DISEÑO Y CONSOLIDACIÓN DE UN CENTRO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA.

LUIS YADIR ARANGO RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE - TOLIMA
2020

DISEÑO Y CONSOLIDACIÓN DE UN CENTRO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LA EMPRESA CIBERSECURITY DE COLOMBIA LTDA

LUIS YADIR ARANGO RAMIREZ

Proyecto aplicado presentada(o) como requisito parcial para optar al título de:
ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Martin Cancelado
Tutora de Curso

Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE-TOLIMA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

A mi madre, hermanos, familia y amigos que me han apoyado en cada decisión que tomo, me fortalecen para seguir adelante y obtener un logro más en mi proyecto de vida aportando cada día cosas que me fortalecen en el ámbito personal y profesional.

AGRADECIMIENTOS

A Dios por permitirme realizar una vez más lo que quiero gracias a las bendiciones y oportunidades que me ofrece, a mi familia por ser mi pilar y mi gran ayuda para lograr los sueños que tanto he anhelado y ser mi mayor motivación para superarme, a la Universidad que brindó una nueva ayuda para fortalecer mi profesión, además de todas las herramientas y conocimientos obtenidos en éste proyecto aplicado, gracias a los tutores que siempre están dispuestos y atentos a colaborarme con dudas y aportes que afianzaron el desarrollo de mi trabajo.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO DE INFORMACION: Es un dato o elemento que tiene valor para la Entidad.

AMENAZA: Es la indicación de un potencial evento no deseado que afecte negativamente la confidencialidad, integridad, disponibilidad o confiabilidad de los activos de información.

CIBERSEGURIDAD: Conjunto de políticas, directrices y métodos para la gestión de riesgos y que son útiles al momento de proteger los activos de una organización.

INCIDENTE: Un Incidente de seguridad de la Información es cualquier evento que vulnere o intente vulnerar la información.

RIESGO: Es la posibilidad que una amenaza explote o penetre una vulnerabilidad de un activo de información, impactando a este activo de información y/o activos asociados, viéndose afectando del mismo modo los objetivos del negocio

VULNERABILIDAD: Es una debilidad de seguridad asociada a un activo de información que puede hacer que una amenaza se haga efectiva.

RESUMEN

En el presente proyecto aplicado se estudia un caso de diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa Cibersecurity de Colombia LTDA. Teniendo como referencia la norma ISO 27001, además se implementa las políticas de seguridad y un plan de continuidad de negocio; se realiza análisis de los diferentes riesgos que existen de acuerdo a los diferentes activos con los que las organizaciones cuenten y dependiendo de este análisis se procede a implementar los mecanismos necesarios para minimizarlos y que los activos funcionen perfectamente y ayuden a cumplir con las metas y objetivos de las entidades.

Por otra parte, para llevar acabo el desarrollo de las actividades del CSIRT se realizarán documentales sobre la CiberSeguridad en Colombia, esto con el fin de estar orientados con la misión de Cibersecurity de Colombia LTDA.

De acuerdo a lo anterior, las empresas enfrentan un problema que radica en la carencia de documentos que les permita actuar de manera oportuna ante un incidente o vulnerabilidad siguiendo una ruta de instrucciones que estén bien definidas, y que les contribuyan a minimizar el tiempo de respuesta, los riesgos, mejorar la calidad de sus servicios, ahorrar dinero, entre otros beneficios que esto traería.

Finalmente, con el desarrollo del proyecto aplicado, se espera lograr respuestas oportunas a las organizaciones que experimentan incidentes en materia de

CiberSeguridad y que se encuentran en riesgos por vulnerabilidades, logrando que puedan alcanzar mejores niveles de seguridad y confianza para sus clientes.

ABSTRACT

In this applied project, a case of design and consolidation of a response center for computer security incidents in the company Cibersecurity de Colombia LTDA is studied. Taking the ISO 27001 standard as a reference, it also implements security policies and a business continuity plan; An analysis is carried out of the different risks that exist according to the different assets that the organizations have and depending on this analysis, the necessary mechanisms are implemented to minimize them and that the assets work perfectly and help meet the goals and objectives of the entities.

On the other hand, to carry out the development of the CSIRT activities, documentaries will be made on Cybersecurity in Colombia, this in order to be oriented with the mission of Cibersecurity de Colombia LTDA.

According to the above, companies face a problem that lies in the lack of documents that allow them to act in a timely manner in the event of an incident or vulnerability by following a route of instructions that are well defined, and that help them minimize response time. , the risks, improve the quality of their services, save money, among other benefits that this would bring.

Finally, with the development of the applied project, it is expected to achieve timely responses to organizations that experience incidents in Cybersecurity and that are at risk due to vulnerabilities, achieving that they can achieve better levels of security and trust for their clients.

INTRODUCCIÓN

El objetivo del presente proyecto es Diseñar y consolidar un centro de respuesta ante incidentes de seguridad informática en la empresa Cibersecurity de Colombia Ltda. través de actividades para consolidarse en el ámbito de CSIRT. Y dar soporte a sus clientes y con el fin de lograr canalizar las vulnerabilidades, ataques y la seguridad de la información que se pueden presentar las organizaciones que requieran la vigilancia permanente de su activo principal que es la información.

El tipo de investigación utilizado en el presente proyecto es descriptivo apoyada desde una investigación de campo y el método de validación es cualitativo. Los participantes de la muestra de esta investigación son organizaciones especialmente en el área de infraestructura.
Dentro del procedimiento se plantea actividades tales como: Monitoreo Continuo y proactivo, Gestión de incidentes de seguridad, Análisis Forense digital y de seguridad, Inteligencia de amenazas y Gestión de Vulnerabilidades todo ello para lograr el objetivo de este caso de estudio.

Cibersecurity de Colombia Ltda. Se encargara del análisis de riesgos, donde se identificarán los activos y el valor de los mismos para las organizaciones que deseen adquirir sus servicios. Además la identificación de amenazas, la evaluación de impacto y la clasificación de los riesgos que pueden estar causando dichas amenazas.

Por otro lado, se buscará la gestión a las respuestas de incidentes cibernéticos de acuerdo a los servicios que las organizaciones contraten con Cibersecurity como son la respuesta a incidentes o la gestión a vulnerabilidades.

Finalmente, el centro de respuestas se encargará de obtener todos los datos necesarios para lograr implementar las políticas de seguridad y establecer el modelo de implementación que requieran las compañías.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La empresa Cibersecurity de Colombia ltda se dedica a la prestación de servicio de seguridad y protección de la información. Su propósito es consolidarse como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT.

En la actualidad existen nuevos delitos que dejan a la sociedad vulnerable a cualquier ataque que los delincuentes planeen. El comportamiento que tienen los ciberdelincuentes hoy en día es a través de los medios tecnológicos como los es el internet lo cual ha producido que las organizaciones creen métodos e implementen nuevos controles de seguridad para poder Salvaguardar su activo principal que es la información.

Cibersecurity ofrece la respuesta a incidentes cibernéticos para gestionar el análisis de las vulnerabilidades que puedan tener las distintas compañías. Además es una forma de lograr prevenir los ataques y cuidar los datos tanto para las organizaciones como para personas.

Por otro lado, se asegura que el centro de respuesta e incidentes y ataques cibernéticos logre la cobertura necesaria con equipos de alta tecnología para dar solución pronta a los ataques contando con una excelente infraestructura en firewall, servidores y proveedores de Internet que logre objetivo principal.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál es la consecuencia que tiene el diseño y fortalecimiento de un centro de respuesta ante incidentes de seguridad informática en el ámbito de CSIRT. En la empresa Cibersecurity de Colombia LTDA?

2 JUSTIFICACIÓN

Teniendo en cuenta que un CSIRT es un Centro de Respuestas ante Incidentes de Ataques Cibernéticos y que está conformado por un equipo de especialista técnicos entrenados para resolver y gestionar incidentes informáticos de alto impacto y la necesidad de implementar un sistema de seguridad en las organizaciones para asegurar su activo más importante como lo es la información, y conociendo que en el mercado existen diversos equipos que pueden complementar los sistemas de seguridad sin inconvenientes y que sus principales objetivos es la seguridad, es de notar que toda empresa debería preocuparse por implementar mecanismos que ayuden a mantener seguros tanto los equipos como usuarios de la organización.

Sin embargo, es importante y necesario que las empresas tomen conciencia de la importancia de proteger la integridad de los datos que manejan en cada una de sus organizaciones, puesto que si deja de un lado el tema podría incurrir en el deterioro de la información y la perdida de los servicios lo cual genera pérdidas económicas.

Es pertinente a demás contar con la estrategia y medidas de seguridad de la información, con el fin de garantizar el funcionamiento adecuado de todos los sistemas, puesto que si se presentan amenazas o ataques que impliquen la pérdida de información, se apliquen los procedimientos correctivos necesarios.

El objetivo es lograr asegurar la información y esto consiste en hacer que los peligros sean conocidos, responsabilizados, dirigidos y minimizados por las organizaciones. Entregando informes detallados de tal forma que sea estructurado,

eficiente y ajustable a los cambios. Estas características deben ser de vital importancia para el entorno de cualquier organización, que incorpore a su gestión las tecnologías de la información y que esté respaldada sobre una plataforma tecnológica que contenga un alto nivel de integración de redes, comunicaciones y un sistema de información para lograr el centro de respuestas a incidentes cibernéticos.

Con el diseño y consolidación de este centro de respuestas a incidentes cibernéticos se pretende que las organizaciones tomen conciencia de las necesidades de seguridad informática y además lograr que estos centro puedan ser el ente que pueda prevenir las vulnerabilidades que en las compañías se dan

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar y consolidar un centro de respuesta ante incidentes de seguridad informática en la empresa Cibersecurity de Colombia LTDA.

3.2 OBJETIVOS ESPECÍFICOS

- Proveer asistencia de los servicios reactivos y proactivos del CSIRT y apoyar a las organizaciones en la protección de la información.
- Fomentar el diseño e implementación de la estructura tecnológica del CSIRT teniendo en cuenta la utilización de herramientas Open Source.
- Crear estrategias para la detección de eventos e incidentes de seguridad de la información, atraves de las distintas herramientas de control de seguridad para lograr reportes objetivos sobre los hallazgos
- Establecer un ambiente de analisis de registros informáticos controlados que permita monitorear, rastrear, realizar los backups de manera aislada.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

En el desarrollo del presente proyecto aplicado, Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa Cibersecurity de Colombia Ltda. Es pertinente crear un espacio donde se identifiquen, analicen y definan la historia de estos centros los cuales se realizaran a través de una revisión de fuentes bibliográficas, teóricas y empíricas.

Inicialmente, los centros de respuesta a incidentes informáticos buscan restituir las actividades con el menor impacto posible para las organizaciones. Son cada día más presente en organismos, instituciones, infraestructura crítica. Su historia inicia hace 28 años cuando un gusano de internet colapso los sistemas interconectados que existían en aquella época. Yolanda (2015-2019). Historias de los CERT- CSIRT. Origen y evolución. Recuperado de *https://www.yolandacorral.com/historia-de-los-cert/?cv=1*

Los grupos de respuesta tienen que ver muchos eventos que se han presentado a lo largo de la historia en temas de seguridad lo cual pone en jaque a muchas organizaciones y a su infraestructura tecnológica. Los avances han permitido la implementación de esquema de CiberSeguridad en las organizaciones, esto radica en la relevancia de los sistemas tecnológicos.

La gran importancia que tienen todos los sistemas tecnológicos en las actividades diarias hace indispensable que, en las organizaciones, se han dado cuenta la

necesidad de crear grupos específicos para lograr mitigar los ataques cibernéticos la cual permitirá resolver los incidentes y lograr proteger el activo principal de cualquier compañía que es la información.

Por otro lado, ya han pasado casi treinta años donde se creó el primero grupo de respuesta a incidentes y ataques cibernéticos. De los cuales se formaron a través de dichos acontecimientos que se fueron dando en las organizaciones y a medida de la implementación tecnológica.

En la actualidad se busca que las empresas no se vean afectadas por los incidentes graves, sino que se logre controlar y dar respuesta al mismo. Además, crear una planeación para la protección de los activos de las empresas, incluyendo los temas de respuestas ante dichos acontecimientos bien sea de equipos propios o de alguna compañía. Con el fin de lograr ayudar cuando los acontecimientos se presenten.

Actualmente en Colombia se cuenta con un grupo de respuestas a incidentes de seguridad informática el cual se encarga de servicios proactivos, servicios reactivos y los sistemas de gestión de seguridad de la información y análisis de *Malware* que está conformado en las distintas entidades. El cual tiene como objetivo garantizar la protección de la plataforma tecnológica, como apoyo a los métodos de CiberSeguridad. Su principal objetivo es lograr el fortalecimiento de las organizaciones para la investigación, prevención y atención de eventos e incidentes de seguridad, que atenten contra la confidencialidad, disponibilidad e integridad de la información sean protegidos.

La seguridad de la información se puede definir como un conjunto procedimientos y medidas, técnicas que permiten proteger la integridad, confidencialidad y disponibilidad de la información.
Integridad: es la correcta verificación de sus métodos y procesos cuando son completos.

Confidencialidad: es conocer que un solo rol de una persona pueda acceder y modificar la información.

Disponibilidad: es permitir que la información esté disponible cuando se requiera. En la presente propuesta dan una breve definición de lo que es seguridad informática se logra aplicar a las empresa que busca mejorar sistemas de seguridad, para esto se debe considerar cuales son los activos más importantes.

Al verificar el activo más importante en la compañía se deben implementar medidas que aseguren y además mantengan este activo en condiciones óptimas que cumpla con las condiciones del pilar de la información, en la siguiente cita se pueden verificar que es y significa un activo como información “Uno de los activos más valiosos para cualquier empresa es la información que maneja. La información es el conjunto de datos que da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la misma a la ruina. Extendiendo este concepto de seguridad al mundo de las telecomunicaciones y la informática, puede entenderse desde dos puntos de vista: seguridad de la información y seguridad informática”. Escrivá Gascó, G., Romero Serrano, R. M., & Ramada, D. J. (2013). *Seguridad informática. referencia* Obtenido de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3217398&ppg=2

Se comprende lo importante que es la implementación de la seguridad para mantener seguro el activo, pero se debe considerar los diferentes ataques que existen a la seguridad informática y que es perjudicial para cualquier compañía que no cuente con un sistema de seguridad, se debe saber cómo es un ataque y que fases comprende, Álvaro Gómez Vieites, “los ciberataques se presentan en varias fases como se presentan a continuación
Explotación de sistemas informáticos.

Hallazgos de vulnerabilidades.
Explotación de las vulnerabilidades detectadas atreves de herramientas como el metaexploit.

Compromiso del sistema: alteración de programas y archivos del sistema para dejar alojados troyanos; la creación de nuevas cuentas vulnerables con altos privilegios administrativos que faciliten poder atacar el sistema infectado.
Vieites, Á. G. (2014). *Gestión de incidentes de seguridad informática.* Obtenido de https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228430&ppg=1

Al identificar los diferentes tipos de ataques se implementan los mecanismos para realizar un sistema de seguridad basado en las normas ISO 27000, “Un Sistema de Gestión de Seguridad de la Información (SGSI), según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Permitirá conocer mejor las organizaciones, cómo funciona y qué se puede hacer para que la situación mejore. Mendoza Penagos, L. P. (2018). *Diseño de un sistema de gestión de seguridad informática para la Empresa GED (Gestión Estrategia y Desarrollo) de la ciudad de Bogotá.* Obtenido de https://repository.unad.edu.co/handle/10596/20723

4.2 MARCO CONCEPTUAL

En el presente proyecto aplicado se van a manejar diferentes términos que se deben conocer y saber de qué se trata. Además, se dará un enfoqué a la terminología que en los centros de incidentes cibernéticos se deben aplicar.

4.2.1 Activo de información: Son los elementos que son de gran utilidad y que tienen un valor para las organizaciones, sus operaciones y su continuidad, que son de vital importancia para que estas logren alcanzar sus objetivos.

4.2.2 Análisis de riesgo**:** manera de operar sistemáticamente para la manipulación de la información para lograr identificar fuentes y proyectar riesgos.

4.2.3. Amenaza**:** se considera todo aquello que sea físico o lógico que genere un incidente, lo cual genera daños materiales o inmateriales a la organización y a sus activos.

4.2.4 Controles de Seguridad**:** Son controles de seguridad que aplica políticas, procedimientos, las prácticas y las aplican a las estructuras organizativas para mantener los riesgos de la seguridad de la información por debajo del nivel de riesgos asumido.

4.2.5 Gestión de Riesgo**:** Proceso de identificación, control y minimización o eliminación, a un costo aceptable, los riesgos que afecten a la información de la organización. Se realiza la valoración del riesgo y el tratamiento del riesgo.

4.2.6 Integridad**:** exactitud en los de la información y sus métodos de proceso.

4.2.7 Impacto: Es la consecuencia en la que incurre la organización cuando un incidente afecta la misma

4.2.8 No conformidad**:** es el incumplimiento de una serie de evidencias que demuestran un requerimiento de control que da margen a la duda para la implementación de medidas que ayudan a preservar la confidencialidad, integridad y disponibilidad de la información.

4.2.9 Riesgo**:** Es la oportunidad de una amenaza logre explotar una vulnerabilidad para realizar un daño a un activo de la información.

4.2.1.1 Seguridad de la Información: es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la misma.

4.2.1.2 Vulnerabilidad: Debilidad que se presenta en las organizaciones cuando se maneja un activo principal como lo es la información que potencialmente permite que una amenaza afecte los activos.

4.2.1.3 CiberSeguridad: es la seguridad que se le otorga a la tecnología con la cual puede estar conformada una organización básicamente en su infraestructura

Ya definidos los diferentes términos que se van a manejar en el proyecto aplicado, se escogen los diferentes aportes que se van a tener en cuenta para el desarrollo y cumplimiento de los objetivos mencionados; se van a tener en cuenta todos los aportes y referencias manejas en el marco teórico puesto que cumplen con las diferentes características que se necesitan para la realización del proyecto además que se tomaran como base para la realización y desarrollo de la actividad.

La real Academia lo define como “Poner en funcionamiento o aplicar métodos, medidas, etc., para llevar algo a cabo.”

Para el desarrollo del proyecto aplicado se toma como referencia del dictionary.

Mecanismos: Para la real academia se define como “Conjunto de las partes de una máquina en su disposición adecuada.
Estructura de un cuerpo natural o artificial, y combinación de sus partes constitutivas Procesos.”

Para el desarrollo de la siguiente actividad se toma como referencia procesos, puesto que se van a implementar diferentes procesos para el cumplimiento de dichos objetivos.

Complementario: Según la real academia se define como “Que sirve para completar o perfeccionar algo.”, se toma está referencia puesto que lo que se hará es completar el sistema de seguridad de la compañía.

Implementación de mecanismos complementarios: Teniendo en cuenta los diferentes términos se definen como la instalación y aplicación de procesos para complementar o perfeccionar un sistema de seguridad.

Mejorar: Según la real academia define mejorar como lo siguiente: “Adelantar, acrecentar algo, haciéndolo pasar a un estado mejor” además contiene otras definiciones “Poner mejor, hacer recobrar la salud perdida”, “Ponerse en lugar o grado ventajoso respecto del que antes se tenía.”; para la implementación del proyecto se tendrá como definición Adelantar, acrecentar algo, haciéndolo pasar a un estado mejor.

Para el desarrollo del proyecto aplicado se va a enfocar por servicio encargado de la seguridad de unas empresas, puesto que se van a implementar sistemas que realizan la seguridad de la información.

Información: Para la real academia el termino información lo define como “Acción y efecto de informar”, “Oficina donde se informa sobre algo”, “Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada”, para el proyecto aplicado se va a tomar como referencia. La comunicación para lograr la adquisición de conocimientos los cuales permitirán precisar lo que se desea.

Informática: se puede definir como una agrupación de conocimientos técnicos y científicos que nos ayudan automatizar procesos por medio de una herramienta como lo son los equipos de cómputo; para la elaboración del proyecto aplicado se va a tomar como definición la automatización de procesos.

Mejorar la seguridad informática y de la información: Teniendo ya los diferentes términos definidos, se toma como definición, Adelantar y mejorar los servicios de seguridad de las compañías enfocadas en los sistemas computacionales que contienen almacenados los archivos de información crítica de la compañía.

Ya definidos los diferentes términos que se van a manejar en el proyecto aplicado, se escogen los diferentes aportes que se van a tener en cuenta para el desarrollo y cumplimiento de los objetivos mencionados; se van a tener en cuenta todos los aportes y referencias manejas en el marco teórico puesto que cumplen con las diferentes características que se necesitan para la realización del proyecto además que se tomaran como base para la realización y desarrollo de la actividad.

4.3 MARCO CIENTÍFICO O TECNOLÓGICO

Actualmente, el colombiano ha desarrollado esfuerzos para atender los temas de CiberSeguridad los cuales son coordinados por el COLCERT y otras entidades como la Policía Nacional coadyuvan la labor.

Para este proyecto, los expertos en Seguridad Informática deben plantear un proceso de CiberSeguridad correctamente documentado que permitirá una adecuada Gestión de los incidentes y vulnerabilidades

Para la documentación de la gestión de incidentes y Vulnerabilidades, se definirá un procedimiento para Gestión de los Incidentes, se realizan las actividades requeridas para dar solución a los incidentes en un primer nivel de servicio que incluya el soporte en sitio.

Se aplicará lo estipulado en el documento externo Manual de ITIL V4.

Se llevará un control y seguimiento de las incidencias a través de un software de reporte de incidencias (GLPI,

Definición de los ANS (Acuerdos de Niveles de Servicio, permite a ambas partes lograr acuerdos en temas como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio entre otros temas que determinan la Calidad del Servicio.

Definición de los Acuerdos de Niveles de operación que corresponde a un acuerdo entre la oficina de tecnologías de la información y otra dependencia solicitante y su

labor es brindar apoyo en la prestación de servicios al solicitante por parte de la oficina de tecnologías de la información.

Es importante mencionar que el desarrollo del Enfoque Directivo alcanzará un nivel de madurez en la medida en que se utilicen las herramientas, Metodologías y demás instrumentos para una adecuada documentación que permitan que una incidencia pueda resolverse y una vulnerabilidad no se explote , de ser así el impacto del riesgo sea mínimo.

4.4 MARCO LEGAL

En Colombia, desde la década de los 90 se ha sancionado un conjunto de leyes que coadyuvan la gestión del estado en cuanto a delitos cibernéticos, a continuación, se menciona la normatividad existente:

1. Ley No 527 de 1999: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

2. Ley No 599 de 2000: Por la cual se expide el código penal. En su artículo No 192, se ratifica la conducta punible de violación ilícita de comunicaciones al establecer el bien jurídico de los derechos de autor y se incluyen algunas conductas relacionadas con el delito informático, tales como el ofrecimiento, venta o compra de equipos para interceptar la comunicación entre personas

3. Ley No 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado ‘de la protección de la información y de los datos’ - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Congreso de Colombia, 2009a).

5 DISEÑO METODOLÓGICO

El centro de respuesta ante incidentes de seguridad informática. Este buscara crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio contratado los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades; donde la tarea es liderar el diseño técnico que permita dar desarrollo a las actividades propias del CSIRT. Por lo tanto, el tipo de investigación utilizado para el presente proyecto es descriptivo donde “busca explicar las propiedades, características y perfiles de personas, grupos u otros fenómenos sometidos análisis” (Danhke, 1998), apoyada desde una investigación de campo que consiste en “la encuesta de datos directamente de la realidad donde ocurren los hechos sin manipular y controlar variables. Estudia los fenómenos en su ambiente natural, el investigador no manipula variables” (Ramirez, 1999).
El método de validación es cualitativo el cual se entiende como “El estudio de la realidad en su contexto natural y como sucede, interpretando fenómenos a partir de un grupo de personas. (Perez, 2007).

5.1 INSTRUMENTO

En el presente proyecto se utilizaron las siguientes técnicas o instrumento propios de la investigación cualitativa.

Entrevista semiestructurada: Según Buendía, Colás y Hernández citado por González (2009), la entrevista es “la recogida de información a través de un proceso de comunicación, en el transcurso del cual el entrevistado responde a cuestiones

previamente diseñadas en función de las dimensiones que se pretenden estudiar planteadas por el entrevistador”

Para el caso de esta investigación se tuvo en cuenta la entrevista semiestructurada porque tiene la posibilidad de que la persona entrevistada pueda aclarar términos y dudas sobre lo que se está indagando. Se basan en una guía de preguntas y el entrevistador tiene la libertad de introducirle preguntas adicionales para precisar conceptos u obtener mayor información sobre el tema investigado.

Se creó una entrevista semiestructurada aplicable al área de infraestructura de diferentes organizaciones especialmente a los cargos de ingenieros de seguridad (oficial de seguridad) e ingenieros de infraestructura Para recolectar información referente al funcionamiento eficaz y eficiente de los Centros de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT. Esta entrevista fue creada a partir de unas categorías pertinentes al tema.

5.1.1 Herramientas a utilizar CSIRT Monitoreo de Red:

5.1.1.1 Wireshark:

Es un software que permite el análisis de protocolos de una red, el cual permitirá realizar detalladamente la conducta de esta y lograr la solución a las comunicaciones.

5.1.1.2 Nmap:

Esta herramienta ayudara a identificar los puertos de comunicación que se encuentre abierto en una red.

5.1.1.3 Tcpdump:

Analiza el tráfico de una red en tiempo real lo transmitido y lo recibido, lo cual permite al usuario obtener un informe con mayor precisión.

5.1.2 Reporte y alertas

5.1.2.1 Nagios:

Es una herramienta que ayuda a monitorizar la red, lo cual permite vigilar los equipos y servicios que se especifiquen, lo cual genera una alerta cuando el comportamiento no es adecuado.

5.1.2.2 Tripwire:

Esta herramienta nos ayuda al monitoreo y a las alertas que se generan cuando se realizan cambios en los registros de un sistema de información. Su objetivo es la integridad de los datos

5.1.3 Auditorias:

5.1.3.1 Zenmap:

Es una herramienta que captura los paquetes IP, lo cual identifica los equipos que se encuentren disponibles en la red. Además, identifica los servicios, sistemas operativos y que tipos de filtros se están utilizando.

5.1.3.2 Nessus:

Es una herramienta que se compone de dos partes una es el servidor el cual se encarga de los ataques mientras el cliente Nessus proporciona una interfaz que es intuitiva para lograr generar los reportes que se requieran.

5.1.4 Escaneo Vulnerabilidades:

5.1.4.1 Metasploit:

Ayuda a proporcionar la información sobre las vulnerabilidades que se presenten realizando un test de penetración el cual ayudara a identificar dichas falencias y desarrollar las firmas para los sistemas de detección de intrusos.

5.1.4.2 Openvas:

Se utilizará esta herramientas dado que cumple con dos servicios uno de ellos es un servidor de escáner el cual se encarga de realizar el análisis de las vulnerabilidades y un cliente que es utilizado para los resultados el mismo.

5.1.5 Analisis forense

5.1.5.1 Autopsy:

Es una herramienta para realizar análisis e investigaciones leves o profundas sobre los archivos y líneas temporales de los ficheros. Se pueden analizar discos de Windows y unix y que estén en sistemas de archivos NTFS, FAT, UFSI1/2, Ext2/3.

5.1.6 Escaneo elementos malicioso

5.1.6.1 Ossec:

Es una herramienta de detección de intrusiones la cual ejecuta el análisis de registros, verificación de integridad, monitoreo de registros de Windows. Además, detecta los rootkits y genera alertas basadas en el tiempo y repuesta activa.

5.1.6.2 Snort:

Es un programa que ayuda a la detección de intrusos que posee una capacidad de almacenamiento en bitácoras en archivos de texto. Además, implementa un motor de detección de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier novedad que se presente.

Estas herramientas se utilizaran con la finalidad de prevenir los incidentes y vulnerabilidades que puedan presentar las organizaciones teniendo como finalidad mitigar los ataques cibernéticos que puedan presentarse.

Finalmente, Los participantes que hacen parte de la muestra de esta investigación, son organizaciones especialmente en el área de infraestructura. La población es una muestra de expertos definida por participantes que brindaron información confiable referente al tema de Centros de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT a partir de las categorías determinadas en la entrevista.

6 DESARROLLO DE LOS OBJETIVOS

6.1 DESARROLLO DE OBJETIVO 1

Teniendo en cuenta que Cibersecurity de Colombia LTDA, es una empresa colombiana que presta servicios de seguridad para la protección de la Información. Y Su propósito es consolidarse como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de CSIRT. Además, busca crear y gestionar las funciones de respuesta a incidentes cibernéticos, ofreciendo servicios que permitan dar soporte a sus clientes teniendo presente el nivel de servicio contratado los cuales pueden ser de respuesta a incidentes o de gestión a vulnerabilidades. Se plantea los siguientes servicios:

6.1.1. Servicios Reactivos:

Son todos aquellos incidentes de seguridad cibernética que ocurre dentro de una infraestructura. De los cuales tenemos los siguientes:

6.1.1.1 Gestión de Incidentes:

Tiene una serie de procesos que se llevan a cabo para dar su respuesta los cuales son: recepción y notificación del incidente, clasificación, análisis y resolución. Ya teniendo esto claro se determina el tipo de impacto potencial y la gravedad del incidente. Posteriormente se asigna un equipo para que diseñe un plan de acción que logre recuperar y mejorar el servicio.

La gestión se llevara acabo de la siguiente manera: el área encargada de realizar la gestión de los incidentes de seguridad lograra identificar las posibles fuentes de ataques las cuales podrían ser en una organización:

- Inadecuada protección de la infraestructura
- Colaboradores descontentos

- Crecimiento de redes
- Falta de creación de contingencias
- Falta de políticas
- Desastres naturales
- Confianza creciente en los sistemas
- Virus
- Explotación de vulnerabilidades, tanto a nivel de host, como de arquitectura de red. Seguridad perimetral
- Ingeniería social
- Negación de servicios
- Hacking
- Robo de información confidencial
- Violación de la privacidad
- Falsificación de identificadores (biométricos)

Los incidentes de seguridad se definirán con estrategias para lograr su erradicación de la siguiente forma:

- Contar con tiempo y recursos necesarios para poner en prácticas las estrategias que se creen.
- Identificar los procedimientos de cada sistema operativo comprometido.
- Identificar los usuarios o servicios comprometidos para proceder a desactivarlos.

Los procedimientos de recuperación se llevaran a cabo teniendo en cuenta que se debe realizar una copia de respaldo actualizada de los sistemas de información, configuración y bases de datos.

- Generar de nuevo la información digital o física, configuración de sistemas de información, cargue manual de la información

- Actualización, instalación de los compontes de seguridad en los sistemas que se vieron comprometidos
- Crear el plan de recuperación de desastres

Por último, se mantendrá informado a las organizaciones sobre la documentación de los eventos e incidentes de seguridad que presenten. Además, se actualizarán las bases de datos de los sistemas de información que tengan las organizaciones. Se integrará los eventos e incidentes a la matriz de riesgos de los activos y para lograr mitigar los incidentes también se deben realizar capaciones a los colaboradores que pertenezcan a la organización y que participen en los temas relacionados a eventos e incidentes de seguridad de la información.

6.1.1.2 Respuestas de vulnerabilidades:

Está conformada por varios procesos que se llevan a cabo la cual incluye parches y aplicaciones para lograr mitigar las vulnerabilidades. A medida que van saliendo los nuevos parches, el CSIRT notifica a todas las partes interesadas para realizar sus respectivas modificaciones.

6.1.1.3 Respuesta ataques cibernéticos:

Es la gestión que se le da sobre los ataques que puedan presentarse a una red o un equipo e informar a las partes interesadas. De tal manera que prever dichos acontecimientos en su sistema.

6.1.2 Servicios proactivos:

Brindan información que contribuya a la protección de la infraestructura tecnológica, de esta manera mejora los procesos de seguridad y con esto se evita los ataques e incidentes que se puedan presentar.

6.1.2.1 Monitoreo continuo tanto interno como externo:

Se realiza la implementación de varios softwares open source que ayudan a detectar los eventos de seguridad de una red. Además, lograr informes automatizados y escanea las vulnerabilidades que se puedan estar presentando. Se manejarán con los siguientes programas

6.1.2.2 Reporte y alertas de seguridad:

Realiza procesos de vigilancia y alertas a seguimiento más avanzado a la infraestructura, teniendo en cuenta que se requiere una interconexión del sistema o la instalación de sensores de seguridad en la infraestructura de la organización.

6.1.2.3 Desarrollo de técnicas y herramientas de seguridad:

Es un campo donde todo el tiempo se debe permanecer actualizado sobre los avances en el campo de la seguridad y de la respuesta a incidentes. Lo cual permite estar al día sobre las aleras, amenazas en evolución, la forma de ataques que surgen, las mejores prácticas y las nuevas normas de servicios.

6.1.2.4 Auditorias de seguridad:

En este servicio se pretende obtener un análisis de la infraestructura o de las aplicaciones, la revisión de las normas de seguridad, el análisis de vulnerabilidades, las pruebas de penetración y el cumplimiento de las normas y estándares.

6.1.2.5 Escaneo de vulnerabilidades:

Distribuir de forma pertinente la información relevante que pueda mejorar los niveles de seguridad con respecto a las amenazas y las vulnerabilidades.

6.1.2.6 Análisis forense: lograr identificar:

Esto permite buscar datos que no son conocidos previamente, tratados de encontrar un patrón o comportamiento determinado, o descubrir información que se encontraba oculta.

6.1.2.7 Escaneo de elementos maliciosos:

Mediante unas aplicaciones open sour se logra identificar qué equipo tiene elementos que sean malicioso para nuestro sistema.

6.2 DESARROLLO DE OBJETVO 2

La conformación de la estructura tecnológica del CSIRIT va estar conformado de la siguiente manera:

6.2.1 Centro de Datos:

Es un cuarto equipado con todos los elementos electrónicos y tecnológicos que guardan toda la información de una organización.

6.2.2 I+D+i (investigación, desarrollo e innovación):

En esta área lo que se pretende es lograr desarrollar e innovar con nuevos elementos que permitan que el centro de repuesta ante incidentes de ataque cibernéticos puedan estar protegidos con mayor eficiencia.

6.2.3 Centro de Operaciones:

Es un área dotada con todos los elementos tecnológicos para realizar el monitoreo continuo y donde se evidencia las vulnerabilidades y ataques que las organizaciones pueden presentar.

6.2.4 Soporte TI:

Es un área técnica que nos ayuda a resolver problemas que puedan presentarse con los usuarios o con la infraestructura.

6.2.5 Coordinaciones:

Área donde se toman las decisiones al respecto de los casos que se estén presentando. Además organiza la forma como se va a trabajare en el centro de respuesta.

6.2.6 Área Logística:

Es el área encargada de asignar los recursos físicos, tecnológicos y de comunicaciones que requiera la organización.

6.2.7 Salón de Formación:

Área para las capacitaciones necesarias sobre los nuevos desarrollos e innovaciones que se estén dando a nivel de seguridad cibernética.

6.2.8 Salón de crisis:

Área donde se construyen proyectos futuros, donde se tiene un laboratorio de pruebas de forma controlada.

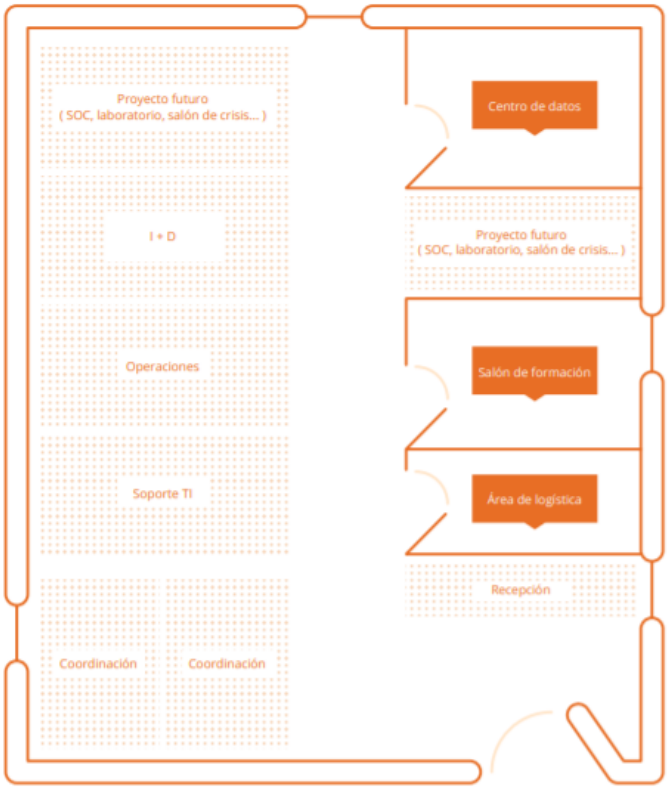


Imagen 1 Diseño Estructura CSIRT

6.2.9 Planificación:

Para la organización del CSIRT se tendrá en cuenta los servicios que debe realizar el centro de atención de incidentes de ataques cibernéticos, donde se da a conocer la secuencia para la ejecución de un sistema de seguridad cibernética, enfocado al mejoramiento continúo de los procesos. Además de la implementación de los diferentes mecanismos que buscan dar solución a los diferentes problemas que expuestos y sobre todo que atentan contra las bases de la información, que son la disponibilidad, integridad y confidencialidad de cada organización.

6.2.10 Implementación:

El plan de implementación está planeado para una duración de 10 meses y se ejecutará en el plazo estimado y se tendrá en cuenta los diferentes ítems y los periodos de ejecución de cada uno, teniendo como referencia esto se realiza el plan de implementación y los periodos de ejecución.

Tabla 1 Plan de implementación.

Ítem	Periodo de ejecución
1. Auditorias	Mes 1.
2. Análisis forense digital y de seguridad	Mes 2
3. Inteligencia de amenazas	Mes 3.
4. Monitoreo Continuo y proactivo	Mes 4.
5. Inteligencia de amenazas	Mes 5.
6. Auditorias.	Mes 6.
7. Gestión de Vulnerabilidades.	Mes 7.
8. Evaluación.	Mes 8.
9. Capacitación departamento de sistemas.	Mes 9.
10. Entrega Propuesta.	Mes 10.

6.2.11 Documentos Generados:

Al realizar el plan de implementación de los mecanismos, se define los diferentes documentos que se generan durante el desarrollo de los diferentes ítems ya especificados y seleccionados.

Tabla 2 Documentos Generados

Ítem	Documentos
1 Auditorias.	Hallazgos de Auditoria.
7. Gestión de Vulnerabilidades.	Vulnerabilidades
2. Análisis forense digital y de seguridad	Análisis de los riesgos forenses.
7 Tratamiento de los riesgos.	Tratamiento de los diferentes riesgos.

9. Capacitación departamento de sistemas.	Registro de asistencias.
10. Entrega Propuesta	Resultado informe

Además de los documentos anteriormente mencionados se entregan también diferentes documentos que se deben implementar antes durante y después de cada ataque, como lo son listas de chequeo, instrucciones, formularios, procedimientos y mecanismos de control. Estos documentos son de suma importancia en la gestión de incidentes de seguridad. Esto con ánimo de que el CSIRT entregue de recomendaciones a cada una de las organizaciones que dese tener los servicios del centro de respuesta de incidentes cibernéticos.

6.3 DESARROLLO DE OBJETVO 3

Las estrategias atención de eventos se llevaran acabo de la siguiente manera:

6.3.1 Gestión de Incidentes:

La Gestión de incidentes será realizada basándonos en el Modelo planteado en la Guía para Gestión y Clasificación de incidentes de Seguridad de la información de MINTIC

El modelo se orienta por cuatro fases:

- Preparación.
- Detección y Análisis
- Contención Erradicación y Recuperación
- Actividades post- Incidente

Dentro de los roles definidos previamente el equipo del CSIRT deberá realizar entre otras las siguientes actividades para el tratamiento y la gestión de incidentes de Seguridad.

- Detección de incidentes:

Monitorear y verificar los controles a fin de identificar posibles incidentes o vulnerabilidades.

- Atención de incidentes de Seguridad:

Recibe y resuelve los incidentes

- Recolección y Análisis de Evidencia Digital:

Toma, preservación, documentación y análisis de evidencia cuando sea requerida

- Anuncios de Seguridad:

Es función del CSIRT informar a los colaboradores y clientes acerca de las nuevas vulnerabilidades, actualizaciones y recomendaciones de seguridad para prevenir incidentes.

- Auditoria y trazabilidad de Seguridad Informática:

El equipo deberá realizar verificaciones periódicas del estado de las plataformas para verificar posibles vulnerabilidades y brechas de seguridad.

- Certificación de productos:

Para garantizar los requerimientos de seguridad actuales el SCIRT valida que las aplicaciones y su funcionamiento.

- Configuración y Administración de Dispositivos de Seguridad Informática:

Se encargaran de la administración adecuada de los elementos de seguridad informática.

- Clasificación y priorización de servicios expuestos:

Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques

- Investigación y Desarrollo:

Actividad consiste en la investigación permanente de nuevas tendencias en herramientas de protección para combatir las posibles incidencias y vulnerabilidades.

Los incidentes y Vulnerabilidades de Seguridad serán atendidos de conformidad con el nivel de criticidad de su impacto.

Tabla 3 Valor del incidente

Nivel de criticidad	Valor	Descripción
Inferior	0,1	Sistema no crítico, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	2,5	Sistemas que apoyan a una sola dependencia o procesos de una entidad
Medio	0,5	Sistemas que Apoyan más de una dependencia o proceso de la entidad.
Alto	0,75	Sistemas que pertenece al área de tecnología y estaciones de trabajo de usuarios con funciones criticas
Superior	1,00	Sistema critico

De cara a los clientes es importante tener en cuenta que los incidentes deben ser debidamente notificados por lo que se hace necesario disponer de un proceso para tal fin ya que el éxito en la gestión de incidentes depende de su documentación.

La persona encargada de decepcionar los incidentes juega un papel clave en la coordinación y asignación de las actividades a quien corresponda.

El CSIRT debe contar con su sistema para incidencias y Vulnerabilidades que será la mesa ayuda para quienes acudan a sus servicios

En la Gestión de Incidentes se integra la ISO-27035 la cual proporciona un enfoque estructurado para:

- Identificar, comunicar y evaluar los incidentes de la seguridad de la información
- Contestar, gestionar los incidentes de la seguridad de la información

- Identificar, examinar y gestionar las vulnerabilidades de seguridad de la información
- Aumentar la mejora de la continuidad de la seguridad de la información y de la gestión de los incidentes, como respuesta a la gestión de incidentes de la seguridad de la información y de las vulnerabilidades.

6.4 DESARROLLO DE OBJETVO 4

Se establece un ambiente de analisis de registros informáticos controlados que permiten monitorear, rastrear, realizar los backups de manera aislada.

Esto se lograr realiza en un ambiente controlado que nos facilita la operatividad que va a tener el CSIRT. Para lograr ver su desarrollo y la operatividad que tiene el centro de respuesta ante incidentes de ataques cibernéticos. Observar el siguiente video:

https://www.youtube.com/watch?v=TeD6eRiZJ18&t=135s

7 CONCLUSIONES

En la actualidad podemos percibir que todo lo que hacemos de trámites y diligencias comunes y corrientes las podemos aplicar al mundo de la tecnología dando un clic para solucionar nuestro día a día. Teniendo en cuenta nuestro mundo moderno el CSIRT de Cibersecurity de Colombia Ltda. En su principal objetivo es lograr consolidarse como un centro de respuesta ante incidentes de seguridad informática es lograr atender, prevenir, solucionar y mitigar todos los ciberataques que se puedan presentar en las diferentes organizaciones que tengan nuestros servicios.

Por otro lado, Cibersecurity de Colombia en sus servicios reactivos y proactivos nos dan la facilidad de poder diagnósticas, prevenir y dar una solución pronta a la situación que pueda presentar alguna de las organizaciones que se encuentre adscriptas a nuestros servicios. Logrando una protección de la infraestructura tecnológica que tenga cada compañía con las mejores herramientas, ambiente y personal calificado para lograr salvo guardar la información y protección de datos de las distintas compañías.

La planificación que se tiene en el CSIRT cuenta con una estructura fundamental que se tiene para el desarrollo de las actividades como son el centro de datos, el I+D+i, centro de operaciones, mesa de ayuda TI, nuestra área logística, el salón de crisis, etc ayuda a que la implementación de todos los sistemas y control de seguridad no logren estar expuestos para poder ser atacados por ciberdelincuentes. Además de que la operación tiene como objetivo darnos un analisis y un resultado o reporte para este tipo se situaciones.

Finalmente, las estrategias que se implementan para dar un resultado oportuno a nuestro clientes van estar ligados de la detección, analisis, contención, erradicación, recuperación y monitoreo contante a toda la infraestructura tecnológica de nuestros clientes con el ánimo de lograr mitigar cualquier ataque que estos pueden presentar.

Por otra parte, todos los ataque que puedan presentar nuestros clientes se ejecutaran en un ambiente controlado con el fin de lograr identificar cual es el propósito del ataque y lograr proteger la información y dar la continuidad de negocio sin que esto se logre ver afectado por dichos ataques. Además de que estamos sujetos a la normatividad colombiana que está dado por el ministerio de las tecnologías de la información.

8 RECOMENDACIONES

Como vivimos en una sociedad en un auge de tecnología lo cual ha provocado que nos volvamos más dependientes de la tecnología esto ha ocasionado que nos volvamos vulnerables para el robo de nuestra información. Por eso CSIRIT de Cibersecurity de Colombia recomienda lo siguiente:

1. Protección de los equipos: todos los dispositivos tecnológicos debes estar actualizados dado que esto previene los huecos de seguridad, junto con el antivirus lograr la protección de los equipos
2. Contraseña fuerte: para cada usuario mínimo debe tener 8 caracteres que este combinado con letras, símbolos y números y no nombres de personas, mascotas o bandas de música.
3. Comprobación de autenticidad de enlaces y perfiles: evitar recibir y aceptar correos de desconocidos dado que hoy en día se presenta el Phishing lo cual hacen para capturar información de la victimas
4. No descargar contenido pirata: preferiblemente descargar contenidos de páginas legales. Dado que esta situación abre la puerta a que puedan realizar ataques a nuestros dispositivos.
5. Realizar copias de seguridad: es fundamental realizar copias de seguridad dado que pueden presentar ataques o pérdidas de información. Esto se hace con el fin de poder recuperarla.

9 BIBLIOGRAFÍA

FERNÁNDEZ SÁNCHEZ, C. M., & Piattini Velthuis, M, Modelo para el gobierno de las TIC basado en las normas ISO, 2012.
Disponible en https://ebookcentral-proquestcom.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3205141&ppg=1

ADMINISTRATIVA, D. G. MAGERIT – versión 3.0. Obtenido de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, 2013 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ALCANTÁRA Flores, J. C. Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo, 2015 disponible en: http://tesis.usat.edu.pe/handle/usat/539

ARANGO PARRADO, A., Arango, C., Arias Solano, G. M., Caballero, J., Cortés, L. A., Cristancho, H. O., & Guzmán Solano, S. L. 2014. Autenticación Basada en Riesgos (RBA). Disponible en: https://repository.ucatolica.edu.co/handle/10983/2181

ARBELÁEZ CORTÉS, R. C. Sistema integral de diagnóstico de la seguridad informática. 2004. Disponible en: https://repositorio.uniandes.edu.co/handle/1992/10268

ARDILA CASTILLO, N., & Torres Torres, D. M. Autentificación, confidencialidad y gestión de claves en un entorno ip.2012. Disponible en: https://repository.unilibre.edu.co/handle/10901/8856

ARIZA BARRERA, D. R. Monografía protocolos copias de seguridad Oracle 2017. Disponible en: https://repository.unilibre.edu.co/handle/10901/11163

ÁVILA PARDO, W., & Ramírez Restrepo, J. L. Escaneo de vulnerabilidades al servidor principal de la empresa. Caso de estudio. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/18321

AYALA ROJAS, N. A. Monografía de estudio sobre la aplicación de seguridad biométrica para la identificación de usuarios en entornos WEB. 2015. Disponible en: https://repository.unad.edu.co/handle/10596/3743

BARRETO CUITIVA, J. H. Manual de seguridad informática para Pymes.2018. Disponible en: https://repository.unad.edu.co/handle/10596/15026

BOTERO TABARES, F. A. propuesta de protocolos en la seguridad de la información en el sector público. 2014. Disponible en: https://repository.ucatolica.edu.co/handle/10983/1287

CANO, J. J. Ciber ataques—La inestabilidad de lo que hemos aprendido en seguridad y control. 2016. Disponible en: https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge-spanish.aspx?utm_referrer=

CASTELLANOS, J. M. AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA EN LA UCF. 2019. Disponible en: http://cienciometrica.com/infometrica/index.php/syh/article/view/73

CORAL OJEDA, J. A. Diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO 27001:2013 en el Centro de Estudios Emssanar Cetem de la ciudad de Pasto. 2017. Disponible en: https://repository.unad.edu.co/handle/10596/11875

DELVASTO RAMÍREZ, R. A. Modelo de Gestión de incidentes de seguridad de la información para PYMES. 2016. Disponible en: https://repository.unad.edu.co/handle/10596/6170

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA. magerit – versión 3.0. 2012 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

EQUIPO DE EXPERTOS UNIVERSIDAD DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? 2016. Disponible en: https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/

ESCRIVÁ GASCÓ, G., Romero Serrano, R. M., & Ramada, D. J. Seguridad informática. 2013. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3217398&ppg=2

ESPINOZA ZALLAS, E., & Rodríguez Pérez, R. Seguridad informática una problemática de las organizaciones en el Sur de Sonora. 2017 Disponible en: http://revistainvestigacionacademicasinfrontera.com/sistema/index.php/RDIASF/article/view/140

FERREYRO, A. L. metodología de la investigación. obtenido de metodología de la investigación 2014. Disponible en:

http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=847674&lang=es&site=eds-live

GIL VERA, V., & Gil Vera, J. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. 2017. Disponible en: https://www.redalyc.org/html/849/84953103011/

GÓMEZ FERNÁNDEZ, L., & Álvarez, A. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. 2012. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3205110&ppg=1

GÓMEZ LÓPEZ, J., & Gómez López, O. D. Administración de sistema operativos. 2014. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228996

GUAPACHA PIEDRAHITA, J. D. Diseño de diplomado virtual en principios de seguridad Informática. 2017. Disponible en: https://repository.unilibre.edu.co/handle/10901/10553

HOYOS MALES, C. E. Seguridad en el transporte y gestión de correos electrónicos, implementación de seguridad en correo outlook 2010. Disponible en: https://repository.unad.edu.co/handle/10596/3657

J, G., BERMEO, J., Villacreses, E., & Guerrero, J. Delitos informáticos: una revisión en Latinoamérica. 2018 Disponible en: http://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/262

LEÓN CEPEDA, L. C. Estructuración del sistema de seguridad de la información en el área de protección de datos para un operador logístico bajo la norma NTC/ISO 27001:2013. 2018 Disponible en: https://repository.ucatolica.edu.co/handle/10983/16149

MATACHANA, Y. Los virus informáticos: una amenaza para la sociedad. (1 de 1 de 2009. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=4&docID=10357400&tm=1466006227313

MENDOZA PENAGOS, L. P. Diseño de un sistema de gestión de seguridad informática para la Empresa GED (Gestión Estrategia y Desarrollo) de la ciudad de Bogotá. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/20723

MIN TIC. (s.f.). ¿Y de seguridad TI qué hacen las entidades? Disponible en: https://www.mintic.gov.co/gestionti/615/w3-article-7083.html

MIN Tic. (s.f.). Modelo de Seguridad. Disponible en: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

OJEDA PÉREZ, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L. A. Delitos informáticos y entorno jurídico vigente en Colombia. 2010. Disponible en: https://repository.javeriana.edu.co/handle/10554/23982

PATIÑO ALPALA, L. O. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, Propolsinecor. 2014 Disponible en: https://repository.unad.edu.co/handle/10596/2742

PENAGOS, E. B.NGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE. 2015 Disponible en: https://repository.unad.edu.co/handle/10596/3629

PLAZAS GARCIA, E. R. Ingeniería social en las empresas colombianas. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/18704

PRADA HERNÁNDEZ, N. M. Diseño de un sistema de gestión de seguridad de la información, alineado con la Norma ISO. 2010. Disponible en: https://repository.javeriana.edu.co/handle/10554/7515

RAYA CABRERA, J., & Raya González, L. Implantación de sistemas operativos. 2014 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228461

REYES, J., Muñoz, C., & Guarda, Seguridad Informática para Pequeñas y Medianas Empresas de la Provincia de Santa Elena. 2017. Disponible en: https://search.proquest.com/openview/ba8fb554f72bbe6b94735e926be36754/1?pq-origsite=gscholar&cbl=1006393

SANABRIA FLÓREZ, Y.. Seguridad informática en Claro Colombia en el área de cuidado al cliente-prevención. 2017 Disponible en: https://repository.ucatolica.edu.co/handle/10983/1327

SANTOS, J. C. Seguridad informática. 2014. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228430&ppg=1

SANTOS, J. C. Seguridad y alta disponibilidad. 2014. Disponible en: https://ebookcentral-proquest-

com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228975&ppg=1

SENADO DE LA REPUBLICA. Ley 1273 de 2009. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

UNIVERSIDAD LIBRE. (s.f.). El decálogo de la seguridad informática. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/247-el-decalogo-de-la-seguridad-informatica

URECHE OSPINO, M. E. Diseño de Políticas de Seguridad Informática basadas en la norma NTC-ISO-IEC 27001:2013 para la universidad de Cartagena centro tutorial Mompox Bolívar. (06 de 04 de 2017). Disponible en: https://repository.unad.edu.co/handle/10596/12027

VALENCIA DUQUE, F. J., Cardona Londoño, A., & Carvajal Portilla, D. L. Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie ISO/IEC 27000 para una entidad pública colombiana.2018. Disponible en: http://repositorio.autonoma.edu.co/jspui/handle/11182/721

VIEITES, Á. G. Gestión de incidentes de seguridad informática. 2014. Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228430&ppg=1

VIEITES, Á. G. Seguridad en equipos informáticos. 2014 Disponible en :https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3229330

VIEITES, Á. G. Seguridad en equipos informáticos. 2014. Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=13&docID=11046412&tm=1466006343174

VILLAGÓMEZ, C. Sistema de detección de intrusiones (IDS). (6 de 12 de 2017). Disponible en: https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

YUDITH, D. Seguridad Informática. 2018. Disponible en: https://instituciones.sld.cu/dnspminsap/seguridad-informatica/

ZAMBRANO BURBANO, R. M. Estudio sobre el conocimiento y la aplicabilidad de la seguridad informática en las empresas. (12 de 02 de 2012). Disponible en: https://repository.unad.edu.co/handle/10596/20152

Fernández Sánchez, C. M., & Piattini Velthuis, M. Modelo para el gobierno de las TIC basado en las normas ISO. 2012. Disponible en: https://ebookcentralproquest.com

ADMINISTRATIVA, D. G. MAGERIT – versión 3.0. Obtenido de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.2013. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ALCANTÁRA FLORES, J. C. Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo. 2015 Disponible en: http://tesis.usat.edu.pe/handle/usat/539

ARANGO PARRADO, A., Arango, C., Arias Solano, G. M., Caballero, J., Cortés, L. A., Cristancho, H. O., & Guzmán Solano, S. L. 2014. Autenticación Basada en Riesgos (RBA). Obtenido de https://repository.ucatolica.edu.co/handle/10983/2181

ARBELÁEZ CORTÉS, R. Sistema integral de diagnóstico de la seguridad informática. 2014. Disponible en: https://repositorio.uniandes.edu.co/handle/1992/10268

ARDILA CASTILLO, N., & Torres Torres, D. M. Autentificación, confidencialidad y gestión de claves en un entorno ip. 2012. Disponible en: https://repository.unilibre.edu.co/handle/10901/8856

ARIZA BARRERA, D. R. Monografía protocolos copias de seguridad Oracle 2017. Disponible en: https://repository.unilibre.edu.co/handle/10901/11163

ÁVILA PARDO, W., & Ramírez Restrepo, J. L. Escaneo de vulnerabilidades al servidor principal de la empresa. Caso de estudio. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/18321

AYALA ROJAS, N. A. Monografía de estudio sobre la aplicación de seguridad biométrica para la identificación de usuarios en entornos WEB. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/3743

BARRETO CUITIVA, J. H. Manual de seguridad informática para Pymes. 2018 Disponible en: https://repository.unad.edu.co/handle/10596/15026

BORDA PÉREZ, M. El proceso de investigación : visión general de su desarrollo.2014 Disponible en: http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.asp

x?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&ebv=EB&ppid=pp_79

BOTERO TABARES, F. A. Propuesta de protocolos en la seguridad de la información en el sector público. 2014. Disponible en: https://repository.ucatolica.edu.co/handle/10983/1287

CANO, J. J. Ciber ataques—La inestabilidad de lo que hemos aprendido en seguridad y control .2016 Disponible en: https://www.isaca.org/Journal/archives/2016/volume-5/Pages/cyberattacks-the-instability-of-security-and-control-knowledge-spanish.aspx?utm_referrer=

CASTELLANOS, J. M. AUTOMATIZACIÓN DE CONTROLES DE SEGURIDAD INFORMÁTICA EN LA UCF.2019 Disponible en: http://cienciometrica.com/infometrica/index.php/syh/article/view/73

Coral Ojeda, J. A. Diseño de un sistema de gestión de seguridad para la red datos bajo la norma ISO 27001:2013 en el Centro de Estudios Emssanar Cetem de la ciudad de Pasto. 2017. Disponible en: https://repository.unad.edu.co/handle/10596/11875

DELVASTO RAMÍREZ, R. A. Modelo de Gestión de incidentes de seguridad de la información para PYMES. 2016. Disponible en: https://repository.unad.edu.co/handle/10596/6170

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA.MAGERIT – versión 3.0. 2012 Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

EQUIPO DE EXPERTOS UNIVERSIDAD DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? 2016. Disponible en https://www.universidadviu.es/la-seguridad-informatica-puede-ayudarme/

ESCRIVÁ GASCÓ, G., Romero Serrano, R. M., & Ramada, D. J. Seguridad informática. 2013 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3217398&ppg=2

ESPINOZA ZALLAS, E., & Rodríguez Pérez, R. Seguridad informática una problemática de las organizaciones en el Sur de Sonora. 2017. Disponible en: http://revistainvestigacionacademicasinfrontera.com/sistema/index.php/RDIASF/article/view/140

FERREYRO, A. L. METODOLOGÍA DE LA INVESTIGACIÓN. Obtenido de METODOLOGÍA DE LA INVESTIGACIÓN: 2014. Disponible en:

http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=847674&lang=es&site=eds-live

GIL VERA, V., & Gil Vera, J. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. 2017. Disponible en: https://www.redalyc.org/html/849/84953103011/

GÓMEZ FERNÁNDEZ, L., & Álvarez, A. Guía de aplicación de la Norma une-iso/iec 27001 sobre seguridad en sistemas de información para pymes. 2012 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3205110&ppg=1

GÓMEZ LÓPEZ, J., & Gómez López, O. D. Administración de sistema operativos. 2014 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228996

GUAPACHA PIEDRAHITA, J. D. Diseño de diplomado virtual en principios de seguridad Informática. 2017. Disponible en: https://repository.unilibre.edu.co/handle/10901/10553

HOYOS MALES, C. E. Seguridad en el transporte y gestión de correos electrónicos, implementación de seguridad en correo outlook 2010. Disponible en: https://repository.unad.edu.co/handle/10596/3657

J, G., Bermeo, J., Villacreses, E., & Guerrero, J. Delitos informáticos: una revisión en Latinoamérica. 2018 Disponible en: http://investigacion.utmachala.edu.ec/proceedings/index.php/utmach/article/view/262

LEÓN CEPEDA, L. C. Estructuración del sistema de seguridad de la información en el área de protección de datos para un operador logístico bajo la norma NTC/ISO 27001:2013. 2018. Disponible en: https://repository.ucatolica.edu.co/handle/10983/16149

MATACHANA, Y. L. Los virus informáticos: una amenaza para la sociedad. (1 de 1 de 2009). Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=4&docID=10357400&tm=1466006227313

MENDOZA PENAGOS, L. P.Diseño de un sistema de gestión de seguridad informática para la Empresa GED (Gestión Estrategia y Desarrollo) de la ciudad de Bogotá. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/20723

MIN TIC. (s.f.). ¿Y de seguridad TI qué hacen las entidades? Disponible en: https://www.mintic.gov.co/gestionti/615/w3-article-7083.html

MIN Tic. (s.f.). Modelo de Seguridad. Disponible en: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

OJEDA PÉREZ, J. E., Rincón Rodríguez, F., Arias Flórez, M. E., & Daza Martínez, L. A. 2010. Delitos informáticos y entorno jurídico vigente en Colombia. Disponible en: https://repository.javeriana.edu.co/handle/10554/23982

PATIÑO ALPALA, L. O. Propuesta de actualización, apropiación y aplicación de políticas de seguridad informática en una empresa corporativa, Propolsinecor. 2014. Disponible en: https://repository.unad.edu.co/handle/10596/2742

PENAGOS, E. B. NGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE. 2015. Disponible en: https://repository.unad.edu.co/handle/10596/3629

PLAZAS GARCIA, E. R. Ingeniería social en las empresas colombianas. 2018. Disponible en: https://repository.unad.edu.co/handle/10596/18704

PRADA HERNÁNDEZ, N. M. Diseño de un sistema de gestión de seguridad de la información, alineado con la Norma ISO. 2010. Disponible en: https://repository.javeriana.edu.co/handle/10554/7515

RAYA CABRERA, J., & Raya González, L. Implantación de sistemas operativos. 2010 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228461

REYES, J., Muñoz, C., & Guarda, T. Seguridad Informática para Pequeñas y Medianas Empresas de la Provincia de Santa Elena. 2017 Disponible en: https://search.proquest.com/openview/ba8fb554f72bbe6b94735e926be36754/1?pq-origsite=gscholar&cbl=1006393

SANABRIA FLÓREZ, Y. Seguridad informática en Claro Colombia en el área de cuidado al cliente-prevención. 2014. Disponible en: https://repository.ucatolica.edu.co/handle/10983/1327

SANTOS, J. C. Seguridad informática. 2014 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228430&ppg=1

SANTOS, J. C. Seguridad y alta disponibilidad. 2014 Disponible en: https://ebookcentral-proquest-

com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228975&ppg=1

SENADO DE LA REPUBLICA. Ley 1273 de 2009. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

UNIVERSIDAD LIBRE. El decálogo de la seguridad informática. Disponible en: http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/247-el-decalogo-de-la-seguridad-informatica

URECHE OSPINO, M. E. Diseño de Políticas de Seguridad Informática basadas en la norma NTC-ISO-IEC 27001:2013 para la universidad de Cartagena centro tutorial Mompox Bolívar. (06 de 04 de 2017). Disponible en: https://repository.unad.edu.co/handle/10596/12027

VALENCIA DUQUE, F. J., Cardona Londoño, A., & Carvajal Portilla, D. L. Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie ISO/IEC 27000 para una entidad pública colombiana. 2018 Disponible en: http://repositorio.autonoma.edu.co/jspui/handle/11182/721

VIEITES, Á. G. Gestión de incidentes de seguridad informática. 2014 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3228430&ppg=1

VIEITES, Á. G. Seguridad en equipos informáticos. 2014 Disponible en: https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/reader.action?docID=3229330

VIEITES, Á. G. Seguridad en equipos informáticos. 2014 Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=13&docID=11046412&tm=1466006343174

VILLAGÓMEZ, C. Sistema de detección de intrusiones (IDS). (6 de 12 de 2017) Disponible en: https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

YUDITH, D. Seguridad Informática. 2018. Disponible en: https://instituciones.sld.cu/dnspminsap/seguridad-informatica/

ZAMBRANO BURBANO, R. M. Estudio sobre el conocimiento y la aplicabilidad de la seguridad informática en las empresas. (12 de 02 de 2012). Disponible en: https://repository.unad.edu.co/handle/10596/20152

ANEXOS

Cibersecurity de Colombia LTDA, es una empresa Colombiana que presta servicios de seguridad para la protección de la Información. Su propósito para el año 2021 es consolidarse como un Centro de Respuesta a Incidentes Cibernéticos en el ámbito de **CSIRT**

Anexo A. Implementación ambiente Controlado

Característica del ambiente:

Relación de la tecnología de Hardware que permitan desarrollar las actividades del CSIRT.

Tener presente como mínimo los siguientes requerimientos:

Para las labores de nuestro CSIRT tenemos el siguiente ambiente con el cual realizaremos todo lo respectivo a los servicios del mismo.

El ambiente que vamos a manejar es un ambiente controlado en el cual hemos virtualizado nuestro servidor principal y el cual tiene las siguientes características:

Hardware:

Disco Duro: 120 GB

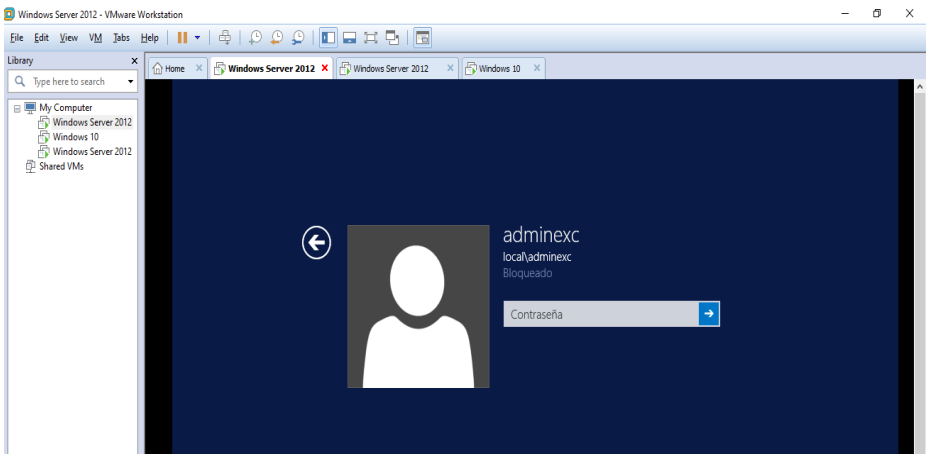
Memoria RAM: 8GB

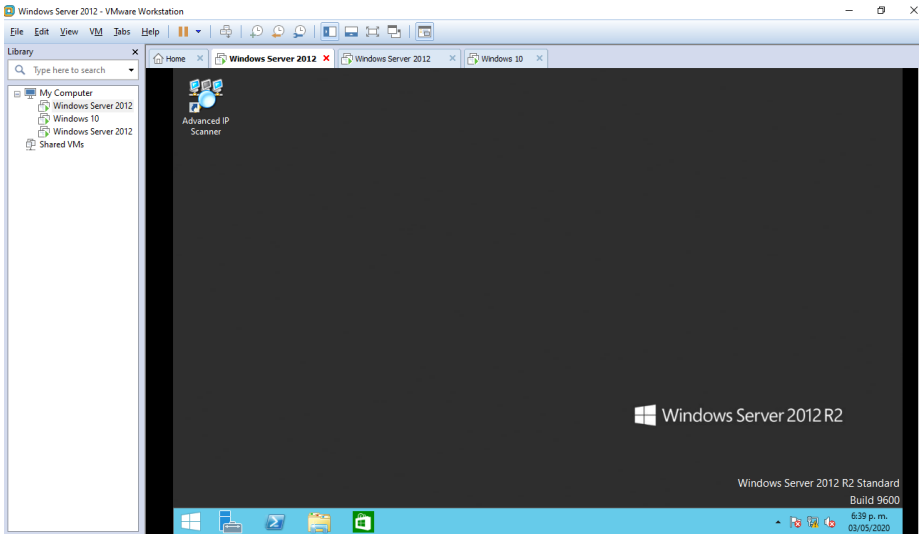
Procesador: Core I 7 2.8 GHZ esta máquina tiene 4 Core

Software: Windows Server 2012

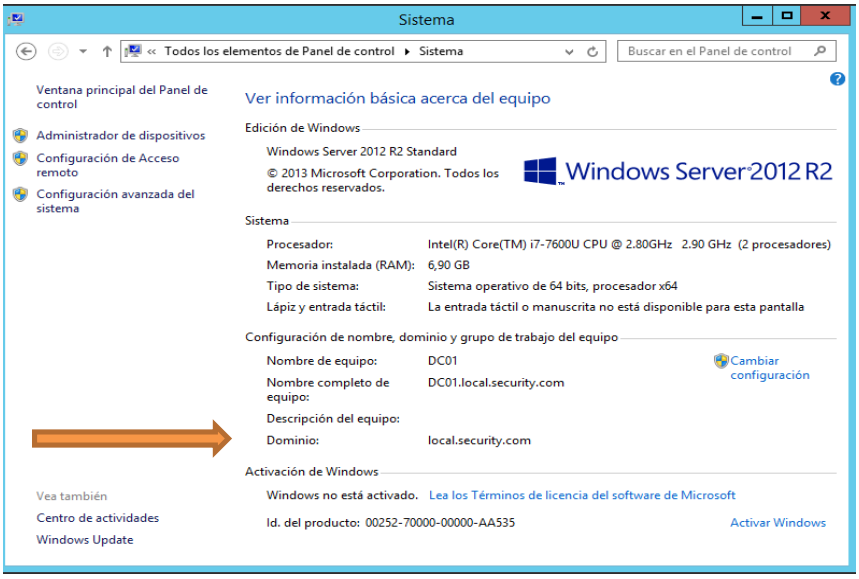
En la siguiente imagen vamos a observar el ambiente controlado de nuestro CSIRT que fue virtualizado en Vware.

En esta primeras imágenes iniciamos sesión en nuestra maquina donde tenemos el servicio de controlador de dominio y demás servicios





El ambiente esta virtualizado en Vware. Todas nuestras maquinas con las herramientas que maneja el centro de incidentes antes ataques cibernéticos.

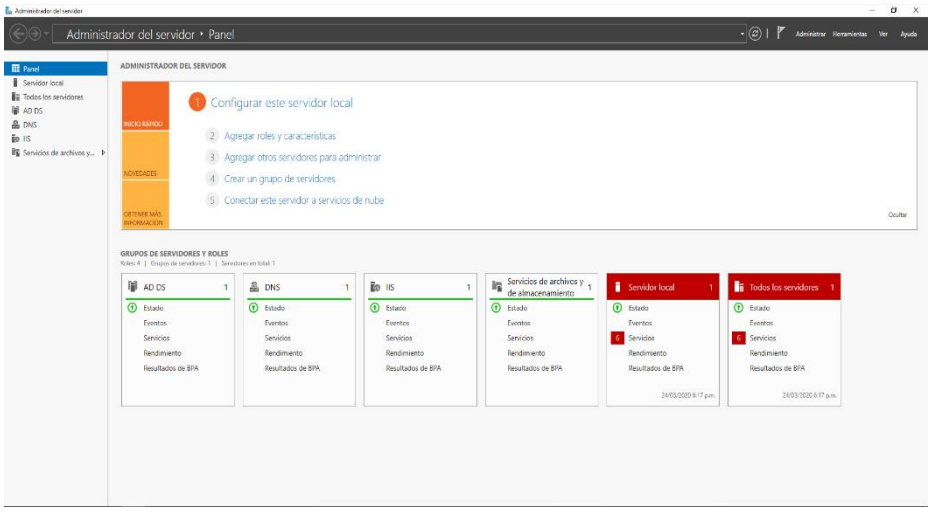


Anexo B. Servidor Web y servidor intranet:

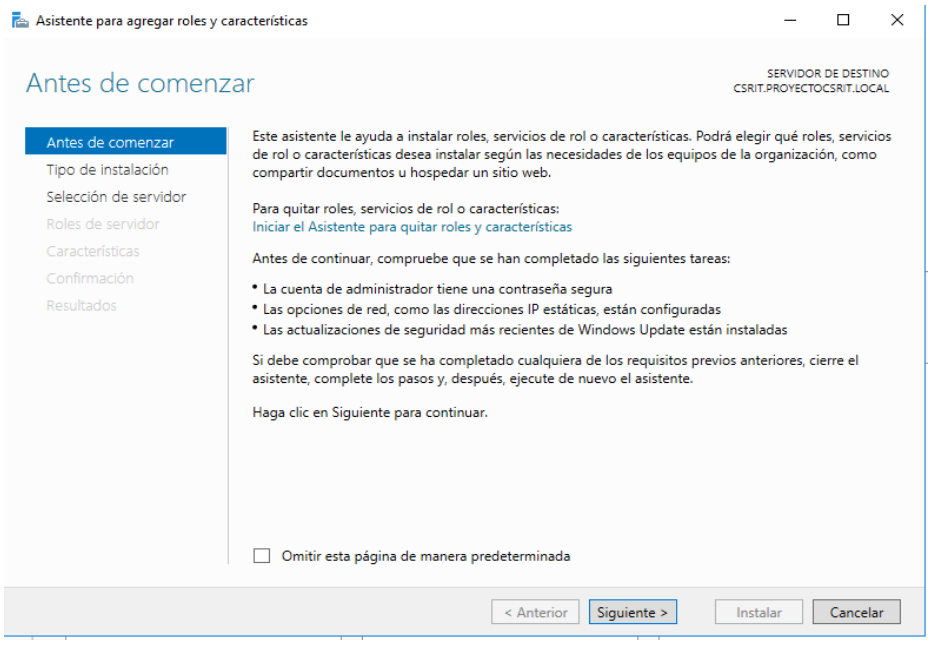
Nuestro servidor web lo activamos con el IIS de la siguiente manera:

Vamos al administrador de servidores y agregamos roles y características

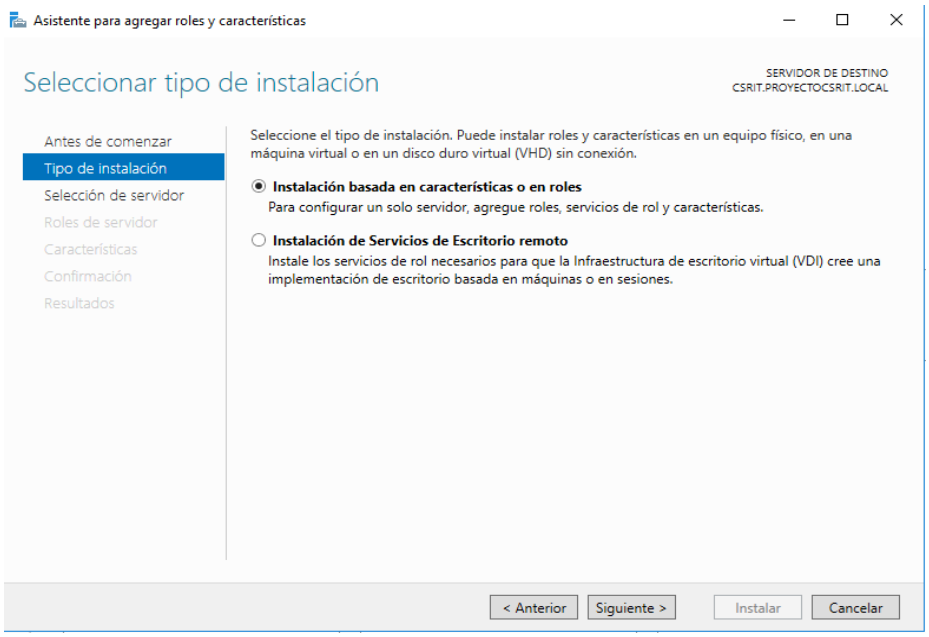
Están allí se nos habilita el asistente de instalación:

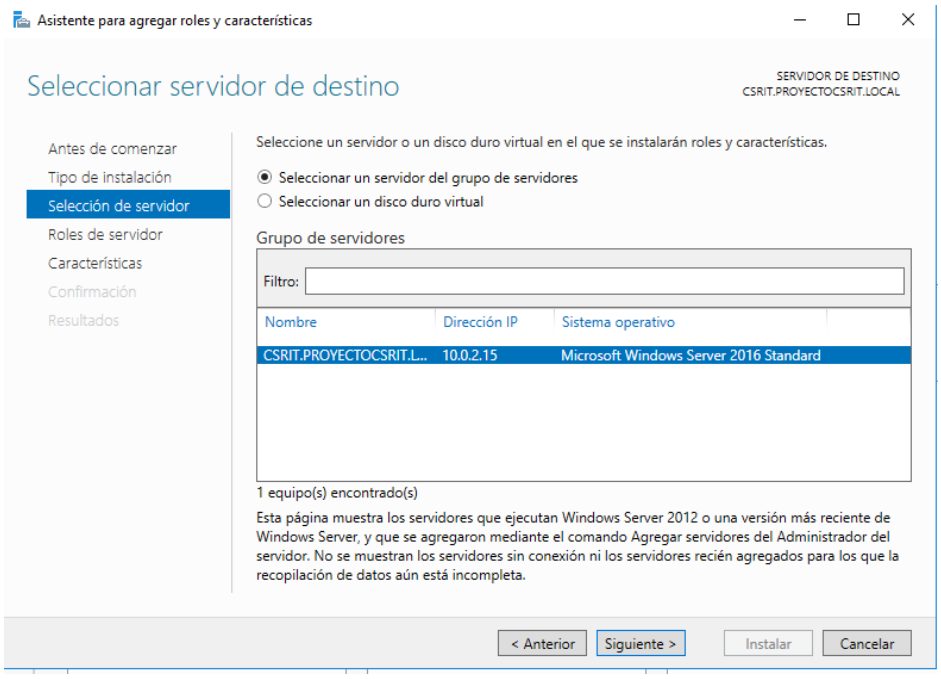


Damos siguiente y escogemos características o roles:

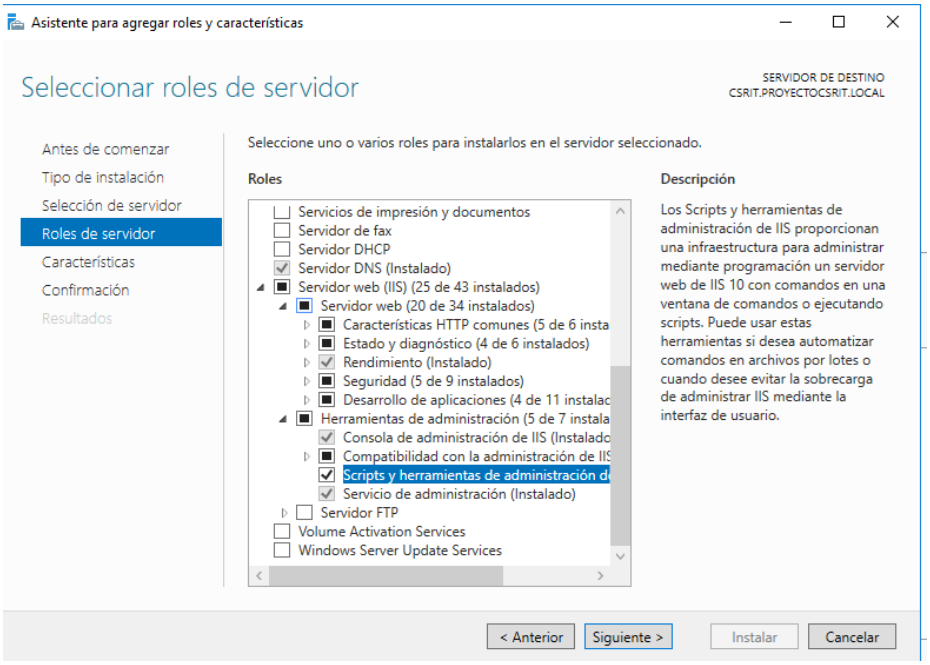


Seleccionamos el servidor con su correspondiente dirección Ip

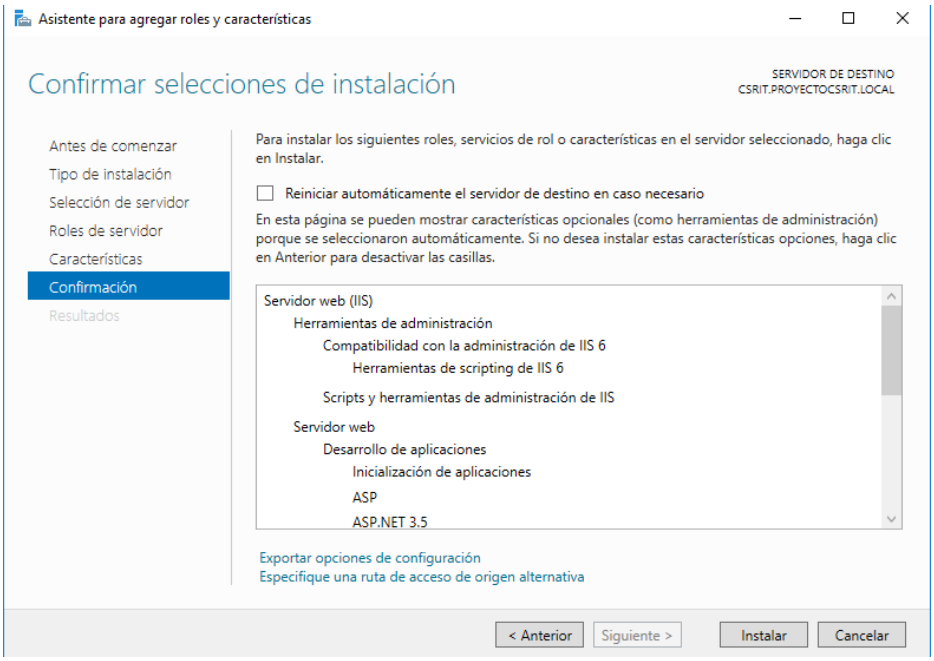




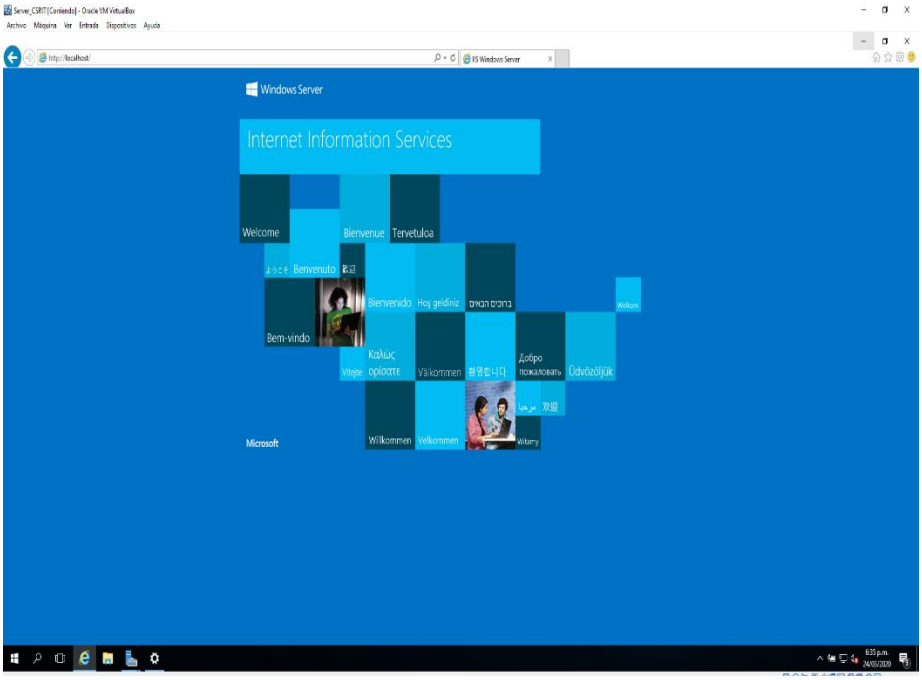
Seleccionamos nuestro servicio que deseamos montar:



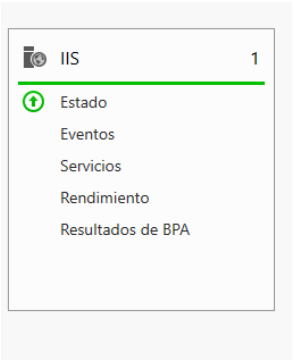
Se confirma su instalación y se espera a termine el proceso y posteriormente se reinicie el equipo



Una vez terminado el proceso e inicie la maquina se valida que nuestro servidor local localhost esté funcionando.



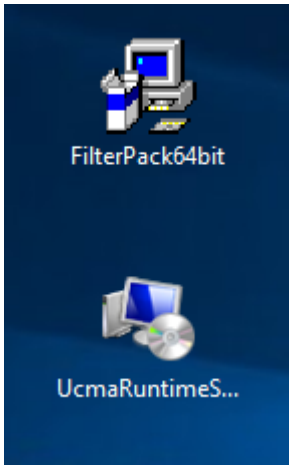
Y observamos que el administrador de servidores encontramos lo siguiente esto quiere decir que nuestro servicio web local está correctamente instalado y validado.



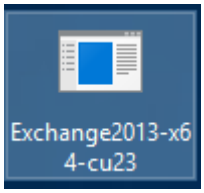
Anexo C. Servidor de Correo Institucional

Para instalar nuestro servidor de correo lo primero que debemos de instalar es nuestro directorio activo que lo realizamos de la misma manera como agregamos nuestro servidor web. Vamos al panel de administraciones de roles de servidor y agregamos los componentes de directorio activo lo instalamos

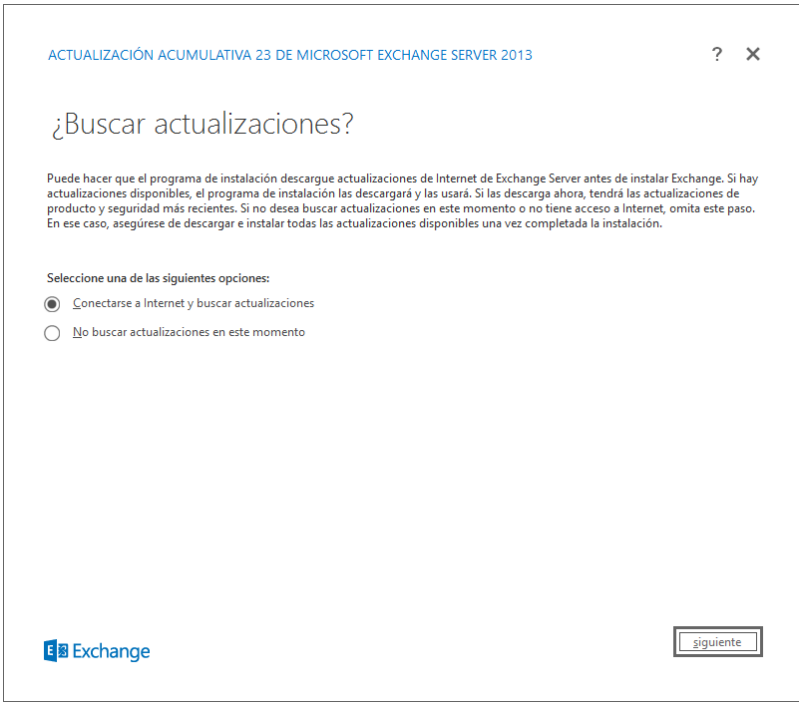
Luego de instalar estos roles y características instalaremos los siguientes complementos para lograr instalar nuestro Exchange 2013

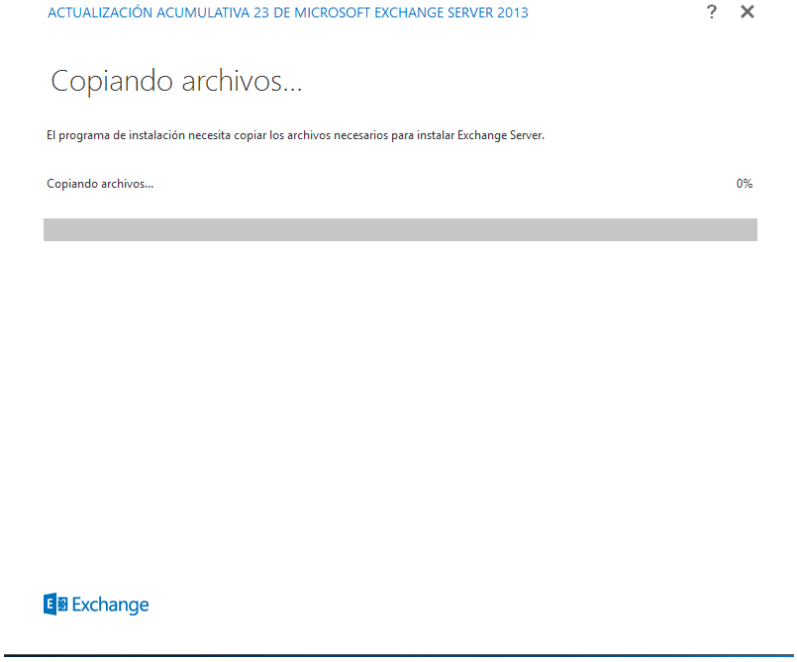


Posteriormente de haber ejecutado estos dos instaladores tenemos que arrancar nuestro Exchange

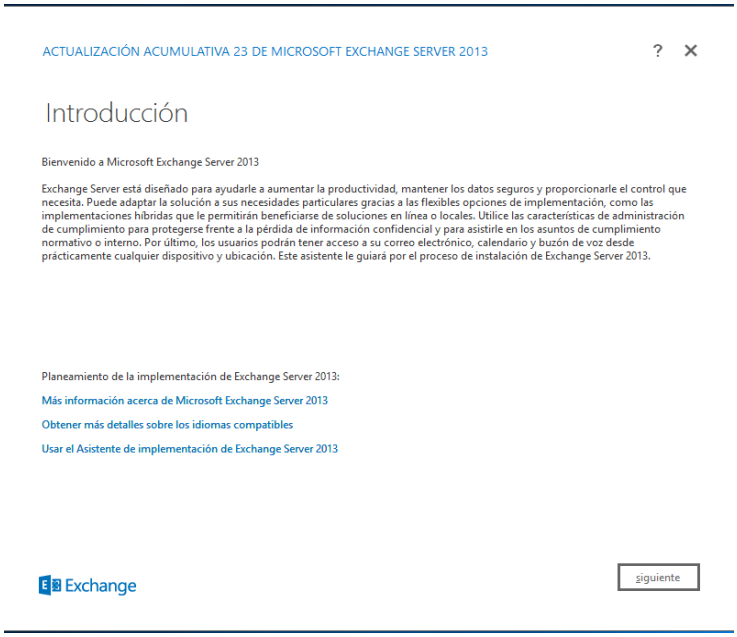


Empezamos con el proceso de instalación del exchage2013

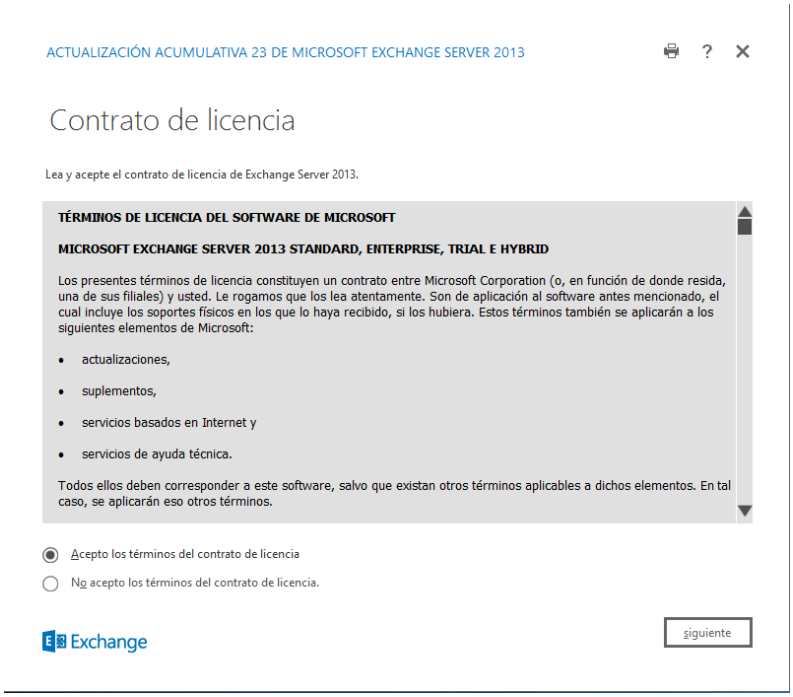


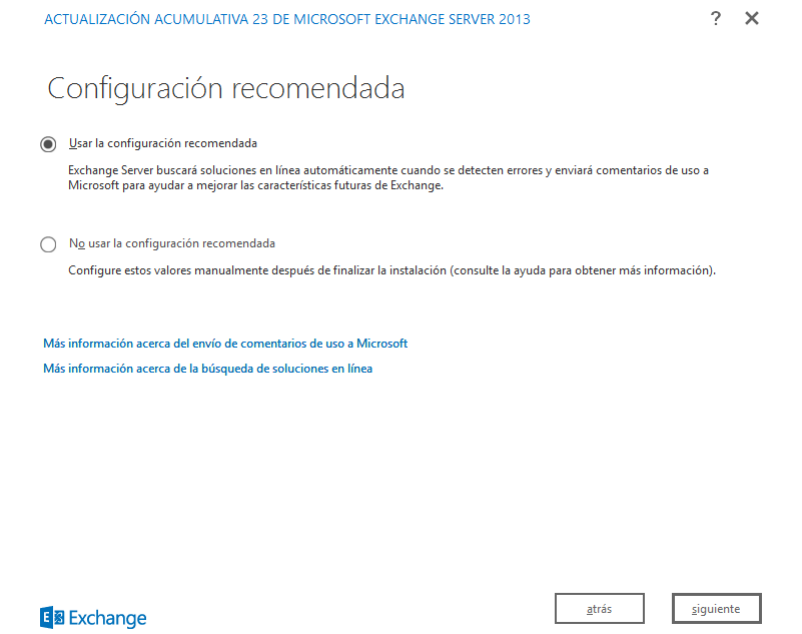


Se inicia el proceso de copiado de los archivos que este requiere

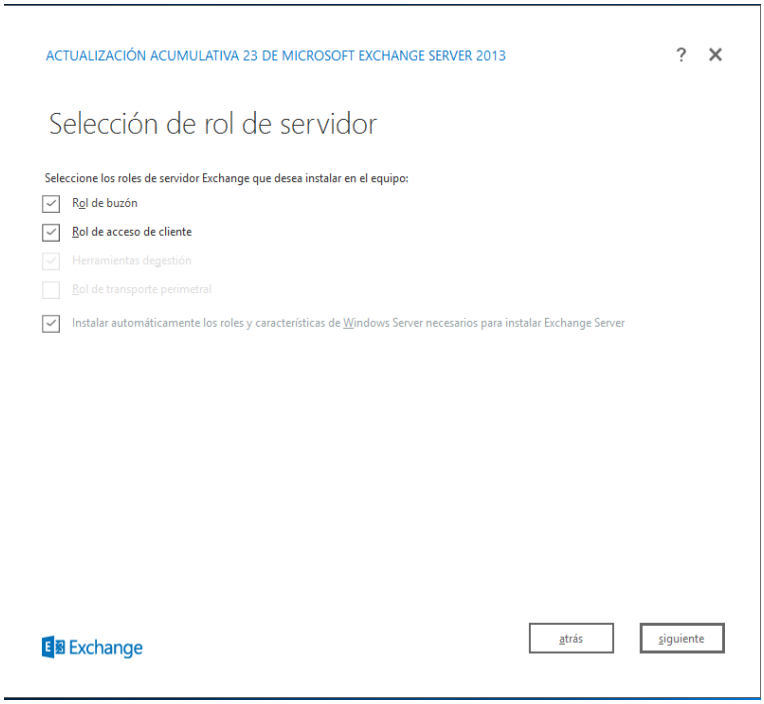


Damos siguiente para iniciar el proceso de configuración del Exchange



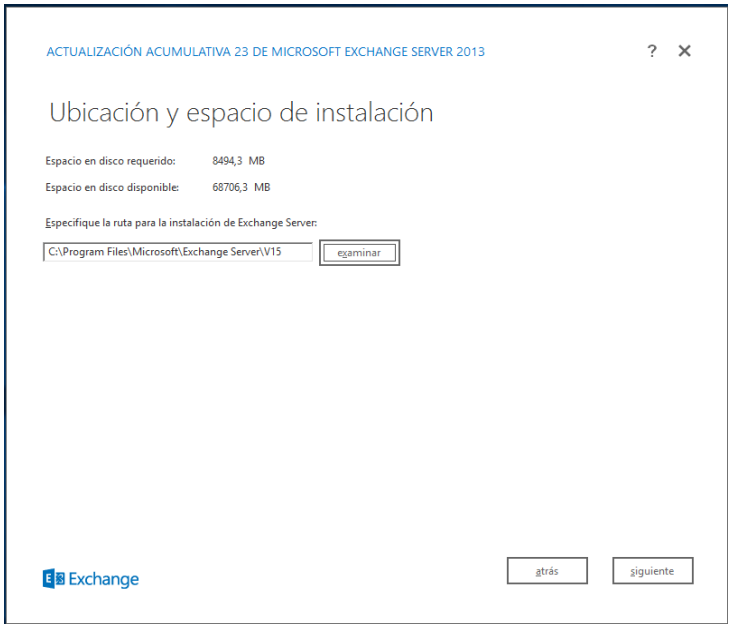


Utilizamos la configuración recomendada

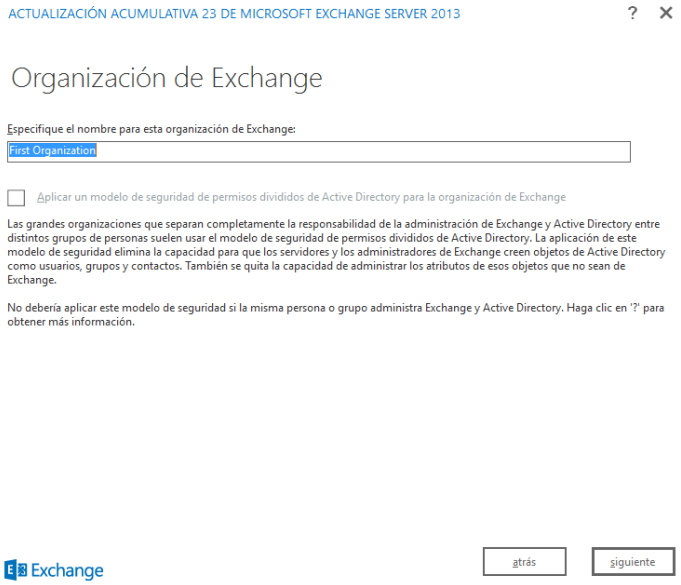


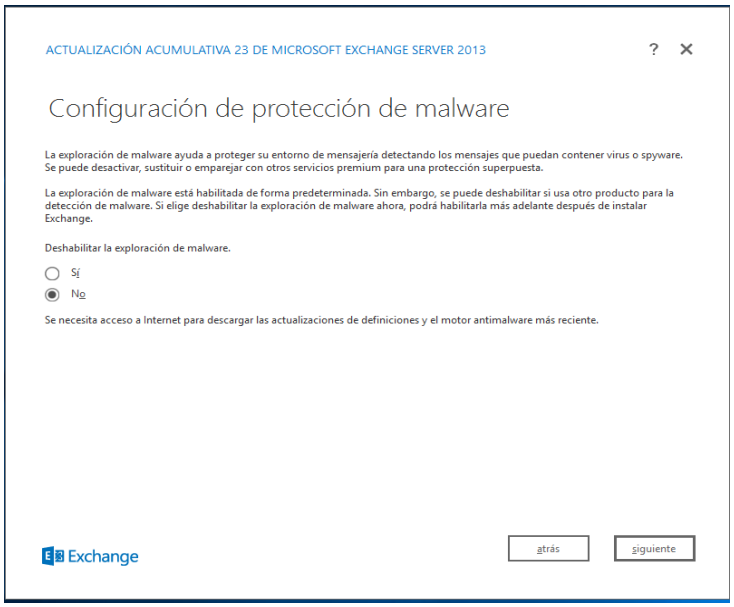
Seleccionamos el rol de buzón, acceso a cliente e instalar automáticamente los roles y características.

Luego nos muestra la ruta donde va quedar instalado nuestro Exchange

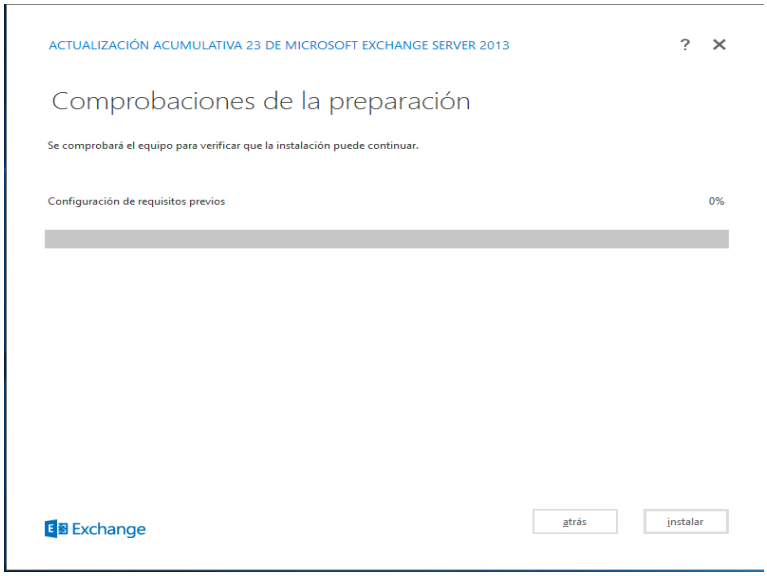


Nombre de la carpeta donde va estar almacenada nuestro servicio de correo

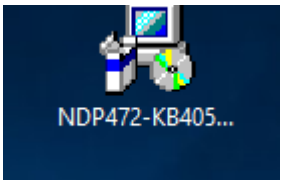




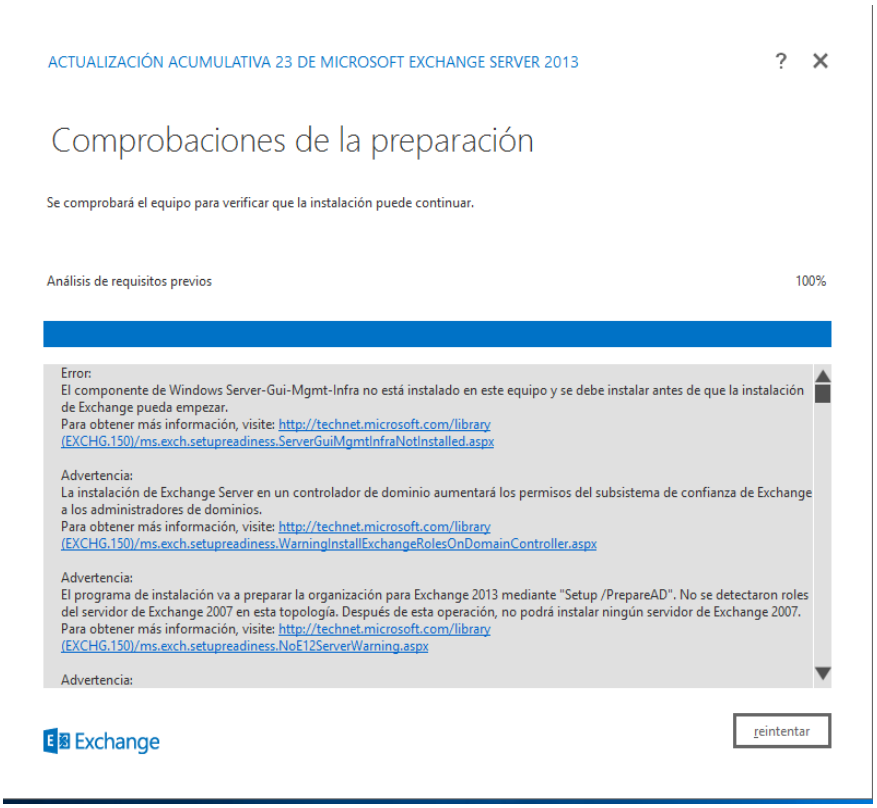
Le decimos que no y obtenemos arrancamos la comprobación de los requisitos para su preparación.



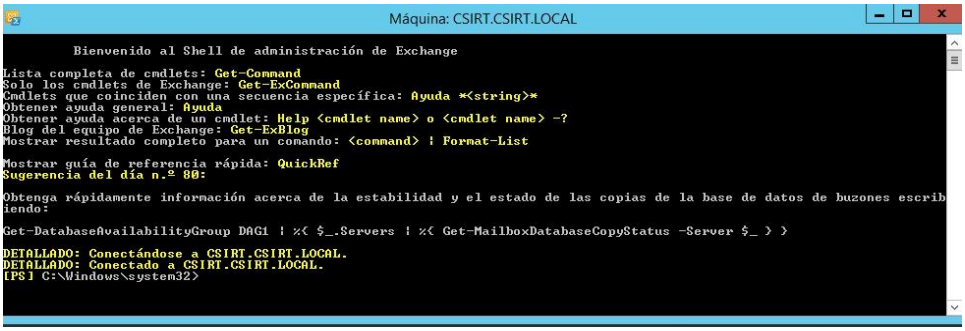
Posteriormente del proceso de instalación no nos deja realizar la instalación de este se instalan otros complementos como es el siguiente:



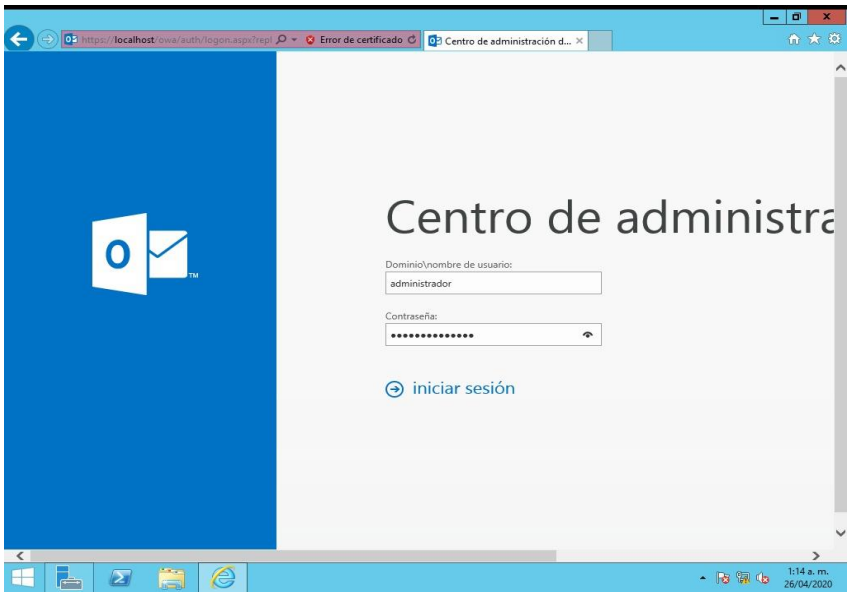
Y se corren todas las actualizaciones de la máquina y persiste el error que tenemos aquí. Esto se trata de realizar en distintas máquina.



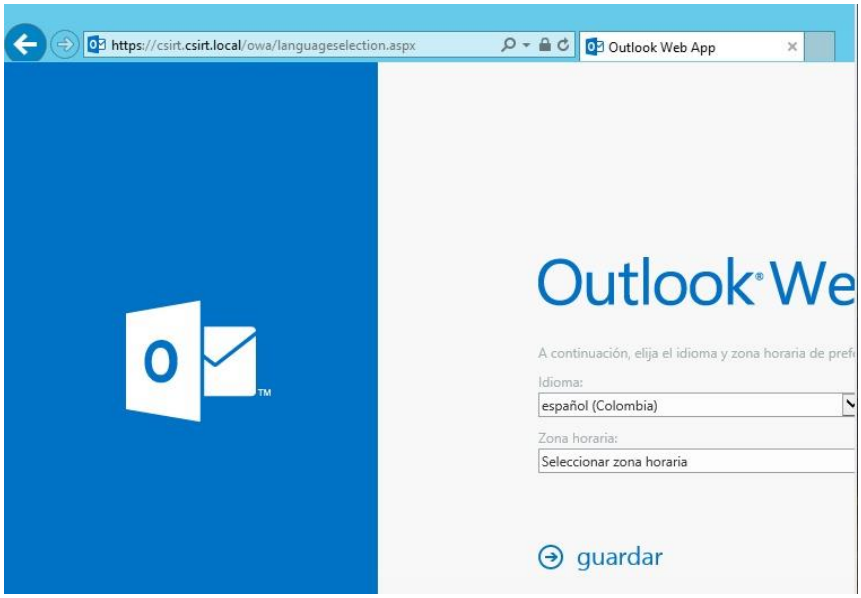
Terminada la instalación ejecutamos el PowerShell del Exchange para validar nuestro dominio.



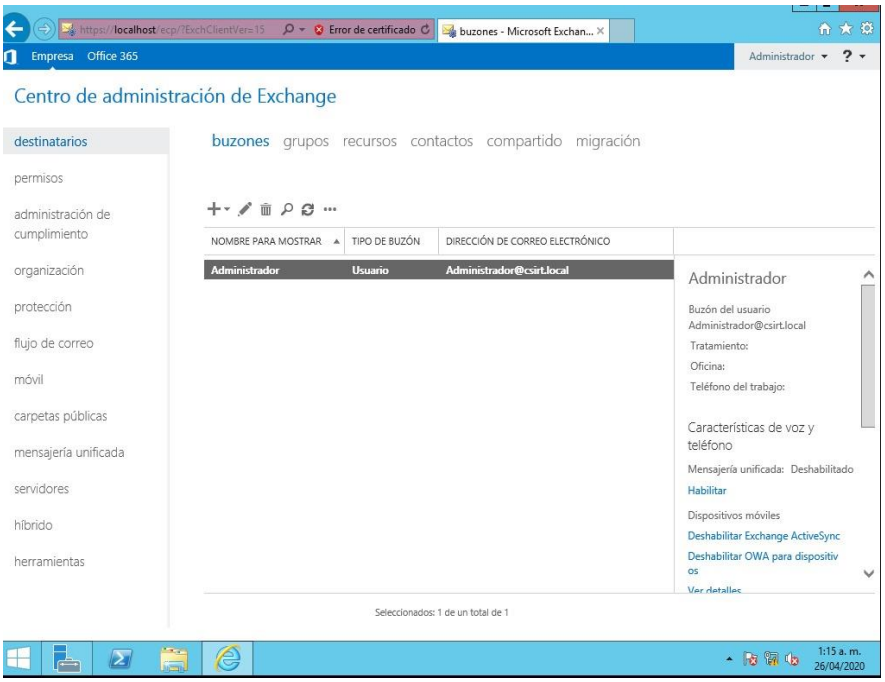
Prueba de funcionalidad



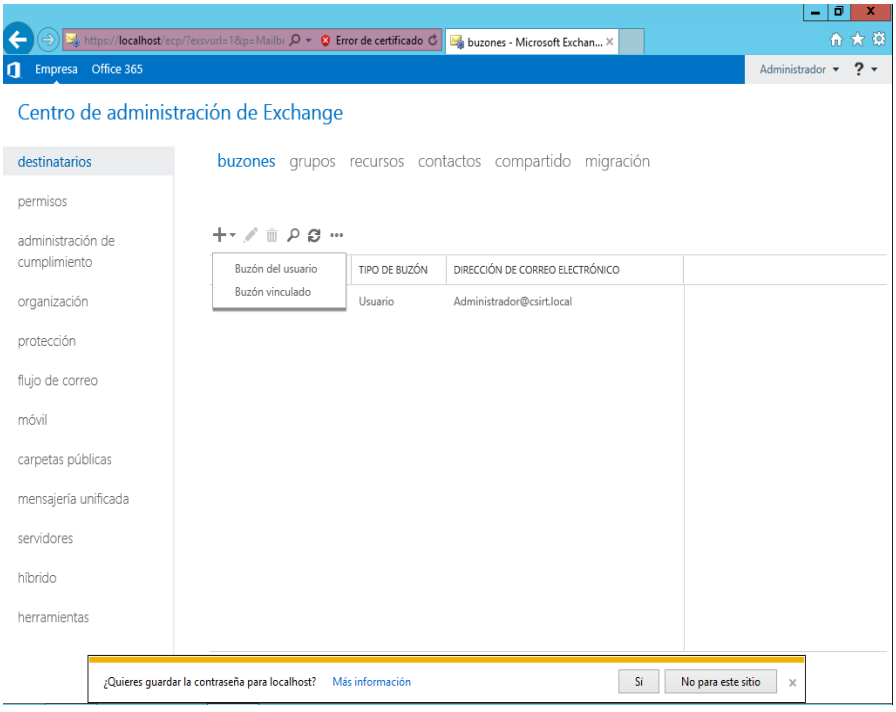
Configuración de la región del correo



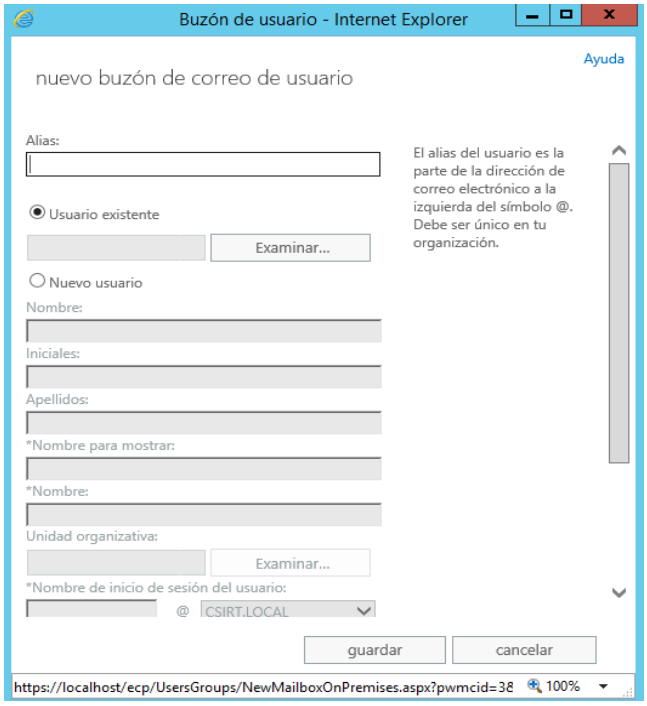
Ingreso a la Consola de administración de correo



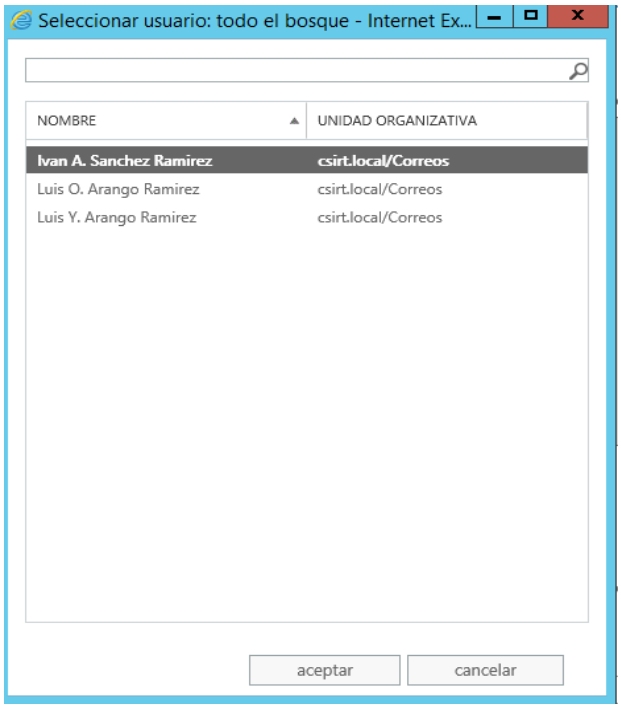
Asociación de cuenta de usuario con el D.A

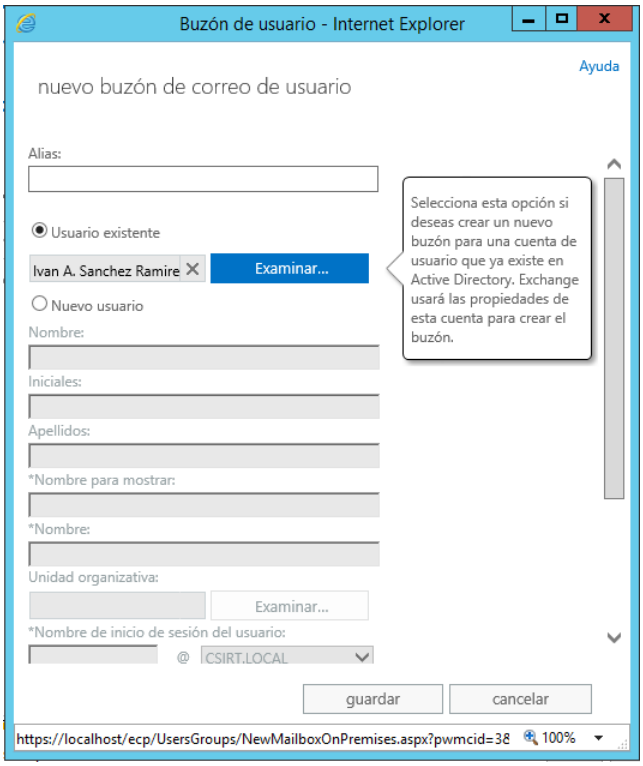


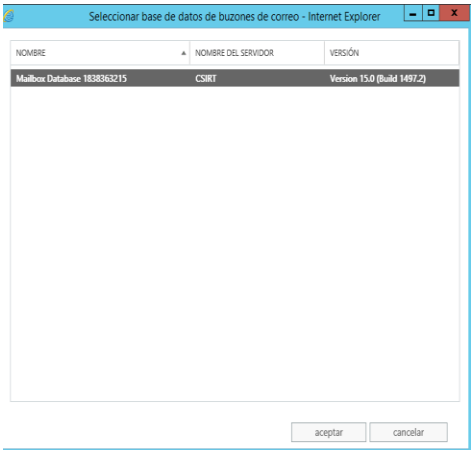
Consulta y asociación cuentas de usuario con el buzón



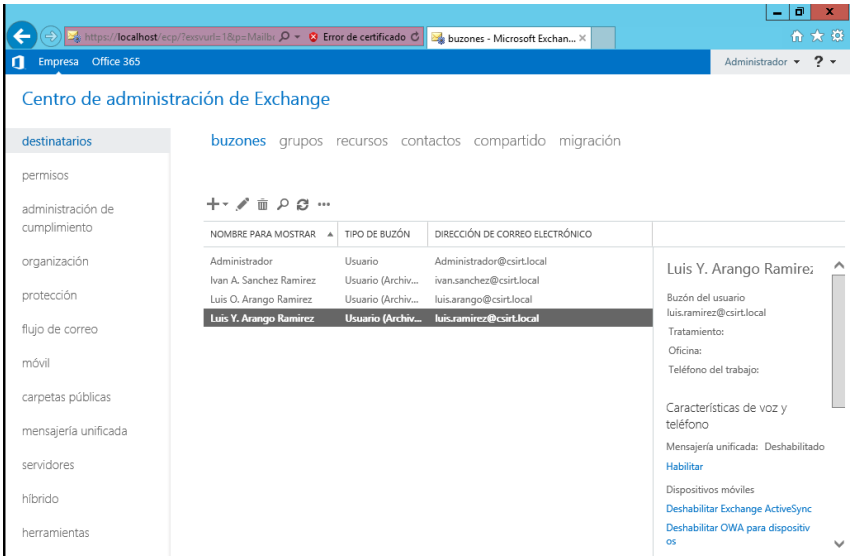
Se asocian las cuentas de usuario el D.A

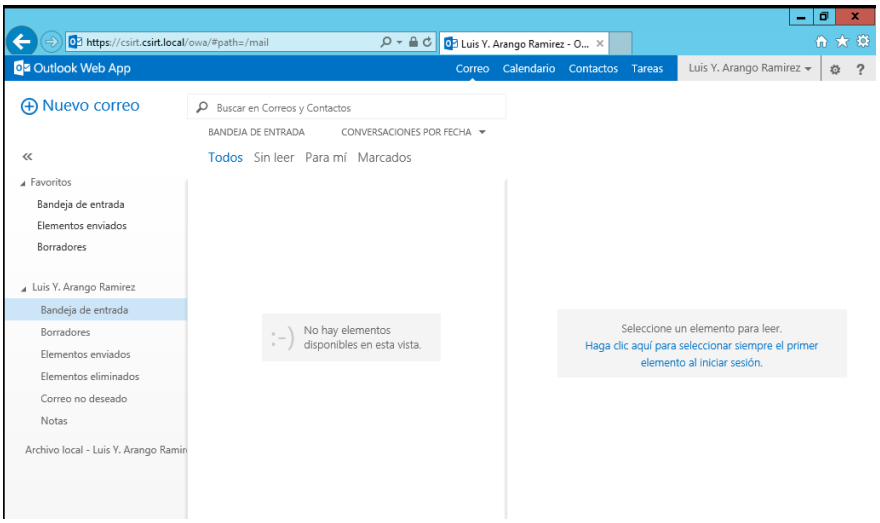






Se configuran buzón por usuario

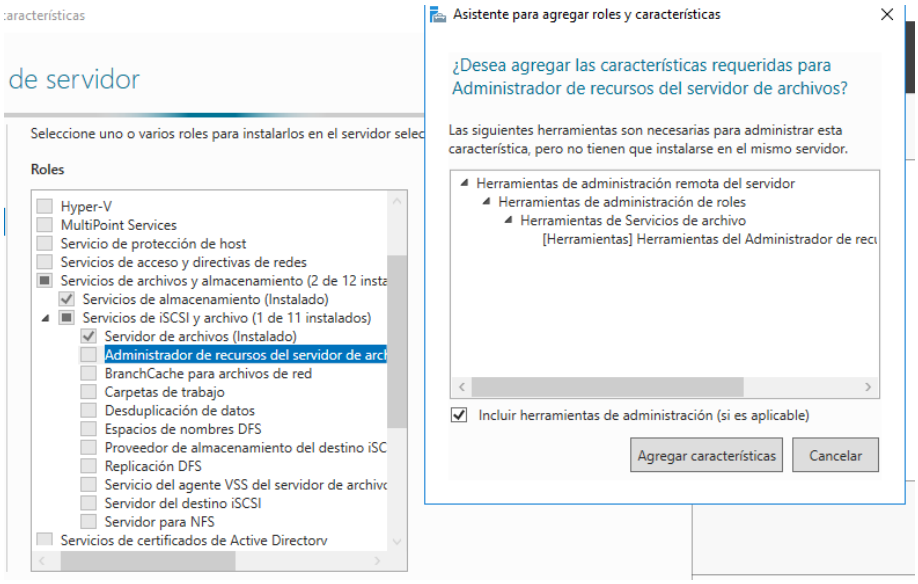


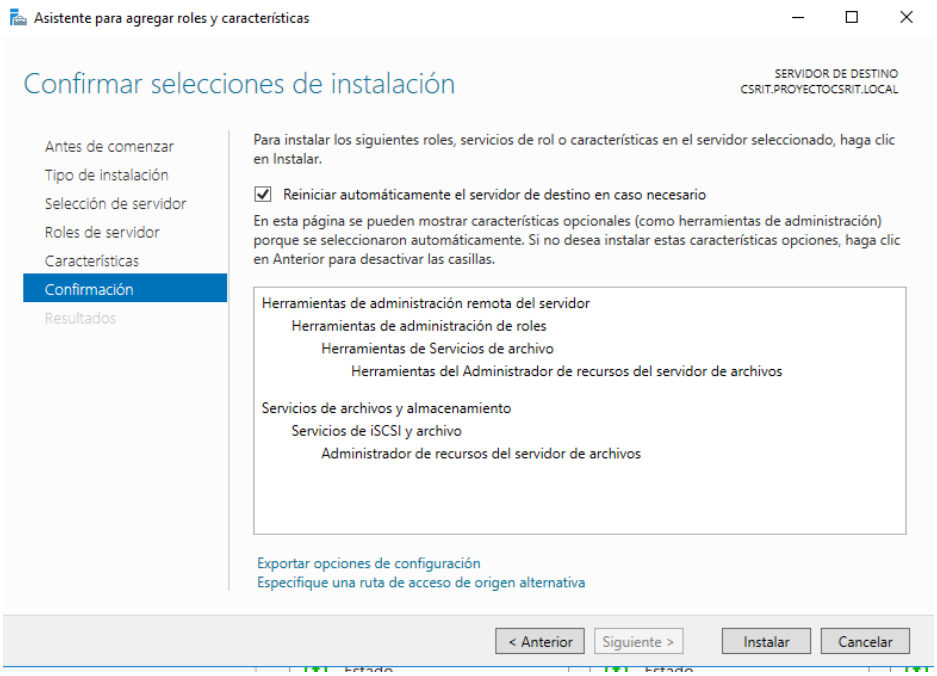


Anexo D. Servidor de Archivos

Para realizar la instalación del servidor de archivo y con el FSRM que es el administrador de recursos del servidor de archivos de la siguiente manera:

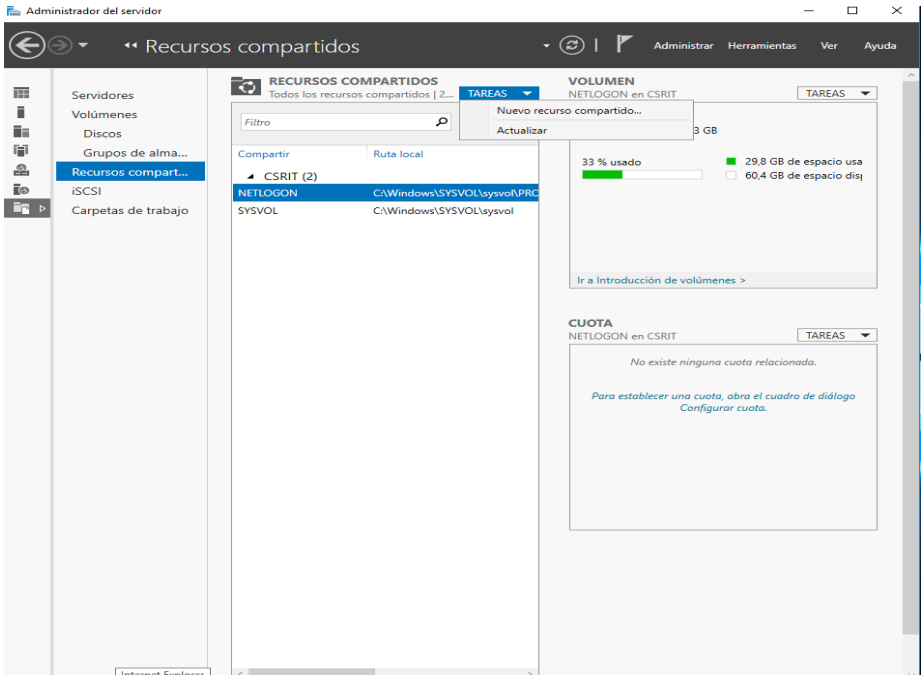
Vamos al administrador de servidores y agregamos los siguientes roles



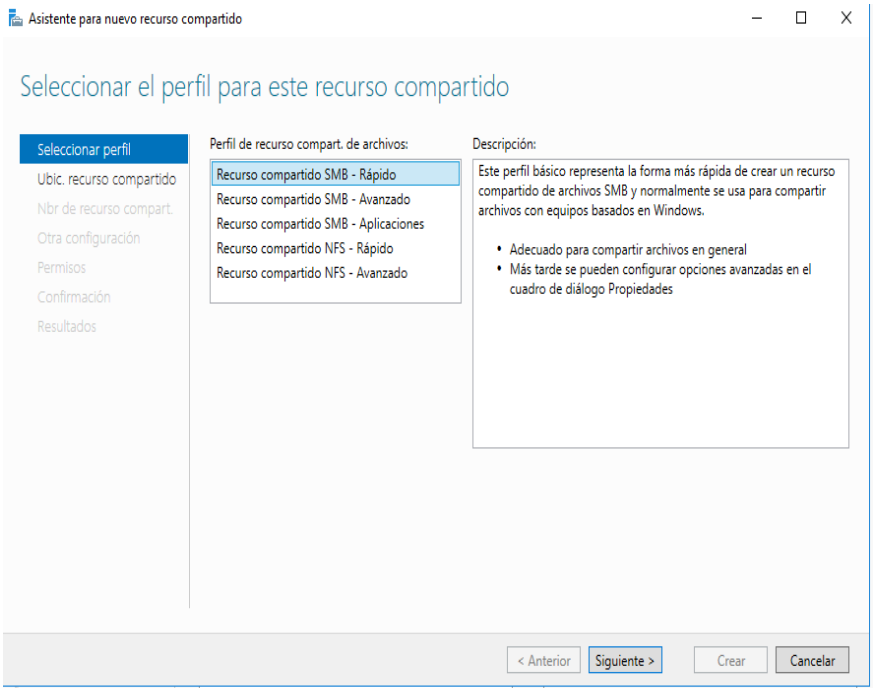


Terminado este proceso vamos a realizar la administración del FileServer desde el mismo de la siguiente manera:

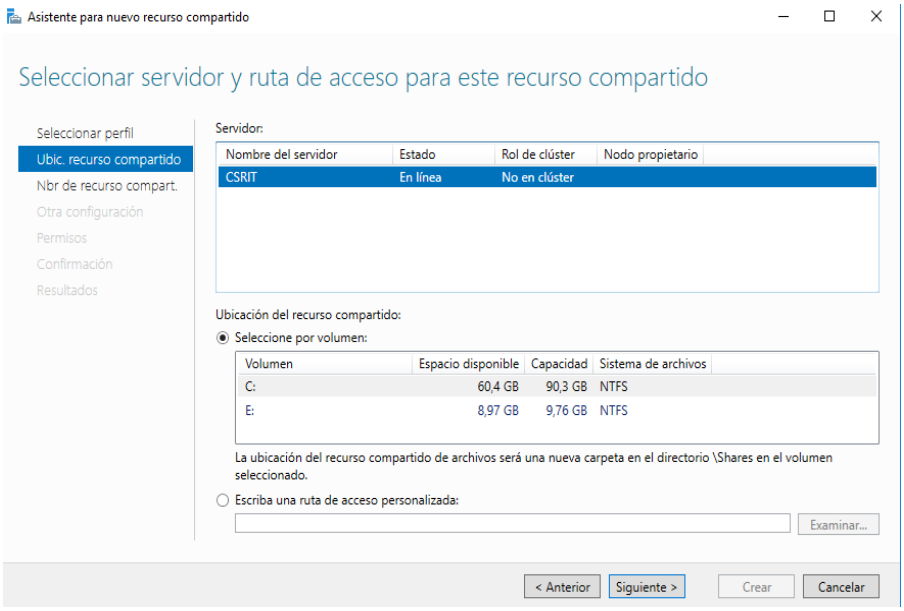
Identificamos la unidad de disco que vamos a compartir bien sea un disco duro externo o una unidad que sea particionada



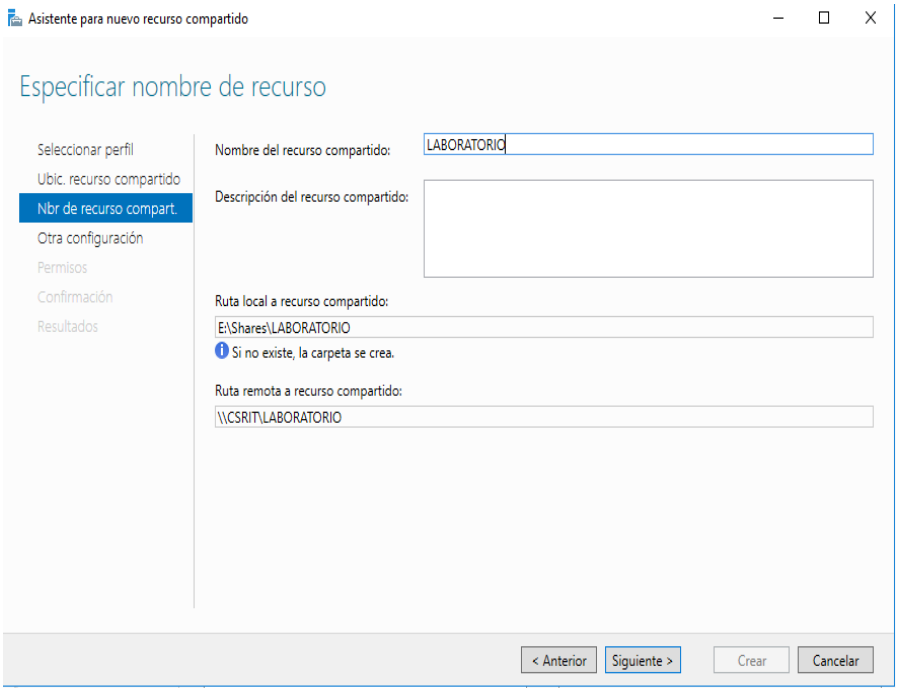
Vamos a la opción de recursos compartidos en ella vamos a tareas y posteriormente escogemos un nuevo recurso compartido.



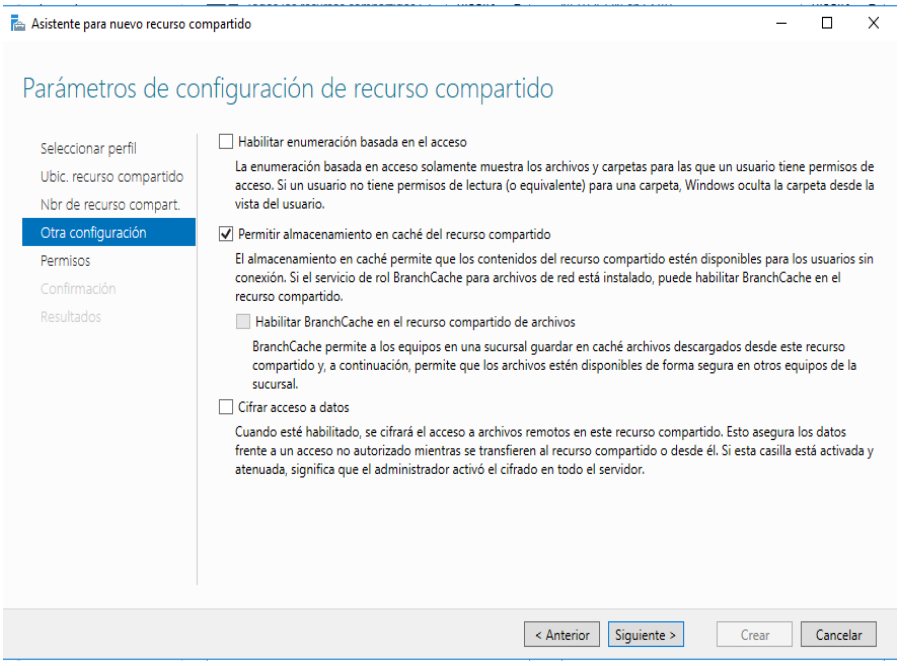
Escogemos el perfil que deseamos compartido en este caso vamos a trabajar con el SMB-Rápido.



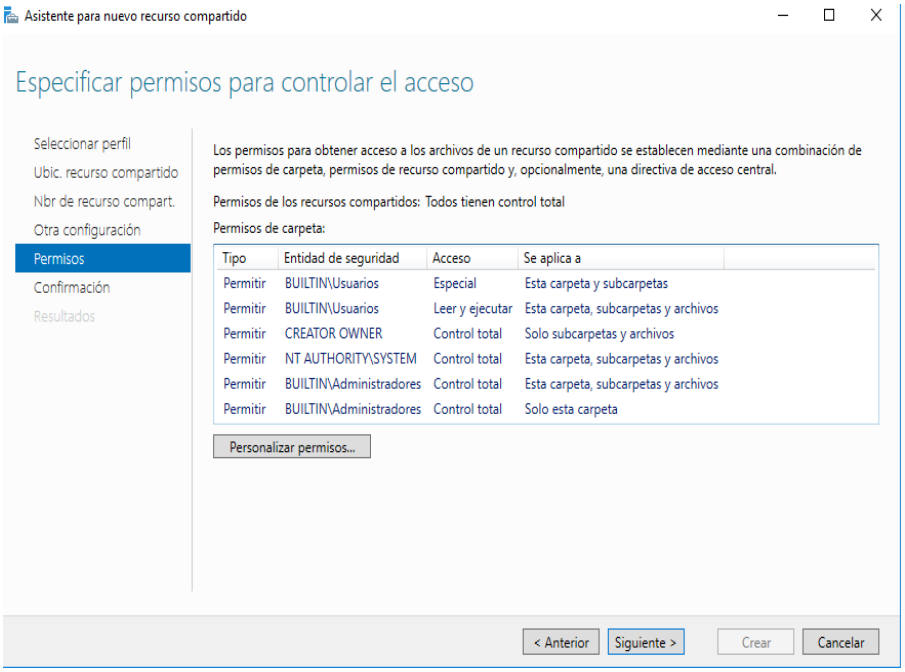
Ahora vamos a seleccionamos la ruta del servidor donde queremos compartir el recurso en nuestro caso es la unidad E:



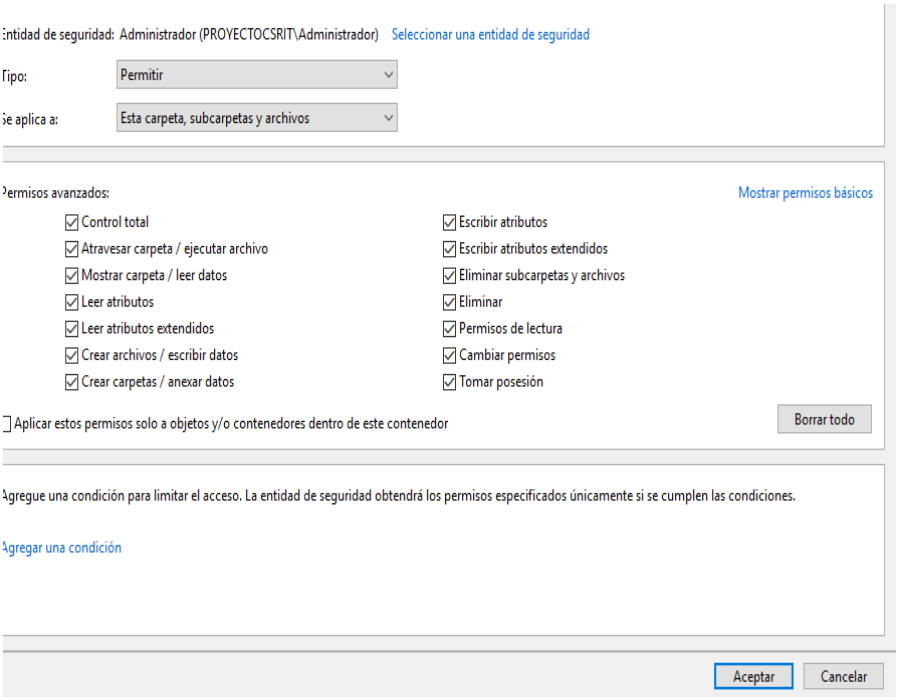
Ahora asignamos el nombre de la carpeta que deseamos compartir. Esta parte nos muestra cómo va aparecer nuestra carpeta compartida a nivel local y a nivel de red.



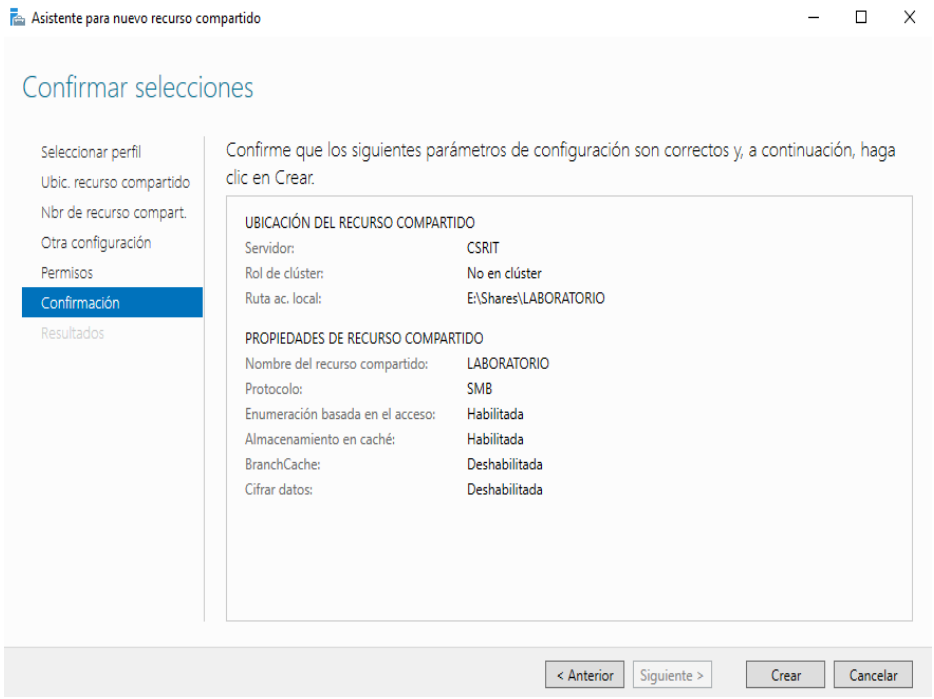
Lo dejamos por defecto en imagen nos muestra las opciones de como parametrizar los recueros compartidos



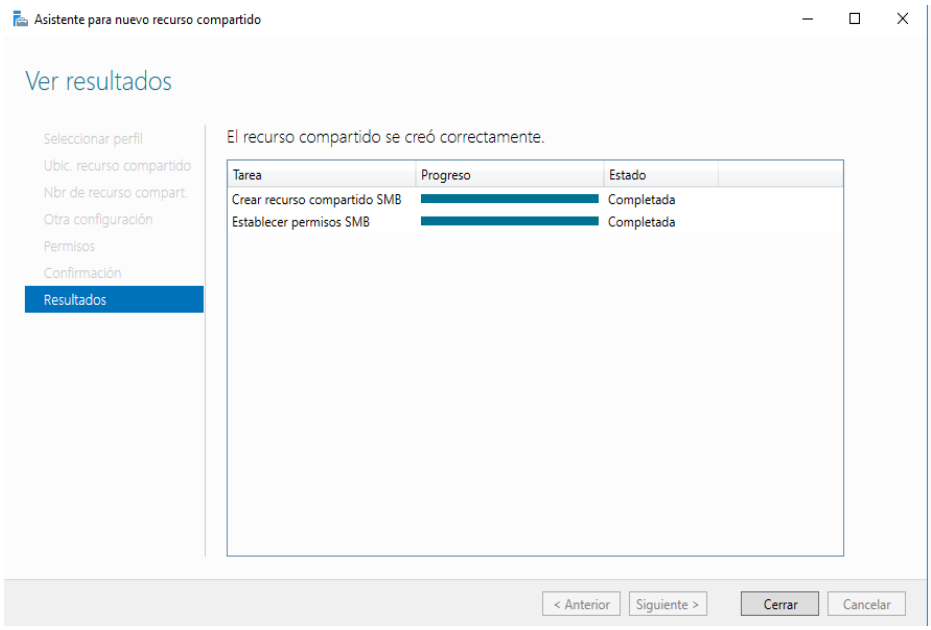
Ahora podemos identificar los permisos y editarlos si es lo necesario.

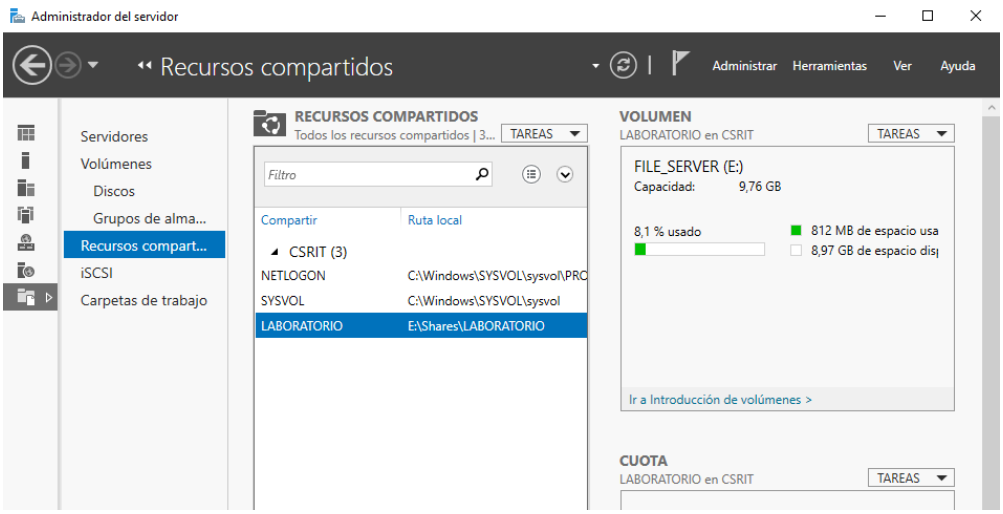


Validamos los permisos a los usuarios que deseemos y demás características y desde allí también podemos realizar auditorías.

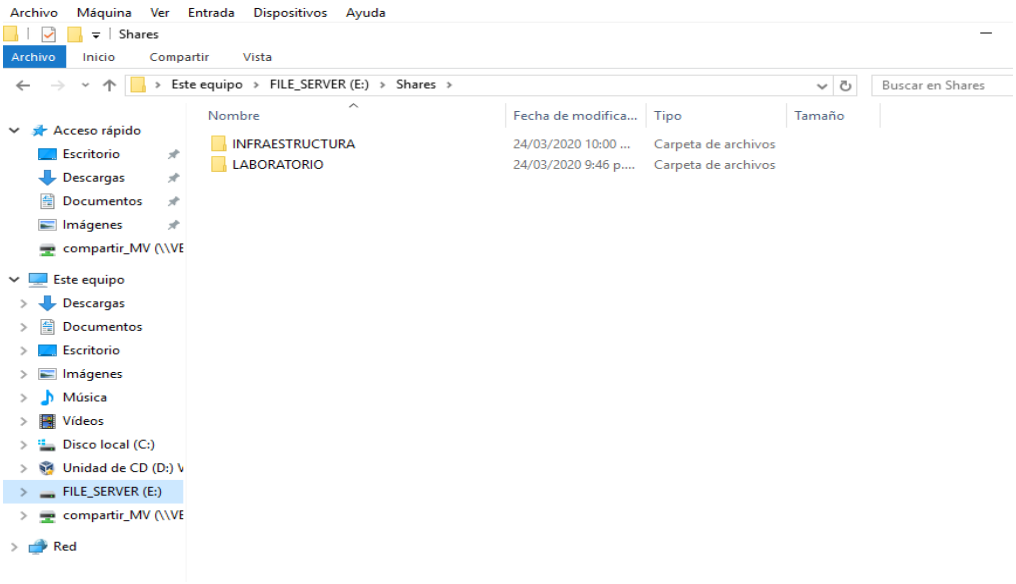


Por ultimo validamos y creamos nuestra carpeta o recurso compartido.





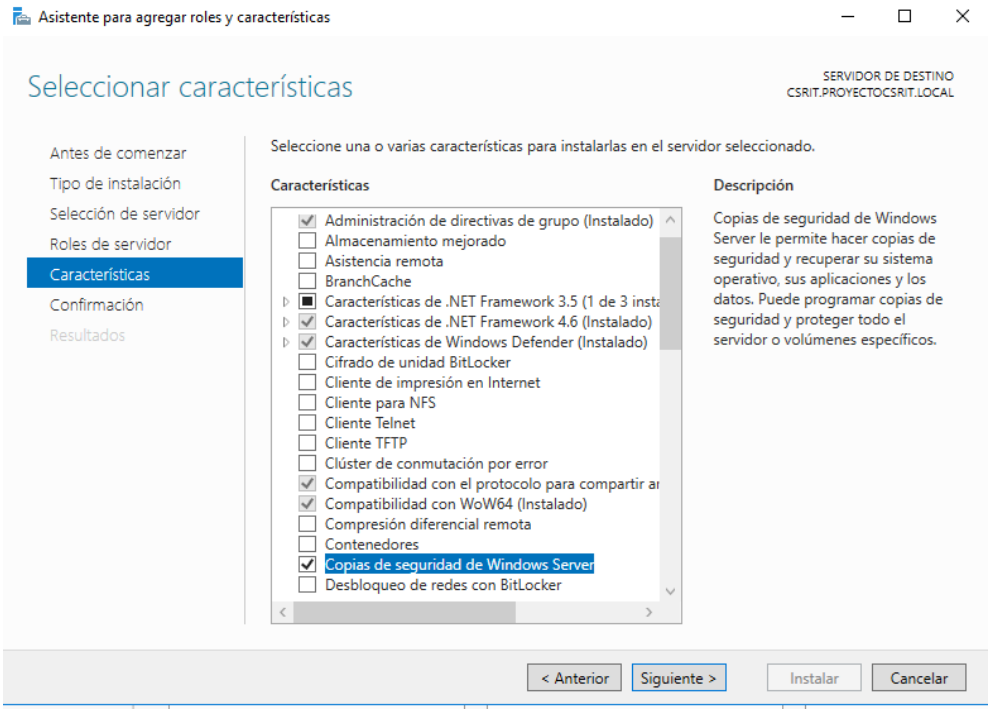
Y tenemos nuestro recurso compartido visto desde el administrador de File_Server



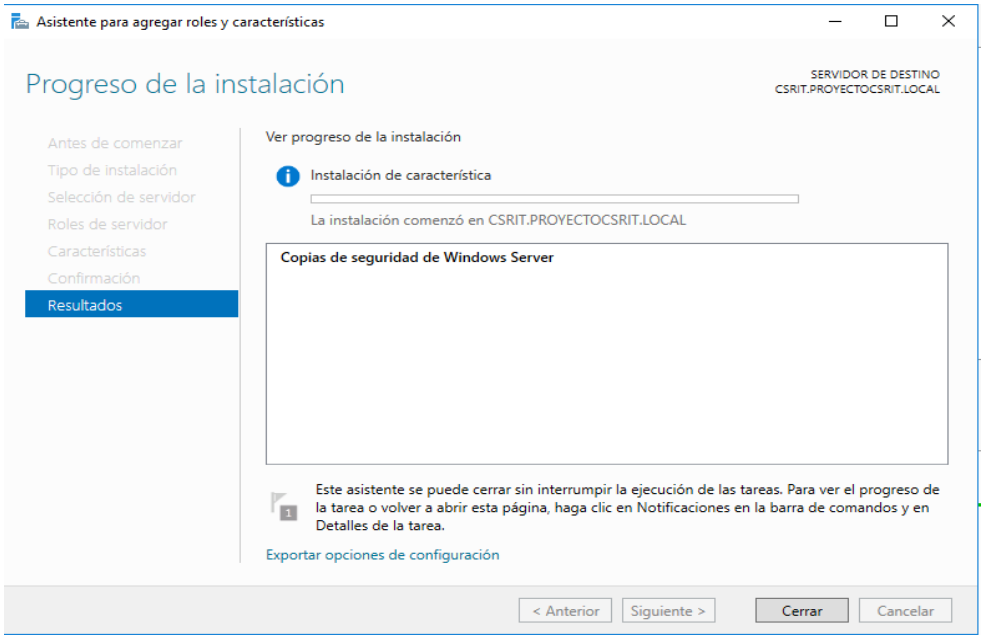
Ahora lo podemos ver desde la unidad que se destinó para dicho proceso. Tener en cuenta que en este momento solo tiene permiso sobre esa carpeta el usuario administrador posteriormente cuando se esté creando usuario se le asignara los permisos respectivos para que puedan visualizar dicha carpeta.

Anexo E. Servidor de copias de Seguridad

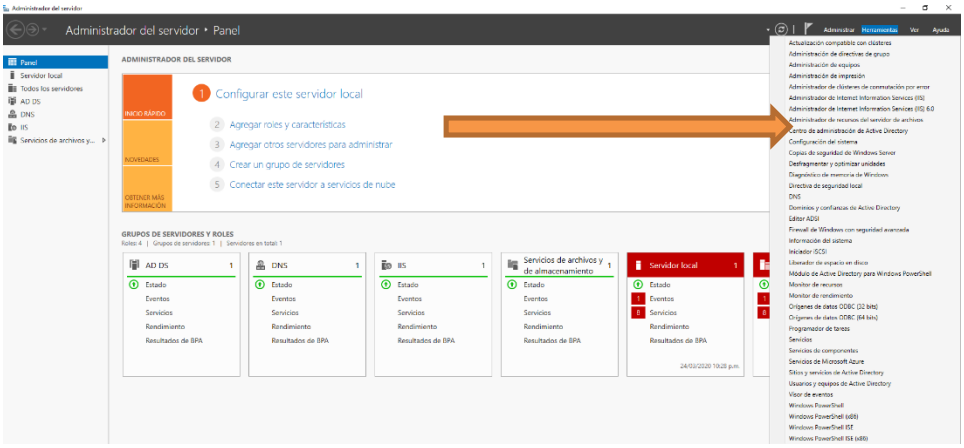
Lo primero que debemos de realizar es agregar en roles y características la opción de copias de seguridad.



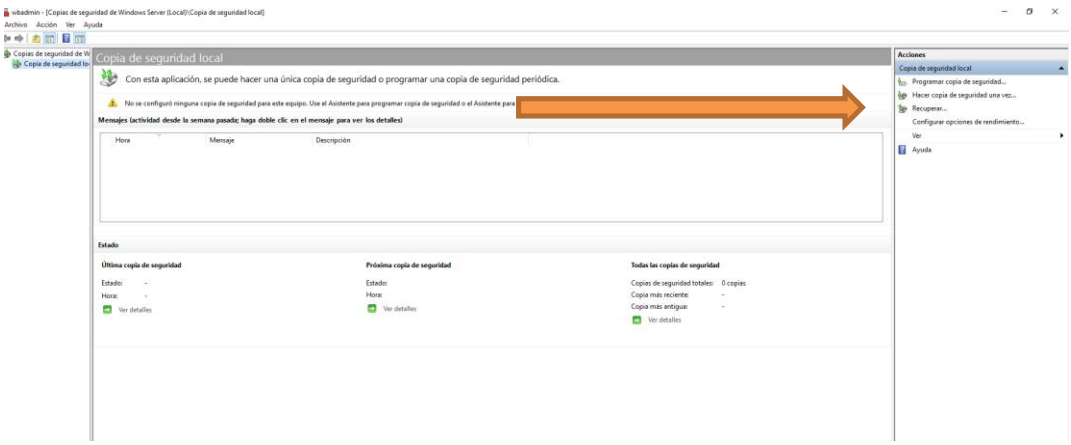
Realizamos la respectiva instalación de la característica que necesitamos



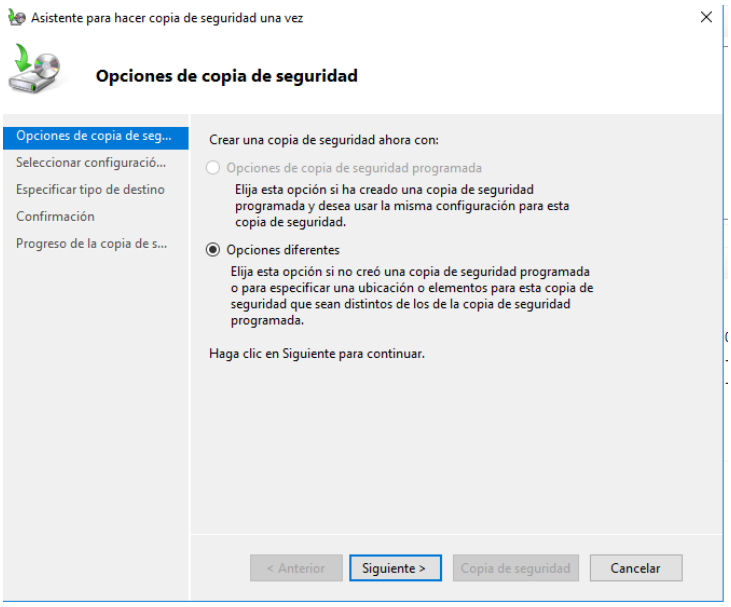
Luego de haber reiniciado mi maquina vamos al administrador de servidores y escogemos en la herramientas copias de seguridad de Windows server.



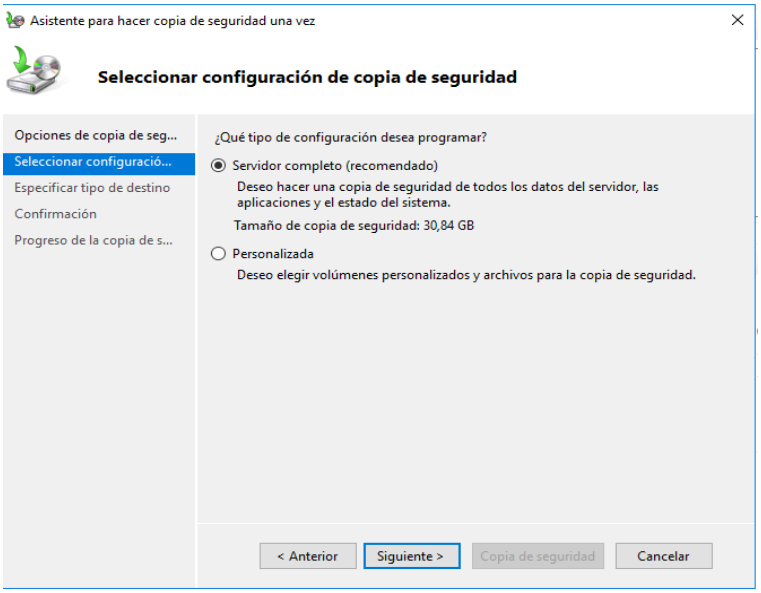
Con eso tenemos al asistente de copias de seguridad



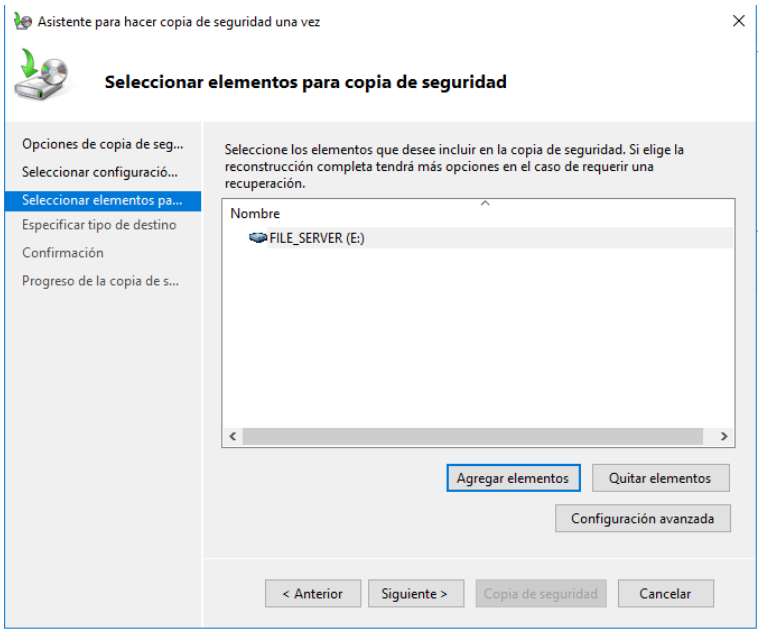
Seleccionamos copia de seguridad y vamos al panel izquierdo y escogemos la opción hacer copia de seguridad por primera vez.



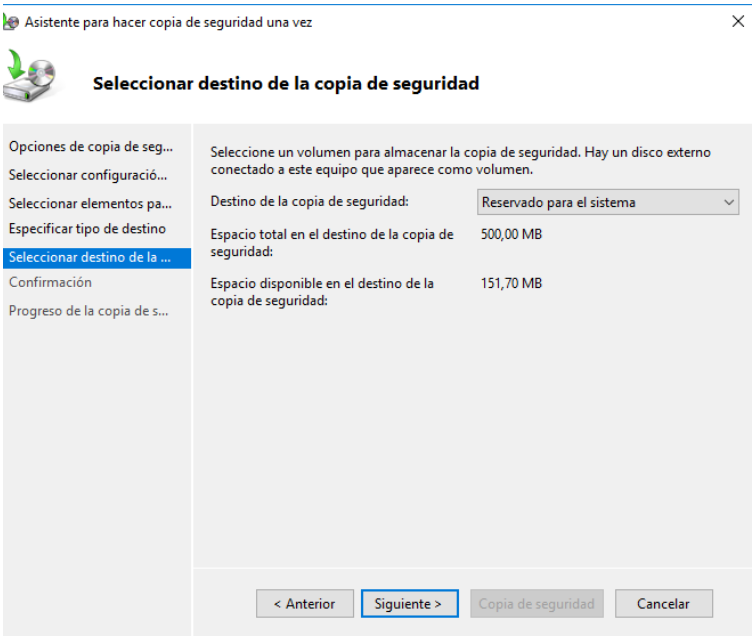
El asistente nos dice lo siguiente y escogemos opciones diferentes que como lo explica en la imagen nos menciona para que funciona esta opción.



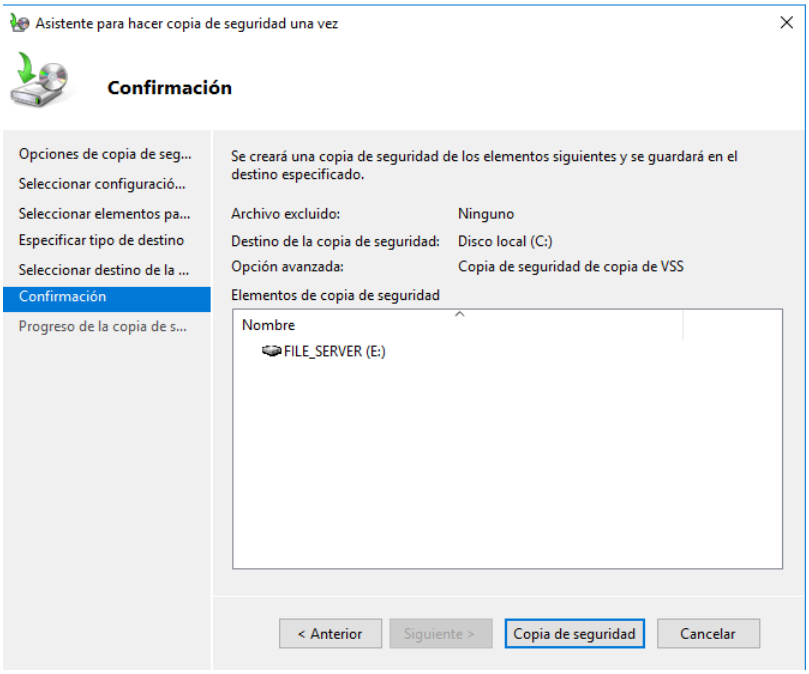
Por defecto nos dice que escojamos el servidor completo este se lleva hasta la imagen del mismo sistema operativo o personalizado donde podemos hacerle backup a una BD por ejemplo.



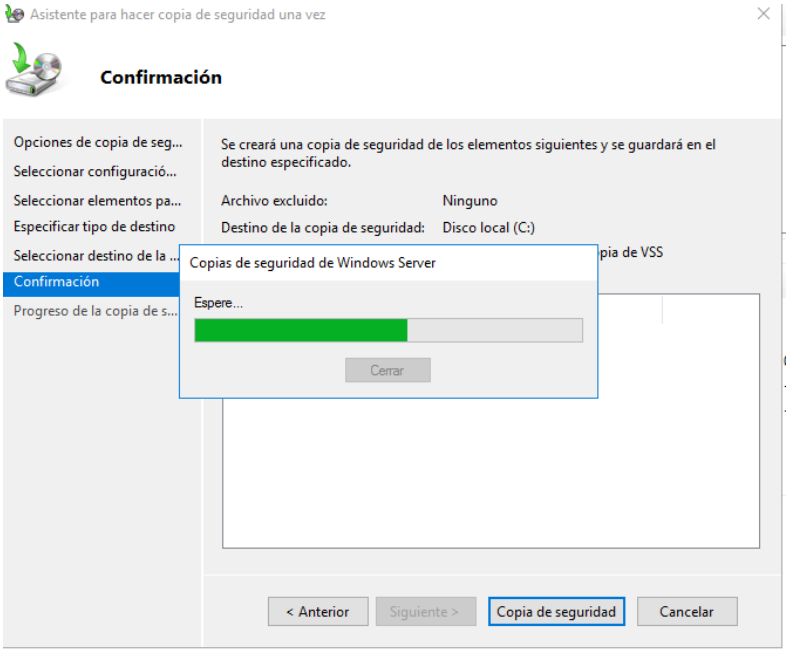
En nuestro caso escogemos personalizada y vamos a realizarle el backup a nuestro FILE_SERVER.

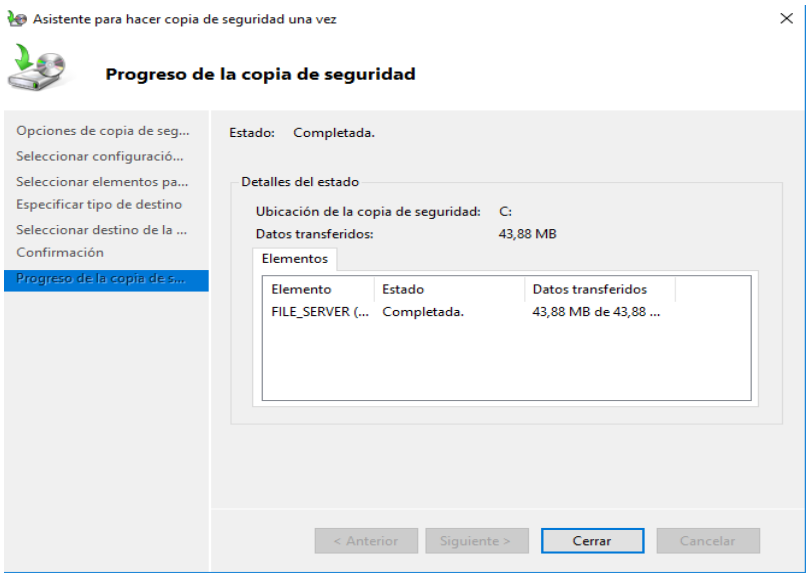


En este momento haces el proceso de manera local aunque se puede establecer la ruta remota para realizar el backup y establecemos la ruta donde se quiere guardar dicho backup.

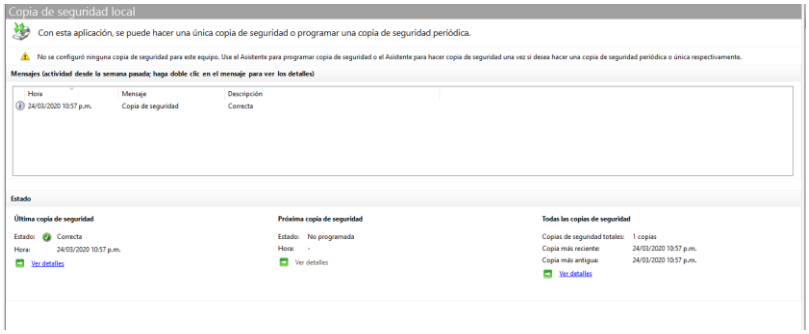


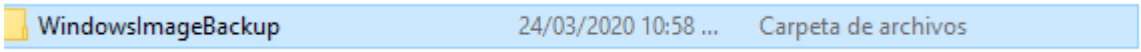
Iniciamos la copia de seguridad de la unidad que vamos a realizar el backup.





Se termina el proceso del backup



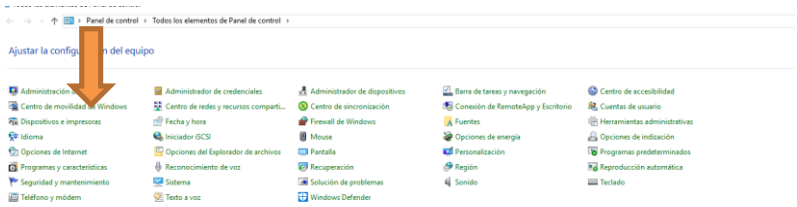


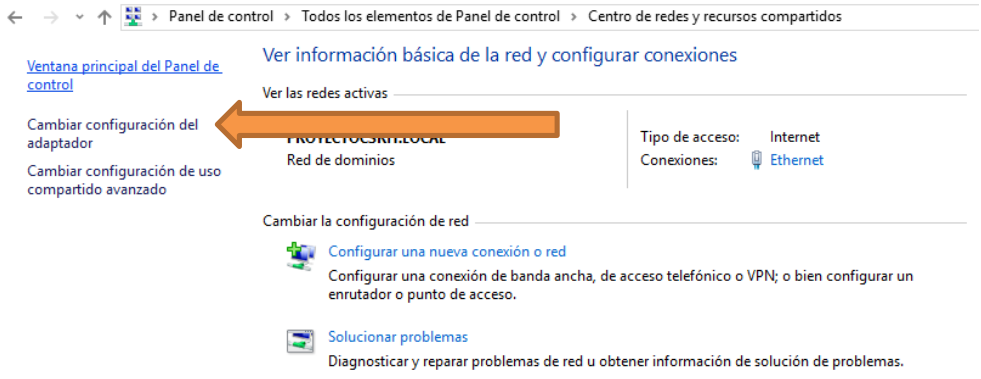
Validación de copia

Anexo F. Servidor DNS

Lo primero que debemos de realizar para el montaje de este servicio es establecer una dirección Ip fija a nuestro equipo de la siguiente manera:

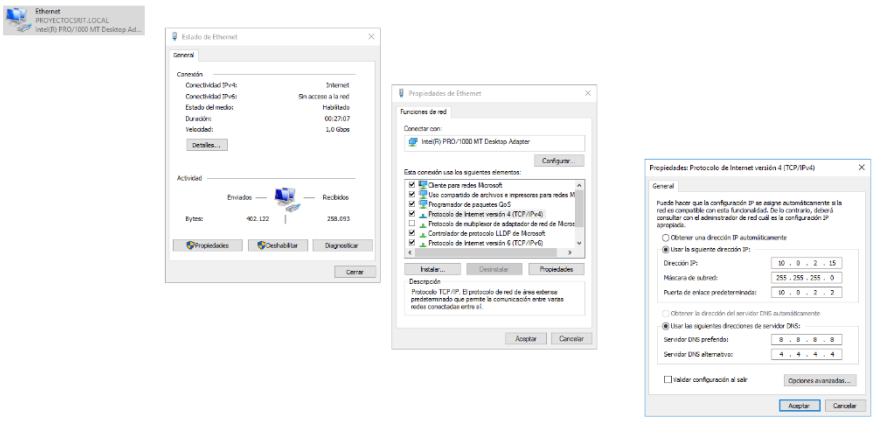
Vamos a panel de control y buscamos centro de redes y recursos compartido



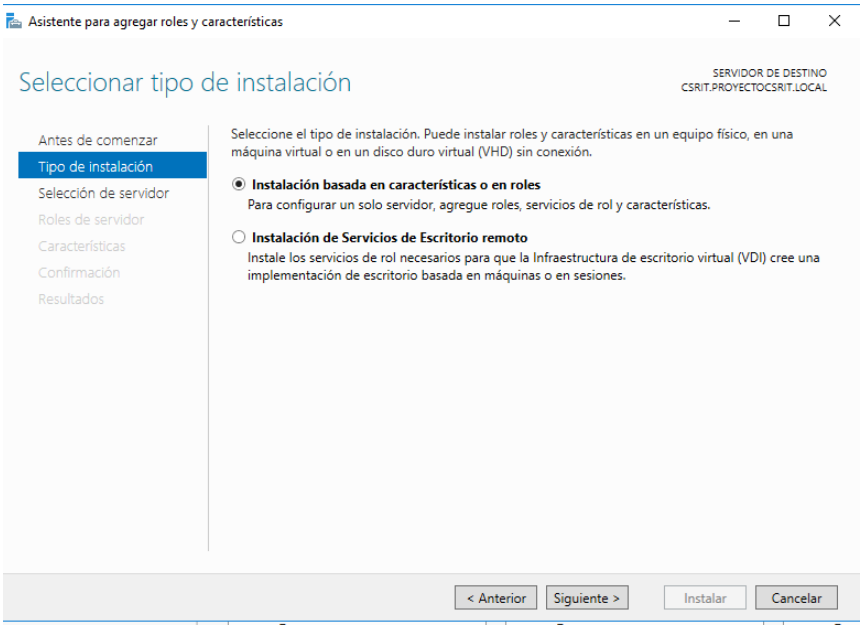


Y damos clic. Sobre el adaptador Seleccionamos la tarjeta red. Propiedades y asignamos la siguiente dirección Ip:

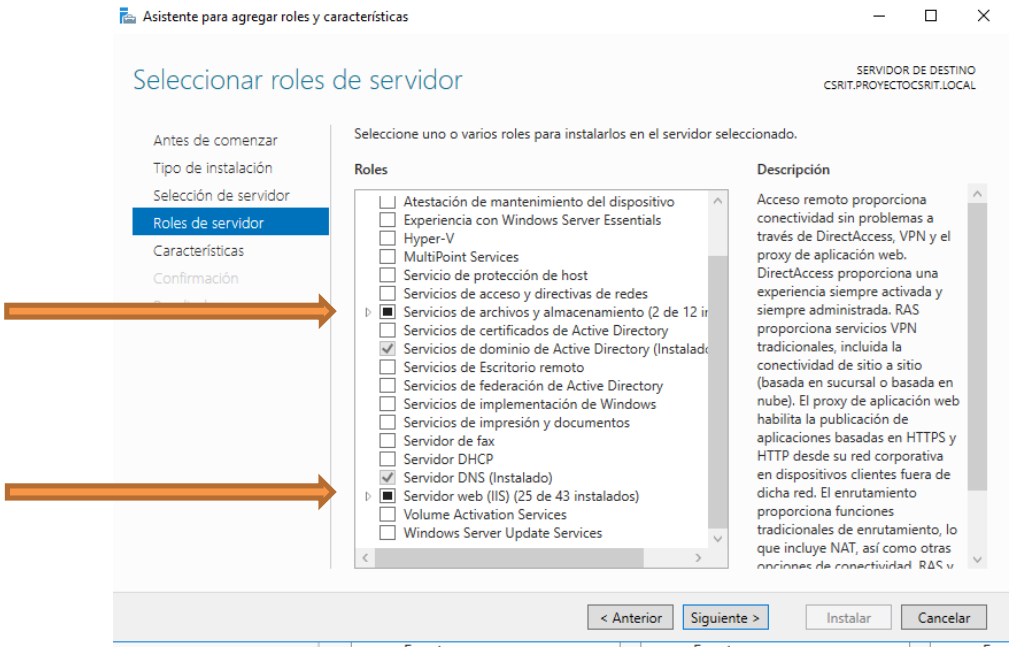
IP:10.5.1.12 , mascara de subred: 255.255.255.0.



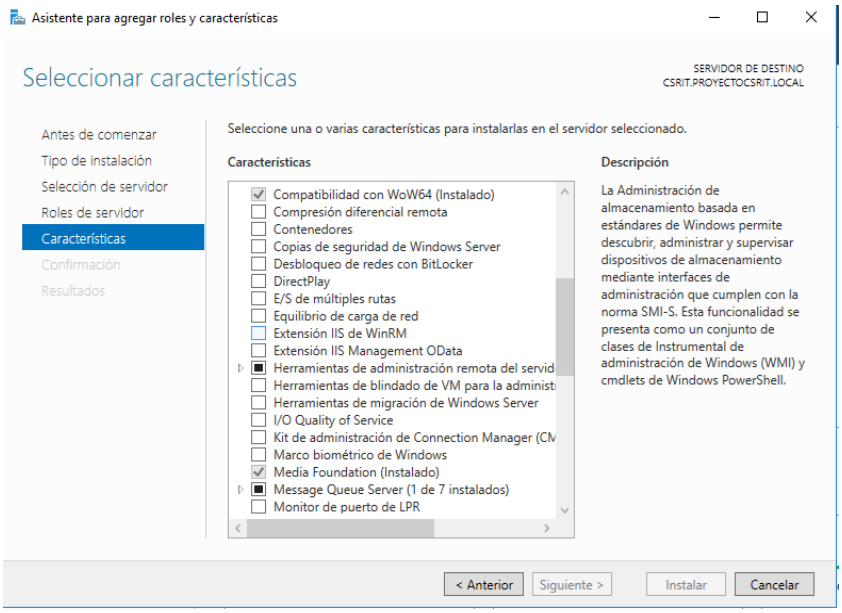
Posteriormente, de haber asignado la ip fija agregaremos en el administrador de servidores los siguientes servicios.



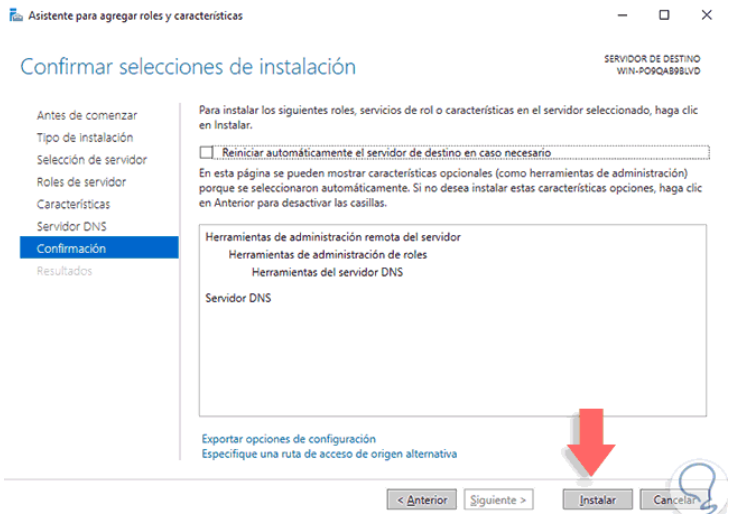
Los roles que vamos a instalar son el servicio de dominio de active directory y el servidor DNS.



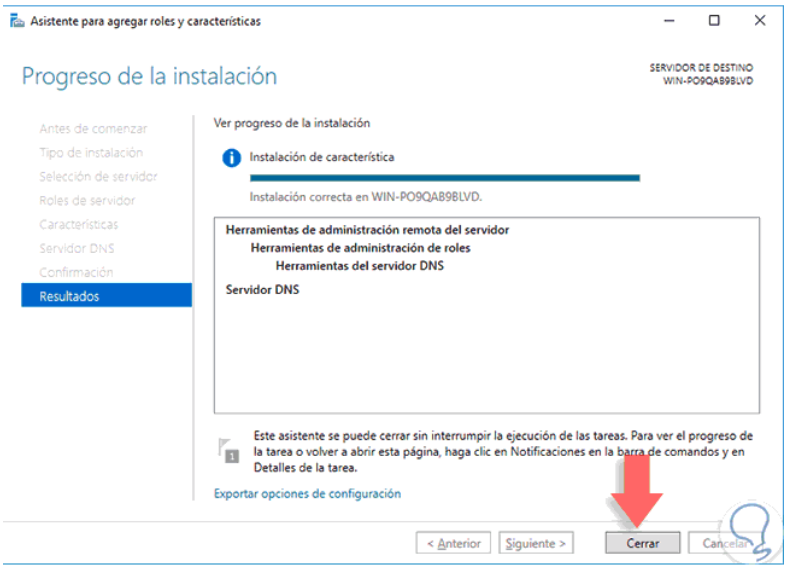
Luego, instalamos la característica de media fundation.



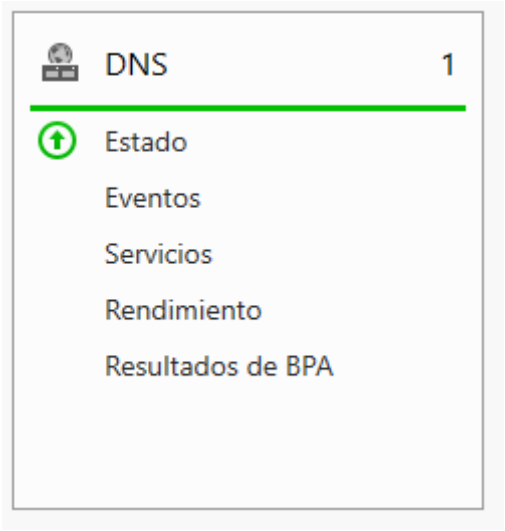
Pulsamos nuevamente Siguiente y en la siguiente ventana no es necesario adicionar alguna característica por lo cual pulsamos Siguiente. En la próxima ventana veremos una descripción sobre la función principal del servidor DNS, pulsamos Siguiente y veremos un resumen del rol a instalar.



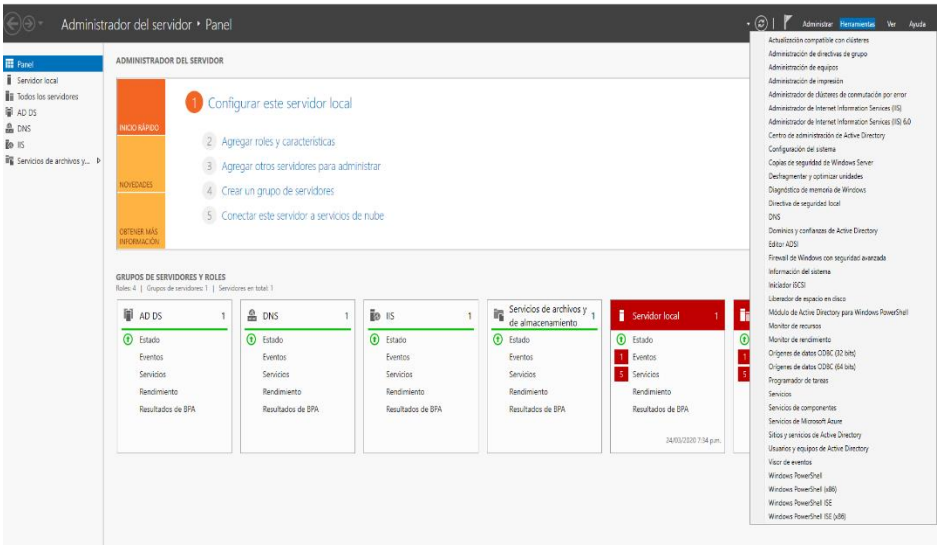
Finalmente veremos que nuestro servicio DNS ha sido instalado de manera correcta. Pulsamos Cerrar para salir del asistente.



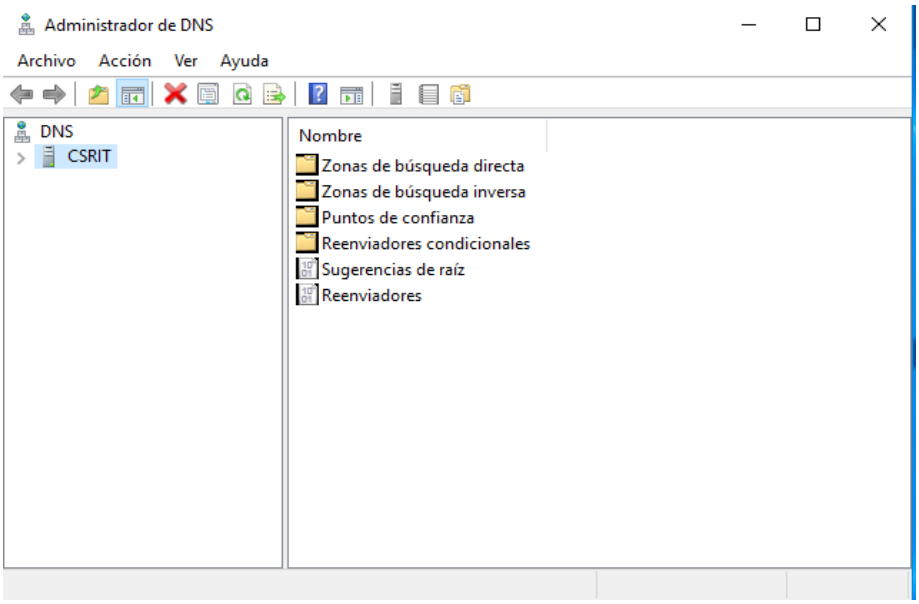
Con esto ya queda instalado nuestro servidor DNS



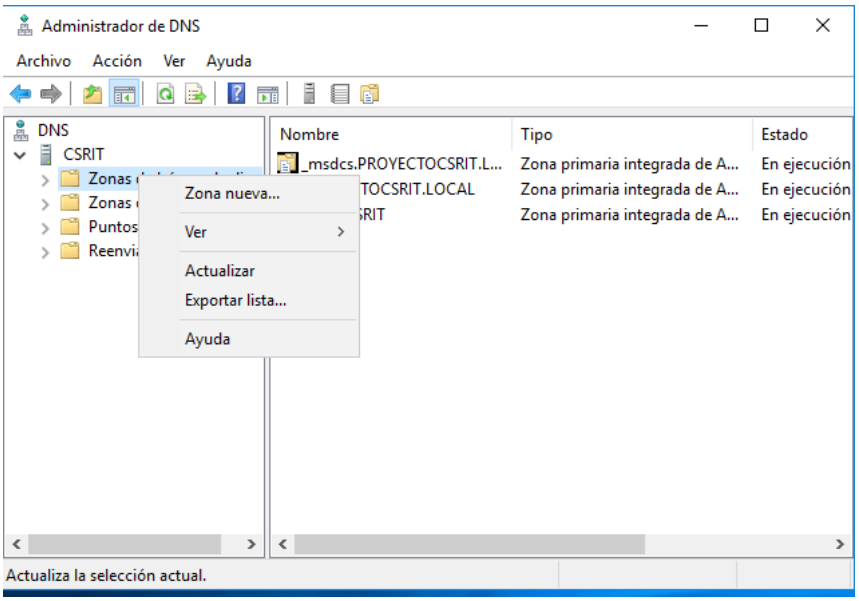
Posteriormente, ingresamos al servicio del DNS para realizar la configuración respectiva de la siguiente manera:



Veremos que se despliega la siguiente ventana. Allí tenemos a mano las principales tareas que podemos realizar sobre el DNS en Windows Server 2016 como las zonas, reenviadores y zonas de confianza.

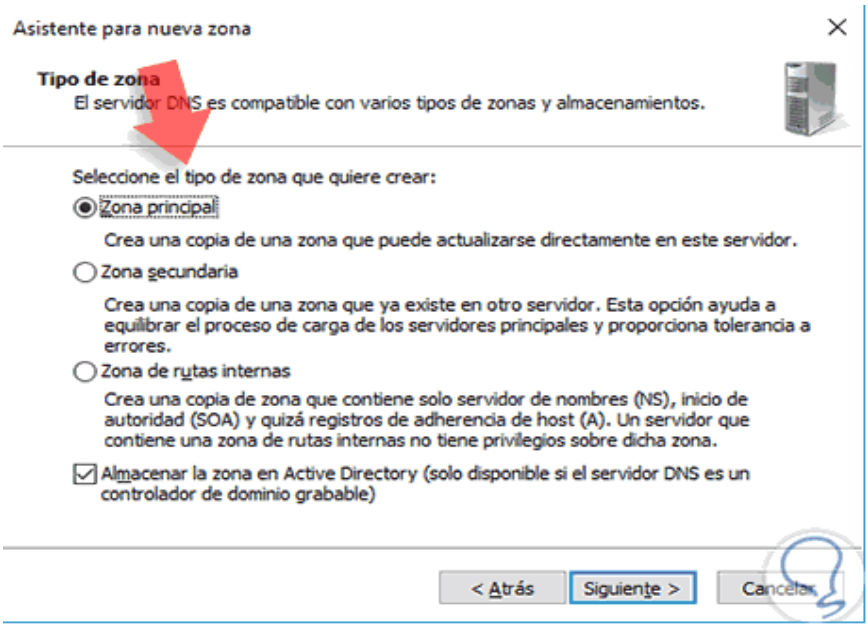


Como vemos cuando promovemos nuestro servidor a controlador de dominio se crean las respectivas zonas directas. Podemos crear una nueva zona para extender las gestiones de nuestro servidor.

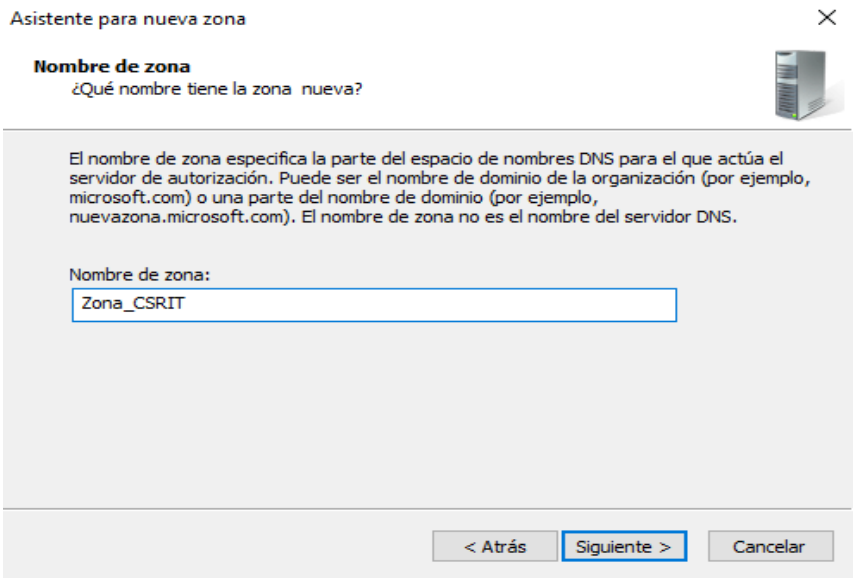


Recordemos que la zona directa nos resuelve los nombres de dominio a direcciones IP mientras que la zona inversa nos resuelve de direcciones IP a nombres de dominio. Para este ejemplo crearemos una nueva zona directa, por ello pulsamos sobre "Zona nueva" y veremos el siguiente asistente.

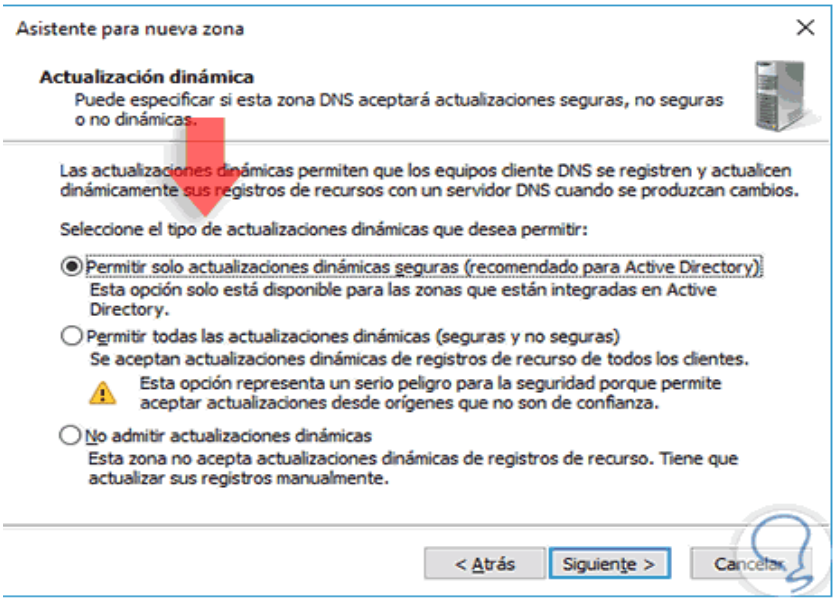
Pulsamos en "Siguiente" y a continuación debemos definir el tipo de zona a crear.



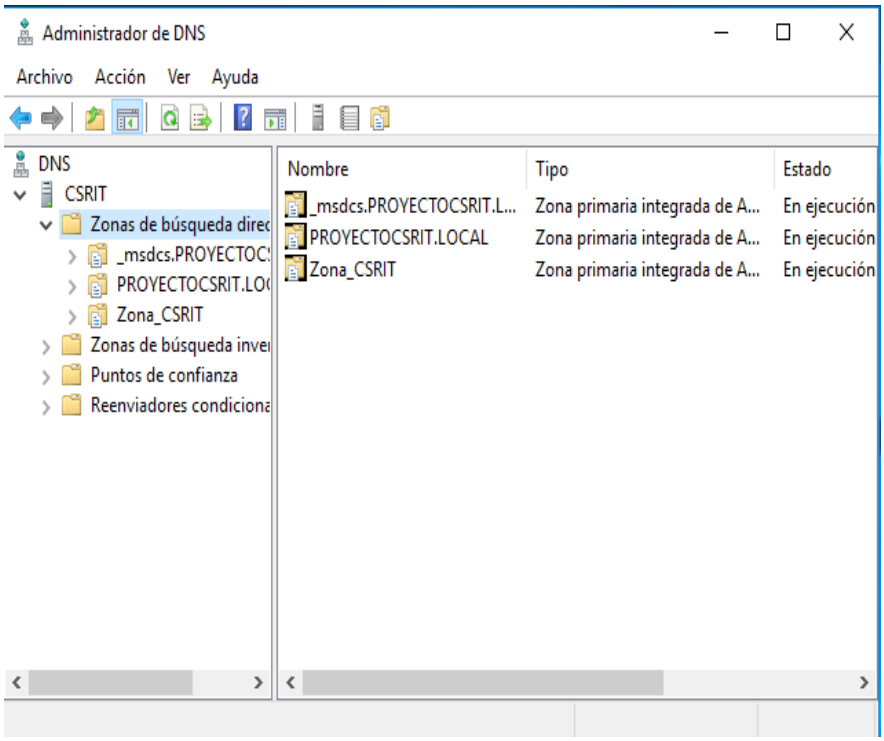
Pulsamos Siguiente y definiremos el nombre de la zona.



Pulsamos de nuevo Siguiente y establecemos la forma en cómo se obtendrán las actualizaciones.



De nuevo pulsamos Siguiente y veremos un resumen de la zona creada.

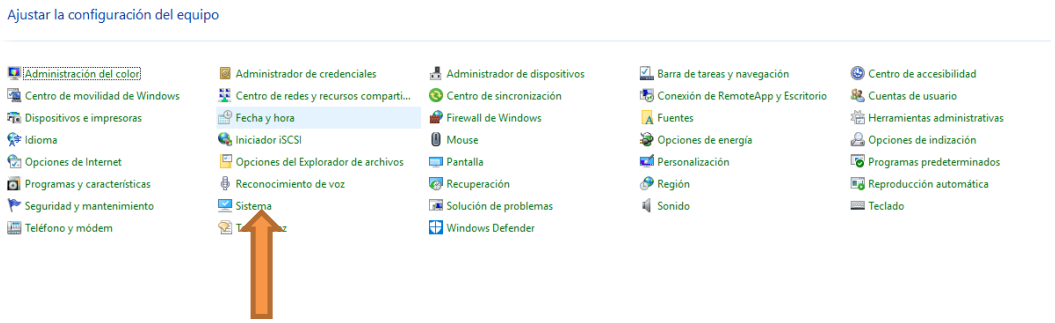


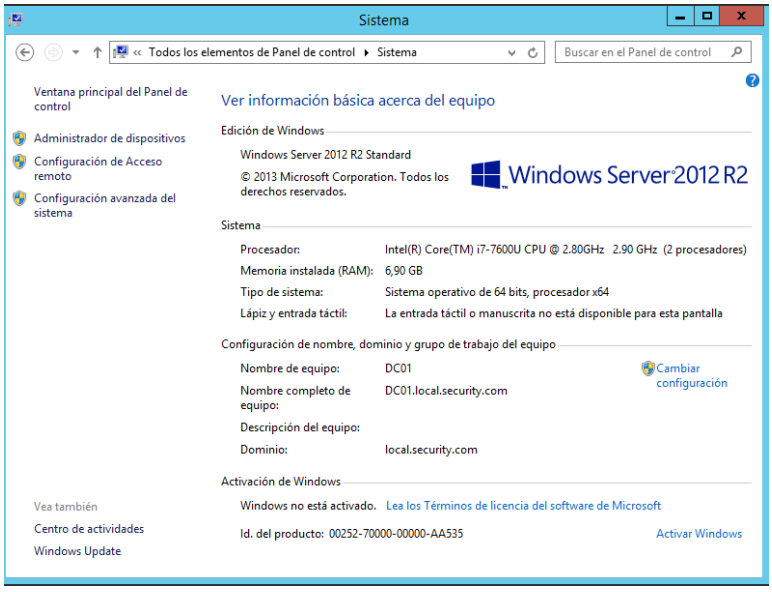
Pulsamos en Finalizar para cerrar el asistente y podremos ver nuestra zona creada.

De esta forma hemos creado nuestra nueva zona y podremos adicionar nuevos hosts, registros, alias, entre otros. De la misma forma podemos establecer una nueva zona inversa para aumentar la capacidad de nuestro DNS en Windows Server 2016.

Ahora configuramos el directorio activo de la siguiente manera:

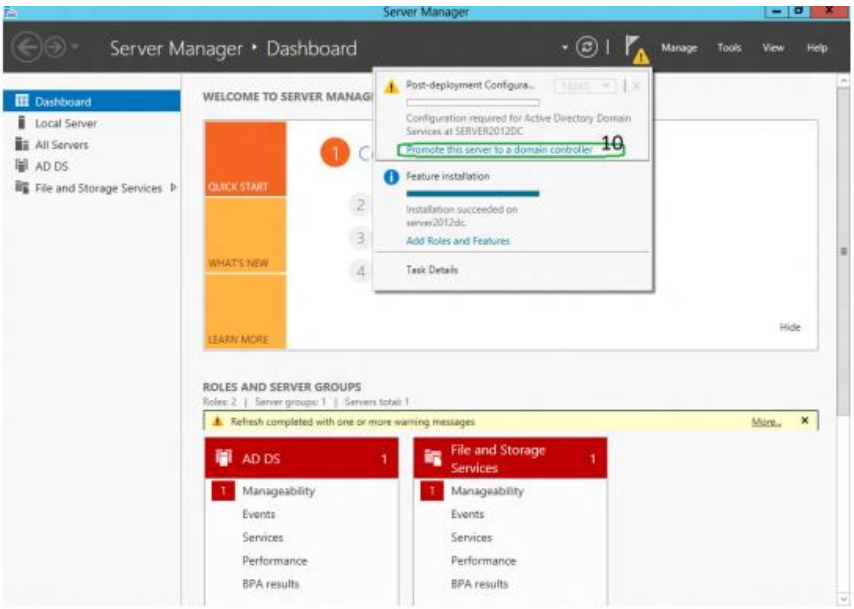
Lo primero que debemos de realizar el asignar un nombre a nuestra máquina de la siguiente manera vamos a panel de control y escogemos la opción sistema



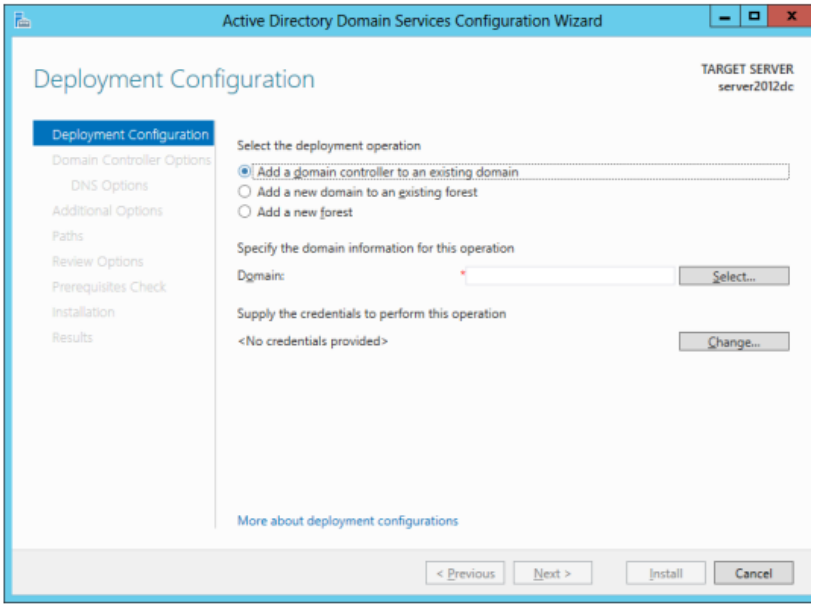


Asignamos un nombre a la maquina

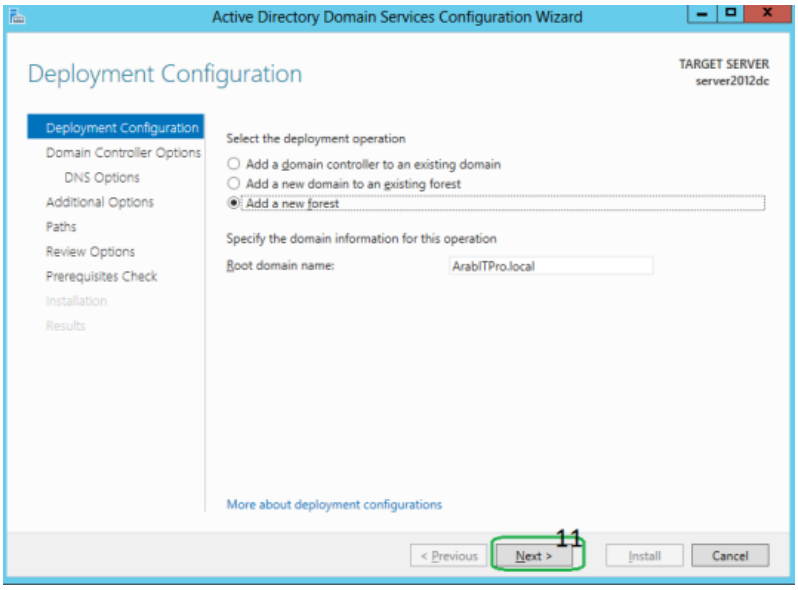
Como ya hemos seleccionado el rol de instalación del directorio activo en el administrador de servidor cuando ya se termina de instalar vamos a la siguiente opción.



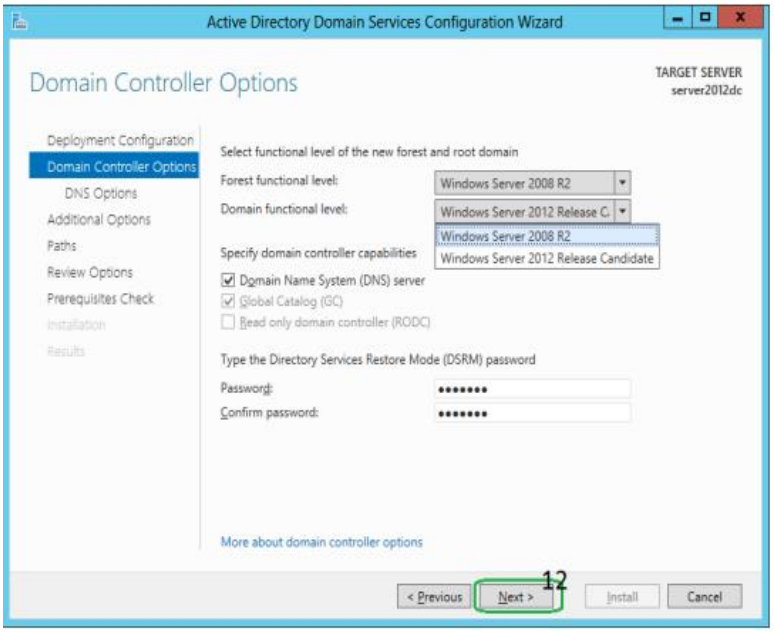
Para crear un nuevo bosque AD llamado "local.security.com", seleccione Agregar un nuevo bosque.



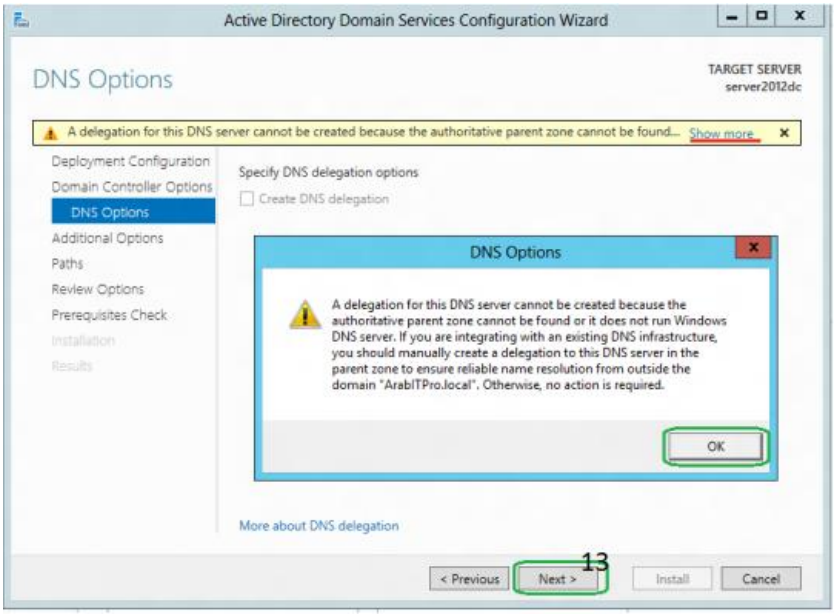
Escriba el nombre de local.security.com



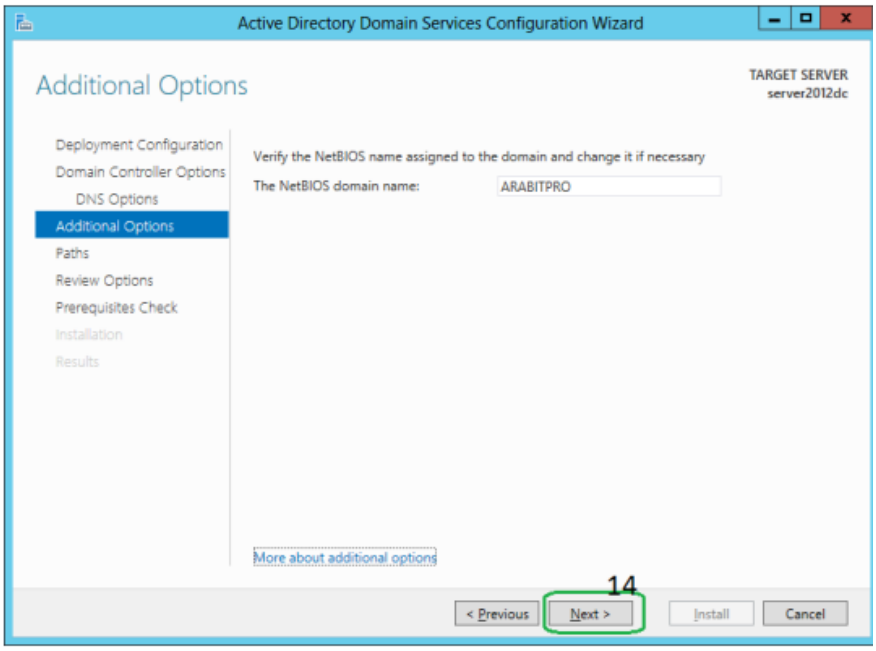
Especificar la FFL, DFL, o no debería ser un servidor DNS y también la contraseña del administrador DSRM. Como puedes ver, ha seleccionado la opción de GC por defecto y no puede anular la selección. La razón de esto es que es el primer DC de la selva de AD y al menos uno debe ser un GC.



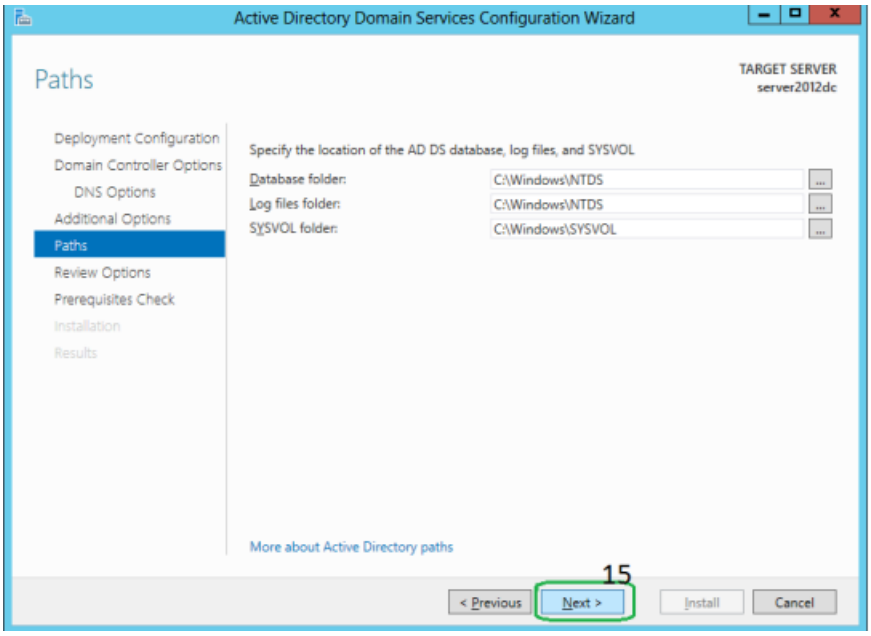
ADVERTENCIA de delegación de DNS.



Comprueba el nombre NetBIOS ya asignado. Local.security.com

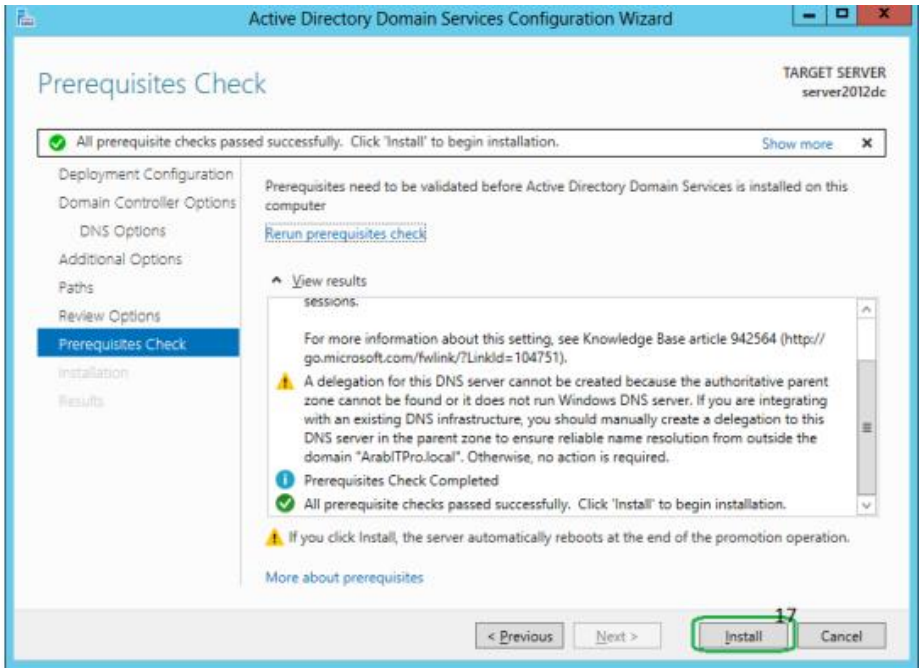


Especifique la ubicación de los anuncios relacionados con carpetas y haga clic en siguiente.

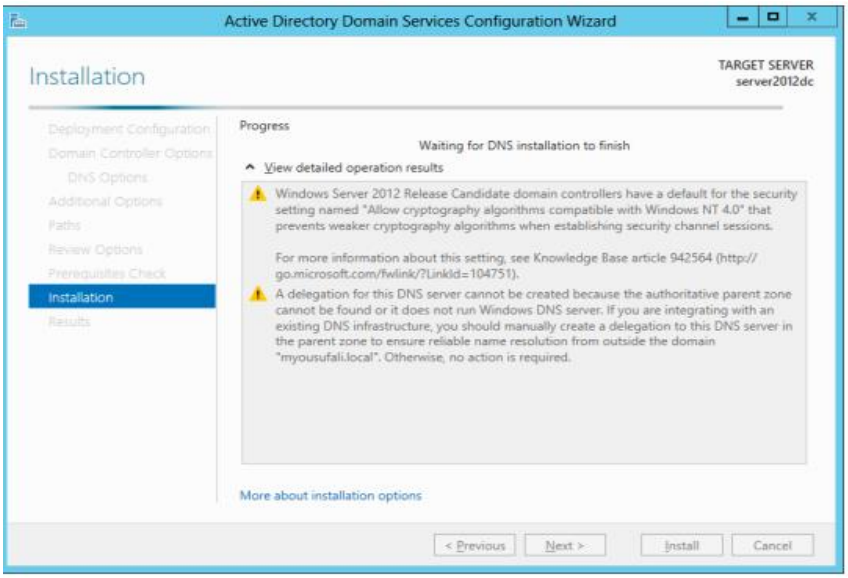


Resumen de todas las opciones de instalación/selecciones.

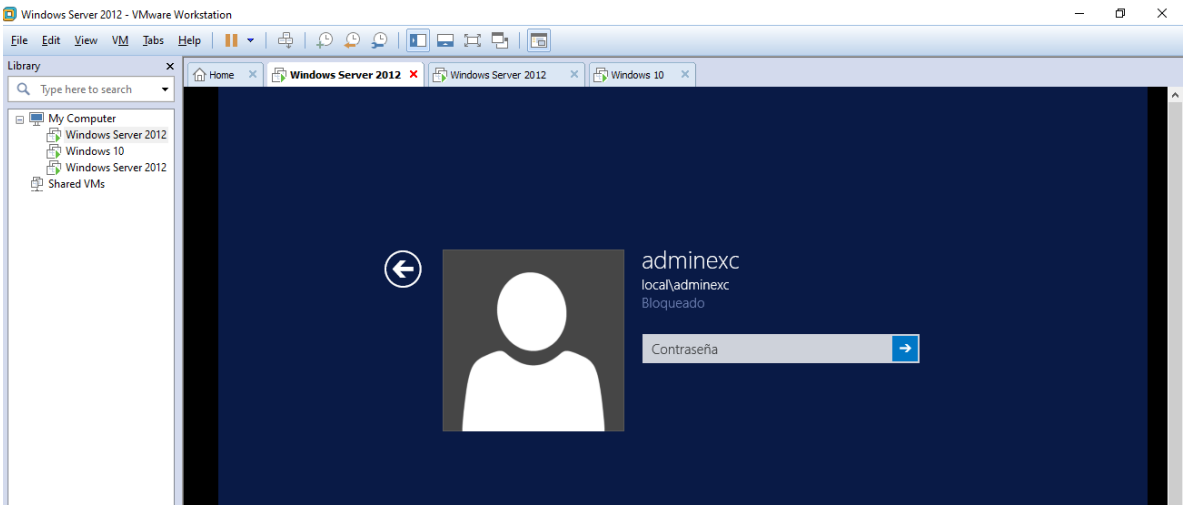
Antes de la instalación actual de AD, se comprueban todos los prerrequisitos. Si todas las comprobaciones prerrequisitos pasan con éxito y haga clic en instalar.



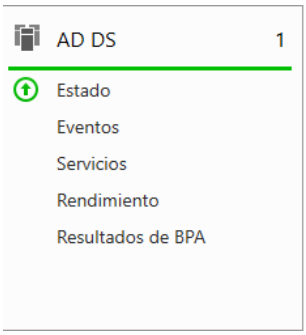
Cuando hace clic en instalar, DNS y la GPMC se instalan automáticamente.



Después de la promoción del servidor a un servidor terminado DC reiniciará automáticamente.

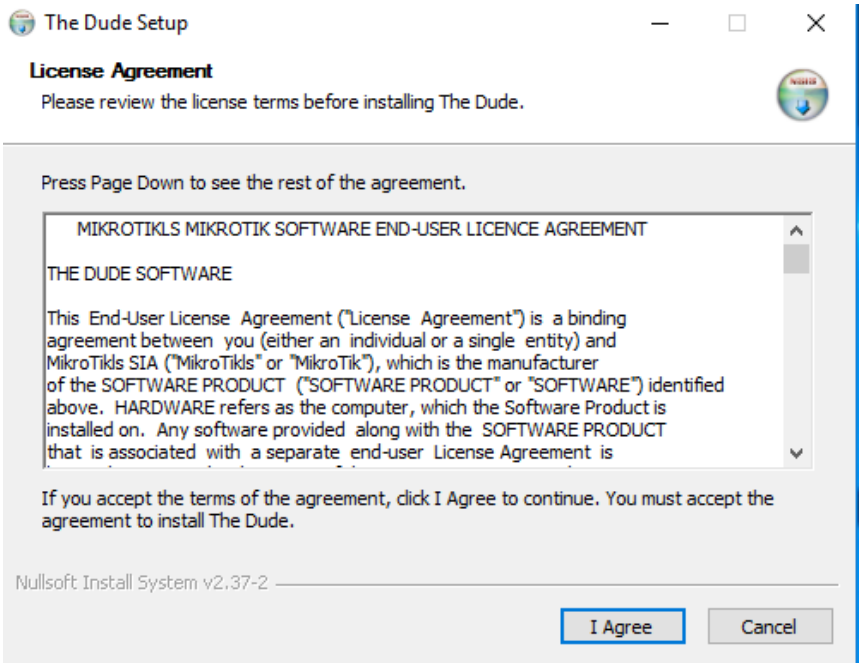


Ya nuestro server aparece con el dominio y observamos en el panel de administrador de servidores lo siguiente:

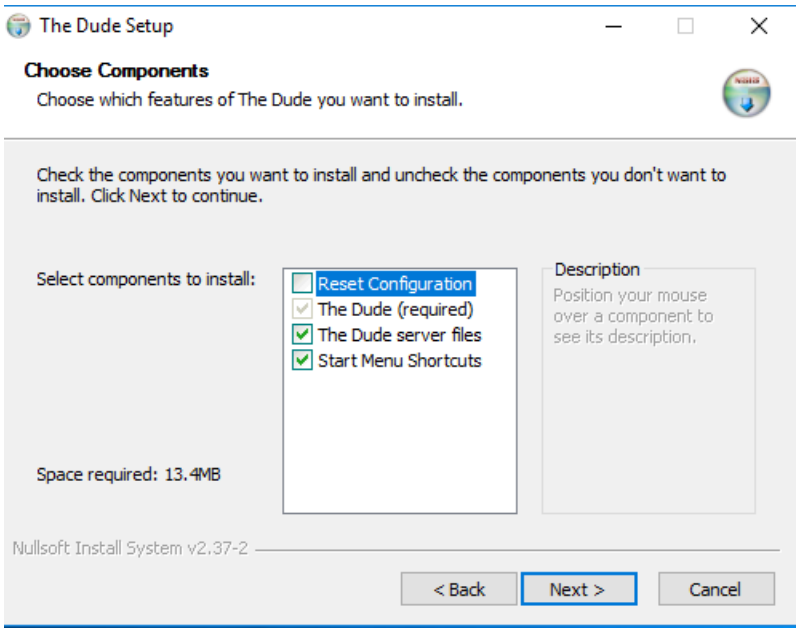


Anexo G. Servidor de Monitoreo y Dispositivos de Conectividad

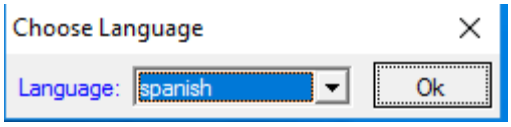
Para nuestro servidor de eventos vamos a realizar montar una herramienta OpenSour llamada The Dude.

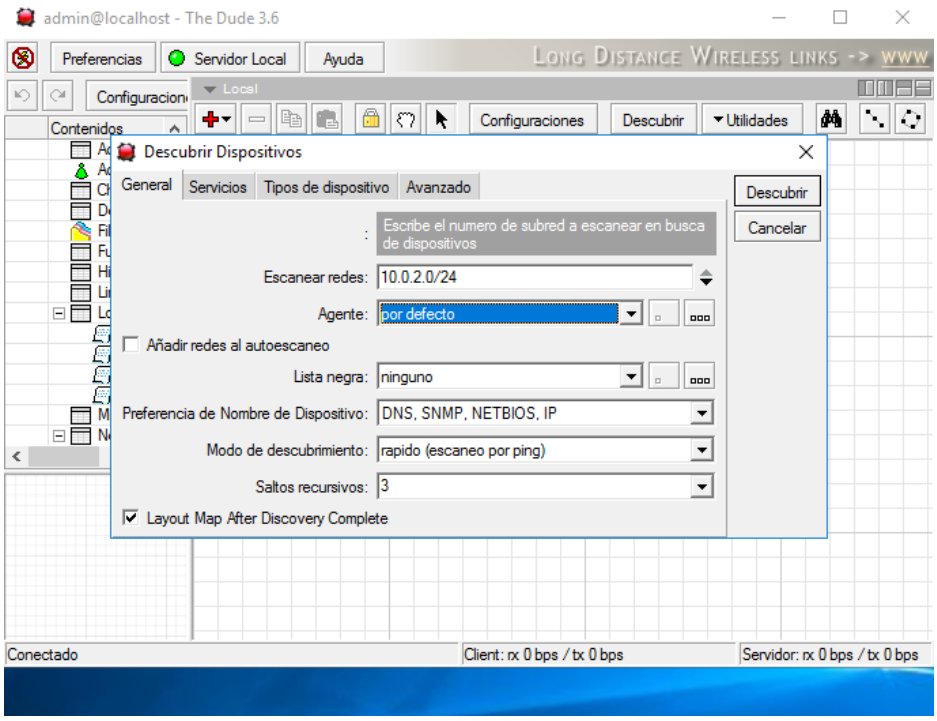


Ejecutamos el instalador

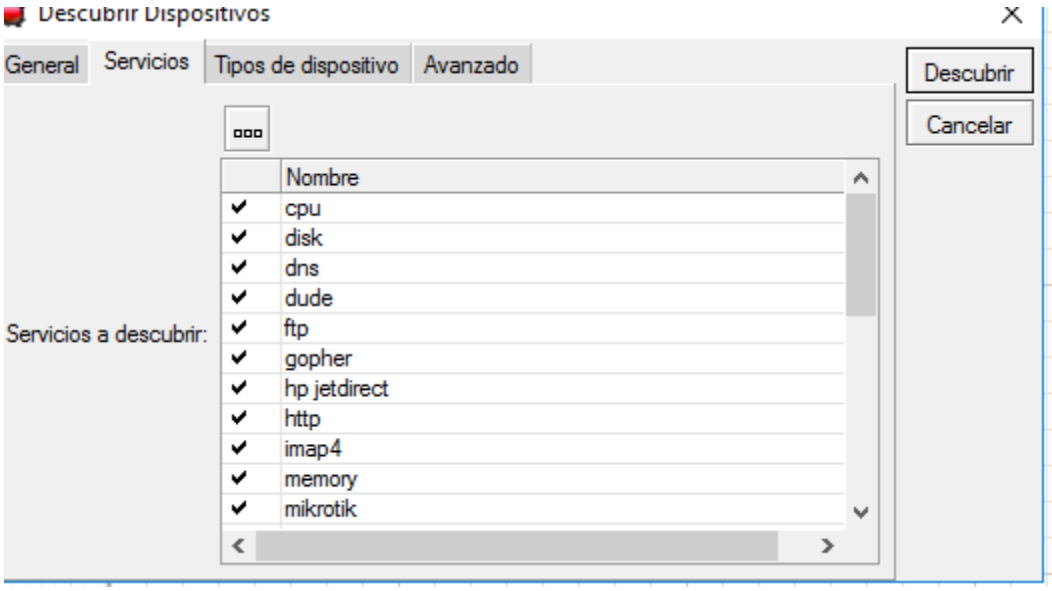


Damos siguiente e instalar

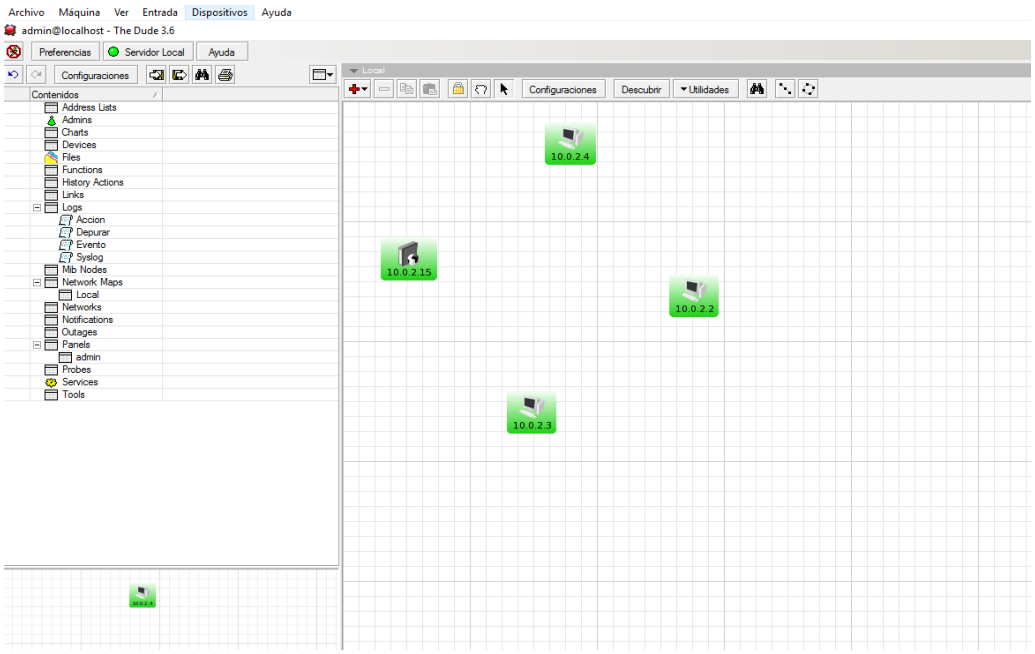




Luego nos tomara nuestro las características de nuestro servidor y que deseamos que monitoreamos.



Selecciono lo servicios que quiero que me muestre en el proceso de escaneo



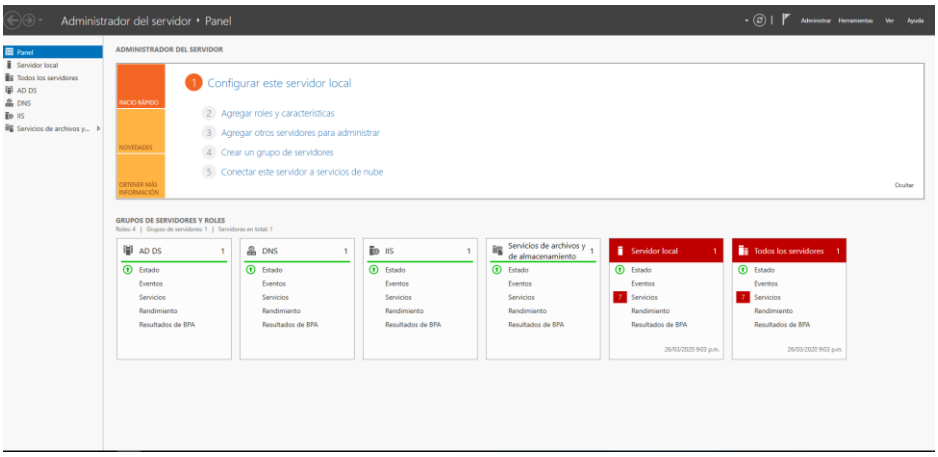
Con esto nos está mostrando el monitoreo de la red y las maquinas que se encuentra en nuestra red y sus características entre ellas la red monitorea.

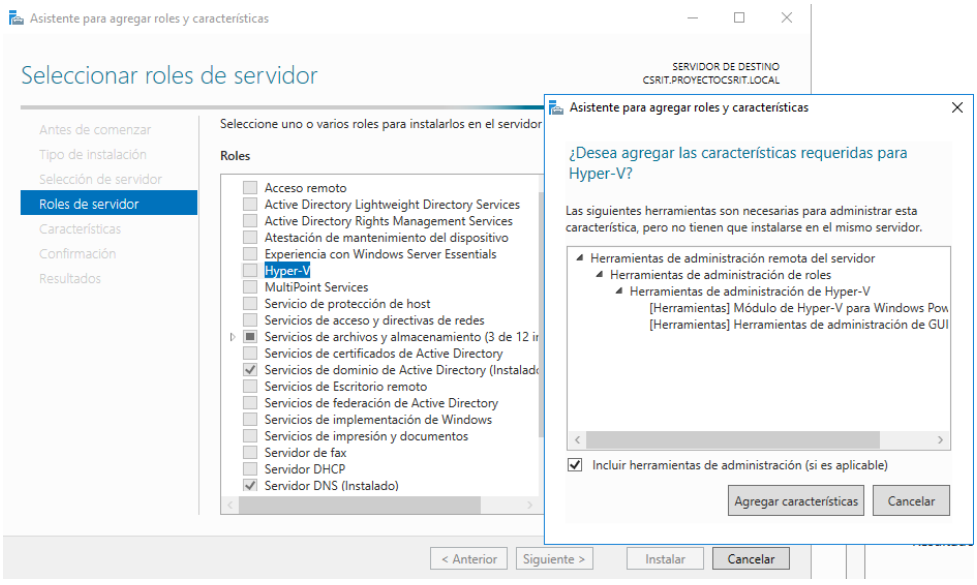
Anexo H. Servidor Sandbox

La implementación del sandbox en Windows server 2016 lo vamos a tratar con hyper-v dado que este cumple con herramientas similares a estos servicios.

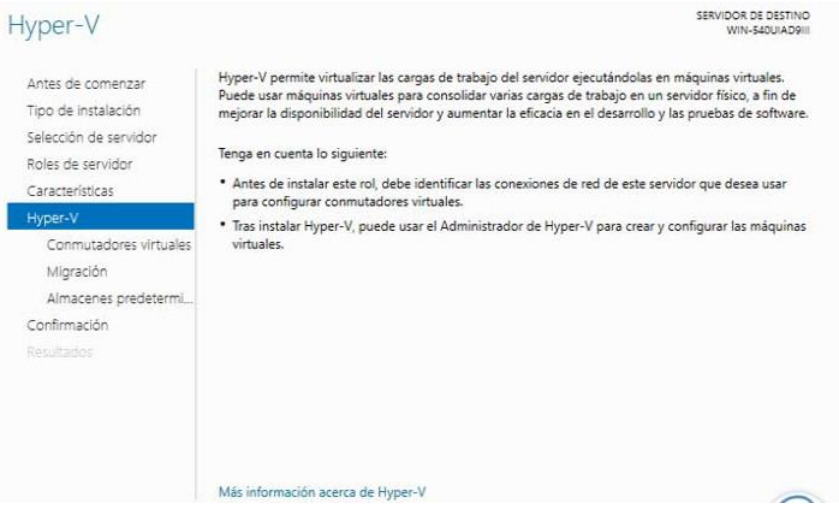
El proceso de instalación es el siguiente:

Ingresamos al administrador de servidores y agregamos el rol de hyper-v





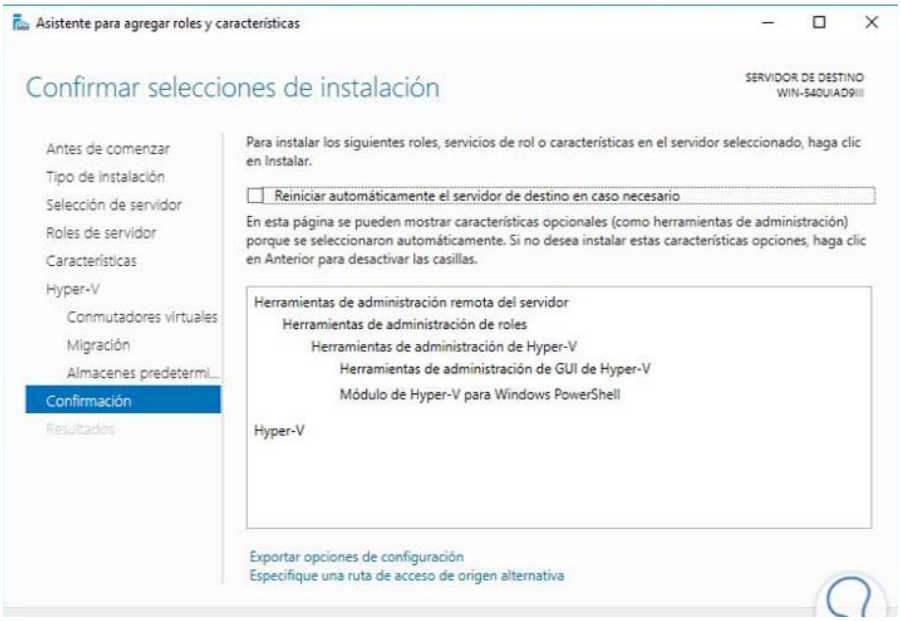
Damos clic en Add Features o Agregar características para incluir dentro de la instalación las herramientas asociadas a Hyper-V. Damos clic en Next



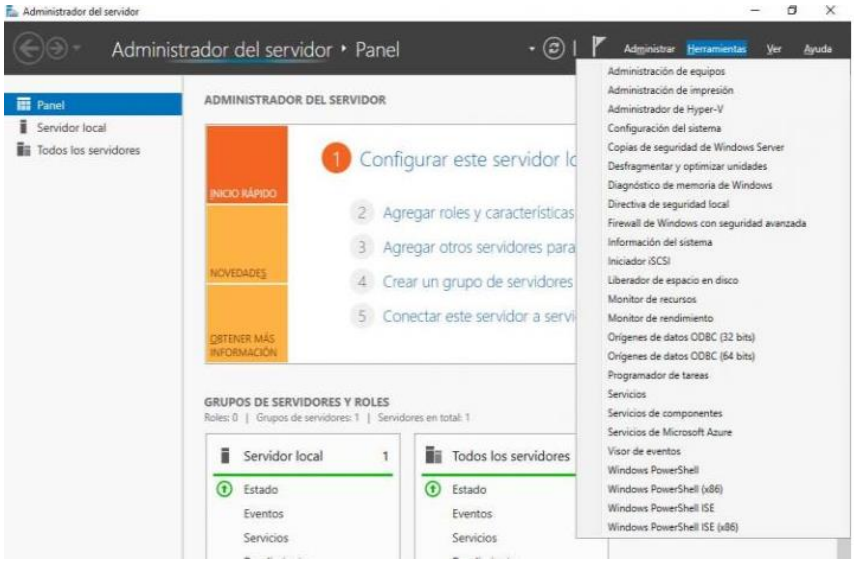
Siguiente para continuar. Si deseamos agregar alguna característica adicional la seleccionamos y pulsamos Siguiente, podremos ver que se despliega la siguiente ventana donde se muestra un resumen acerca de Hyper-V.

En la siguiente ventana debemos seleccionar el conmutador virtual para el respectivo adaptador de red que tengamos, es importante anotar que se creará un conmutador virtual por cada adaptador, simplemente seleccionamos el adaptador y pulsamos Siguiente.

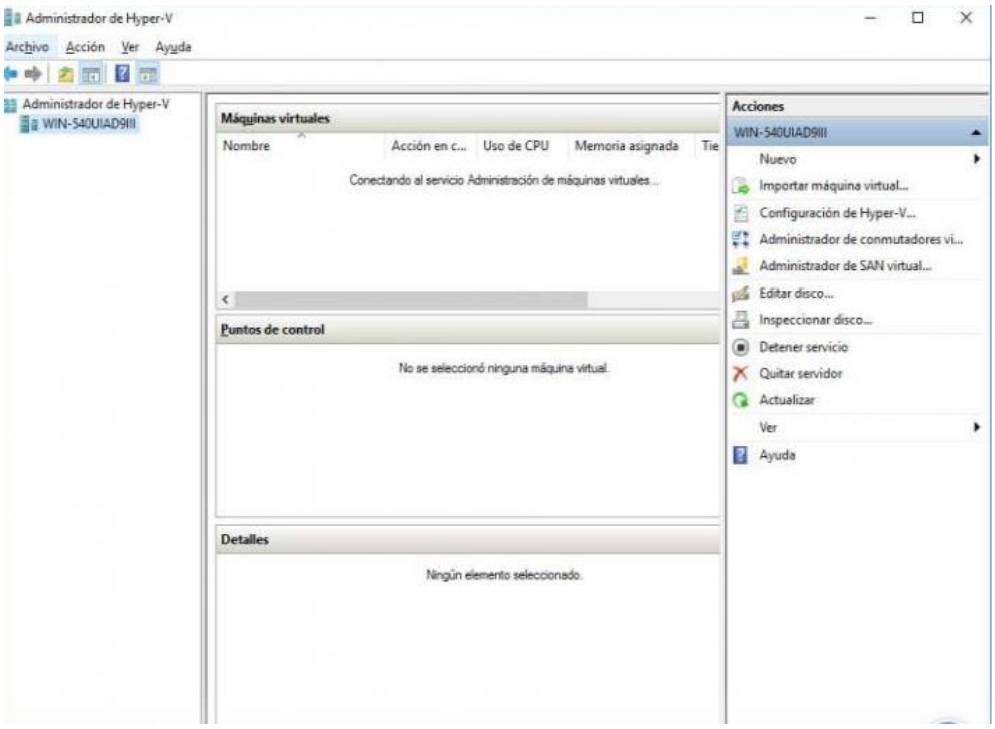
En la siguiente ventana debemos elegir si deseamos que Hyper-V envíe y reciba migraciones en vivo de máquinas virtuales y de la misma forma debemos establecer el protocolo con el cual se autenticará Hyper-V, CredSSp o Kerberos. En este caso habilitaremos el servidor para que reciba las migraciones en vivo. Damos clic en Siguiente y debemos establecer (Recomendado dejar la ruta por defecto) donde se han de almacenar los discos duros virtuales, una vez establecido pulsamos Siguiente y podremos ver un resumen de las características y roles a instalar.



Una vez se haya instalado el rol de Hyper-V debemos reiniciar el servidor para aplicar los cambios necesarios. Ahora para ejecutar Hyper-V abrimos el Server Manager o Administrador del Servidor y desplegaremos la opción Herramientas o Tools y allí elegimos la opción Administrador de Hyper-V.



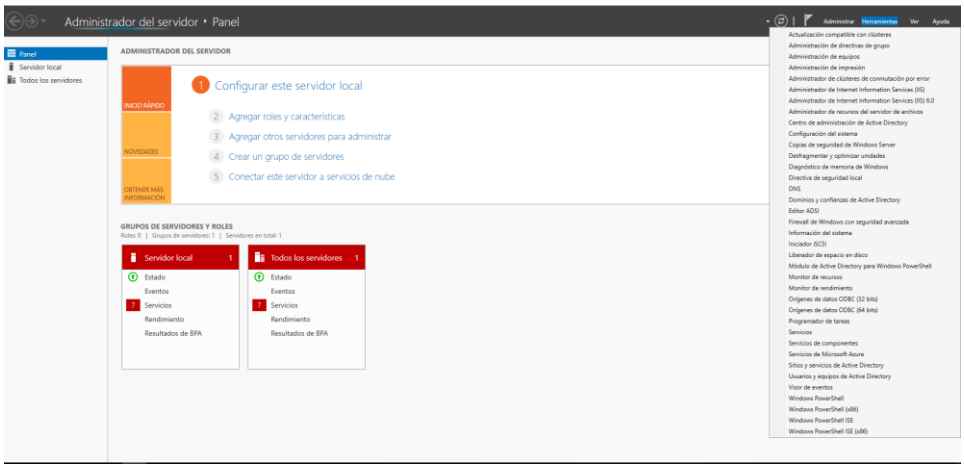
Y tenemos nuestro servidor de virtualización.



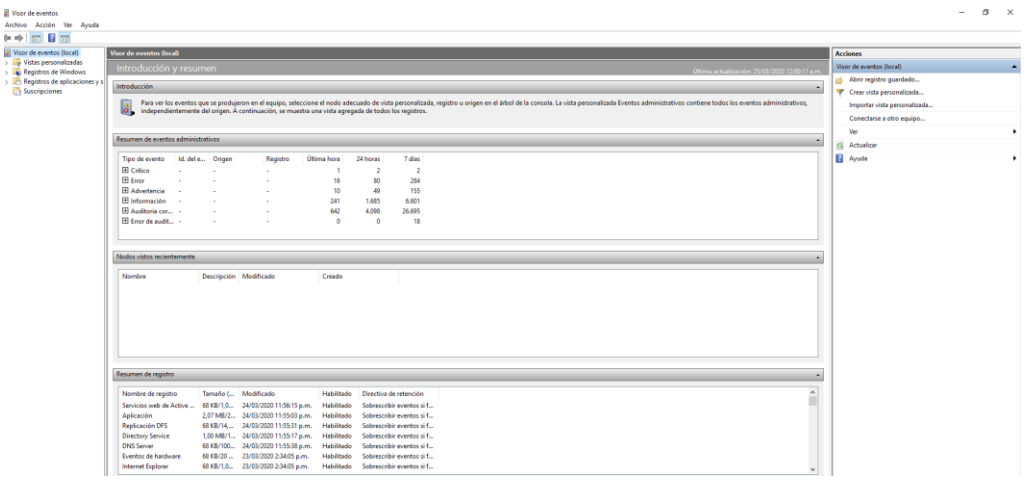
Anexo I.Herramientas de CSRIT

Correlacionador de Eventos

El correlacionador de eventos lo vamos a manejar desde las herramientas que nos ofrece Windows server 2016 y desde la administrador de servidores.



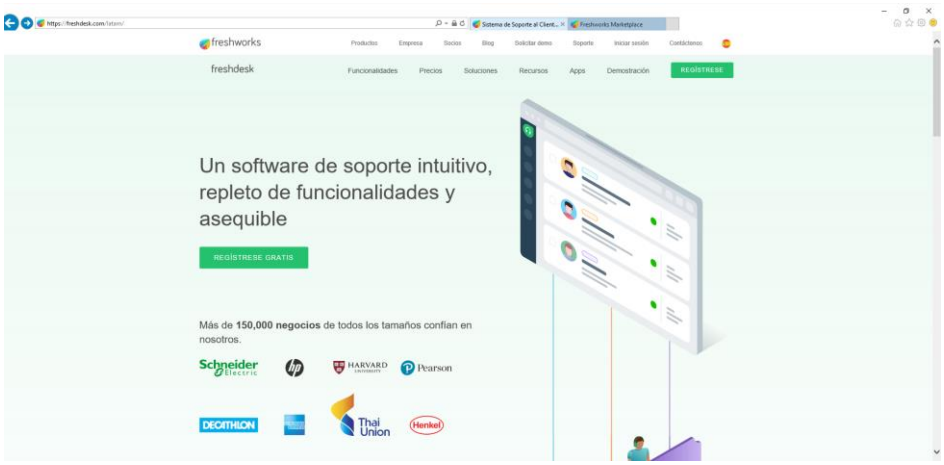
Desde esta herramienta podemos clasificar los eventos que se pueden presentar en la maquina como en las maquinas que estén relacionadas con el mismo server en esta caso con el controlador de dominio.



Por eso podemos clasificarlos por eventos como lo son: registros de Windows entre ellos aplicaciones, seguridad, instalación, sistema y eventos reenviados.

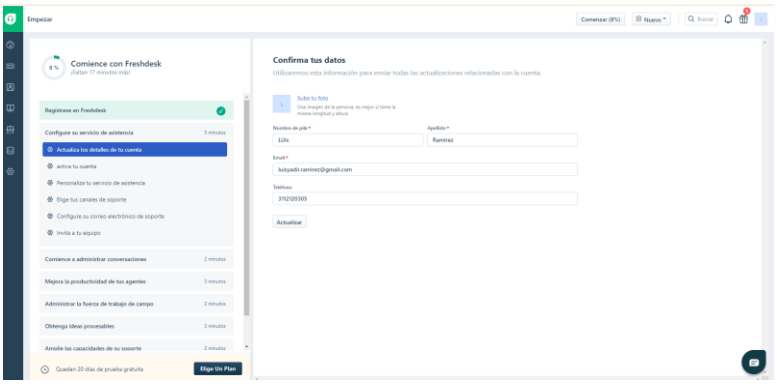
Registro y seguimientos de incidentes

Para realizar nuestro seguimiento y registro de los incidentes utilizare la siguiente herramienta que es online totalmente openSour solo basta con registrarnos obtendremos.



Abrimos el link https://www.softwaredegestionlibre.com/2017/06/activar-plan-gratuito-help-desk.html

Nos registramos dice que 21 días pero cuando ingresamos activamos la licencia vitalicia



CSRIT-PROYECTO user activation Recibidos ×

CSRIT-PROYECTO <support@luisyadirramirez.freshdesk.com>
para mí

inglés › español Traducir mensaje

Hi LUis Ramirez,

You have been added as an agent in CSRIT-PROYECTO.

Click on the URL below to activate your account:

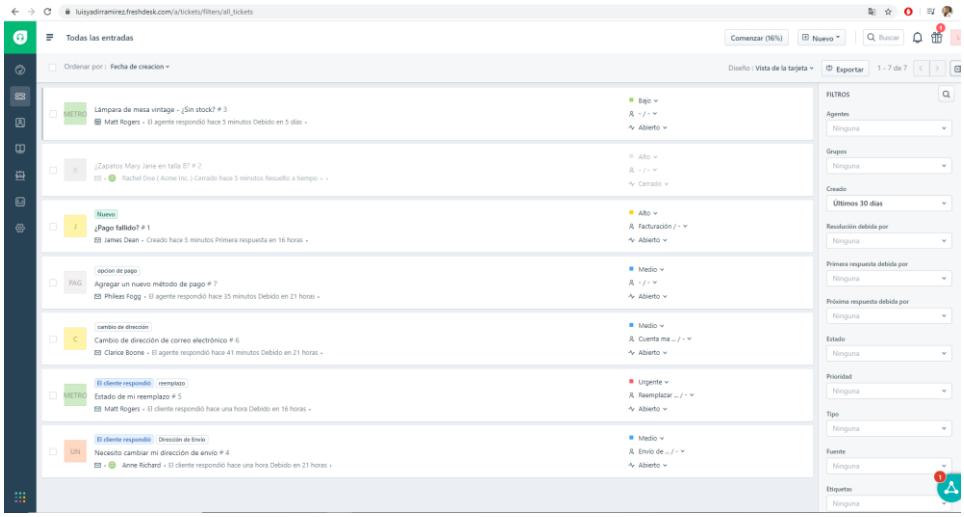
https://luisyadirramirez.freshworks.com/invite/82672d48-d740-4530-9c23-c9747de35e09

If the URL does not work, try copying and pasting it into your browser. If you continue to have problems, please feel free to contact us.

Regards,
CSRIT-PROYECTO

P.S. New to Freshdesk? Learn how to use the helpdesk by enrolling in the Freshdesk Academy.

Este es el entorno de ingreso para la gestión de los tickets y aquí realizamos la activación de la misma



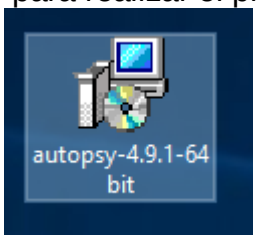
Con esta herramienta podemos desarrollar lo siguiente:
Estos son los beneficios gratis:

✓ Puedes obtener tickets por correo electrónico
✓ Notificaciones automáticas por correo electrónico
✓ Agregar etiquetas a tickets, soluciones y contactos
✓ Combinar tickets
✓ Agregar notas privadas y públicas a los tickets
✓ Exportar tickets

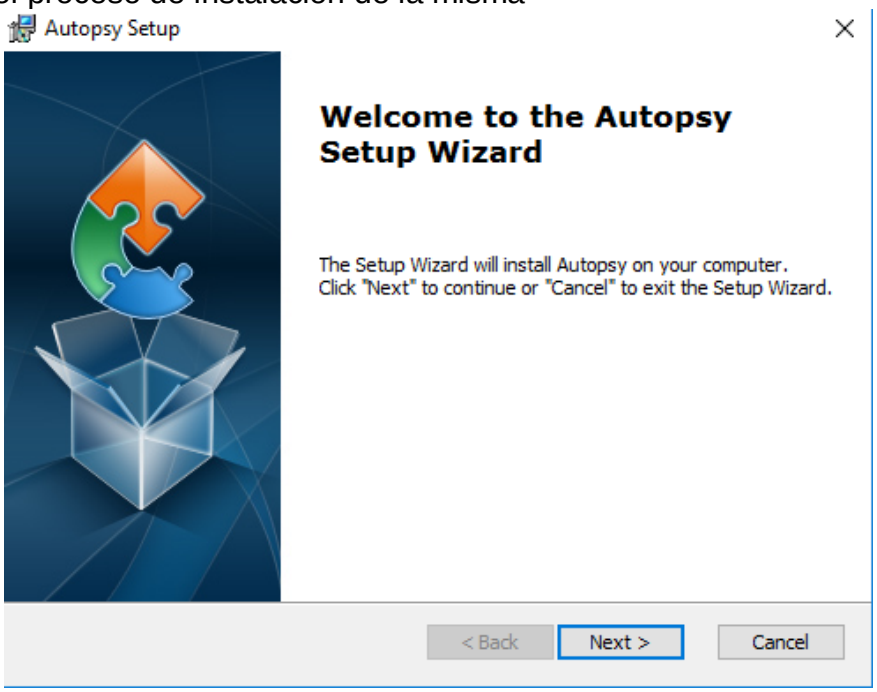
✓ Canal estándar de Twitter
✓ Canal estándar de Facebook
✓ Correo electrónico a base de conocimientos
✓ Capacidad de editar metatítulos, descripciones y palabras claves
✓ Freshdesk para iOS
✓ Freshdesk para Android
✓ Aplicación HTML5 móvil optimizada
✓ Widget de comentarios integrado y emergente personalizable
✓ Rendimiento de agentes y grupos

SERVICIO ESPECIAL DE INFORMÁTICA FORENSE

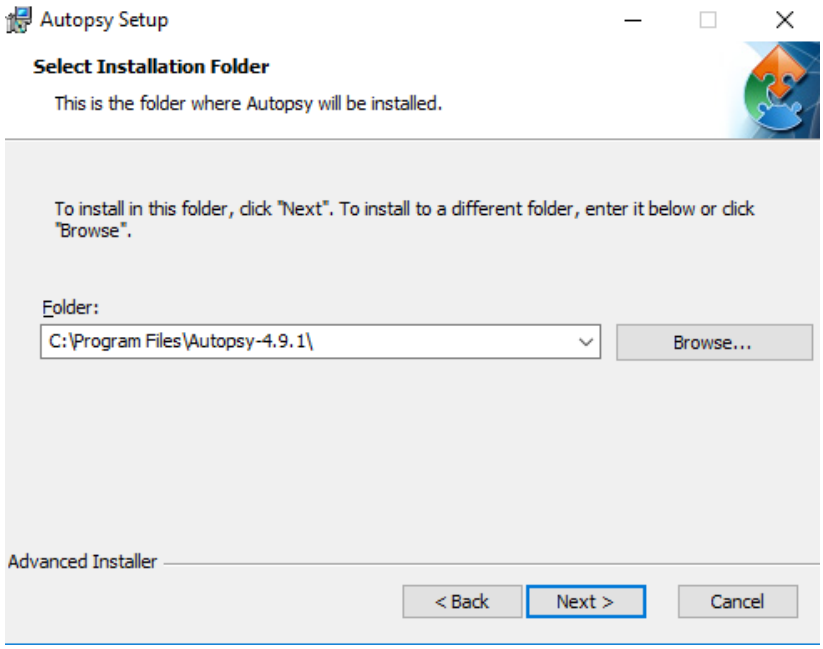
La herramienta que voy a utilizar para realizar el proceso forense es autopsy

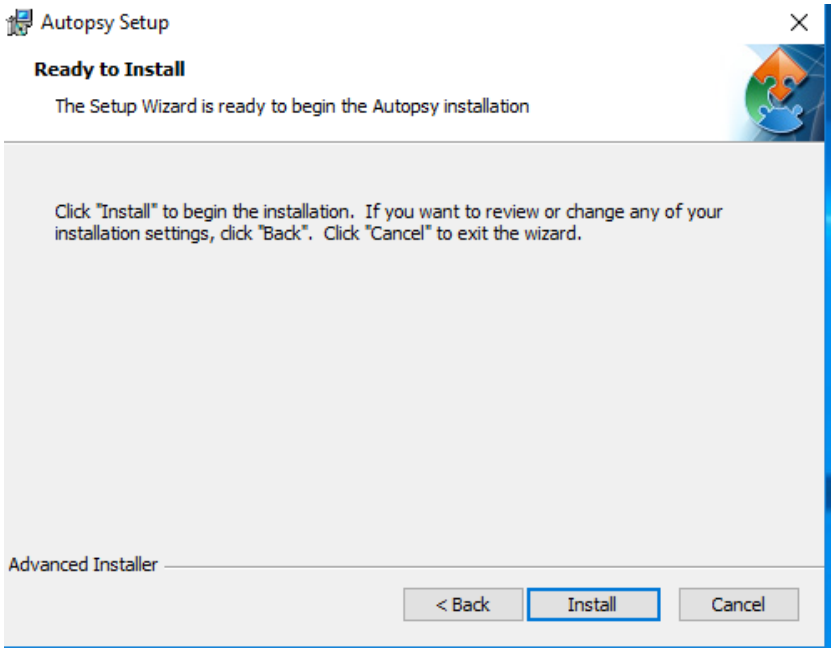


Iniciamos el proceso de instalación de la misma



Damos siguiente para continuar con la instalación del aplicativo





Es una herramienta para realizar el analisis forense

Imagen116: Autopsy

Las ventajas que esta herramienta tiene son las siguientes:

Explorador de datos, files, metadatos, data unit

Con esta gran herramienta podemos analizar una imagen forense, con el propósito de encontrar alguna pista que nos sirva de utilidad en el caso a resolver

Su diseño estructural es poderosamente eficiente.

Soporta el análisis de diferentes sistemas de archivos tales como (NTFS, FAT, UFS1/2, Ext2/3).

Es eficiente para realizar un análisis forense porque cuenta con distintos modos en su configuración.

Permite la validación de la integridad de la imagen, verificando los hashes en md5.

Permite la generación de reportes que son de gran utilidad en hallar las pistas encontradas y realizar su respectivo análisis.

Establece búsquedas de archivos profundamente en todo su sistema de archivos.