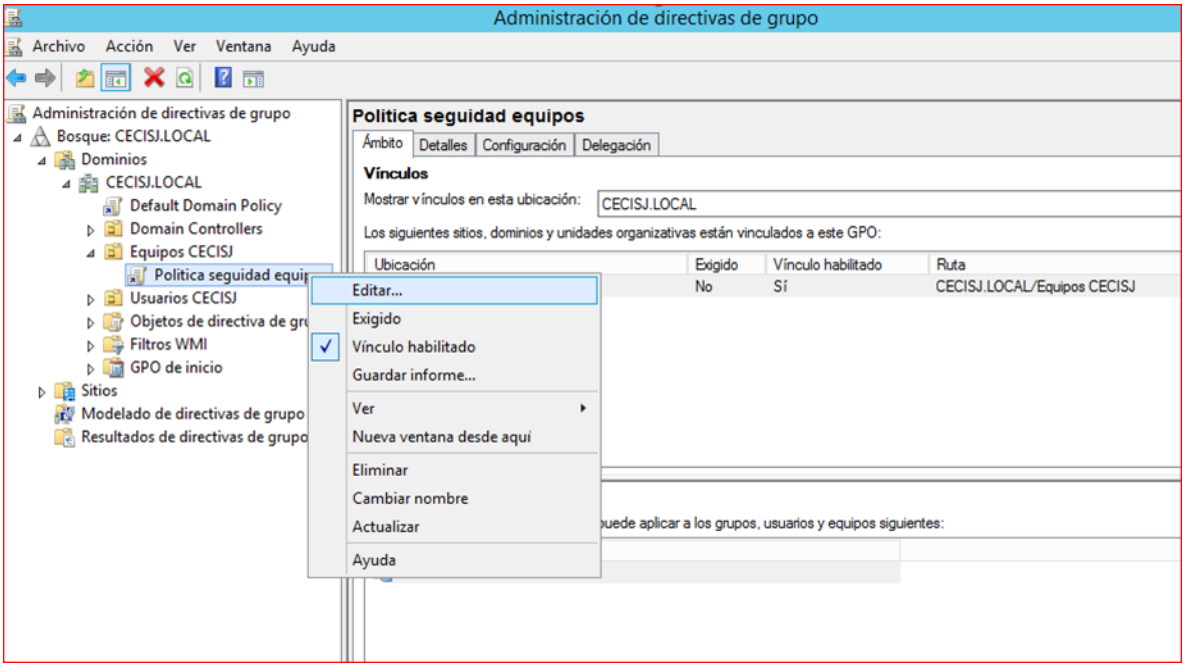
Fuente: elaboración propia.

Figura 93: Creación de política de equipo 3



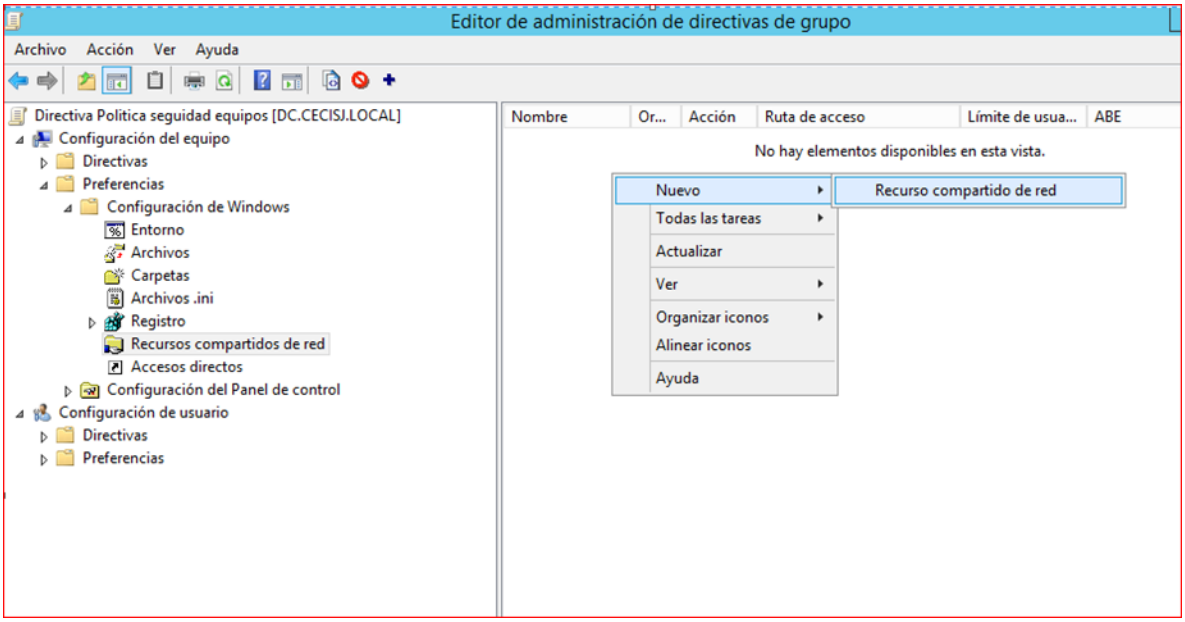
Fuente: elaboración propia.

Figura 94: Creación de política de equipo 4



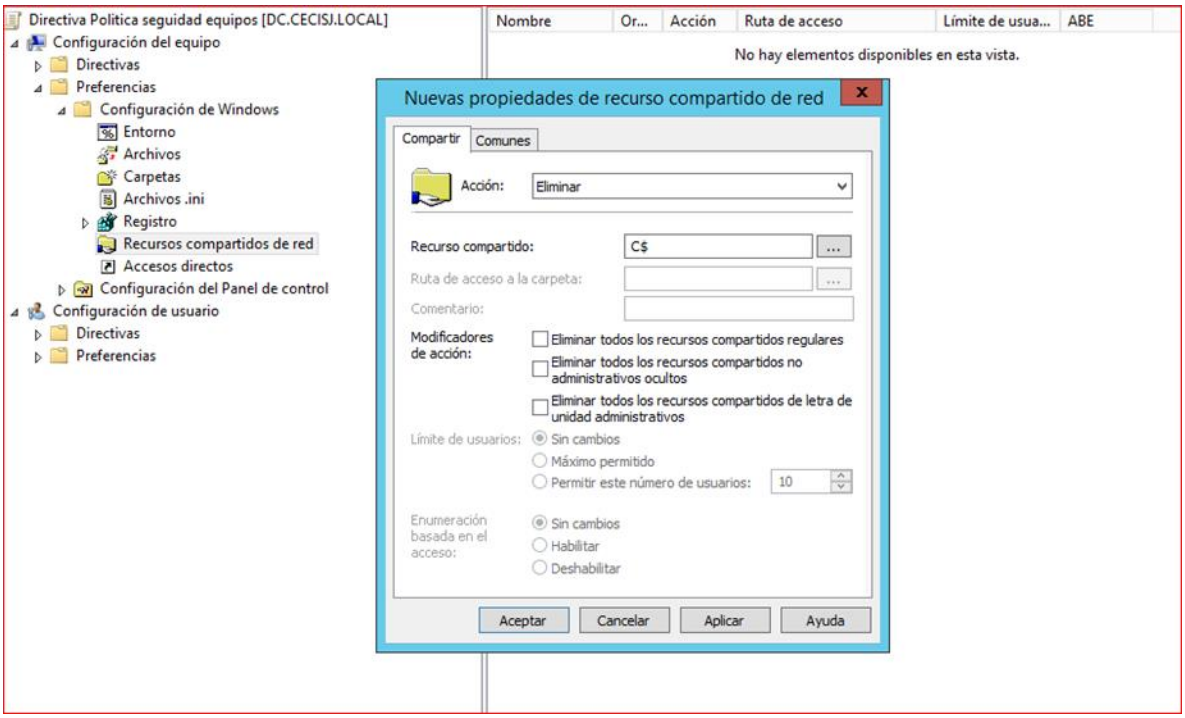
Fuente: elaboración propia.

Figura 95: Creación de política de equipo 5



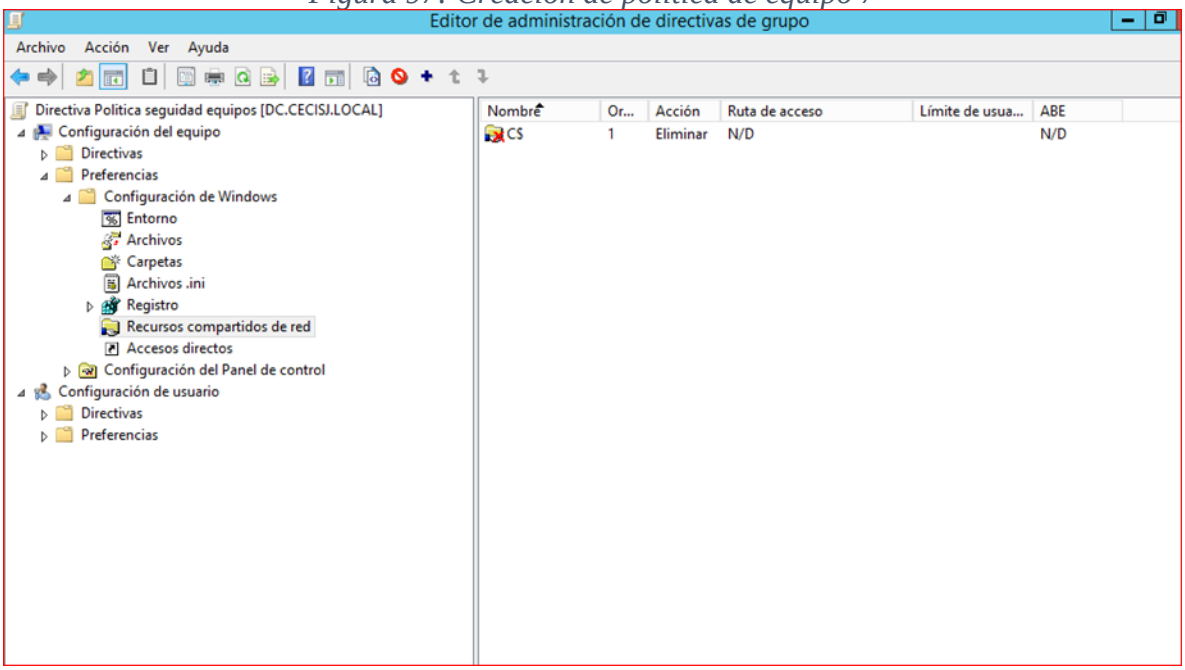
Fuente: elaboración propia.

Figura 96: Creación de política de equipo 6



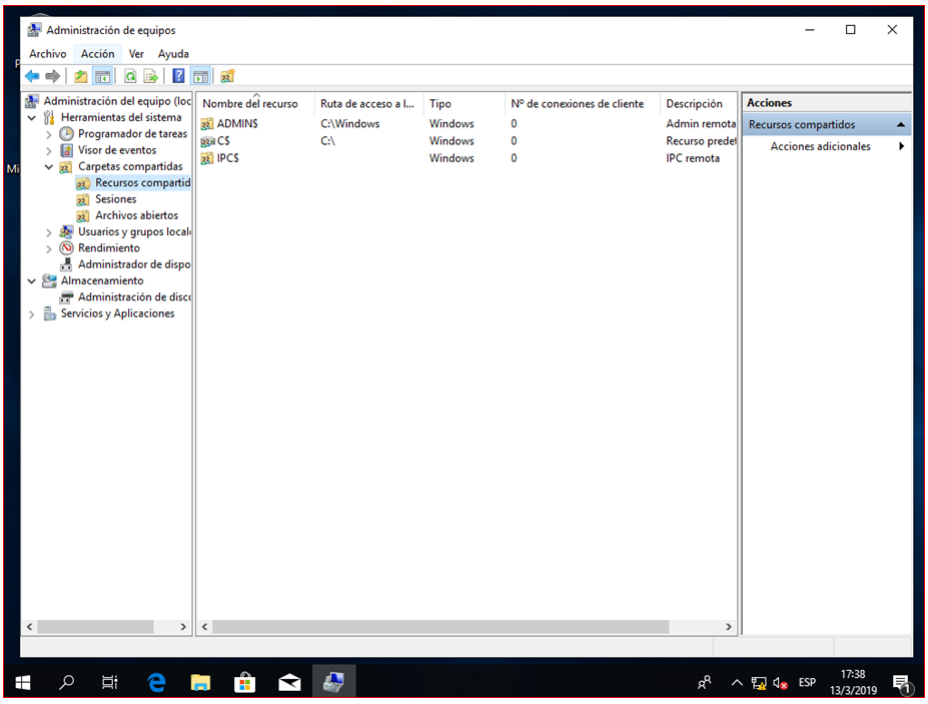
Fuente: elaboración propia.

Figura 97: Creación de política de equipo 7



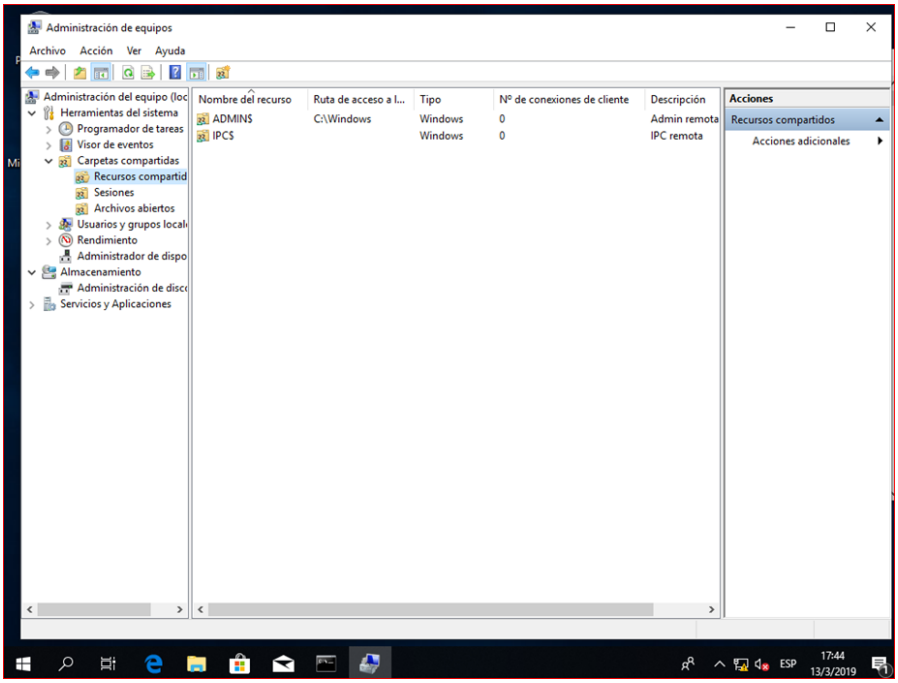
Fuente: elaboración propia.

Figura 98: Verificación antes de aplicar la política



Fuente: elaboración propia.

Figura 99: Verificación después de aplicar la política



Fuente: elaboración propia.

Una vez que se cuenta finalizada la configuración del servidor, se propone a continuación recomendaciones de seguridad para la red y equipos del laboratorio del CECI.

5.3 Recomendaciones de seguridad en la red y equipos del laboratorio del CECI.

En este apartado se van a bridar recomendaciones para el CECI con respecto a seguridad, control, acceso y filtrado de la red, utilizando un firewall e instalando una solución de antivirus que ayude a mantener los equipos más seguros.

5.3.1Firewall[8]

Un firewall funciona como un primer mecanismo de defensa en la red, su objetivo básico es evitar que terceros logren intrusiones a la red y sus equipos según las políticas de red que haya definido la organización o usuario responsable. Esas intrusiones o accesos no deseados pueden robar información privada o confidencial, así como denegación de servicios o acceso a la red entre otros.

Es muy importante que en todas las empresas se cuente con un firewall para minimizar las posibilidades de ataques, algunas ventajas de contar con este tipo de software son las siguientes:

- Protege de intrusiones: restringe el acceso a ciertos segmentos de la red de una organización.
- Protección de información privada: define distintos niveles de acceso a la información para los diferentes grupos de usuarios con que cuenta la organización.

Para el caso del CECI se propone una solución de firewall gratuito que brinda protección a sus equipos y red sin significar un gasto para el CECI, el nombre de esta solución es Comodo Firewall, a continuación, se detallan algunas de sus características:

- Firewall: módulo principal de cortafuegos.
- Sandbox: permite ejecutar aplicaciones en un ambiente aislado del sistema operativo, en caso de que se tratara de una aplicación maliciosa.
- HIPS: monitorea la actividad del sistema según reglas predefinidas anteriormente con el fin de reconocer comportamientos sospechosos del sistema, cuando reconoce este tipo de comportamiento detiene el programa o proceso sospechoso.

[8] A partir de Comodo Cybersecurity (2019) y Guadalupe (2011)

- Viruscope: Monitorea las actividades de los procesos en ejecución y genera alertas si detecta actividad sospechosa.
- Filtro Web: Permite bloquear el acceso a sitios web por diferentes categorías.

Este software incluye dentro de sus componentes un antivirus, sin embargo, se recomienda complementar la seguridad de los equipos instalando uno que sea especializado y dedicado a ese objetivo.

Las figuras 100, 101, 102 y 103 muestran los pasos para su instalación una vez realizada la descarga desde el sitio oficial: www.personalfirewall.comodo.com.

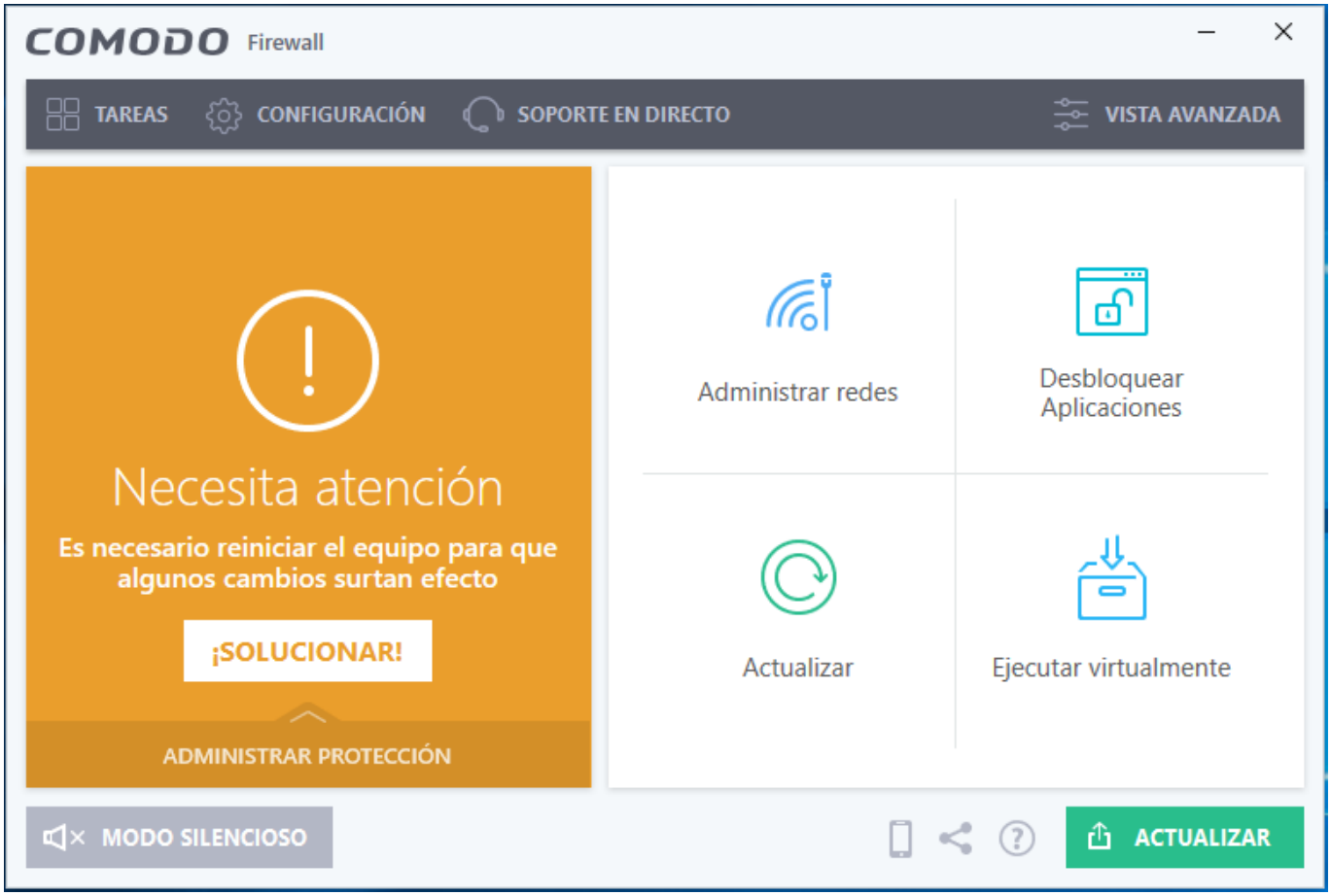
Figura 100: Sitio de descarga oficial Comodo Firewall

Fuente: elaboración propia.

Figura 101: Instalación Comodo Firewall 1

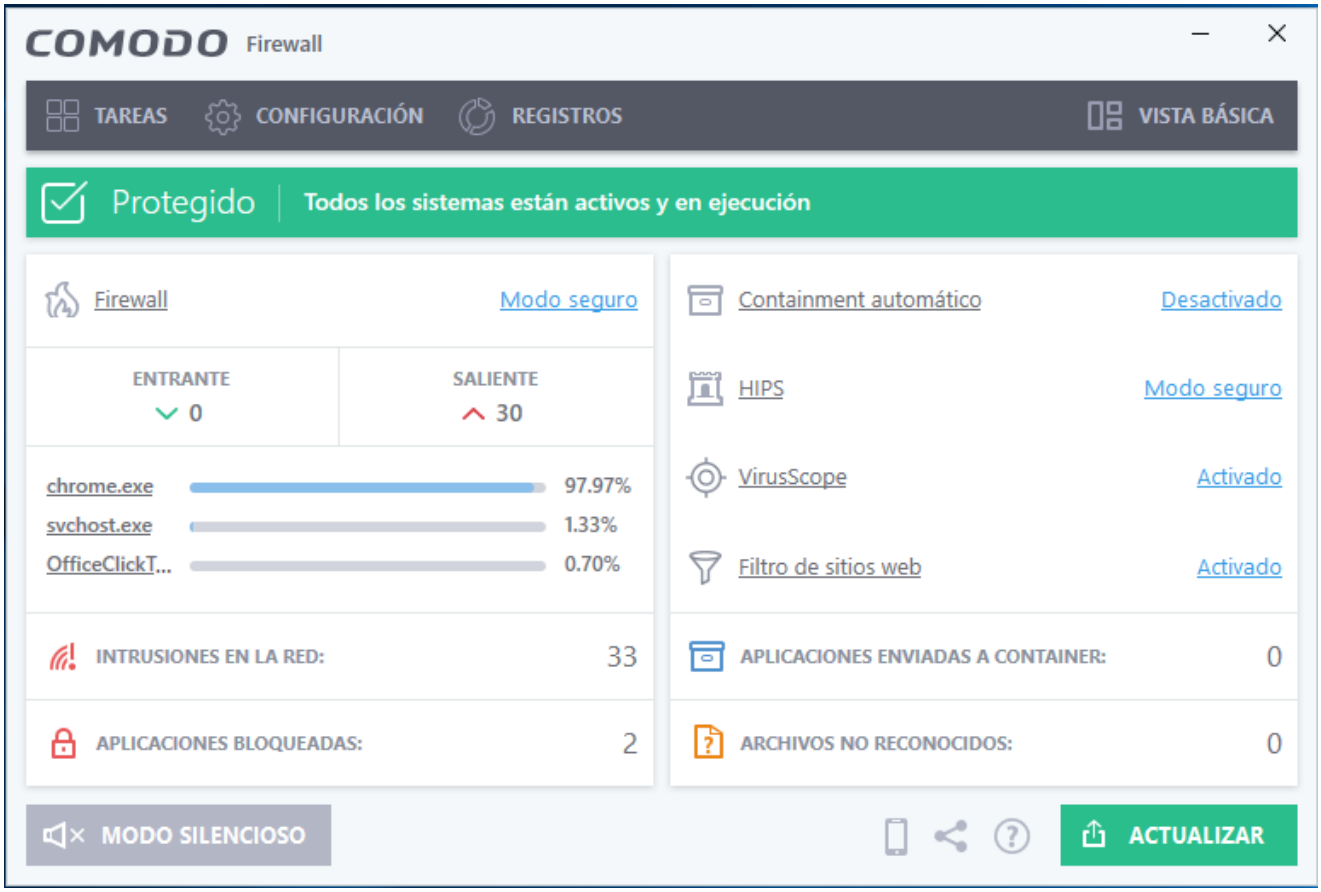
Fuente: elaboración propia.

Figura 102: Instalación Comodo Firewall 2



Fuente: elaboración propia.

Figura 103: Instalación Comodo Firewall 3



Fuente: elaboración propia.

5.3.2 Antivirus[9]

Un antivirus es un programa de computadora cuyo propósito es combatir y erradicar los virus informáticos; es una solución para minimizar los riesgos, pero no garantiza que estos no se materialicen.

Para mantener el sistema estable y seguro el antivirus debe estar siempre actualizado, tomando siempre medidas preventivas y correctivas. Un buen antivirus es uno que se ajuste a las necesidades de la organización.

Para el caso del CECI y considerando las limitaciones presupuestarias se recomienda utilizar un antivirus gratuito pero que sea confiable y de fácil utilización, como lo es Bitdefender Antivirus.

A continuación, algunas de las funcionalidades que ofrece:

- Diseño minimalista, lo cual hace mínimo el consumo de recursos.
- El software ofrece una velocidad optimizada y mejor rendimiento multiplataforma.
- Escanea automáticamente los equipos en segundo plano mediante la detección basada en la nube, y luego realiza un análisis más profundo si encuentra algún software malicioso o señales de alerta.
- Herramienta de Anti-phising.
- Protección multimedia contra ransomware.
- Herramienta para eliminación de archivos de forma segura y permanente.

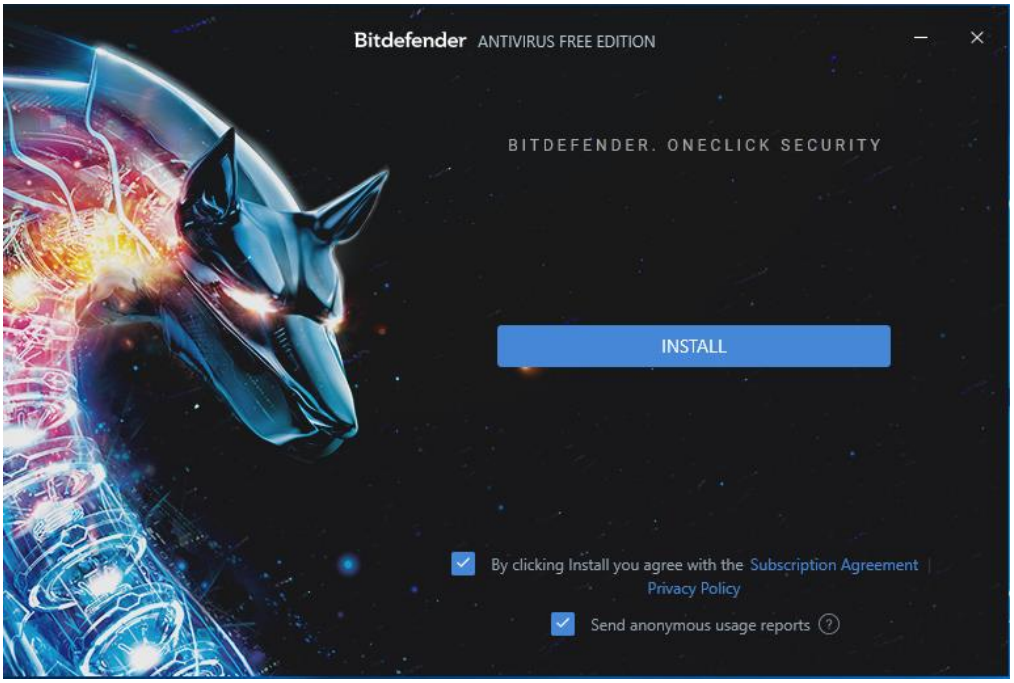
En las figuras 104, 105, 106 y 107 podemos ver el proceso de descarga del Antivirus Bitdefender desde el sitio oficial: www.bitdefender.com/solutions/free.html y el proceso de instalación.

[9] A partir de Guadalupe (2011) y Bitdifender (2019)

Figura 104: Sitio de descarga desde la página oficial

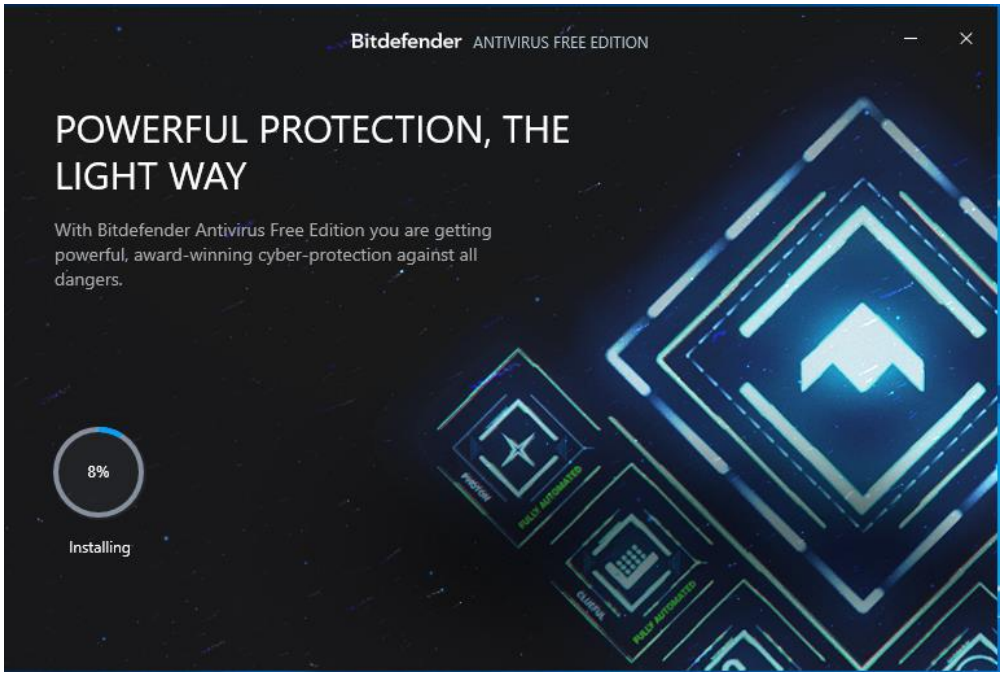
Fuente: elaboración propia.

Figura 105: Instalación Antivirus Bitdefender 1



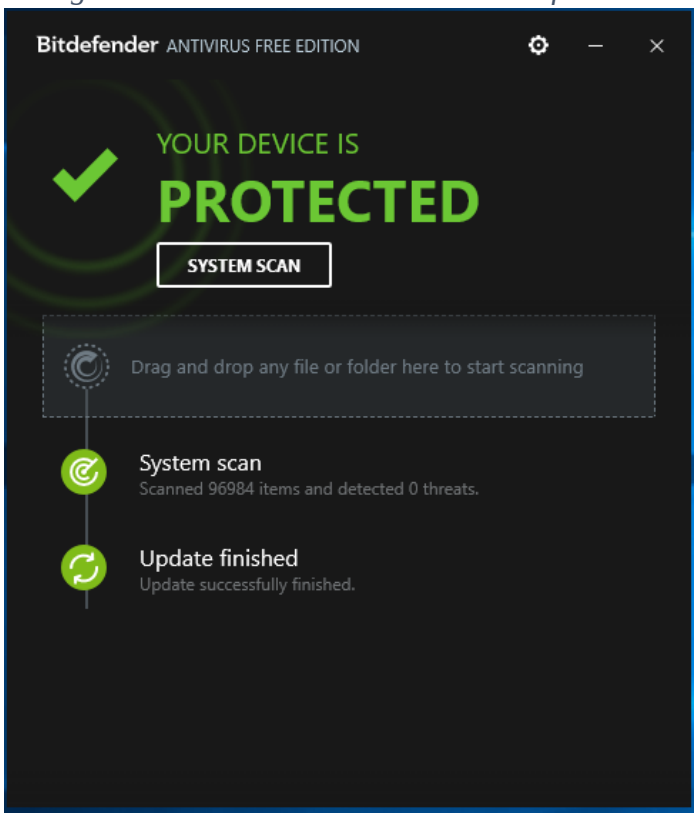
Fuente: elaboración propia.

Figura 106: Instalación Antivirus Bitdefender 2



Fuente: elaboración propia.

Figura 107: Instalación Antivirus Bitdefender 3



Fuente: elaboración propia.

5.4 Lineamientos de seguridad del CECI[10]

Como se ha mencionado en el documento, la seguridad informática es un proceso que administra y evalúa los riesgos en el uso de los dispositivos tecnológicos en una determinada organización, en este caso el CECI.

Es decir, busca salvaguardar los laboratorios de cómputo, sus procedimientos operacionales, ante cualquier evento natural o humano que de forma intencional o por accidente puedan afectarlos.

Estos lineamientos buscan regular el control, acceso, registro y uso a los equipos del laboratorio e instalaciones del CECI, de modo que se espera que toda persona que utilice los servicios que ofrece el CECI conozca y acepte estos lineamientos.

Es importante mencionar que los mismos siguen el esquema normativo de seguridad de la norma ISO27001 que establece las mejores prácticas de seguridad informática.

La ISO27001 es una norma internacional cuyo objetivo es dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requisitos de la organización, la legislación y las regulaciones.

Busca el aseguramiento, la confidencialidad e integridad de los datos y la información, así como de los sistemas que la procesan, esto permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos (ISOTools, 2019).

[10] Este apartado fue elaborado con base en CVS (2014), Universidad Latina de Panamá (2012), UNED (2017), Norma ISO/IEC 17799.

5.4.1 Objetivo del lineamiento

Dotar de la información necesaria en el más amplio nivel de detalle a los usuarios y encargados del CECI de los lineamientos que deben cumplir y utilizar para proteger el hardware y software de la red institucional, así como la información que es procesada y almacenada en estos.

5.4.2 Responsabilidad

El encargado del CECI o la persona que el delegue en su ausencia está a cargo de supervisar los laboratorios de cómputo. El tendrá la responsabilidad de autorizar el acceso al laboratorio de cómputo. Además, es responsable directo de la ejecución de todos los procedimientos de seguridad en estas áreas y tiene que velar de que todos los materiales y equipos en estas áreas no sean sacados sin la previa autorización y justificación.

La persona delegada del MICITT se encarga de canalizar todos los requerimientos tecnológicos.

5.4.3 Lineamientos de seguridad

Seguridad organizacional

a) Los servicios de la red y equipos del CECI son prioritariamente de uso académico, de investigación y de capacitación. El uso recreativo está sujeto a la disponibilidad del equipo.

b) El encargado del CECI o la persona en quien expresamente delegue esta función en su ausencia, se encargará de:

    a. Velar por la seguridad de los activos informáticos.

    b. La capacitación en temas de seguridad informática.

    c. El cumplimiento de los lineamientos establecidos.

    d. La atención de sugerencias o quejas con respecto al funcionamiento de los activos.

c) El MICITT es la entidad encargada de asignar el personal técnico para el mantenimiento de los equipos de cómputo del CECI.

d) El encargado del CECI informará cualquier modificación a estas normas.

e) Si el usuario encuentra que el equipo que se le ha entregado está defectuoso o el laboratorio en condiciones no propicias, debe comunicarlo de inmediato al encargado, de lo contrario se le hace responsable del mismo, es decir, asumirá la responsabilidad, por ello deberá revisarlo al momento de la entrega.

f) Por ningún motivo el usuario podrá alterar el funcionamiento normal del equipo, así como intentar repararlo en caso de falla. En este último caso se deberá reportar la situación al encargado.

g) Toda persona que use las instalaciones o el equipo del CECI deberá dejar el área de trabajo limpia y las sillas en su lugar.

h) Toda persona que ingresa como usuario para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información.

Seguridad lógica

a) Cada usuario es responsable de los mecanismos de control de acceso que les sean proporcionado, su nombre de usuario y contraseña necesarios para acceder a la red y a la infraestructura tecnológica del CECI.

b) El encargado del CECI o la persona a quien este delegue la función en su ausencia, proporcionará las contraseñas de acceso necesarias para el uso de la red y la infraestructura tecnológica. Las contraseñas serán temporales.

c) El usuario es responsable exclusivo de mantener a salvo su contraseña.

d) El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios, en caso contrario se podría incurrir en una denuncia penal por mal uso de los servicios informáticos de la organización.

e) Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que serán sujetos de monitoreo de las actividades que realiza en Internet, que existe la prohibición al acceso de páginas no autorizadas, así como la descarga de software sin la autorización y supervisión de la persona encargada.

f) El acceso a la configuración del sistema operativo o de los servidores es únicamente permitido al encargado del CECI o personal del MICITT.

g) Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas e identificadas propiamente, en ningún momento se obviarán situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

h) Se adquirirá y utilizará software únicamente de fuentes confiables. En caso de ser necesaria la adquisición de software de fuentes no confiables.

i) Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

j) El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal asignado por el MICCIT, terceras personas contratadas para el servicio o estudiantes que realizan su TCU y cuentan con la debida autorización del encargado del CECI.

k) Se llevará un registro del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación. Estos mantenimientos se realizarán 2 veces al año y se efectúan en todos los equipos informáticos.

Seguridad física

a) El cableado de red se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

b) Los servidores con problemas de hardware deberán ser reportados al MICITT y retirados sus medios de almacenamiento.

c) Los equipos o activos críticos de información y proceso deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el encargado y las personas responsables por esos activos.

d) Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los equipos.

e) El CECI debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.

f) Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

g) Queda terminantemente prohibido que el usuario abra o destape los equipos de cómputo.

h) El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

i) El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.

j) Las estaciones de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

k) Los usuarios no deben mover o reubicar los equipos de cómputo, tampoco instalar o desinstalar dispositivos periféricos.

l) Únicamente el personal autorizado por el encargado del CECI o el MICITT podrá llevar a cabo los servicios y reparaciones al equipo informático.

Ahora bien, estos lineamientos se pueden operativizar en las siguientes normas que se pueden colocar en un lugar visible en el CECI:

Normas para el uso del laboratorio del CECI

1. Para mantener un comportamiento de respeto entre los usuarios que se encuentran en el CECI se:
    a. Debe mantener la disciplina
    b. Prohíbe comer y beber dentro del CECI.
    c. Restringe el uso de la estación de trabajo a una persona por equipo de cómputo; a excepción de sesiones de capacitación en la que se requiera otra forma de organización.
    d. No se permite ver fotos ni mantener imágenes sobre la pantalla que ofenda a otras personas.
    e. No se permite ejecutar software, como juegos, chat, entre otros que ponga en riesgo la seguridad informática.
    f. Debe respetar y acatar instrucciones que entregue el encargado del laboratorio o tutor a cargo.
    g. Se prohíbe realizar cualquier acto que contradiga con las buenas costumbres (peleas, decir improperios, etc.).

2. La persona encargada del CECI o a quien este delegue la función tendrá que velar por el buen estado de los equipos y el mobiliario del CECI.
3. Los equipos son de exclusiva responsabilidad de los usuarios, una vez que los usuarios se encuentren utilizándolos.
4. Los usuarios deberán, antes de abrir sus unidades de almacenamiento masivo (memoria USB, celulares, tarjetas de memoria, entre otros), analizar el dispositivo con el antivirus instalado en todas las computadoras y en caso de ser necesario realizar la limpieza, evitando el daño de los equipos.
5. No se permite tener acceso directo a los servidores de las salas, copiar software o modificar los archivos que se encuentren allí.
6. No se debe efectuar daño físico al hardware o mobiliario dispuestos en el CECI.
7. No se debe mover los equipos o componentes del Laboratorio sin previa autorización, tales como: mouse, cámara y teclados, entre otros.
8. No se debe instalar componentes ajenos al Laboratorio (impresoras, calculadoras, unidades externas) o cargar software sin previa autorización.
9. No se debe manipular el cableado que conecta al equipo computacional.
10. No se debe manipular, ni eliminar el software de configuración de cada equipo para propósito personal.
11. Queda prohibido utilizar las computadoras para visualizar material pornográfico o de extrema violencia.
12. No descargar software de Internet.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Posterior a la propuesta descrita para el mejoramiento de la infraestructura tecnológica del CECI de San Juan de Santa Bárbara de Heredia se puede concluir:

1. Tanto el problema como los objetivos generales y específicos planteados al inicio del proyecto se alcanzaron satisfactoriamente.
2. La definición del problema permitió identificar las causas de las debilidades en la infraestructura y seguridad informática del CECI, entre las que se encuentran la ausencia de una configuración de red LAN y de un equipo autoritativo para gestionarla; así como, de mecanismos de seguridad y control de la red informática. También se pudo identificar los efectos, entre los cuales se pueden enumerar: bajo rendimiento de internet, ausencia de comunicación entre los equipos, ausencia de un dominio de red con mejores prácticas configuradas, riesgo de intrusiones y ausencia de controles de seguridad informática en el laboratorio.
3. Se realizaron diagnósticos administrativos y técnicos que permitieron identificar con mayor claridad las brechas entre la realidad y las mejores prácticas informáticas en el CECI.
4. El diagnóstico administrativo evidenció que el CECI no contaba al momento de la investigación con una misión, visión y objetivos propios, sino que respondían a la misión, visión y ejes estratégicos del MICITT. Aunado a esto se encuentra que para el funcionamiento del CECI se requiere la colaboración de aliados estratégicos, como la ADI de San Juan de Santa Bárbara de Heredia la cual asume la administración de dicho centro.

A la vez dicho diagnóstico develó que, aunque en el MICITT se establecen reglas para el uso del laboratorio del CECI, algunas de estas no se están cumpliendo y representan riesgos y amenazas para la seguridad informática y la integridad de los equipos.

5. El diagnóstico técnico permitió inventariar la infraestructura tecnológica a nivel físico y lógico del lugar donde se realizó el estudio; lo que a su vez permitió reconocer que el CECI cuenta con equipo de cómputo básico de acuerdo con sus funciones y las posibles necesidades de los usuarios. También develó que existe software con licencias vencidas, el antivirus es el que trae el sistema operativo por defecto, no existen dispositivos de red o software que controlen el tráfico web, las computadoras se encuentran conectadas por medio de una red inalámbrica, lo cual representa una desmejora de rendimiento, además cuenta con seguridad básica de contraseña de acceso configurada por el proveedor de internet.
6. La propuesta elaborada responde a los objetivos planteados y está en consonancia con los entregables.
    a. En relación al primer objetivo de proponer la configuración de la red alámbrica del CECI San Juan de Santa Bárbara se establece un área de cobertura LAN, configuración TCP/IP y una topología jerárquica lo que permite resolver el problema de la ausencia de una red que vincule los nodos. Se reconoce como limitación que el presupuesto del CECI es limitado y por tanto no se pueda contar con los insumos para configurarla en el corto plazo.
    b. En relación al segundo objetivo que plantea la implementación y configuración de un servidor se recomendó el uso de un servidor que funcione como DNS, DHCP y dominio. Y se presentan los pasos para su configuración utilizando Windows

Server 2012 R2, en este proceso se trabajaron algunas de las mejores prácticas recomendadas, como lo son creación de grupos, usuarios, roles y permisos. Como limitación se encuentra que el CECI no tiene personal técnico de planta y que la persona encargada no tiene formación en tecnología, de modo que se depende de procesos como trabajos finales de graduación o trabajos comunales universitarios para hacerlo una realidad y darle el mantenimiento y administración adecuado.

c. Respecto al tercer objetivo de describir los requerimientos básicos de seguridad informática para la red y equipos del CECI, se consideró las limitaciones presupuestarias y de personal técnico capacitado por lo que se plantean dos soluciones gratuitas amigables e intuitivas con el usuario como lo son Comodo Firewall y Bitdifender Antivirus. Esto cierra la brecha y riesgos identificados en el diagnóstico aumentando significativamente la seguridad para la red y los equipos.
d. En el último objetivo sobre las políticas de seguridad informática se siguió lo planteado en la norma ISO17799 en los niveles de seguridad organizacional, seguridad lógica y seguridad física. Los lineamientos propuestos toman en cuenta la realidad del CECI por lo que se excluyen algunas de las normas que no podrían aplicarse. Además, se facilita un listado de normas para el laboratorio del CECI que puede ser colocado visiblemente en el laboratorio para que sea conocido por todos los usuarios.

6.2 Recomendaciones

A continuación, se detallan las recomendaciones más importantes derivadas del proceso de construcción del presente proyecto de graduación.

1. Se recomienda al CECI gestionar alianzas estratégicas con actores locales e institucionales para obtener un mayor presupuesto que le permita llevar a cabo esta propuesta de mejoramiento y otras que son necesarias para cumplir con los objetivos de la organización.
2. Se recomienda gestionar o contratar una persona con conocimientos técnicos comprobados que pueda mantener y administrar los equipos del laboratorio. Esto además garantizará la continuidad y calidad del servicio.
3. A futuro se considera importante adquirir equipos audiovisuales como los son proyectores, con el fin de facilitar las capacitaciones que allí se imparten.
4. Certificar la instalación eléctrica con el fin de que no se afecten los equipos por picos de corriente causados por no tener una apropiada instalación o falta de mantenimiento de esta. Se debe realizar mantenimiento preventivo a los equipos al menos dos veces al año.
5. Se recomienda llevar un inventario de activos y sus características, así como un control de equipos dañados que deben ser referidos al MICITT.
6. En relación a la seguridad del local, se recomienda restringir el acceso físico mediante un portón eléctrico que limite el acceso de personas con fines destructivos y que pongan en riesgo a los facilitadores y usuarios.
7. Fortalecer y mantener las alianzas estratégicas con las universidades para el desarrollo de trabajo finales de graduación.
8. Invertir en un aire acondicionado que mantenga una temperatura segura para los equipos y no sufran sobrecalentamientos.

Bibliografía

Aguilera, P. (2010). *Seguridad informática.* Madrid: Editex.

Baptista, P., Fernández, C., & Hernández, R. (1991). *Metodología de la Investigación (1ª Ed).* México: McGraw - HILL INTERAMERICANA.

Barrantes, R. (2010). *Investigación. Un camino al conocimiento. Un enfoque cuantitativo y cualitativo.* San José, Costa Rica: EUNED.

Belloch, C. (2012). *Las Tecnologías de la Información y Comunicación en el aprendizaje.* Valencia, España: Depto MIDE. Universidad de Valencia.

Bitdefender. (10 de Marzo de 2019). *Bitdefender.es*. Obtenido de https://www.bitdefender.es/solutions/antivirus.html#av_features

Carrión, H. (2014). Modelo de sostenibilidad de telecentros. *XXV Jornadas en Ingeniería Eléctrica y Electrónica*, 296.

Centro de Estudios Tecnológicos Industrial y de Servicios. (Febrero de 2016). *Medios Físicos y dispositivos de red.* Obtenido de https://ofimatica4-equipof.wixsite.com/redesmedios/single-post/2023/02/01/Topolog%C3%ADas-de-redes

Chen, S. (2016). Modelo de sostenibilidad para Centros Comunitarios Inteligentes de Costa Rica. *Revista e-Ciencias de la Información*, 1-21.

Comisión Interamericana de Telecomunicaciones. (Setiembre de 2005). *Organización de los Estados Americanos.* Obtenido de http://www.oas.org/en/citel/infocitel/2005/septiembre/seguridad_e.asp

Comodo Security Solutions. (10 de Marzo de 2019). *www.comodo.com*. Obtenido de https://www.comodo.com/

ConceptDraw. (Febrero de 2019). *ConceptDraw*. Obtenido de https://www.conceptdraw.com/How-To-Guide/picture/Computer-and-networks-Local-area-network-diagram.png

Contreras, E., Varas, S., & Hojman, D. (1999). *Telecentros Comunitarios: una propuesta de desarrollo para.* Chile: Departamento de Ingeniería Industrial. Universidad de Chiel.

CVS. (2014). *POLÍTICAS Y NORMAS DE SEGURIDAD.* Córdoba, España: Corporación Autónoma Regional de los Valles Sinu y del San Jorge .

Delgadillo, K., Gómez, R., & Sotll, K. (2002). *Telecentros... ¿para qué? Lecciones sobre telecentros comunitarios en América Latina y el Caribe.* Canada: IDRC. Fundación Chasquinet, PAN Américas.

DINADECO. (18 de 01 de 2019). *DINADECO.* . Obtenido de Sistema Nacional de Registro de Asociaciones: http://www.dinadeco.go.cr/snra.html

Doina, F. (Febrero de 2019). *Metodología para la Gestión de la Seguridad Informática.* Obtenido de Infomed Instituciones - Dirección Nacional Seguridad y Protección MINSAP: https://instituciones.sld.cu/dnspminsap/files/2013/08/Metodologia-PSI-NUEVAProyecto.pdf

Dussan, A. (2006). Política de seguridad informática. *Entramado*, 86-92. Recuperado el 27 de Febrero de 2019, de https://www.redalyc.org/pdf/2654/265420388008.pdf

Espinoza, J. (2015). *IMPLEMENTACIÓN DE UN LABORATORIO DE AUDIO VISUALES PARA EL*. Guayaquil – Ecuador: ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Gómez, Á. (2017). *Enciclopedia de la Seguridad Informática. 2ª edición.* Madrid: RA-MA.

Guadalupe, A. (2 de Octubre de 2011). *informaticabach2.blogspot*. Obtenido de informaticabach2.blogspot.com

Herrera, H. (19 de Febrero de 2007). *Gestiópolis.* Obtenido de Diagnóstico Administrativo: https://www.gestiopolis.com/diagnostico-administrativo/

IES VALLE INCLÁN. (27 de Febrero de 2019). *Aula virtual IES Valles Inclán.* Obtenido de https://www.edu.xunta.gal/centros/iesvalleinclan/aulavirtual2/pluginfile.php/14217/mod_resource/content/1/Tema%20redes%20y%20seguridad.pdf

Jensen, M., & Esterhuysen, A. (2001). *Manual para los telecentros comunitarios de África. Consejos para lograr su sustentabilidad. Còmo establecer un telecentro comunitario para propósitos múltiples en África.* París, Francia: Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

López, J., & Figueroa, W. (12 de Junio de 2018). *Redes de datos en instituciones de educación básica y media.* Obtenido de Eduteka: http://eduteka.icesi.edu.co/articulos/RedEscolarDatos

MICITT. (22 de Febrero de 2019). *Información CECI*. Obtenido de https://www.ceci.go.cr/zf_Web/Index/infoceci/ceci/278

MIDEPLAN. (8 de Marzo de 2018). *Documentos. MIDEPLAN.* Obtenido de https://documentos.mideplan.go.cr/share/s/3sMj6MvoRnSE8WGzyMqtNQ

MIDEPLAN. (2018). *Plan Nacional de Desarrollo e Inversión Pública del bicentenario 2019-2022.* San José, Costa Rica: MIDEPLAN.

Molina, C. (27 de Febrero de 2019). *Redtauros.com.* Obtenido de http://www.redtauros.com/Clases/Fundamentos_Redes/02_Topologia_de_Red.pdf

Moreno, L. (Marzo de 2019). *www.http://usuaris.tinet.cat/acl/html_web*. Obtenido de www.http://usuaris.tinet.cat/acl/html_web: http://usuaris.tinet.cat/acl/html_web/redes/topologia/topologia_2.html

Municipalidad Santa Bárbara. (2009). *Plan de Desarrollo Local Cantón de Santa Bárbara.* Santa Bárbara, Heredia, Costa Rica: Municipalidad de Santa Bárbara.

ORI. (s.f.). *Variables.* Obtenido de http://ori.hhs.gov/education/products/sdsu/espanol/variables.htm

PNDT. (2015). *Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 "Costa Rica: Una Sociedad Conectada.* San José, Costa Rica: MIDEPLAN.

PROSIC. (2006). *Hacia la sociedad de la información y el conocimiento en Costa Rica.* San José, Costa Rica: Programa sociedad de la información y el conocimiento. Universidad de Costa Rica.

PROSIC. (2007). *Hacia la sociedad de la información y el conocimiento en Costa Rica.* San José, Costa Rica: Programa sociedad de la información y el conocimiento. Universidad de Costa Rica.

PROSIC. (2018). *Hacia la sociedad de la información y el conocimiento en Costa Rica.* San José, Costa Rica: Programa sociedad de la información y el conocimiento. Universidad de Costa Rica.

Regueyra, M. G. (2001). Aprendiendo con las TIC: una experiencia universitaria. *Revista Actualidades Investigatibvas en Educación*, 1-29.

UNED. (2017). *Instructivo para Uso de Laboratorios.* San José, Costa Rica: Centro de Planificación y Programación Institucional. Dirección de Tecnología, Información y Comunicación.

Universidad Hispanoamericana. (2018). *Manual proyecto de graduación. Escuela Ingeniería Informática.* . San José, Costa Rica.: Inédito.

Universidad Latina de Panamá. (2012). *Normas de Seguridad de los Laboratorios de Cómputo.* Panamá: Universidad Latina de Panamá.