Universidad Zaragoza
1542

Trabajo Fin de Grado

Virtualización de un servidor en base a un software libre que cumpla con las STIC de seguridad del CCN

Autor

DAC de Trx. Dª. Cristina Latorre Domec

Directores

Director académico: Dra. Dª. Lacramioara Dranca

Director militar: Cap. de Trx. D. Marco Ondicol Aragonés

Centro Universitario de la Defensa-Academia General Militar

2023

[PÁGINA INTENCIONADAMENTE EN BLANCO]

"La virtualización no es sobre máquinas físicas o incluso software. Se trata de la capacidad humana para ver el mundo de nuevas maneras".

[PÁGINA INTENCIONADAMENTE EN BLANCO]

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a mi familia, en especial a mis padres, por estar siempre ahí y en darme su apoyo incondicional.

En segundo lugar, me gustaría agradecer a la Brigada Aragón I, en especial al Batallón del Cuartel General I por darme la oportunidad de realizar ahí las prácticas, la acogida que me han dado y la ayuda brindada.

En tercer lugar, quisiera dar mi agradecimiento a la Compañía de Transmisiones I por hacerme sentir como un miembro más de la compañía desde el primer día del periodo de prácticas. En especial a su Capitán jefe, el Capitán de Transmisiones Don Marco Ondicol Aragonés, director militar de este trabajo, ya que sin su ayuda y guía no se habría podido realizar el presente trabajo.

En cuarto, y último lugar, me gustaría agradecer a mi directora académica, la Doctora Doña Lacramioara Dranca, la completa disponibilidad para resolver mis dudas y la ayuda prestada.

[PÁGINA INTENCIONADAMENTE EN BLANCO]

RESUMEN

En la actualidad, la Brigada Aragón I posee recursos de hardware que no están siendo utilizados plenamente debido a la falta de licencias de software necesarias para sus operaciones. La implementación del software libre podría resolver esta situación, permitiendo aprovechar al máximo los recursos disponibles y facilitando la ejecución de sus actividades. En la Brigada Aragón I el software libre de virtualización será estudiado como una alternativa válida y gratuita para optimizar el uso de este hardware en lugar de utilizar software con licencia.

Toda organización es recelosa de su seguridad, sobre todo cuando se trata de información sensible, más aún en el caso de una organización de carácter militar como es el Ejército de Tierra. Por ello, toda alternativa que se proponga a los medios actuales debe superar una comparativa en el campo de la seguridad. La virtualización no es una excepción. De hecho, dado que es una tecnología de soporte que alberga otras aplicaciones de carácter crítico, se trata de un elemento en el que la seguridad es si cabe más importante.

En consecuencia, el objetivo de este proyecto es evaluar la viabilidad de implementar un servidor basado en software libre, específicamente Proxmox, que cumpla con los estándares de seguridad establecidos por el Centro Criptológico Nacional (CCN).

Para ello, tras una exhaustiva investigación que incluyó revisión bibliográfica, pruebas y análisis, se probó la posibilidad de adaptar las directrices de seguridad del CCN para VMware, software de virtualización de licencia privada empleado actualmente en la Brigada Aragón I, y Linux para el propuesto software libre de virtualización Proxmox. Se desarrolló una guía basada en las directrices del CCN, adaptadas y aplicadas específicamente a Proxmox.

Como resultado de esta investigación, se ha llegado a la conclusión de que Proxmox es un software libre seguro que puede ser implementado en la Brigada Aragón I y, potencialmente, en otras unidades del Ejército de Tierra, como una solución de virtualización. No obstante, tras una evaluación exhaustiva de las STIC-442 para Vmware y STIC-619 para CentOS, se ha determinado que no satisface los criterios de seguridad establecidos por el CCN, ya que Proxmox carece de ciertas herramientas que son exigidas por las guías.

PALABRAS CLAVE

Virtualización, software libre, Esquema Nacional de Seguridad, Centro Criptológico Nacional, Proxmox.

ABSTRACT

Currently, Aragon I Brigade possesses hardware resources that are not being fully utilized due to the lack of necessary software licenses for its operations. The implementation of open-source software could address this situation, allowing for the maximization of available resources and facilitating the execution of its activities. In Aragon I Brigade open-source virtualization software will be explored as a valid and cost-free alternative to optimize the use of this hardware instead of employing licensed software.

Every organization is cautious about its security, especially when dealing with sensitive information, especially in the case of a military organization such as the Army. Therefore, any proposed alternative to current means must undergo a security comparison. Virtualization is no exception. In fact, as it is a supporting technology for hosting other critical applications, it is an element in which security is even more crucial.

Consequently, the purpose of this project is to assess the feasibility of implementing a server based on open-source software, specifically Proxmox, that complies with the security standards established by the National Cryptologic Center (CCN).

After conducting extensive research which involved literature review, testing, and analysis, we explored the possibility of adapting CCN's security guidelines for VMware, the privately licensed virtualization software being used by Aragon I Brigade, and Linux for the proposed open-source virtualization software, Proxmox. Based on CCN's guidelines, a guide was developed which was specifically tailored to Proxmox.

As a result of this investigation, it has been concluded that Proxmox is a secure open-source software that can be implemented in Aragon I Brigade, and potentially in other units of the land army as a virtualization solution. However, it has been determined that Proxmox lacks a number of security tools required by CCN guidelines, and therefore does not fulfill the criteria for STIC-442 for VMware and STIC-619 for CentOS.

KEYWORDS

Virtualization, free software, National Security Scheme, National Cryptological Center, Proxmox.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

BIOS	Basic Input/Output System
BRIG I	Brigada Aragón I
Cap.	Capitán
CCN	Centro Criptológico Nacional
CIATRANS	Compañía de Transmisiones I
CNI	Centro Nacional de Inteligencia
DAC	Dama Alférez Cadete
DAFO	Debilidades, Amenazas, Fortalezas y Oportunidades
DL	Difusión Limitada
ENS	Esquema Nacional de Seguridad
ET	Ejército de Tierra
IP	Internet Protocol
ISO	Organización Internacional de Normalización
KMS	Key Management System
LXC	Contenedores Linux
OSI	Open Systems Interconnection
Proxmox VE	Proxmox Virtual Environment
RAID	Redundant Array of Independent Disks
RAM	Memoria de Acceso Aleatorio
SSH	Secure Shell
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TCP	Transmission Control Protocol
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Máquina Virtual

1. INTRODUCCIÓN

El trabajo que a continuación se expone fue realizado con motivo de la finalización del Grado de Ingeniería de Organización Industrial (Perfil Defensa) y de las Prácticas Externas realizadas en la Brigada Aragón I, en la CIATRANS I (Compañía de Transmisiones I), en la ciudad de Zaragoza.

1.1 Ámbito de aplicación

Actualmente la Brigada Aragón I, y por extensión otras unidades del ejército cuentan con material hardware desaprovechado que paradójicamente necesitan en la ejecución de sus actividades. Este desaprovechamiento se debe al limitado número de licencias de software[1], mientras que el material en supuesto exceso proviene de las diferentes campañas de actualización. Pese a los esfuerzos de dotar a las unidades con los medios necesarios, estas se encuentran infradotadas y necesitan emplear los medios que en principio han sido sustituidos. Es aquí donde el empleo del software libre puede aportar una solución.

El desarrollo software tradicionalmente ha sido llevado a cabo por corporaciones que mejoran y mantienen sus productos con afán de lucro. Por ello como es lógico, protegen sus activos con licencias que evitan su copia ilegítima. Ante esto, y con la popularización de la computación en las últimas décadas han ido surgiendo comunidades de programadores que realizan tareas similares a las de dichas corporaciones de forma altruista. Si además de esta disponibilidad de adquisición también poseen un código accesible para el usuario, de forma que este puede modificar el código o desarrollarlo se considera software libre. Por tanto, las propiedades que han hecho ganar popularidad a este tipo de software son su prácticamente inexistente coste, el control que tiene el usuario sobre él, y en relación a ello, la flexibilidad y adaptación.

El campo de estudio de este trabajo es la virtualización, por lo que en adelante las referencias que se hagan a software siempre serán relativas a esta tecnología.

La virtualización permite aprovechar los recursos reales para crear entornos virtuales aislados sobre un mismo soporte físico. Para ello administra los recursos y los separa de forma lógica en procesos independientes que se ejecutan con un intermediario que es el software de virtualización (VMware, 2023).

Consecuencia de ello la virtualización tiene ventajas tales como (Ciberseguridad, 2020):

- La mejora en la protección de ataques al hardware[2]. Al ejecutarse en un entorno aislado y no controlar directamente los dispositivos hardware, cualquier ataque cuyo objetivo sea afectar a este se ejecutará en un entorno lógico y no directamente sobre los controladores[3] del dispositivo.

[1] Software. Es el conjunto de instrucciones lógicas que permiten emplear las capacidades del hardware para realizar tareas, tanto visibles y útiles para el usuario, como transparentes a este que forman parte de los procesos del sistema (Cualificaciones, 2023).

[2] Hardware. Es el soporte físico del sistema. Se trata del conjunto de elementos electrónicos interconectados entre sí que permiten el procesado, almacenamiento y transporte de la información en forma de pulsos eléctricos (Cualificaciones, 2023).

[3] Controladores. Comúnmente conocidos como drivers, son software que permiten el control de elementos hardware. No realizan procesos que generen un producto en sí mismo, sino la comunicación entre elementos hardware para integrarlos en el sistema. Ejemplo el teclado, permite realizar entradas al sistema, o el de una memoria externa, que permite la comunicación de esa memoria, mediante la lectura o escritura, pero también los ventiladores del propio ordenador, o la fuente de alimentación, regulando temperatura y tensión respectivamente.

- La mejora de la supervivencia, que es la resistencia de un sistema frente un error que de otra forma provocaría pérdidas irreparables. Esta se debe tanto a la separación de tareas en máquinas independientes, lo cual hace que la pérdida de una no comprometa a las otras, como mediante el uso eficiente de matrices de discos, lo que sería un empleo ineficiente para una única máquina.

- La mejora de la eficiencia, al poder asignar con precisión los recursos disponibles. Esto permite que máquinas físicas de gran capacidad alojen una variedad de máquinas virtuales. Además, la asignación no es rígida, pudiendo cambiarse si las necesidades de una máquina cambian o las condiciones de explotación así lo exigen.

- Escalabilidad. Las máquinas virtuales se pueden clonar, crear una copia exacta de la máquina virtual. Esto aumenta considerablemente la velocidad de configuración en contra parte a la configuración dispositivo a dispositivo que implicaría el uso de máquinas físicas independientes.

A su vez, y de forma complementaria, el campo de este trabajo es el estudio del software libre como alternativa al licenciado.

En convergencia a lo expuesto anteriormente, el software libre de virtualización que será objetivo de estudio en la Brigada Aragón I, como alternativa válida y gratuita al software de virtualización de pago, es el denominado Proxmox VE.

El tratamiento de la información no queda solo en herramientas que facilitan su gestión, sino también en la necesidad de proteger dicha información. Incluso antes de la presencia de tecnologías digitales la información se ha considerado un recurso crítico, más aún en entornos relacionados con la defensa de un Estado. Por ello, el concepto de securización de los sistemas es tan relevante. Un sistema que dé funcionalidades, pero no pueda garantizar la seguridad de su información, pierde su utilidad.

Debido a que el concepto de seguridad total es irreal si existe una comunicación entre máquinas, dado que existe un canal que introduce vulnerabilidad, el concepto de grado de seguridad surge como alternativa al de seguridad plena. A mayor sea el grado de seguridad, más complejo tiende a ser el sistema, al introducir mayor número de elementos de control. Por ello, la seguridad tiene un coste asociado en recursos, bien de forma directa, bien en la pérdida de comodidades, lo que hace necesario determinar el nivel óptimo de seguridad según el sistema que se requiera securizar. En el ámbito administrativo esta realidad requiere de un revestimiento burocrático. A raíz de esto se hace evidente la necesidad de catalogar el nivel de seguridad de un sistema en base a sus requisitos regulatorios y por extensión de la aparición de un organismo que acredite dicho nivel. En España dicho organismo es el Centro Criptológico Nacional (CCN).

El CCN mantiene una actividad de generar unas guías de Seguridad de Tecnologías de la Información y la Comunicación o STIC. Dichas guías consisten primero, en la exposición de unas generalidades sobre el sistema y los requisitos que debe tener para considerarse seguro, para posteriormente desarrollar, hasta el grado de ser instrucciones, la aplicación de dicha configuración. Sin embargo, esa actividad no ha conseguido abarcar todos los sistemas existentes en el mercado. Uno de esos sistemas que aún no poseen una guía de securización por parte del CCN es Proxmox VE, lo cual, entre otras causas, motiva este trabajo.

1.2 Estructura de la memoria

La memoria se estructura en cinco partes:

- **Introducción**: Se plantea la situación de partida poniendo en contexto la razón del desarrollo del trabajo, así como con el ámbito que trata. También se plantea la estructura a seguir.

- **Objetivos, alcance y metodología**: Se describe el objetivo principal con el desglose de los objetivos específicos. Además, se delimita el alcance del trabajo y se indican los métodos de obtención de información, análisis y desarrollo para alcanzar los objetivos.

- **Marco teórico**: En esta sección se presenta una exposición teórica exhaustiva que abarca todos los elementos clave que serán analizados en el contexto de este estudio. La finalidad es proporcionar una base sólida y detallada, que permita comprender en profundidad los conceptos, teorías y enfoques que serán aplicados en la investigación.

- **Desarrollo de análisis y resultados**: Se procede a una exhaustiva exposición de los objetivos específicos, detallando minuciosamente cada uno de ellos junto con el plan de ejecución correspondiente.

- **Conclusiones**: Se presentan todas las restricciones identificadas durante el curso de la investigación, se resume de manera concisa los resultados obtenidos y se evalúa el grado de cumplimiento de los objetivos establecidos inicialmente en el proyecto.

2. OBJETIVOS Y METODOLOGÍA

2.1 Objetivos

El objetivo principal de esta investigación es estudiar la posibilidad de configurar un servidor[4] de virtualización basado en un software libre, en este caso Proxmox VE, que cumpla con las normas e instrucciones el Centro Criptológico Nacional, de tal forma que pueda sustituir o complementar el uso del software de licencia privada dentro de la Brigada Aragón I.

La consecución de este objetivo principal se ha trabajado a partir de los siguientes objetivos específicos:

- Instalar el software de virtualización Proxmox VE en los servidores de los centros de transmisiones, en los cuales, dentro de lo posible, se aplicará la securización.
- Comprobar que tras la aplicación de las medidas de securización no se han perdido las funcionalidades.
- Realizar una guía de securización para el software Proxmox.

2.2 Alcance

Para establecer el alcance de la investigación, la labor de investigación se divide en cuatro fases: Documentación, Estructuración de la información, Análisis de la información y Resultados. Al mismo tiempo, se establecen las siguientes tareas:

- Análisis del funcionamiento del software que se utiliza en la Brigada Aragón I y el software libre propuesto para conocer los conceptos sobre los que se asienta la investigación.
- Pruebas de laboratorio para comprobar en qué medida el software libre se puede configurar para que cumpla con las condiciones de seguridad establecidas por la entidad acreditadora.
- Implementación en el servidor de la Compañía de Transmisiones de la Brigada Aragón I de dicho software de virtualización para extraer conclusiones sobre las necesidades concretas.

[4] Un servidor es un sistema informático que proporciona servicios, recursos, datos o programas informáticos a otros dispositivos. Los servidores están diseñados para gestionar solicitudes, almacenar información y distribuir recursos de manera eficiente a los usuarios o a otros sistemas en la red.

Para exponer el desarrollo temporal de la investigación, se ha confeccionado un diagrama de Gantt explicativo en el que figuran las tareas y etapas de la investigación (ver Anexo I) En la siguiente tabla se observan dichas tareas y etapas:

Tabla 1: Tareas e hitos del Diagrama de Gantt. Fuente: Elaboración propia.

Nº	Nombre
1	Presentación a la Unidad
2	Identificar los objetivos y el alcance de la investigación
3	Documentación
4	Realizar análisis del funcionamiento del software
5	Entregar Propuesta del TFG
6	Estructuración de la información
7	Realización de pruebas de laboratorio
8	Despedida de la Unidad
9	Incorporación a la Academia General Militar
10	Redacción de la memoria
11	Revisiones y correcciones
12	Entrega final

El proyecto comenzó el día 4 de septiembre con la presentación al Teniente Coronel jefe del Batallón del Cuartel General de la Brigada Aragón I. Finalmente, dicho proceso de investigación concluye el 24 de noviembre con la finalización de la redacción de la memoria.

2.3 Metodología

Para la consecución de los principales hitos se empleará como principal método cualitativo la experimentación. Se realizará la configuración siguiendo las formas que admite el entorno de trabajo de Linux y el empleo de algunas guías de otros software como modelo.

En cuanto a los recursos empleados para la investigación se ha tenido acceso en todo momento a manuales y publicaciones de la materia. También, continuamente se ha consultado y entrevistado al personal y los expertos que componen la CIATRANS I. Finalmente, cabe destacar la integración en el régimen de trabajo y la realización de ejercicios de instrucción con dicha Compañía, con el correspondiente acceso a todo su personal, medios y conocimiento.

Otros métodos de análisis cualitativos como el análisis de debilidades, amenazas, fortalezas y oportunidades (DAFO) o herramientas de gestión como el diagrama de Gantt se han empleado desde el primer momento en la toma de decisiones sobre los objetivos y alcance del proyecto.

3. MARCO TEÓRICO

3.1 Fundamentos de virtualización

Para comprender la virtualización hay que tener claro el concepto de máquina virtual frente a real. Una máquina virtual tiene que ser capaz de hacer las mismas funciones que haría una maquina real con la diferencia de que la máquina virtual no existe de la misma forma que la real.

Aunque es incorrecto decir que una máquina virtual no existe físicamente, dado que sí emplea recursos cuyo soporte es físico, es una imagen reduccionista pero práctica para comprender que se trata de una máquina que existe de forma lógica (Romero, 2011).

Existen varios tipos de virtualización, en el que cada uno sirve para satisfacer unas necesidades. Entre los más comunes destacan la virtualización de servidores, el cual permite ejecutar múltiples sistemas operativos y aplicaciones en un solo servidor físico, y la virtualización a nivel de sistema operativo[5] (Contenedores) que permite ejecutar múltiples instancias aisladas de un sistema operativo en un solo host físico. A diferencia de las máquinas virtuales, los contenedores comparten el mismo kernel del sistema operativo subyacente, lo que los hace más ligeros y rápidos. El kernel es el núcleo del sistema operativo que controla y coordina todas las actividades del sistema, permitiendo una interacción suave y segura entre el hardware y el software.

Un contenedor se refiere a una unidad de software que encapsula una aplicación y todas sus dependencias, incluyendo bibliotecas, herramientas y configuraciones necesarias para que la aplicación se ejecute en cualquier entorno operativo (ver Figura 1).

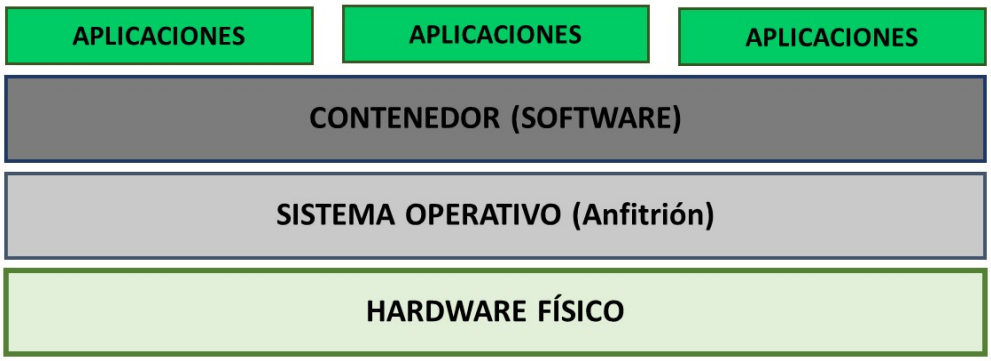

Figura 1. Esquema de un contenedor informático. Fuente: Elaboración propia

Entonces, la pregunta natural es: ¿Cuál es la ventaja de virtualizar? Si de todas formas se está empeñando una máquina física y se están bloqueando sus recursos. La respuesta a esta pregunta es triple:

1. La subsistencia de la máquina, al poder esta almacenarse en imágenes (copia en código binario).

2. La seguridad, al poder proteger el soporte hardware de un ataque a sus controladores, así como tener un mayor control a los canales de acceso.

[5] Sistema Operativo. Es el conjunto de instrucciones lógicas y controladores básicos que permiten el funcionamiento de otros programas al manejar el acceso a discos, memorias y procesadores, así como los periféricos elementales de entrada y salida.

3. La asignación eficiente de recursos al poder dimensionar la máquina a sus necesidades, por pequeñas que sean, sin empeñar en ellas toda la potencia de una máquina física.

La Figura 2 es un esquema de una máquina virtual en el que se observa que dentro del software de virtualización se crean las máquinas virtuales, en la que cada una de ellas se le puede asignar los recursos que estas necesiten, siendo independientes unas de otras.

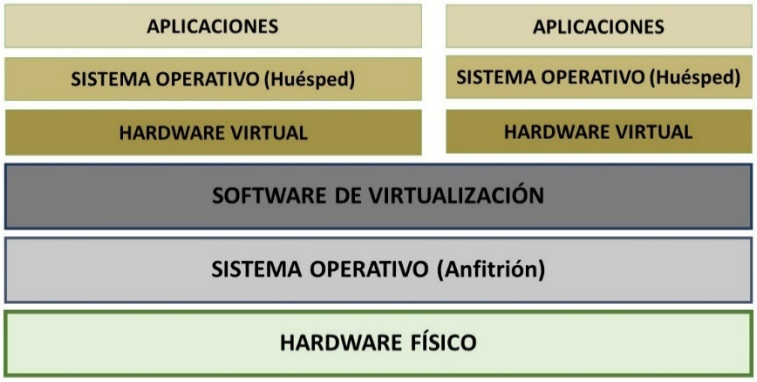

Figura 2. Esquema de una Máquina Virtual. Fuente: Elaboración propia.

Tanto las máquinas virtuales como los contenedores están controladas por un hipervisor (Hat, 23 de marzo de 2023). Un hipervisor es una capa de software de virtualización que permite crear, administrar y ejecutar varias máquinas virtuales dentro de un único servidor, así como diferentes sistemas operativos.

El hipervisor se encarga de separar los recursos de la máquina virtual del sistema de hardware y de distribuirlos adecuadamente (ver Figura 3).

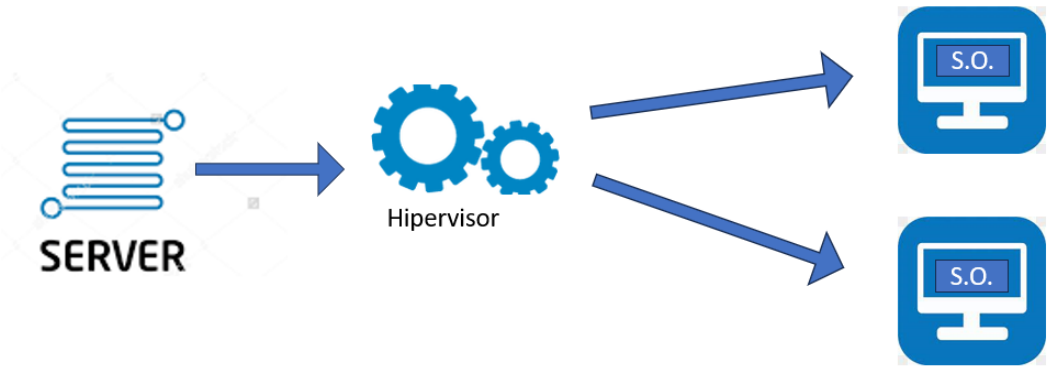

Figura 3. Esquema de un hipervisor. Fuente: Elaboración propia.

Dentro de los recursos más críticos por velocidad de servicio está la lectura y escritura de disco. La virtualización permite aprovechar al máximo una de las soluciones que hay a esta problemática, las RAIDs (Redundant Array of Independent Disks o Redundant Array of Inexpensive Disks) de discos.

RAID es una tecnología de almacenamiento que combina múltiples discos duros en un solo sistema de almacenamiento para mejorar el rendimiento, la redundancia y/o la capacidad de almacenamiento. En un hipervisor, la configuración RAID se utiliza para los discos que almacenan las máquinas virtuales y otros datos críticos del sistema. La elección del nivel de RAID depende de los requisitos específicos de rendimiento, redundancia y capacidad de almacenamiento del entorno virtualizado (Garcia, 2023).

La RAID en un hipervisor se utiliza para mejorar la confiabilidad y la disponibilidad del sistema, así como para proporcionar una mejor capacidad de recuperación en caso de fallo de disco.

3.2 Software de virtualización con licencia privada: VMware

El software de virtualización VMware EXSi 7.0 se utiliza en la Brigada Aragón I para la realización de las maniobras en las cuales se tienen que ofrecer unos servicios. VMware ofrece un software para crear y gestionar máquinas virtuales en las cuales se ejecutan las aplicaciones necesarias para ofrecer los servicios requeridos por el jefe.

Respecto a su facilidad de uso y sus funcionalidades, ofrece características clave como migración para mover máquinas virtuales sin tiempo de inactividad y alta disponibilidad para reiniciar automáticamente máquinas virtuales en hosts alternativos en caso de fallo. También permite instantáneas[6] y clonación para facilitar la recuperación y el despliegue rápido.

VMware contiene algunos inconvenientes o desventajas para el uso que se da en el Ejército como: su naturaleza propietaria que conlleva altos costos, especialmente para las organizaciones que necesitan funciones avanzadas y soporte. Además, para aprovechar sus capacidades, se necesitan servidores específicos, lo que implica costos adicionales. A pesar de tener una interfaz amigable, su configuración avanzada puede ser compleja, requiriendo habilidades técnicas (VMware, 2023).

3.3 Software de virtualización libre: Proxmox VE

Proxmox Virtual Environment (Proxmox VE) es software de virtualización de código abierto basado en Debian Linux. Combina tecnologías de virtualización como máquinas virtuales (VM) y contenedores Linux (LXC) en un solo sistema, lo que permite a los usuarios crear y gestionar entornos virtuales de manera eficiente.

Proxmox VE incluye funcionalidades avanzadas como migración[7] de máquinas, alta disponibilidad y almacenamiento definido por software[8], lo que la convierte en una opción popular para entornos empresariales y de desarrollo. Al ser de código abierto, Proxmox VE es gratuito y ofrece una alternativa económica y versátil para la virtualización (GmbH., 2023).

Proxmox es el software libre propuesto en la CIATRANS I. Este ofrece una serie de ventajas respecto al software de VMware ESXi 7.0 entre las cuales destacan:

- En primer lugar, que es una solución de código abierto y gratuita, eliminando costos de licencia, a diferencia de VMware.

---

[6] Instantánea: es una copia del estado actual de una máquina virtual o de un sistema informático en un momento específico. Esta instantánea incluye el estado de la memoria, el disco duro virtual y otros dispositivos virtuales en ese punto particular en el tiempo. Al tomar una instantánea de una máquina virtual, se crea un punto de restauración que permite a los usuarios revertir la máquina virtual a ese estado específico en caso de problemas o para realizar pruebas sin afectar el entorno de producción.

[7] Migración: proceso de transferir sistemas o aplicaciones de software de una máquina o entorno de hardware a otro. Esto puede implicar la transferencia de datos, configuraciones, software y otros recursos.

[8] Almacenamiento definido por software (SDS). es una tecnología que permite gestionar el almacenamiento de datos utilizando software en lugar de depender exclusivamente del hardware de almacenamiento tradicional

- En segundo lugar, Proxmox ofrece flexibilidad al admitir tanto máquinas virtuales como contenedores Linux, mientras que VMware se centra en máquinas virtuales. Además, Proxmox destaca por su interfaz de usuario intuitiva y fácil configuración y su comunidad activa que brinda soporte y contribuye a mejoras continuas.

- En tercer lugar, ofrece una robusta escalabilidad[9] y alta compatibilidad con una amplia gama de hardware y sistemas operativos para instalar a modo de máquina virtual, lo que lo convierte en una opción versátil para entornos virtuales.

3.4 Esquema Nacional de Seguridad.

El Esquema Nacional de Seguridad o ENS es una normativa que tiene como objetivo establecer los principios que regulan y aseguran el acceso, integridad, disponibilidad y veracidad de la información empleada en medios electrónicos en o relacionados con las Administraciones Públicas (CCN., 2023)

El Esquema Nacional de Seguridad de España tiene seis objetivos principales:

- Crear las condiciones necesarias de confianza para el uso de los medios electrónicos por parte de los ciudadanos en su relación con las Administraciones Públicas.

- Introducir elementos y metodologías comunes en materia de seguridad de las tecnologías de la información para las Administraciones Públicas.

- Aportar un lenguaje común para facilitar la interacción entre las diferentes Administraciones, así como la comunicación de los requisitos de seguridad de la información a la Industria.

- Promover la gestión continua de la seguridad.

- Promover la prevención, detección y corrección para mejorar la resiliencia ante ciberamenazas y ciberataques.

- Servir como modelo de buenas prácticas.

El ENS establece tres niveles de seguridad:

1. Bajo: Este nivel se aplica a sistemas y servicios que manejan información no clasificada pero que requieren una protección adecuada contra amenazas comunes y ataques sencillos. Es el nivel mínimo de seguridad establecido por el ENS y se enfoca en medidas básicas para garantizar la confidencialidad, integridad y disponibilidad de la información.

2. Medio: Este nivel se aplica a sistemas y servicios que manejan información sensible y requieren una protección más avanzada contra amenazas y ataques. Se centra en medidas de seguridad adicionales para proteger la información clasificada y garantizar un nivel de seguridad adecuado frente a amenazas moderadas.

3. Alto / Difusión limitada: Este nivel se aplica a sistemas y servicios que manejan información clasificada o que son considerados críticos para la seguridad nacional. Requiere medidas de seguridad muy robustas para proteger la información altamente sensible contra amenazas avanzadas y ataques sofisticados. Este nivel de seguridad es el más alto establecido por el ENS y exige una protección extensiva y medidas de control muy rigurosas.

Estos niveles de seguridad del ENS proporcionan un marco para evaluar y clasificar la seguridad de los sistemas y servicios electrónicos en España, asegurando que se apliquen las

[9] Escalabilidad: capacidad de un sistema, aplicación o red para manejar un crecimiento incremental de carga de trabajo o usuarios sin sacrificar el rendimiento.

medidas de seguridad adecuadas en función del nivel de sensibilidad de la información que manejan.

La información clasificada es: “información relativa a materia clasificada como secreta o confidencial, cuya revelación puede causar perjuicio al titular de la información, especialmente si se trata de información que puede afectar a la seguridad del Estado.”

Los grados de clasificación de la información clasificada en España, de mayor a menor son:

- Secreto (S)
- Reservado (R)
- Confidencial (C)
- Difusión Limitada (DL)

3.5 Centro Criptológico Nacional

El Centro Criptológico Nacional (CCN) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo (CCN-CERT, 2023).

El Centro Criptológico Nacional (CCN) fue establecido en 2004 y está afiliado al Centro Nacional de Inteligencia (CNI). La Ley 11/2002, del 6 de mayo, que regula el CNI, confiere a este centro la responsabilidad de gestionar las funciones relacionadas con la seguridad de las Tecnologías de la Información y la protección de información clasificada.

Por lo tanto, su objetivo principal es mejorar la seguridad cibernética en España. Funciona como el centro nacional de alerta y respuesta, colaborando para responder de manera veloz y eficaz a los ciberataques y abordando activamente las amenazas cibernéticas. Esto incluye coordinar a nivel estatal las diferentes capacidades de respuesta a incidentes y centros de operaciones de ciberseguridad ya existentes.

Todo esto se hace con el propósito final de lograr un ciberespacio que sea más seguro y fiable. Esto implica la protección de información clasificada, según lo establecido en el artículo 4.F de la Ley 11/2002, así como de la información sensible. Además, se trabaja en la defensa del Patrimonio Tecnológico de España, en la capacitación de profesionales expertos, en la implementación de políticas y procedimientos de seguridad, y en la utilización y desarrollo de tecnologías más apropiadas para alcanzar estos objetivos (BOE, 2002).

En las responsabilidades del Centro Criptológico Nacional se incluye la coordinación, fomento y creación de soluciones que aseguren la seguridad de los sistemas y mejoren la administración de la ciberseguridad en todas las organizaciones, facilitando así una defensa más efectiva contra los ciberataques.

STIC DE SEGURIDAD DEL CCN

Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT, que es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del CCN (CCN-CERT, 2023).

Existen diferentes series de STIC, cada una de ellas se centra en un sistema operativo o software en el que se explica el procedimiento para poder aplicar la seguridad requerida.

La Serie CCN-STIC-600 establece las configuraciones mínimas de seguridad de otras tecnologías como Linux, entre otras. En concreto la serie CCN-STIC 619B tiene interés para este trabajo, establece la configuración segura de CentOS Linux, en la cual se basará la securización de Proxmox, al ser este un hipervisor basado en Linux.

También tiene interés para este trabajo la serie CCN-STIC 442, guía de seguridad para VMware, en busca de similitudes que puedan resultar relevantes a la hora de securizar un hipervisor.

Para comprobar que las STIC se han aplicado de forma correcta, el CCN tiene diversas soluciones. Entre ellas, se encuentra la herramienta de CLARA (CCN-CERT, 2023), solución que se intentará aplicar en el proyecto.

CLARA es una herramienta para analizar las características de seguridad técnicas definidas a través del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3.6 Modelo OSI

El modelo abierto de interconexión de sistemas o por sus siglas en inglés OSI (Open Systems Interconnection) es un marco de referencia que permite comprender la forma en que se comunican las maquinas. Aunque este está dividido en siete capas, hay capas más complejas que pueden tener varios protocolos que trabajan de forma jerarquizada, lo que podría entenderse como capas independientes. Es por esto por lo que debe entenderse este modelo como un marco y no como un dogma. En la Figura 4 se ven las diferentes capas en la que está dividido el modelo, siendo el nivel físico la capa 1 y el nivel de aplicación la capa 7.

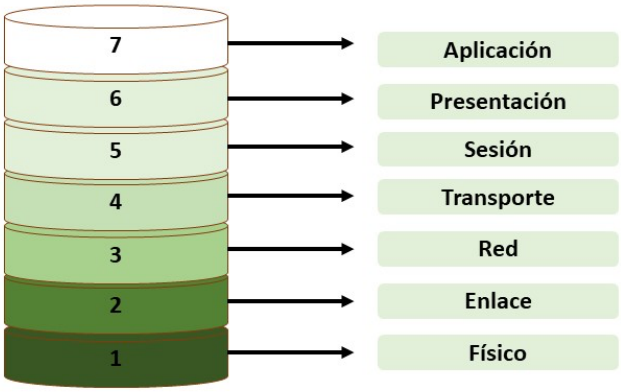

Figura 4. Esquema de modelo OSI. Fuente: Elaboración propia

En este modelo la capa 1 es la que engloba todos los medios físicos, los protocolos que regulan la forma de los conectores, las frecuencias en la comunicación inalámbrica, los voltajes. Mientras que el resto de las capas, de la 2 a la 7 van profundizando en la complejidad de la información que aportan, desde el enlace entre dispositivos, hasta la información útil que emplea la aplicación.

Dentro de este marco las capas que más interesan de cara a la seguridad son:

- La capa 1 (nivel físico), protegiendo el dispositivo de conexiones no autorizadas. Esta capa se encuentra en la parte inferior del modelo OSI (ver Figura 7). Es la encargada de la transmisión física de datos sobre un medio de comunicación, como cables de cobre, fibra óptica o señales inalámbricas.

- La capa 3 (nivel de red), configurando su red para que ignore las peticiones o las respuestas cuyo origen no sea conocido. Su misión es hacer llegar la información a la red adecuada y dentro de esta al dispositivo destino, aunque este último paso sería más responsabilidad de la capa 2 o de enlace. El protocolo más utilizado en esta capa es el protocolo de internet o IP por sus siglas en inglés. Este protocolo encapsula la información de las capas superiores y le añade una cabecera para indicar la dirección de origen y destino. Los elementos de red solo leen esta cabecera y si no son ellos el destino ignoran el contenido del resto del mensaje.

- La capa 4 (nivel de transporte), que es la encargada del flujo de datos y de la distribución de la información a los procesos adecuados. Una vez la información llega al dispositivo correcto, se debe distinguir qué proceso necesita de esa información, puede pertenecer a una petición de información web o un correo, entre muchos otros. Para distinguir a quien va destinado la capa cuatro añade su propia cabecera, similar a la capa 3, pero en este caso identifica el puerto TCP o UDT que ha solicitado la información o que permanece a la escucha según el protocolo. Como se puede observar, la capa transporte incorpora un gran abanico de conceptos que es menester desarrollar debido a la necesidad de comprender adecuadamente el concepto de puerto para poder realizar un adecuado análisis de la seguridad, que es el objeto de este estudio (Lopera, 2023)

4. DESARROLLO: ANÁLISIS Y RESULTADOS

4.1 Análisis de la problemática

En la actualidad la Brigada Aragón I emplea en sus servidores de virtualización software de licencia privada como es el VMware. El uso de estos servidores con esta característica no supone un problema de funcionabilidad, dado que cumple con las exigencias de seguridad y proporciona el servicio que requiere. Sin embargo, el alto número de servidores en desuso, para los cuales no se tienen las licencias necesarias para este software privado, supone un problema.

Ante esta situación cabe plantearse el uso del software libre Proxmox como alternativa a la hora de explotar estos servidores, por lo que se ha realizado un análisis de Debilidades, Amenazas, Fortalezas y Oportunidades (DAFO).

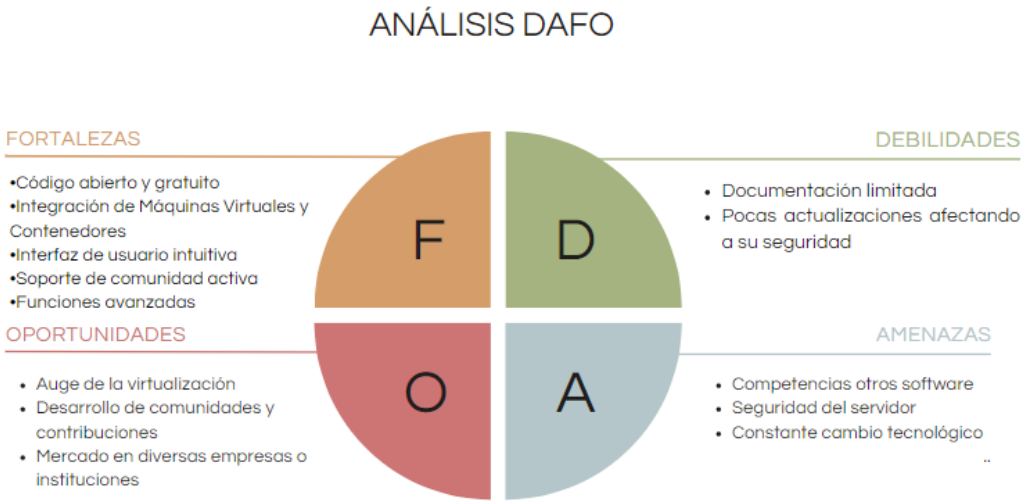

Figura 5. Análisis DAFO del uso del software de virtualización Proxmox. Fuente: Elaboración propia.

En base al análisis interno del análisis DAFO, como se observa en la Figura 5 podemos extraer las siguientes fortalezas acerca del software libre.

- Código abierto y gratuito: Al ser software libre, Proxmox cuenta con una comunidad activa de usuarios y desarrolladores. Esto facilita el soporte técnico, la resolución de problemas y la colaboración en el desarrollo continuo.

- Integración de Máquinas Virtuales y Contenedores: Proxmox ofrece una flexibilidad al admitir tanto la virtualización de máquinas como de contenedores. Esto permite a los usuarios adaptar la plataforma a sus necesidades específicas y escalar fácilmente según los requisitos del entorno.

- Interfaz de uso intuitiva: La interfaz de usuario de Proxmox proporciona una experiencia de usuario amigable que facilita la administración de recursos y la supervisión del rendimiento de las MV y contenedores.

- Soporte de comunidad activa: Proxmox aprovecha la fuerza de una comunidad activa de usuarios y desarrolladores. Esto no solo garantiza un soporte sólido, sino que también fomenta la colaboración y la mejora continua del software.

- Funciones avanzadas: Proxmox incluye herramientas integradas para realizar copias de seguridad y restaurar MV y contenedores de manera eficiente. Esto es esencial para garantizar la disponibilidad y la integridad de los datos en entornos de virtualización.

De tal forma se extraen las siguientes oportunidades acerca del software Proxmox:

- Auge de la virtualización: Debido a su capacidad para optimizar recursos hardware, ha mejorado la eficiencia, la reducción de costes y ha facilitado la gestión de infraestructuras tecnológicas.

- Desarrollo de comunidades y contribuciones: La comunidad de Proxmox y los desarrolladores tienen la oportunidad de crear complementos y extensiones que amplíen las funcionalidades de la plataforma. Esto podría mejorar su versatilidad y atraer un conjunto más amplio de usuarios.

- Mercado en diversas empresas o instituciones: Proxmox presenta oportunidad significativa para ser adoptado por empresas, o en este caso por instituciones, que buscan soluciones de virtualización económicas y flexibles.

Las debilidades que se extraen del análisis DAFO de Proxmox son las siguientes:

- Documentación limitada: La falta de recursos detallados dificulta la comprensión y la resolución de problemas para nuevos usuarios. La dependencia de la comunidad para obtener información específica afectando en la experiencia del usuario causa una debilidad en la adopción del software. La identificación de esta debilidad se ha derivado de la observación directa, ya que los expertos en el área de información de la Brigada Aragón I no disponen de ningún tipo de documentación acerca de Proxmox.

- Pocas actualizaciones afectando a su seguridad: La falta de actualizaciones regulares podría dejar el sistema vulnerable a la seguridad. La no aplicación oportuna de estas actualizaciones podría comprometer la integridad y escalabilidad del sistema.

Las amenazas extraídas del análisis son las siguientes:

- Competencias a otros software: La competencia con soluciones de virtualización propietarias, como VMware, puede representar una amenaza para la adopción de Proxmox en entornos empresariales, donde la preferencia por proveedores establecidos y confiables es común.

- Seguridad del servidor: Las preocupaciones de seguridad y cumplimiento asociadas con el código abierto podrían ser una amenaza en entornos que requieren auditorías y cumplimiento estricto, como es el caso del ET. La percepción de menor seguridad podría afectar la adopción de Proxmox.

- Constante cambio tecnológico: La rapidez con la que evolucionan las tecnologías de virtualización puede representar una amenaza si Proxmox no puede adaptarse rápidamente a las nuevas tendencias y tecnologías emergentes.

Como podemos extraer del análisis interno DAFO, las fortalezas responden al problema expuesto, por lo que debe estudiarse si la amenaza de seguridad se puede solventar o no.

Para ello se ha procedido a la instalación del software de virtualización Proxmox en uno de los ordenadores prestados por la CIATRANS I de la BRI I.

El nivel se securización empleado en el presente trabajo es el de difusión limitada. Este nivel se considera el nivel más alto del ENS. Esta elección se debe a que las únicas guías accesibles para aplicar esta seguridad son las STIC establecidas por el ENS, dado que las de la información clasificada son de uso oficial interno para las Fuerzas Armadas.

4.2 Instalación del servidor

Para instalar Proxmox, es necesario contar con la imagen del sistema en formato .iso. El primer paso implica obtener esta imagen desde el sitio web oficial de Proxmox. Posteriormente, se debe preparar un dispositivo de memoria de arranque[10] utilizando esta imagen. Este dispositivo actuará como la fuente de carga del sistema en lugar del sistema operativo preexistente en el ordenador o del firmware[11] por defecto. Para llevar a cabo este proceso, se utiliza el software Rufus, que permite configurar una memoria flash[12] USB[13] para que funcione como dispositivo de arranque, acción conocida como "bootear". En el Anexo II se explica detalladamente.

Una vez que la memoria flash ha sido configurada como dispositivo de arranque, se inserta en el ordenador en el que se planea instalar Proxmox y se inicia el sistema. Es crucial ingresar a la BIOS[14] del ordenador para evitar que el sistema operativo predeterminado tome el control del proceso de arranque. La forma de realizar esta acción varía según el modelo del ordenador, pero por lo general, cada fabricante designa una tecla específica para acceder a la BIOS. En el caso de este trabajo, el ordenador es de marca HP, y se accede a la BIOS mediante la tecla F10.

Una vez que el sistema arranca desde el dispositivo de memoria de arranque, se procede a configurar los parámetros de instalación solicitados por el sistema.

Es importante remarcar los requisitos mínimos del sistema. Para ello no se debe tener en cuenta solo los exigidos por el hipervisor, sino también los recursos que se le van a asignar a las máquinas.

Estos requisitos hardware mínimos del sistema donde se va a instalar Proxmox son:

- Procesador en 64bits, de preferencia con múltiples núcleos
- Placa Base con soporte para virtualización.
- 2 GB en RAM
- Discos duros rápidos
- Soporte para RAID por hardware
- Tarjetas de red Gbit

Se debe de sumar la RAM de las máquinas virtuales que se van a crear.

En este caso el software ha sido instalado en un ordenador HP 15s cuyas características técnicas son:

- Procesador Intel Core i5 1355u
- Memoria RAM de 16 GB

---

10 Memoria de arranque: es un tipo de memoria que almacena el firmware de inicio, conteniendo las instrucciones fundamentales para iniciar el sistema operativo y permitir el funcionamiento del dispositivo al ser encendido. Es esencial para la inicialización del hardware y el proceso de arranque del sistema.

11 Firmware. Es un software que está grabado de forma física en ciertos componentes, permitiendo las funciones fundamentales para la unión de hardware y software.

12 Memoria flash: es un tipo de memoria no volátil que retiene datos incluso cuando la energía se corta.

13 USB. Por sus siglas en inglés bus en serie universal. Se trata de un protocolo de conexión en serie. Define tanto el formato lógico de entrega como la forma de las conexiones físicas.

14 BIOS. Por sus siglas en inglés sistema básico de entrada y salida. Es el firmware básico que permite el control de las instrucciones elementales del sistema hardware. Acceso a discos, memoria, órdenes de lectura y escritura.

- Disco duro con capacidad de 1TB

4.2.1 Configuración inicial

Al iniciar Proxmox VE se deben configurar unos parámetros iniciales individuales para cada usuario.

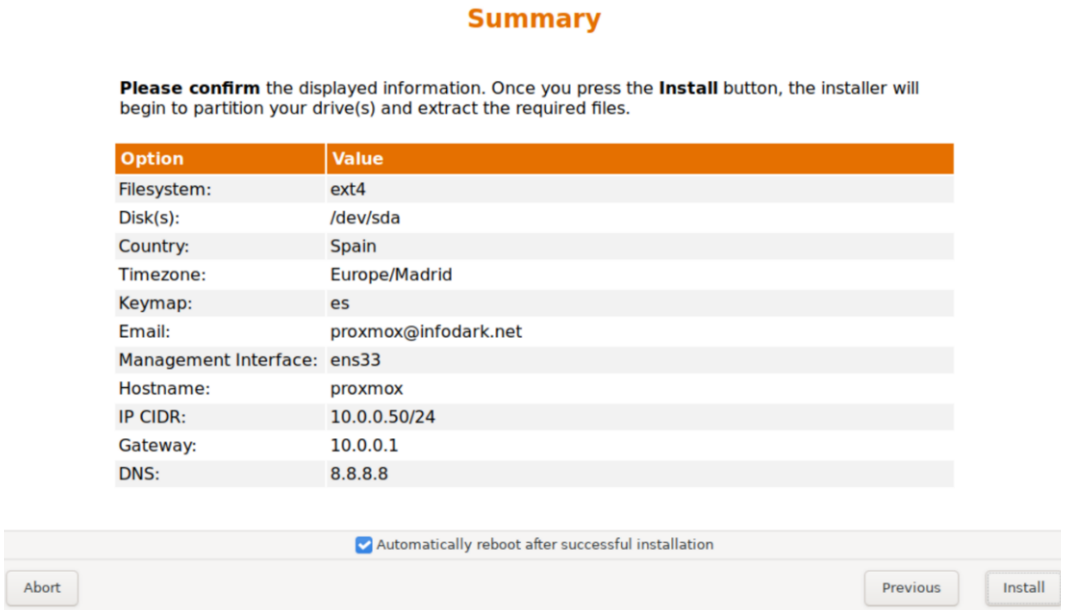

Figura 6. Resumen de los parámetros iniciales de la instalación de Proxmox. Fuente: Elaboración propia.

Es necesario especificar la ubicación, disco de instalación, datos para la cuenta de administrador y configuración de red. Posteriormente el instalador completará la instalación en automático. Como se observa en la Figura 6 se han introducido unos parámetros de idioma, país y región. Además, en este caso el servidor ha sido instalado en el disco sda, este es el primer disco duro del sistema.

Además, se debe configurar una dirección IP para identificar al servidor en la red, de forma que sea accesible. Se debe establecer su Gateway, que es el puerto de salida, establecido por defecto. En este caso como se muestra en la Figura 6, la dirección dada al servidor es 10.0.0.50/24. Esta dirección IP usa el sistema CIDR, empleado para asignar y gestionar direcciones IP. Este sistema representa la dirección IP y la máscara de subred, que se encuentra separada por una barra. Esta máscara determina qué parte de una dirección IP se utiliza para identificar la red y qué parte se reserva para identificar dispositivos individuales en esa red. En este caso la mascará de subred es la 24. Estas direcciones IP a utilizar son públicas, es decir, son visibles por internet. El rango a utilizar IP es libre, por lo cual no se tienen que emplear ninguna dirección específica.

Una vez instalado nos dirige a la consola, en la que nos muestra la dirección IP que se había introducido anteriormente. En dicha dirección se observa el puerto 8006, establecido por defecto. Dicho puerto se utiliza para dirigir el tráfico de red a un servicio específico. Véase Figura 7.

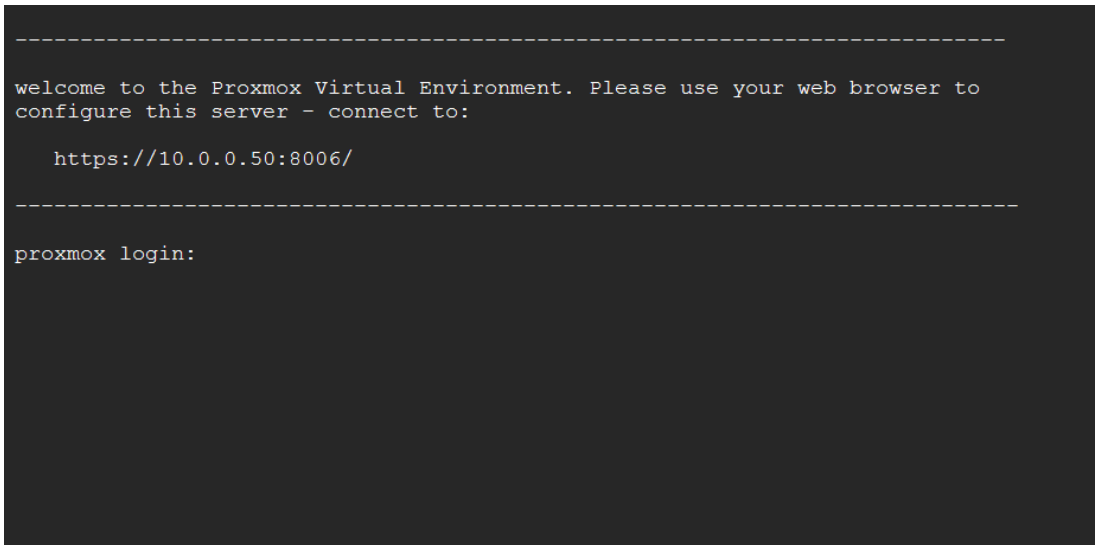

Figura 7. Consola al finalizar la instalación del servidor Proxmox. Fuente: Elaboración propia.

La configuración se realiza vía web utilizando la dirección IP que se indica al finalizar la instalación. Hay que utilizar el usuario root[15] y la contraseña que se indicó.

A la aplicación web que controla el hipervisor se accede a través del navegador, con la dirección IP que se configuró en la instalación con ese propósito. El acceso se realiza de forma remota empleando otro ordenador en modo de administrador. La conexión entre el ordenador servidor y el administrador ha sido a través de un cable UTP (Unshielded Twisted Pair), el cual se utiliza en el estándar ethernet para interconexión de dispositivos de red, que tiene cuatro pares de dos conductores eléctricos aislados y entrelazados para anular las interferencias, con conector RJ45, que es un estándar de capa física para la conexión mediante cable de cobre de 8 hilos. Como se muestra en la Figura 8, al introducir la dirección IP nos dirige a la página de inicio de Proxmox, a través de la cual se crean las máquinas virtuales y la posterior securización.

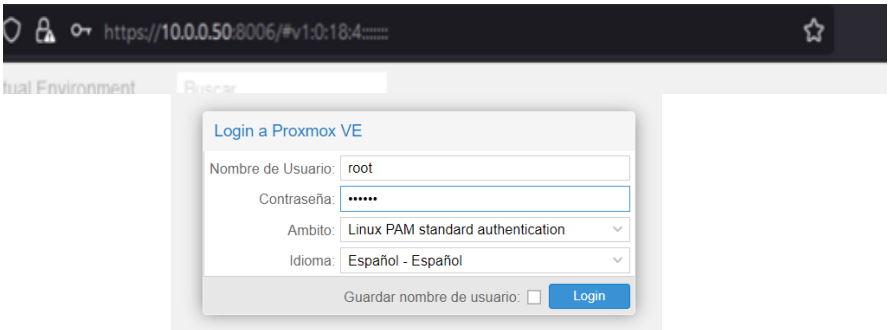

Figura 8. Usuario y contraseña para introducir de la página inicial de Proxmox. Fuente: Elaboración propia.

4.3 Creación de las máquinas virtuales

[15] Usuario root: usuario administrador principal del sistema.

Como se mencionó anteriormente, Proxmox es una plataforma de virtualización que permite la creación de máquinas virtuales y contenedores. Para este proyecto, se optó por utilizar sistemas operativos de código abierto en las máquinas virtuales para promover el uso de herramientas de distribución libre y aprovechando que no necesitan licencia. Dentro de las opciones de sistemas operativos Linux, se eligió la distribución Fedora debido a su interfaz gráfica ligera y eficiente en el consumo de recursos.

El enfoque de este trabajo se centra en securizar el servidor, lo que implica establecer configuraciones seguras para las relaciones entre las máquinas. Para llevar a cabo las pruebas, se han creado dos máquinas virtuales basadas en Fedora Linux.

El primer paso para crear las máquinas virtuales es contar con la imagen del sistema operativo en formato .iso. La carga de esta imagen .iso en el servidor Proxmox es un proceso intuitivo que se realiza a través del menú gráfico proporcionado por el hipervisor.

Una vez que la imagen .iso se encuentra en Proxmox (ver Figura 9), se procede a seleccionar la opción de crear una nueva máquina virtual en la pestaña correspondiente. Dentro de esta pestaña se presentan todos los parámetros que se pueden configurar para la nueva máquina virtual. Estos parámetros pueden diferir para cada máquina virtual específica. En este escenario, se han configurado dos máquinas virtuales con sistema operativo Linux, dotadas cada una de un núcleo de procesador y una memoria de 2048 MB.

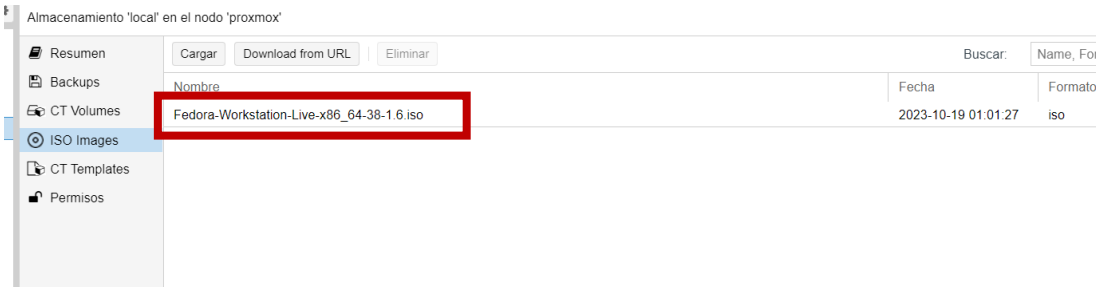

Figura 9. Cargar la imagen .iso Fedora en el servidor Proxmox. Fuente: Elaboración propia.

Tal como se indica en la Figura 10, se presenta una síntesis de todos los parámetros que han sido establecidos para las máquinas mencionadas.

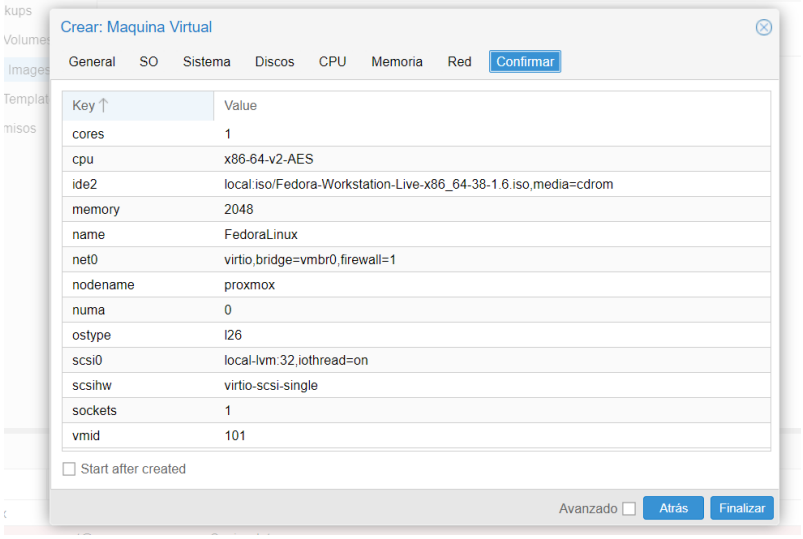

Figura 10. Cuadro resumen de los parámetros configurados para la MV. Fuente: Elaboración propia.

4.4 Redes entre máquinas virtuales y la interconexión de estas

La interconexión entre máquinas posibilita su comunicación e intercambio de datos. En este contexto, surge la interrogante sobre qué tipo de información necesita una máquina de otra. Aquí entra en juego el concepto de servicio: una máquina contiene datos que otra máquina requiere, ya sea como parte de un proceso o como información valiosa en sí misma. En esta dinámica, la máquina que proporciona el servicio asume el papel de servidor, mientras que la que demanda el servicio actúa como cliente. Las máquinas pueden establecer relaciones en el mismo nivel jerárquico en modelos de punto a punto, aunque es más común encontrarse en configuraciones donde una máquina siempre hace las funciones de servidor, mientras que las demás operan como clientes, configuración conocida como cliente-servidor (Lopera, 2023).

En el modelo cliente-servidor, una máquina aloja los servicios a los que otras máquinas accederán. El servidor mantiene puertos en estado de escucha, esperando solicitudes por parte del cliente. Una vez que se realiza la petición, se establece la comunicación y el cliente puede acceder a los servicios ofrecidos. Este enfoque presenta ventajas como la escalabilidad y la permanencia, que implica la disponibilidad del servicio en línea sin depender de un terminal específico de usuario. Además, simplifica la auditoría al permitir el registro de todas las actividades en una única máquina. Esta centralización facilita también la implementación de políticas de seguridad basadas en la identidad del usuario.

La configuración previamente mencionada resulta inviable si las máquinas no están interconectadas. Para lograr esto, se han seguido los siguientes pasos:

En primer lugar, es necesario establecer un puente de comunicación entre las máquinas. Para hacerlo, se accede a una función administrativa, pestaña denominada nodo Proxmox, en la cual se encuentran nuestras máquinas virtuales, y se crea un nuevo puente Linux desde la pestaña de red.

En segundo lugar, una vez creado este puente debe ser asignado a las máquinas virtuales específicas que se requieren interconectar. Dentro de la configuración de hardware de estas máquinas virtuales, se añade este puente recién creado. Es esencial tener presente que todas las máquinas que se deseen configurar en el modelo cliente-servidor deben estar asociadas al mismo puente. Cuando varias máquinas están conectadas al mismo puente, se habilita la comunicación entre ellas. Cuando se configura este puente se le asocia un puerto por defecto que será utilizado posteriormente.

Para permitir que las máquinas accedan a Internet, es necesario asignar un adaptador de red[16] a este puente. Para lograrlo, en la configuración del puerto (Ver Figura 11), se debe asignar en el apartado “Puertos de puente” el puerto de interconexión que se ha creado anteriormente para las máquinas virtuales.

[16] Adaptador de red o tarjeta de red: es un componente hardware que permite que un dispositivo se conecte a una red

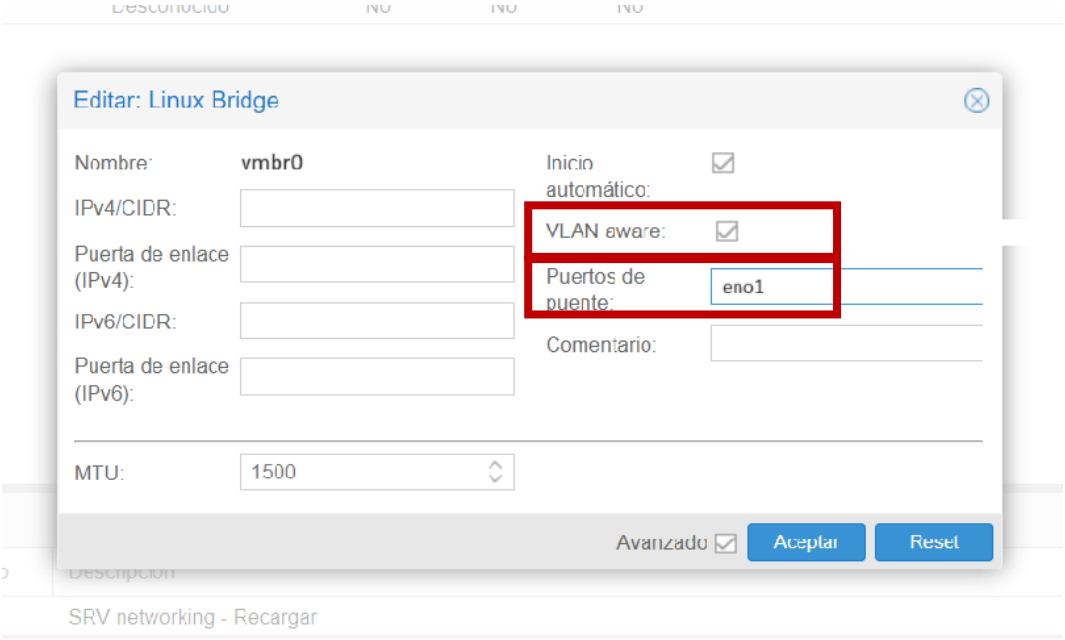

Figura 11. Asignar VLAN aware a una MV. Fuente: Elaboración propia.

En la Figura 11 se observa que en la pestaña “puerto de puente” esta asignado el puerto *eno1*. Este puerto se asigna por defecto dado que es el único disponible. En caso de que hubiese más puertos, en dicha pestaña se abriría un desplegable con todos los puertos disponibles y se seleccionaría el correcto. En Proxmox, existe la opción de aplicar las redes creadas a las máquinas que se consideren pertinentes, y esto se logra mediante el uso de una tecnología de redes que permite segmentar una red física en múltiples redes lógicas o subredes virtuales, VLAN (Virtual Local Area Network). En este contexto, es necesario activar la opción "VLAN aware" dentro de la misma pestaña. Esta configuración posibilita el control del flujo de datos, lo que implica que una máquina puede estar conectada a una red de usuarios y no necesariamente comunicarse con otra máquina conectada a una red de impresoras, por ejemplo.

Este enfoque brinda la capacidad de asegurar nuestra red y proporciona acceso selectivo a las máquinas según la red a la que se necesita conectar.

4.5 Análisis de las medidas a aplicar

Completada la configuración inicial, véase la instalación del servidor, creación de las MV y la interconexión entre estas, es necesario realizar el análisis de los elementos que intervienen en la seguridad.

En el proceso de securizar Proxmox, se han seguido las pautas establecidas por las STIC-CCN. Se ha consultado específicamente la STIC 442 de VMware (CCN, 2020) y la STIC 619B de CentOS (CCN, 2020) debido a su relevancia en entornos de trabajo similares. La elección se basa en la similitud de sus entornos de software (Tanto Proxmox como VMware son sistemas de virtualización) y en el sistema operativo Linux en el que se basa Proxmox, dado que no hay STIC para la distribución Linux Debian. Estos documentos sirvieron como referencia para implementar las medidas de seguridad necesarias en el servidor.

Las medidas a analizar que han sido examinados en este estudio provienen de las normativas STIC que se han mencionado previamente. Se analizan aquellas de carácter general en el mismo orden en el que aparecen en las guías, siendo el Anexo III un cuadro resumen de todas las directrices que exige el CCN para VMware y CentOS.

4.5.1 Control de acceso

El control del acceso engloba todas las acciones, tanto preparatorias como ejecutivas, destinadas a definir qué individuo o qué recurso del sistema puede acceder a través de una acción específica. Cualquier medida de control de acceso tiene como objetivo encontrar un equilibrio entre la facilidad de uso y la seguridad del sistema, de modo que la seguridad aumenta conforme se establece una categoría específica de protección.

4.5.1.1 Requisitos de Acceso

La configuración de grupos, forma de organizar y administrar usuarios de manera eficiente, con el propósito de definir los permisos de acceso a través de estos grupos representa un aspecto de vulnerabilidad que merece ser investigado en Proxmox. Este requisito de acceso se encuentra detallado en la STIC 442 de VMware, específicamente en la página 8 de dicho documento. En esta guía, se implementa la sustitución del uso de la cuenta de servicio local, cuenta local predefinida que usa el administrador de control de servicios, por una serie de cuentas de servicio virtuales, las cuales pueden tener acceso a la red en un entorno de dominio. Esta estrategia limita la vulnerabilidad del sistema, ya que, en caso de compromiso de una cuenta, esta no tiene autorización para operar sobre los demás servicios. Sin embargo, Proxmox no ofrece esta opción, siendo una posible alternativa la creación de grupos como medio de gestión de permisos como se ha mencionado previamente. Lo cual, si bien es una solución que aborda el problema de privilegios, y corrige de forma equivalente la vulnerabilidad derivada de una cuenta, no es una solución contemplada en las guías.

4.5.1.2 Segregaciones de funciones y tareas

La implementación de la segregación de funciones basada en actividades se considera un requisito crítico. Este enfoque establece estructuras de autorización y supervisión para prevenir la concentración de poder en manos de un solo individuo, lo que podría resultar en posibles actividades ilícitas. Es esencial personalizar cuidadosamente los roles y privilegios, detallando específicamente las acciones permitidas para cada usuario. En este contexto, se recomienda evitar la dependencia de grupos o roles[17] administrativos prediseñados. Esta práctica se encuentra respaldada por las directrices detalladas en la STIC 442 (página 9) y la STIC 619 (página 10). En el caso de CentOS la segregación de auditoria se realiza a través de la herramienta Audit, dicha herramienta se encuentra descrita en la página 10 de la STIC 619. Respecto a esta STIC no se ha encontrado ninguna aplicación para Proxmox que lo implemente.

4.5.1.3 Proceso de gestión de derechos

El proceso de administración de derechos de acceso implica la consolidación de estos derechos de manera que se aplique el principio de mínimo privilegio. Esto implica reducir los privilegios de cada usuario al nivel mínimo necesario para cumplir con sus responsabilidades. De acuerdo con las pautas establecidas en la STIC 619, el comando *sudo* ofrece un control de acceso altamente configurable. Cuando un usuario común intenta ejecutar un comando, sudo verifica sus permisos y permite la ejecución solo si está autorizado para ese comando específico, como se detalla en la página 11 de la STIC 619. Esta práctica asegura que el principio de mínimo privilegio se aplique de manera exhaustiva incluso a los administradores de los servidores y servicios gestionados por la organización. En el caso de Proxmox al iniciarse con el usuario root no es necesario ejecutar el comando sudo.

[17] Roles: funciones específicas que un usuario puede desempeñar en un sistema.

4.5.1.4 Mecanismos de autentificación

Dentro de las operaciones comunes en la gestión de sistemas de información, la autenticación es el primer proceso que se lleva a cabo. Antes de acceder a datos, administrar recursos o utilizar servicios, es necesario informar al sistema sobre la identidad del usuario. La forma en que se autentica, como se describe en las STIC 442 y STIC 619 en sus páginas 10 y 11 respectivamente, debe ajustarse según la importancia de la información, siguiendo diferentes criterios. En niveles críticos, está prohibido depender únicamente de autenticadores basados en claves específicas. Se requiere la implementación de un segundo factor de autenticación, como dispositivos físicos o tecnologías biométricas. Para esto, se deben usar algoritmos que hayan sido aprobados por el CCN, como se indica en la guía CCN-STIC-807.

En el caso de CentOS se configura una contraseña para el gestor de arranque GRUB y en el caso de VMware existe un mecanismo específico proporcionado por este que posibilita el cifrado de las contraseñas, existiendo previamente un servidor KMS (Key Management System), que se utiliza para gestionar la activación de licencias software. En este proyecto, se ha implementado seguridad en la base de datos de usuarios como solución a esta vulnerabilidad mediante la encriptación del directorio donde se almacenan las contraseñas. Para la encriptación de dicho directorio se han ejecutado unos comandos descritos en el apartado 4.6. En cuanto al segundo factor de autenticación, se ha considerado la posibilidad de utilizar un dispositivo hardware YubiKey.[18] Sin embargo, en este proyecto en particular, no se ha utilizado dicha opción debido a problemas relacionados con su adquisición.

4.5.1.5 Acceso local

En el contexto del acceso local al servidor, es esencial considerar restricciones específicas para la fecha y hora de acceso. Esta práctica está contemplada en la categoría alta del Esquema Nacional de Seguridad (ENS), tanto para VMware como para CentOs, como se detalla en las páginas 12 y 13 de sus respectivas guías. Tanto VMware como CentOS poseen funciones internas que imponen dichas restricciones.

Sin embargo, en el caso de Proxmox, no dispone de una funcionalidad interna dedicada para imponer limitaciones temporales en la interfaz web para los usuarios. A pesar de esto, es posible implementar medidas para ejercer control sobre el acceso basado en la hora y la fecha mediante ajustes en las configuraciones del firewall. Es importante señalar que no se ha realizado ninguna configuración específica para esta práctica en Proxmox.

4.5.1.6 Acceso remoto

Para gestionar el acceso remoto al servidor, se implementará una sección de activos que determina las conexiones remotas permitidas y las no permitidas, estableciendo un proceso de autenticación previa. Este enfoque es obligatorio en las categorizaciones de seguridad más altas del Esquema Nacional de Seguridad (ENS), como se especifica detalladamente en la página 12 del documento STIC 442 VMware. La solución es complementar el empleo de listas blancas, que protegen contra ataques aleatorios, con el empleo de protocolos de conexión segura como el SSH. Esta vulnerabilidad se encuentra descrita en el apartado 4.6 con los comandos necesarios para la creación de listas blancas.

4.5.2 Medidas de Protección

Finalmente, un aspecto vulnerable que merece análisis es la seguridad en las máquinas virtuales. Implementar medidas de seguridad implica seguir el principio de mínima funcionalidad y exposición, lo que implica desactivar los componentes que no se utilizarán según el propósito específico de la máquina virtual.

[18] YubiKey es un dispositivo de seguridad física que se utiliza como una forma de autenticación de dos factores (2FA) y como una llave de seguridad para el proceso de autenticación de múltiples factores (MFA).

En entornos de redes clasificadas, se debe considerar la implementación del arranque seguro UEFI siempre que sea factible. UEFI Secure Boot es un estándar de seguridad que garantiza que las máquinas virtuales solo arranquen con software confiable, tal como se hace en las máquinas físicas por el fabricante. En máquinas virtuales, es posible implementar UEFI Secure Boot de manera similar a las máquinas físicas. En sistemas operativos compatibles, cada fase del proceso de arranque, incluidos la secuencia inicial de arranque, el kernel y los controladores del sistema operativo, están firmados para garantizar su integridad. Este enfoque se deriva de las pautas de protección de la información establecidas en la STIC 442, detalladas en la página 16. UEFI es de aplicación en VMware y en Proxmox. Para habilitarlo, se debe seleccionar la opción correspondiente en la sección de discos. Para ello hay que seleccionar "EFI x86_64" en el campo BIOS.

Además de las medidas señaladas explícitamente por las STIC, hay aspectos vulnerables que se intuyen por las condiciones generales de seguridad mencionadas en la introducción de las guías. Estos elementos son objeto de análisis detallado.

Proxmox sigue el modelo cliente servidor, la comunicación por acceso remoto al servidor es una de las posibles vías de acceso a este, como se ha mencionado anteriormente. El protocolo que permite esta comunicación remota se denomina Secure Shell (SSH)

Es un protocolo de red que permite la comunicación segura entre un cliente y un servidor a través de una conexión cifrada. Sin embargo, si no se configura adecuadamente, SSH puede ser una vulnerabilidad potencial. En Proxmox VE el puerto por el que se establece esta conexión SSH es el puerto 22.

Desde el punto de vista del modelo OSI, el transporte de datos se lleva a cabo en la capa de transporte (capa 4). SSH utiliza el protocolo TCP (Transmission Control Protocol) en la capa de transporte para establecer la conexión entre el cliente y el servidor.

Además, para evitar los ataques fuerza[19] en Proxmox VE se puede proteger el sistema mediante herramientas software como Fail2ban. Esta aplicación de base Linux funciona monitoreando los archivos de registro del sistema y otros registros específicos para identificar patrones de comportamiento malicioso. Cuando detecta ciertos patrones, como múltiples intentos de inicio de sesión fallidos desde una misma dirección IP, Fail2Ban toma medidas automáticas para proteger el sistema como el indexado de esa dirección en una lista negra. De entre opciones análogas, se recomienda Fail2ban dada su facilidad de configuración. Para solventar dicha vulnerabilidad, Fail2ban ha sido instalado en Proxmox cuyos comandos para su ejecución se encuentran descritos en el apartado 4.6.

4.6 Securizacion del servidor Proxmox

En este apartado se detallará el proceso de securización aplicado al servidor, el cual se fundamenta en las STIC previamente explicadas en la sección anterior. Este proyecto se centrará exclusivamente en las acciones relacionadas con las capas 3 y 4, dado que son las capas en las que su seguridad se realiza mediante firewalls y la implementación de protocolos, así como en las técnicas de cifrado basadas en software que no están asociadas a una capa específica de comunicación entre máquinas.

4.6.1 Implementación de las medidas previamente analizadas en la capa 3

En relación con la capa 3, como se ha indicado previamente, y como solución a la vulnerabilidad descrita en el apartado 4.5.1.6, acceso remoto, es necesario administrar el

[19] Ataques fuerza: tipo de ataque en entorno de ciberdefensa en el cual un atacante intenta descubrir una contraseña o clave de cifrado probando todas las combinaciones posibles hasta encontrar la correcta.

acceso remoto al servidor mediante la definición de las direcciones que están autorizadas y aquellas que no lo están.

Con este propósito, se han establecido listas blancas de direcciones IP, las cuales contienen direcciones específicas que están permitidas para interactuar o acceder a recursos designados. Cualquier elemento que no esté incluido en la lista blanca se encuentra bloqueado o prohibido de acceder. Este nivel de seguridad no protege al sistema de ataques dirigidos[20], pero sí reduce su exposición en la red. Para crear dicha lista blanca se deben ejecutar los siguientes comandos en la terminal.

Iptables -F

Iptables -A INPUT -s 192.168.1.x -j ACCEPT

Iptables -A INPUT -j DROP

El primer comando descrito elimina todas las reglas existentes. El segundo comando añade la dirección IP específica (donde 'x' representa la dirección IP designada). El tercer comando bloquea todas las demás conexiones entrantes.

Si se quiere comprobar las reglas que se han establecido, se deberán guardar previamente y se observan al ejecutar el comando:

Iptables -L

En la Figura se muestra las direcciones IP configuradas, en este caso han sido la 192.168.1.2 y la 192.168.1.4. Estas direcciones IP han sido seleccionadas de forma aleatoria.

```
root@proxmox:~# iptables -A INPUT -s 192.168.1.2 -j ACCEPT
root@proxmox:~# iptables -A INPUT -s 192.168.1.4 -j ACCEPT
root@proxmox:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.1.2          anywhere
ACCEPT     all  --  192.168.1.4          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@proxmox:~#
```

Figura 12. Configuración de las listas blancas. Fuente: Elaboración propia.

Una vez ejecutados estos comandos se debe reiniciar el servidor con el comando:

reload

Para solventar la vulnerabilidad descrita en el apartado 4.5.2, medidas de protección, de esta misma capa, se presenta la configuración de Fail2ban que se ha implementado para prevenir los intentos de ataque de fuerza bruta:

get update

[20] Acciones maliciosas llevadas a cabo por ciberdelincuentes con el objetivo de comprometer sistemas de una entidad particular.

install fail2ban

fail2ban restart.

El primer comando descrito actualiza los repositorios existentes. El segundo comando permite la instalación del software Fail2ban. Dicha aplicación establece una configuración por defecto, la cual no ha sido modificada. El tercer comando ejecuta el reinicio del servidor para su correcta instalación.

En la Figura 13 se observan los parámetros ejecutados con su correcta instalación.

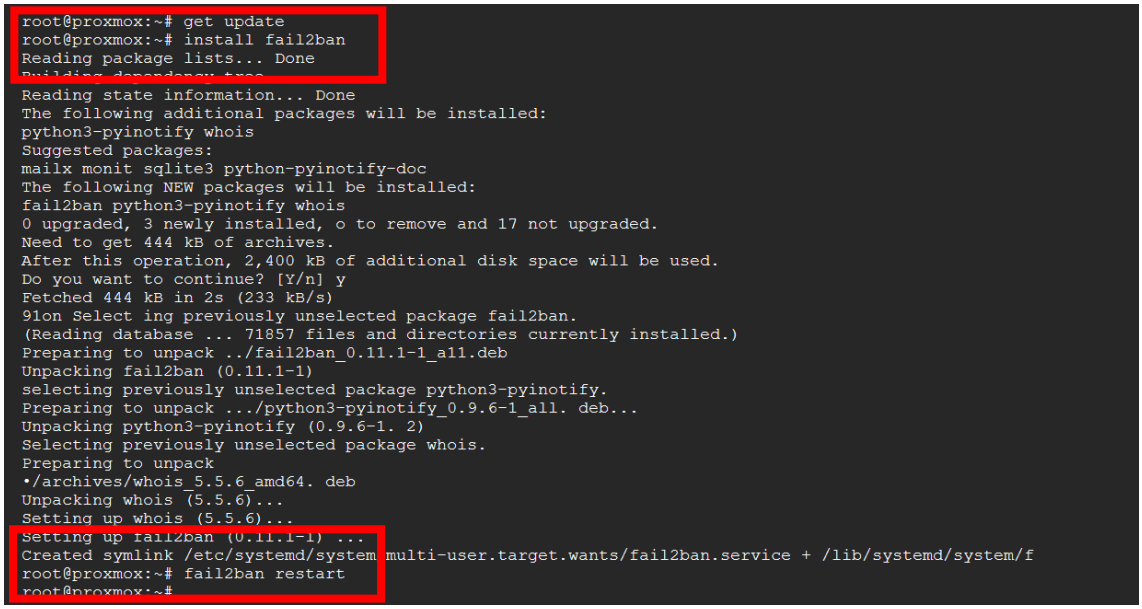

Figura 13. Instalación de Fail2ban en Proxmox. Fuente: Elaboración propia.

Para securizar la base de datos de los usuarios, solución a la vulnerabilidad descrita en el apartado 4.5.1.4, mecanismos de autentificación, se ha encriptado el directorio en el que se almacenan las contraseñas. Se ha seguido la siguiente configuración:

Apt update

Apt install encfs

Mkdir /mnt/encfs_mount/

Encfs /var/encfs_data /mnt/encfs_mount

Fusermount -u /mnt/encfs_mount

El proceso comienza con la actualización e instalación de EncFS[21] como primer paso. Luego, el tercer comando se utiliza para crear un directorio en el cual se montará el sistema de archivos cifrado. En este caso, se ha optado por utilizar un directorio preexistente llamado "mnt" en Proxmox y se le ha asignado el nombre "encfs_mount" para el directorio montado.

[21] EncFS es un sistema de archivos cifrado de código abierto y fácil de usar para sistemas basados en Unix/Linux. Permite a los usuarios crear un directorio cifrado en su sistema de archivos que actúa como un contenedor para almacenar datos sensibles. Los datos dentro de este directorio están cifrados y solo son accesibles después de que el usuario proporciona la clave de cifrado adecuada.

Posteriormente, el cuarto comando se emplea para iniciar EncFS y montar el sistema de archivos cifrados. Durante este proceso, EncFS solicita que se configure una contraseña para el sistema de archivos cifrados. Se debe ingresar y confirmar la contraseña cuando se solicite.

Para acceder a los datos cifrados, se utiliza el comando *encfs_mount*, dentro de la ruta "/mnt/encfs_mount/. Estos datos están cifrados y se almacenan de manera segura en el directorio cifrado original.

Finalmente, el último comando se ejecuta para desmontar el sistema de archivos cifrados y garantizar la seguridad de los datos. Siempre que se desee acceder a los datos cifrados, es necesario montar nuevamente el sistema de archivos cifrados y proporcionar la contraseña que se estableció previamente como se observa en la Figura 14.

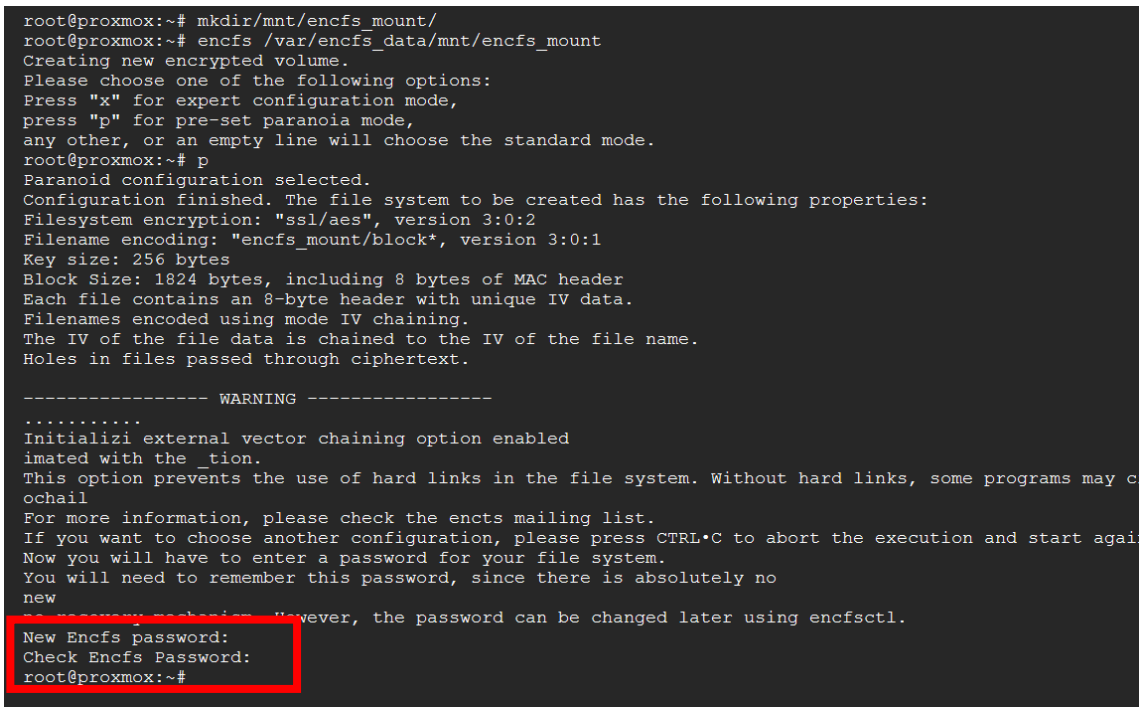

Figura 14. Contraseña de EncFs para los datos cifrados. Fuente: Elaboración propia.

4.6.2 Medidas de protección aplicadas en la capa 4

Una vez que se ha implementado la seguridad en la capa 3 del modelo OSI (capa de red), se procede a asegurar la capa de transporte (capa 4).

En esta etapa, se llevará a cabo el proceso de cierre de todos los puertos y, posteriormente, se abrirán únicamente aquellos que son necesarios para el funcionamiento del sistema. Los puertos que se abrirán incluyen el 8006, que se utiliza para acceder a la interfaz web del servidor Proxmox y los puertos del 5900 al 5999, ambos inclusive, que se emplean para las conexiones de consola de las máquinas virtuales. Este enfoque limita el acceso a través de los puertos esenciales, aumentando así la seguridad del sistema.

Es importante remarcar que este paso solo debe llevarse a cabo si se tiene acceso directo a la terminal. Pues si se trabaja de forma remota y se cierra el puerto 22 (protocolo SSH) se pierde comunicación con la máquina, de tal forma que debe de quedar abierto.

Para llevar a cabo este paso se ejecutarán los siguientes comandos en la terminal:

iptables -F

iptables -P INPUT DROP

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 8006 -j ACCEPT

iptables -A INPUT -p tcp --dport 5900 -j ACCEPT

iptables-save

En este procedimiento de configuración del firewall en Proxmox, inicialmente se procede a eliminar todas las reglas existentes y se establece la política predeterminada para bloquear cualquier conexión entrante, siendo estas las acciones llevadas a cabo por los primeros dos comandos. Luego, se especifican las aperturas selectivas de los puertos 22, 5900 y 8006, permitiendo las conexiones SSH, el acceso a la interfaz web de Proxmox y la consola de las máquinas virtuales respectivamente, mediante la ejecución de los comandos correspondientes a estos puertos. Finalmente, el último comando es utilizado para preservar las nuevas configuraciones del firewall, asegurando su persistencia incluso después de un reinicio del sistema. En la Figura 15 se observa de forma gráfica los únicos puertos que se han dejado abiertos en el servidor. Dado que son puertos lógicos y no se pueden representar de forma física, se han representado con un ordenador.

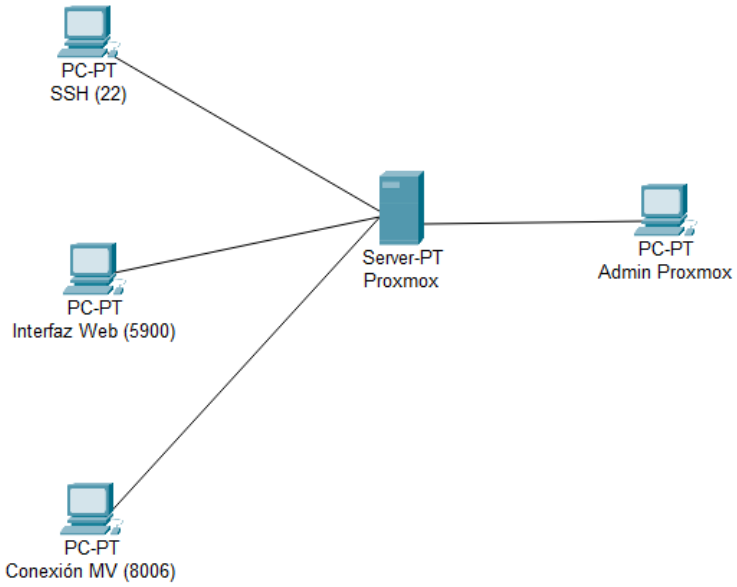

Figura 15. Esquema gráfico de los puertos abiertos en Proxmox. Fuente: Elaboración propia con Packet Tracer.

En la Figura 16 se observa la consola en la que se ven los únicos puertos abiertos.

```
root@proxmox:~# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@proxmox:~# iptables -A INPUT -p tcp --dport 8006 -j ACCEPT
root@proxmox:~# iptables -A INPUT -p tcp --dport 5900 -j ACCEPT
root@proxmox:~# iptables-save
# Generated by iptables-save v1.8.9 on Wed Nov 8 19:42:55 2023
*raw
:PREROUTING ACCEPT [241:42728]
:OUTPUT ACCEPT [96:8398]
COMMIT
# Completed on Wed Nov 8 19:42:55 2023
# Generated by iptables-save v1.8.9 on Wed Nov 8 19:42:55 2023
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [2:134]
-A INPUT -p tcp -m tcp --dport 22
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8006 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 5900 -j ACCEPT
COMMIT
# Completed on Wed Nov 8 19:42:55 2023
root@proxmox:~#
```

Figura 16. Consola de Proxmox con los puertos abiertos. Fuente: Elaboración propia.

En el Anexo IV se encuentran los comandos descritos paso a paso para la securización del servidor.

4.7 Aplicación de herramientas de análisis de la seguridad: CLARA

En esta sección se detalla el procedimiento de implementación de la herramienta de seguridad denominada CLARA

La aplicación CLARA ha sido adquirida desde el sitio web oficial del CCN. Esta aplicación está estructurada en varios componentes que han sido comprimidos en una carpeta denominada CLARA-LINUX-ENS dentro de una memoria USB. Una vez que esta carpeta ha sido descomprimida, se inicia el proceso de ejecución en el entorno Proxmox.

Para llevar a cabo este proceso, es necesario establecer un directorio específico donde se pueda montar el archivo de Clara. En este contexto, se ha generado un directorio denominado CLARA dentro del directorio var, que es inherente a Proxmox. Tal como se muestra en la Figura 17, el directorio CLARA ha sido creado y se ha accedido a él.

```
root@proxmox:~# mkdir /var/CLARA
root@proxmox:~/ CLARA#
```

Figura 17. Creación del directorio CLARA. Fuente: Elaboración propia.

El segundo paso implica montar la memoria USB que contiene la carpeta de Clara. Como se muestra en la Figura 18, se emplea el comando 'mount' para montar la memoria USB dentro del directorio creado previamente.

```
root@proxmox:~# mount /dev/sbd1 var/CLARA
```

Figura 18. Comando para montar la memoria USB. Fuente: Elaboración propia.

Una vez que la memoria USB ha sido montada en nuestro directorio designado, el siguiente paso implica copiar el archivo "clara.tar.gz" contenido en la carpeta Clara, que ya está montada en dicho directorio. Este archivo se copia al equipo de destino y se descomprime en una ubicación temporal (el directorio 'temp' específico de Proxmox). Como se indica en la Figura 19, se debe ejecutar el siguiente comando para llevar a cabo este procedimiento.

```
root@proxmox:~/ tar -xzvf clara.tar.gz -C/temp
```

Figura 19. Comando para descomprimir un archivo en Proxmox. Fuente: Elaboración propia.

El paso subsecuente consiste en ejecutar el archivo con extensión .sh contenido dentro de la carpeta clara.tar.gz. Para llevar a cabo esta acción, tal como se representa en la Figura 20, se procede a ejecutar el comando siguiente:

```
root@proxmox:~/ temp# sh CLARA-Linux.sh
```

Figura 20. Comando para ejecutar un archivo en Proxmox. Fuente: Elaboración propia.

Una vez ejecutado el comando, se deberá esperar que se termine el despliegue de CLARA y se muestre el mensaje “CLARA listo para ejecución”, ver Figura 21.

```
root@proxmox:~/ temp# sh Clara-Linux.sh
================================================
============================================
CLARA Standalone
================================================
============================================
================================================
================================================
copiando programa CLARA...
CLARA copiado.
================================================
============================================
CLARA listo para ejecución.
root@proxmox:~/ temp#
```

Figura 21. Despliegue correcto de CLARA. Fuente: Elaboración propia.

Por último, para iniciar la herramienta CLARA, se procede a ejecutar las instrucciones que se detallan a continuación, tal como se muestra en la Figura 22.

```
root@proxmox:~/ temp# cd /var/clara
```

Figura 22. Carpeta de despliegue “clara”. Fuente: Elaboración propia.

Para iniciar un análisis en el equipo será necesario ejecutar el comando descrito en la Figura 23 con los parámetros permitidos por esta (ver Anexo V):

```
root@proxmox:~/ clara# ./Clara-analyze -ens=alta
```

Figura 23. Comando ejecución de análisis. Fuente: Elaboración propia.

Una vez ejecutado el comando, habrá que esperar unos minutos (dependiendo del equipo y del número de elementos a analizar) para obtener el resultado de la ejecución. La ventana de comandos quedará en espera hasta que se termine el análisis, de tal manera que cuando vuelva a responder, significará que ya ha concluido el análisis.

Como consecuencia de la ejecución de la herramienta, se generan diversos recursos durante y después del análisis de cada sistema. Durante el proceso, la herramienta crea una carpeta temporal llamada 'tmp', situada en el directorio '/var/clara/CLARA/tmp', donde se almacenan datos temporales. Al finalizar la ejecución, esta carpeta temporal se limpia, eliminando todos los archivos que contiene.

Adicionalmente, se crea de manera persistente una carpeta de informes o resultados, según lo configurado en la herramienta. Esta carpeta se encuentra en '/var/clara/CLARA/reports' y contiene la siguiente información:

1. Un archivo con formato ".enc": Este archivo se utiliza al exportar el análisis.

2. Informe ejecutivo: Proporciona una visión global del análisis realizado y sus resultados. Se presenta en formato de texto plano y lleva el sufijo "_InformeEjecutivo" en su nombre.

3. Informe técnico: Almacena los datos técnicos del sistema analizado y los resultados obtenidos. Se presenta en formato de texto plano y lleva el sufijo "_InformeTecnico" en su nombre.

En este contexto, los informes mencionados no estaban disponibles en los directorios designados. Como resultado, el análisis del sistema no pudo llevarse a cabo y, por ende, la herramienta CLARA no fue utilizable en este proyecto.

4.8 Registro de incidencias

Durante el proceso de aseguramiento del servidor, surgieron dificultades significativas relacionadas con los comandos necesarios para llevar a cabo la securización. La STIC 916 CentOs emplea ciertos comandos que Proxmox, al ser una plataforma basada en Debian y ambos sistemas operativos en Linux, no puede ejecutar. Estos comandos específicos estaban detallados en el manual oficial de Debian.

Durante el análisis de los elementos vulnerables se han desarrollado las STIC implementadas por VMware y CentOS para difusión limitada. Dentro de este contexto, algunas de estas soluciones han sido adaptadas para su configuración en el entorno de Proxmox, mientras que para otras se han formulado propuestas de resolución.

A modo resumen se ha creado una tabla que recoge todas medidas dentro de una o varias STIC en las que se ha basado el trabajo y cuál de estas medidas han sido implementadas en Proxmox, cuales se ha propuesto una solución y cuales no han sido posibles.

Tabla 2: Cuadro de las STIC basadas para Proxmox. Fuente: Elaboración propia

Medida STIC	¿Se ha aplicado la STIC?	Posible solución, sin llegar a implementarla	Solución Proxmox
Requisitos de acceso	No	Mediante la creación de grupos	
Segregación de tareas y funciones	No		
Proceso de gestión de derechos de acceso	Si		Usuario “root”
Mecanismos de autentificación	Cumple parte de la STIC	Adquisición de Yubikey	Encriptación de directorios de contraseñas
Acceso local	No		Cambios de fecha y hora en la configuración del firewall
Acceso remoto	Si		Creación de listas blancas
Medidas de protección Seguridad en MV	Si		Fail2ban UEFI

Por otro lado, el empleo de la herramienta CLARA, que habría facilitado el análisis del sistema, además de ser en sí misma el contraste que emplea la entidad acreditadora, se vio frustrado por un fallo en su código que hacía que se ejecutase sin generar informe.

5. CONCLUSIONES

En la actualidad, el Ejército de Tierra dispone de hardware en desuso, el cual podría ser necesario para las operaciones diarias de las unidades, dado que el suministro de hardware actual es limitado. La escasa disponibilidad de licencias de software y sus altos costos han llevado a la obsolescencia de gran parte del material, ya que no es posible adquirir licencias para todo el equipo.

Esta coyuntura ha suscitado la consideración de adoptar software libre como una alternativa a las soluciones de software con licencia privada.

El objetivo de este proyecto es implementar un servidor de virtualización basado en software libre que cumpla con las STIC de seguridad del CCN. Sin embargo, tras la finalización del proyecto y los análisis realizados en el estudio, se concluye que es posible garantizar la seguridad del servidor, aunque no cumple con las STIC de seguridad del CCN.

Como consecuencia de este objetivo principal, se llevaron a cabo varios objetivos específicos:

- Durante la instalación del servidor de virtualización, se configuró en uno de los ordenadores proporcionados por la Brigada de Inteligencia (BRI I). Como conclusión, se determina que dicho software puede ser instalado en cualquier ordenador que cumpla con los requisitos mínimos de hardware para su implementación.

- Al revisar todas las directrices impuestas por el Centro Criptológico Nacional (CCN) para el nivel alto o de difusión limitada, específicamente diseñadas para la distribución CentOS y el software de virtualización VMware, se puede concluir que la gran mayoría de estas directrices pueden ser aplicadas en Proxmox mediante sus comandos correspondientes y aunque no cumplan de forma rigurosa las STIC impuestas por el CCN, muchas de ellas se pueden complementar con medidas alternativas. Aquellas directrices que no pudieron implementarse en Proxmox se debieron principalmente a limitaciones de adquisición o incompatibilidad con el sistema Debian subyacente.

- Se ha observado que la herramienta CLARA, utilizada para análisis en este proyecto, no es compatible con Debian, lo que limitó su utilidad en esta investigación. Estos hallazgos subrayan la necesidad de considerar cuidadosamente la compatibilidad y la disponibilidad de las herramientas y directrices al seleccionar plataformas de virtualización para garantizar una securización efectiva según los estándares del CCN.

6. REFERENCIAS BIBLIOGRÁFICAS

Aoki, O., 2023. *Guía de referencia de Debian.* s.l.:s.n.

BOE, 2002. *Boletín Oficial del Estado.* [En línea]
Available at: https://www.boe.es/eli/es/l/2002/05/06/11

CCN., 2023. *Centro Criptológico Nacional. Esquema Nacional de Seguridad (ENS.* [En línea]
Available at: https://ens.ccn.cni.es/es/que-es-el-ens

CCN, 2020. *Implementación de seguridad sobre CentOS 8,* s.l.: s.n.

CCN, 2020. *Implementación de seguridad sobre VMware VSPHERE 6.7,* s.l.: s.n.

CCN-CERT, 2023. *Centro Criptológico Nacional.* [En línea]
Available at: https://www.ccn-cert.cni.es/es/sobre-nosotros/centro-criptologico-nacional.html

CCN-CERT, 2023. *Centro Criptológico Nacional.* [En línea]
Available at: https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic.html

CCN-CERT, 2023. *Centro Criptológico Nacional.* [En línea]
Available at: https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic.html

Ciberseguridad, I. N. d., 2020. *La virtualización puede ser la solución a tus problemas.* [En línea]
Available at: https://web.archive.org/web/20200109120624/https://www.incibe.es/protege-tu-empresa/blog/virtualizacion-puede-ser-solucion-tus-problemas

Cualificaciones, I. N. d. l., 2023. *Glosario de terminos utilizados en sistemas de gestión de información.* s.l.:s.n.

Garcia, J., 2023. *¿Qué es un sistema RAID de discos duros y qué tipos hay?.* [En línea]
Available at: https://hardzone.es/tutoriales/montaje/raid-discos-duros/

GmbH., P. S. S., 2023. *Proxmox VE..* [En línea]
Available at: https://www.proxmox.com/en/proxmox-virtual-environment/overview

Hat, R., 23 de marzo de 2023. *Red Hat.* [En línea]
Available at: https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor

Lopera, C. J. M., 2023. *Arquitectura de Protocolos,* s.l.: s.n.

Lopera, C. J. M., 2023. *Capa de Presentación,* s.l.: s.n.

Romero, Y. F., 2011. *Virtualización ,* s.l.: ISSN 1729-3804.

VMware, 2023. *VMware.* [En línea]
Available at: https://www.vmware.com/es/solutions/virtualization.html

VMware, 2023. *VMware.* [En línea]
Available at: https://www.vmware.com

ANEXOS

Anexo I: Diagrama de Gantt

Anexo II: Carga de Proxmox en el programa Rufus

Anexo III: STIC de seguridad en VMware y CentOS

Anexo IV: Comandos de securización en Proxmox

Anexo V: Parámetros para la ejecución de CLARA

Anexo I: Diagrama de Gantt

En el siguiente anexo se observa el diagrama de Gantt realizado con ProjectLibre

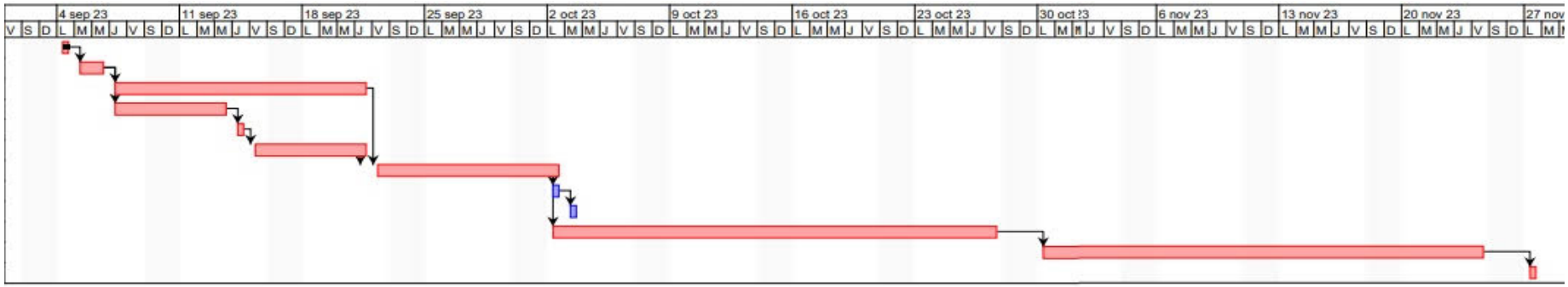

Figura 24. Diagrama de Gantt sobre desarrollo temporal. Fuente: Elaboración propia con ProjectLibre.

Anexo II: Carga de Proxmox en el programa Rufus

En el siguiente Anexo se describen los pasos de la descarga de Proxmox y Rufus, y la posterior carga de Proxmox dentro de la memoria USB a través de Rufus.

Descarga del software a través de la página oficial de este:

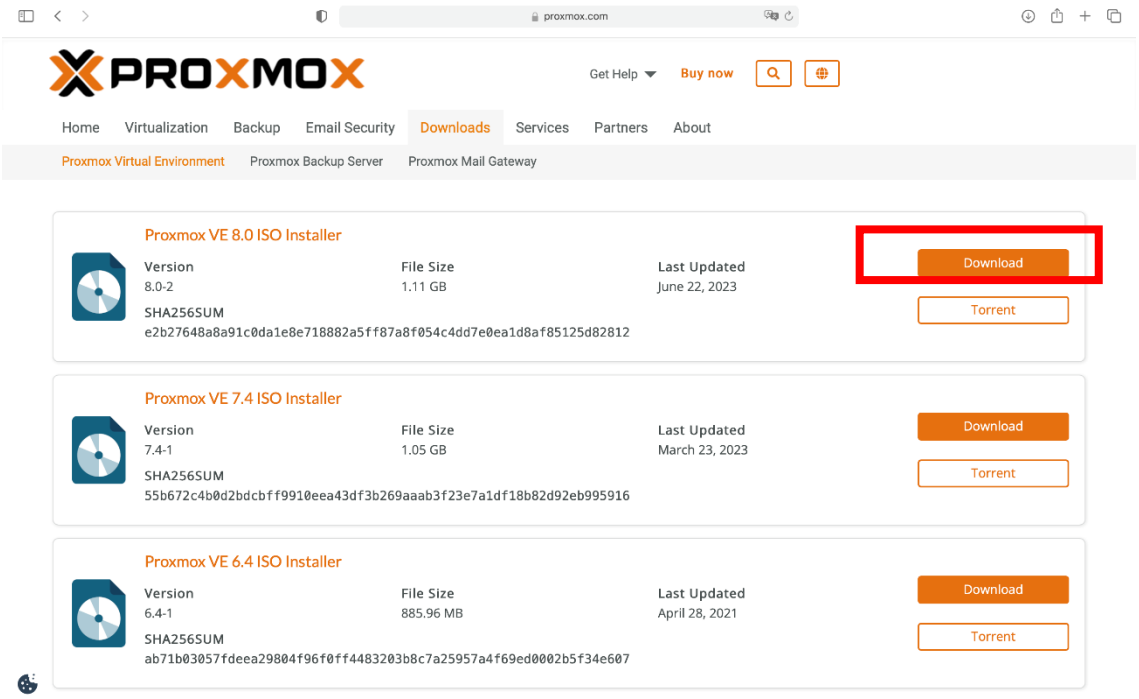

Figura 25. Descarga de Proxmox desde la página oficial. Fuente: Elaboración propia.

Descarga del software a través de la página oficial de este:

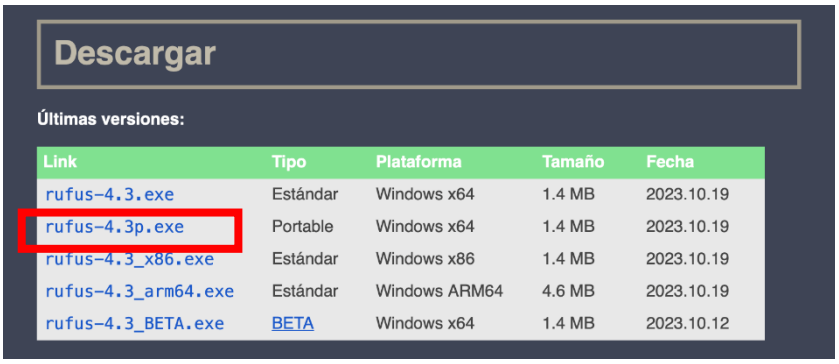

Figura 26. Versión para descargar del software Rufus. Fuente: Elaboración propia.

Como cargar el archivo .iso Proxmox en Rufus dentro de una memoria USB:

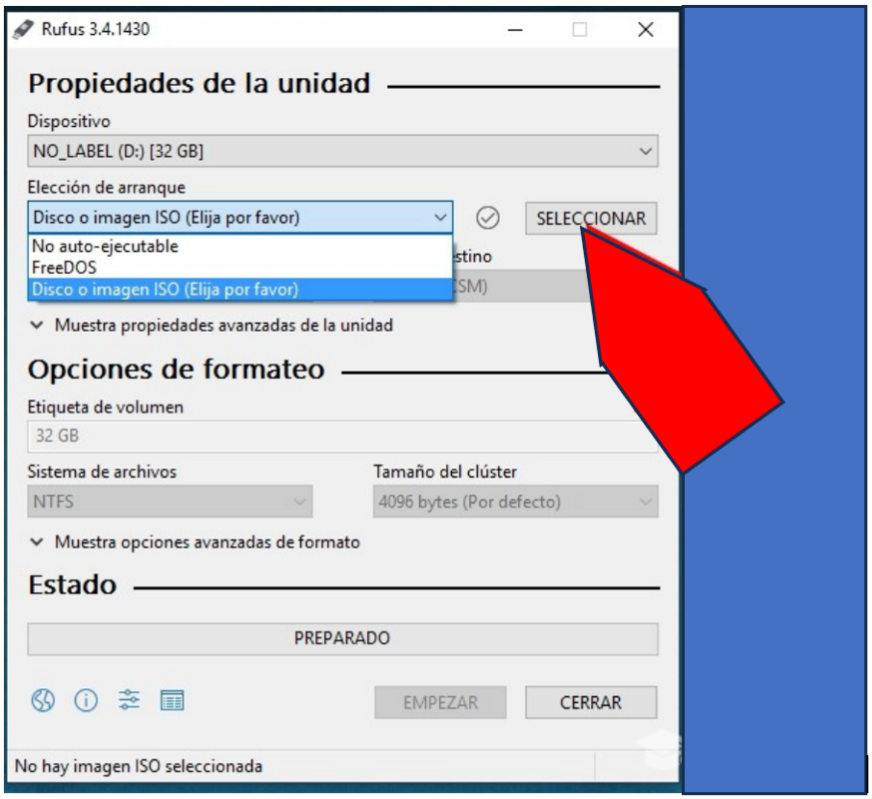

Figura 27. Pestaña de Rufus que permite la carga del archivo .iso Fuente: Elaboración propia.

Anexo III: STICs de seguridad en VMware y CentOS

En el presente anexo se establece un cuadro con las diferentes medias a aplicar exigidas por las STIC 442 y 619 B respectivamente exigidas por el ENS para el nivel de Difusión Limitada (DF). Estas medidas han sido aplicadas, en la medida de lo posible, en el servidor Proxmox.

Tabla 3: Cuadro de las medidas exigidas por el ENS para VMware y CentOS. Fuente: Elaboración propia.

Aplicación de medidas en VMWare STIC 442	Aplicación de medidas CentOS STIC 619
Control de acceso	Control de acceso
Requisitos de acceso	Requisitos de acceso
Segregación de funciones y tareas	Segregación de funciones y tareas
Proceso de gestión de derechos de acceso	Proceso de gestión de derechos de acceso
Mecanismos de autentificación	Mecanismos de autentificación
Acceso local	Acceso local
Acceso remoto	Acceso remoto
Explotación	Explotación
Configuración de la seguridad	Configuración de seguridad
Gestión de la configuración	Mantenimiento
Registro de actividad de los usuarios	Registro de actividad de los usuarios
Medidas de protección	Medidas de protección
Protección de las comunicaciones	Protección en las comunicaciones
Protección de la información	Protección de la información
	Protección de los equipos

A continuación, se adjunta un cuadro resumen de las medidas analizadas en Proxmox, siendo la referencia las medidas impuestas por la STIC 442 VMware y la STIC 619 CentOS adjuntas en el cuadro anterior.

Tabla 4: Medidas analizadas en Proxmox. Fuente: Elaboración propia.

Medidas analizadas en Proxmox
1. Control de acceso
1.1. Requisitos de acceso
1.2. Segregación de funciones y tareas
1.3. Proceso de gestión de derechos de acceso
1.4. Mecanismos de autentificación
1.5. Acceso local
1.6. Acceso remoto
2. Medidas de protección

Anexo IV: Comandos de securización de Proxmox

En el presente Anexo se proporciona un registro, a modo cuaderno de campo, de los comandos necesarios y la secuencia apropiada para llevar a cabo la seguridad del servidor

1. Creación de las direcciones IP permitidas (Listas blancas)

Iptables -F

Iptables -A INPUT -s 192.168.1.x -j ACCEPT

Iptables -A INPUT -j DROP

2. Seguridad del directorio donde se almacenan las contraseñas

Apt install encfs

Mkdir /mnt/encfs_mount/

Encfs /var/encfs_data /mnt/encfs_mount

Fusermount -u /mnt/encfs_mount

3. Cierre de todos los puertos

Iptables -F

Iptables -P INPUT DROP

4. Abrir los puertos 22, 5900 y 8006 necesarios para funcionamiento del sistema

Iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Iptables -A INPUT -p tcp --dport 8006 -j ACCEPT

Iptables -A INPUT -p tcp --dport 5900 -j ACCEPT

Anexo V: Parámetros para la ejecución de CLARA

La herramienta CLARA necesita ciertos parámetros durante su ejecución, los cuales permiten iniciar un análisis y determinar el nivel de clasificación. Como se mencionó anteriormente, CLARA se utiliza en modo consola y requiere la configuración de ciertos parámetros para llevar a cabo un análisis y definir el grado de clasificación deseado. En dicho Anexo se encuentran los diferentes parámetros para ejecutar en CLARA según las necesidades requeridas.

Tabla 5: Tabla de parámetros a ejecutar en CLARA. Fuente: Elaboración propia.

Parámetro	Subparámetro	Valores admitidos
--analyze		
--analyze		Indica al programa que se va a inicar un análisis. Es obligatorio.
--ens		
--ens=	- Alta - Media - baja	Permiten elegir el grado de clasificación de las opciones disponibles del ENS
Idioma		
es-ES en-GB		Permite elegir el idioma en el que se genera el archivo. Si no se indica, por defecto los informes se generan en español.