Entorno de desarrollo en Cloud para la integración de herramientas de Ciberseguridad

Iván Lorenzo Alcaina

Resumen– A menudo, en las empresas relacionadas con las tecnologías de la información, surge la necesidad de disponer de un entorno de desarrollo en el cual probar todos los servicios, que posteriormente serán implantados en la infraestructura de la empresa del cliente. La realización de este proyecto, se enfocó en crear un entorno de desarrollo que contuviera las herramientas dedicadas a la Ciberseguridad necesarias para llevar a cabo testeos previos a implantaciones finales. Para lograr este objetivo se creó un servidor *Cloud*, el cual aloja un conjunto de máquinas virtuales que disponen del *Software* necesario para proveer al sistema de herramientas dedicadas a la gestión de identidades y accesos. La utilización del entorno de desarrollo logró mejorar la metodología de trabajo de la empresa en la cual se realizó, ya que la posibilidad de operar previamente a las implantaciones en entornos de producción, permite identificar errores en etapas más tempranas. Este cambio en la metodología, consiguió mejorar la calidad final de los servicios ofrecidos por parte de la empresa.

Palabras clave– Ciberseguridad, Cloud, Cooperación, Desarrollo, Disponibilidad, Gestión de Identidades y Accesos, Investigación, Redes, Resiliencia

Abstract– Often, in companies related to information technologies, the need arises to have a development environment in which to test all the services that will later be implemented in the infrastructure of the client's company. The realization of this project was focused on creating a development environment containing the tools dedicated to cybersecurity necessary to carry out tests prior to final implementations. To achieve this goal, a Cloud server was created, which hosts a set of virtual machines that have the necessary software to provide the system with tools dedicated to identity and access management. The use of the development environment managed to improve the work methodology of the company in which it was carried out, since the possibility of operating prior to deployments in production environments, allows to identify errors at earlier stages. This change in the methodology improved the final quality of the services offered by the company.

Keywords– Availability, Cybersecurity, Cooperation, Cloud, Development, Identity and Access Management, Network, Research, Resilience

1 Introducción

En muchas ocasiones, las distintas instalaciones y servicios ofrecidos por las empresas de las Tecnologías de la Información (TI) influyen directamente en el desarrollo de las actividades que se llevan a cabo en el entorno de producción de los clientes, esto es debido a que en la mayoría de los casos se necesita modificar ciertos parámetros que pueden repercutir directamente en el comportamiento de las aplicaciones y servicios utilizados por los trabajadores. Operar directamente en el entorno de producción acarrea molestias y cortes de servicio, esto se logra mitigar mediante la utilización de infraestructuras de desarrollo totalmente independientes del entorno de producción. En el entorno de desarrollo se realizan las primeras fases del proyecto sin influir en los servicios dedicados al *end user*.

Debido a estos motivos, en las empresas de TI crece la necesidad implícita durante el desarrollo de proyectos, de

• E-mail de contacto: ivan.lorenzoA@autonoma.cat
• Mención realizada: Tecnologías de la Información
• Trabajo tutorizado por: Ramon Martí (DEIC)
• Curso 2021/22

disponer de un entorno de desarrollo y testeo exhaustivo de las soluciones posteriormente aplicadas a los clientes [1].

Este proyecto ha sido realizado en la empresa ITechGrup Innovación en Tecnologías de la Información S.L. [2], dedicada al ámbito de la ciberseguridad y las tecnologías de la información (TI). Dentro de la empresa se identificó la necesidad de crear un entorno de desarrollo para testear las soluciones ofrecidas relacionadas con la Ciberseguridad, principalmente con la gestión de identidades y accesos.

El objetivo principal de este proyecto fue diseñar, crear e implementar un entorno de desarrollo para ITechGrup que permitiese llevar a cabo testeos previos a implantaciones finales. Esto se logró mediante la implementación de una infraestructura *Cloud* [3] que contiene todas las máquinas virtuales necesarias para instalar e integrar las múltiples soluciones *software* de las que se disponen. *Cloud* permite tener un entorno de desarrollo de alta disponibilidad, escalabilidad y accesibilidad múltiple [4].

El entorno de desarrollo obtenido, mejora la metodología de la empresa a la hora de realizar ejecuciones previas a puestas en marcha de distintos proyectos, adaptar esta metodología al nuevo entorno, logra mejorar la calidad final de los servicios ofrecidos y la satisfacción de los clientes.

Cabe destacar que paralelamente a la realización de este proyecto, también se llevó a cabo una migración del entorno de producción actual de la empresa ITechGrup a la nueva infraestructura creada. El foco de este trabajo se centró en la creación del entorno de desarrollo.

2 Estado del arte

Actualmente, en el ámbito empresarial se están dedicando esfuerzos a proteger la infraestructura de los servicios proporcionados, mediante la utilización de gestión de identidades, accesos y autenticación multi factor. Estas prácticas son una buena opción para prevenir posibles fallos de seguridad que pueden acarrear problemas graves.

A día de hoy existen muchas empresas que se dedican a crear *software* dedicado a la ciberseguridad, por ejemplo, IBM [5] y Okta [6] son dos grandes empresas que ofrecen un catálogo de productos orientados a la gestión de identidades y accesos. En este proyecto se trabajó con el catálogo de productos que provee la empresa Micro Focus [7], la cual a través de su línea de negocio NetIQ ofrece una gran variedad de soluciones empresariales, no tan solo para la gestión de identidades y accesos, sino que también proporciona otras funcionalidades destacables como autenticación multi factor, gestión de contraseñas, monitorización, herramientas para auditar y gobernanza digital.

El punto fuerte de Micro Focus respecto a sus competidores es que el catálogo de productos que ofrece es mucho más amplio, aparte, la principal ventaja es que todo el *software* está pensado para que se integre en la infraestructura de la empresa cliente de la forma más sencilla posible.

Otra característica importante a destacar, es que Micro Focus está aliado con Yubico [8], empresa que se dedica a hacer tokens físicos que almacenan credenciales y certificados, esto proporciona una seguridad extra, debido a que el usuario porta consigo el hardware necesario para autenticar a los servicios de la empresa.

Por ejemplo, un caso de uso fruto de la asociación de Yubico y Micro Focus implantado por parte de ITechGrup, fue un proyecto realizado para la empresa farmacéutica Hipra, el cual proporcionó un método de acceso multi factor seguro y cómodo que otorgaba una solución de autenticación multi factor distinta a los métodos biométricos, ya que los trabajadores por temas de protocolo llevaban ropa incompatible con este tipo de métodos.

En cuanto al sistema operativo (SO) que utilizan las máquinas virtuales de este proyecto, SUSE Linux [9] proporciona grandes ventajas a la hora de adaptarse a las necesidades de las aplicaciones de NetIQ. También, a través de Rancher, ofrece la única plataforma de gestión de Kubernetes abierta, lo cual permite innovar y adaptarse rápidamente.

3 Objetivos

Este proyecto tiene como objetivo principal mejorar la metodología de trabajo de la empresa en la cual se ha llevado a cabo, a través de la creación de un entorno de desarrollo *Cloud*, que contiene las herramientas dedicadas a la Ciberseguridad necesarias para llevar a cabo testeos previos a implantaciones finales. Desglosando el objetivo principal, se extrajo que se deben alcanzar los siguientes objetivos comentados a continuación en orden de prioridad:

Montaje del servidor Cloud: El montaje del servidor *Cloud* es clave para el desarrollo del proyecto, ya que sin la infraestructura *Hardware* necesaria no se puede llevar a cabo la ejecución de los siguientes pasos. Dentro de esta tarea se lleva a cabo la contratación [10], instalación y configuración del *Cloud*.

Creación e interconexión de máquinas virtuales: Una vez ya preparado el servidor, se debe crear, configurar e interconectar las máquinas virtuales necesarias que vengan determinadas por la arquitectura diseñada.

Instalación y configuración de los productos: Cuando se disponga de todas las máquinas virtuales necesarias, se procede a instalar, configurar e integrar todos los productos del catálogo que se mencionan más adelante. Este objetivo es el más costoso de todos los mencionados, ya que el proceso de instalación juntamente con la integración de los servicios tiene una complejidad alta.

Configuración de Proxy Servers y Single Sign On (SSO): Finalmente, una vez se disponga del ambiente de desarrollo ya creado y configurado, se proporciona *Single Sign On* (SSO) [11] y se mejora la seguridad de la infraestructura mediante la utilización de *Proxy Servers* que actúan de intermediarios de las redes privadas virtuales.

4 Metodología

Este proyecto se desarrolló bajo el marco de las metodologías ágiles [12] popularmente utilizadas en el desarrollo de *software*. Más concretamente se siguió el método SCRUM, ya que el proyecto se llevó a cabo en una empresa y hubo que alinear este proyecto con su manera de trabajar.

SCRUM es una metodología que descompone un proyecto con un objetivo general en pequeños subobjetivos que se van llevando a cabo durante iteraciones cortas.

Durante una iteración se realizan las etapas de análisis, desarrollo y testeo. En este proyecto se definieron iteraciones semanales, y al final de estas, se llevaron a cabo reuniones con el equipo involucrado para abordar los distintos temas desarrollados y poner las opiniones en común.

Esta metodología es muy beneficiosa debido a que mediante reuniones periódicas se puede llevar un seguimiento de las distintas tareas, y se permite alinear el objetivo común con el desarrollo de estas. El punto fuerte de las metodologías ágiles es que el proyecto se somete a una revisión continua, lo cual permite prevenir que un error pequeño pueda convertirse en un error mayor debido al efecto *snowball* [13].

Para gestionar las distintas tareas y subtareas se utilizó la herramienta Jira [14], ya que es el producto utilizado por los trabajadores de la empresa. Jira proporciona una visión en columnas que se corresponden con los distintos estados del proyecto, es adaptable, personalizable y compartida.

5 PLANIFICACIÓN

En este proyecto se llevó a cabo una planificación en seis tareas divididas en subtareas, que se muestran en el diagrama de Gantt (*figura 3 en el anexo*) y se explican a continuación.

5.1. Estudio preliminar

Esta tarea se centra en captar información para adquirir conocimiento sobre el tema y asentar las bases del proyecto a través de un análisis técnico. Finalmente, se diseña la arquitectura del proyecto.

5.1.1. Recolección de información

Durante el desarrollo de esta subtarea se extraen distintos enlaces de interés recogidos en este documento, y se indaga en distintos proyectos existentes que sirven de inspiración.

5.1.2. Análisis técnico

Posteriormente, se lleva a cabo un análisis técnico para extraer los requisitos que debe satisfacer la realización de este proyecto, a través de reuniones con el *Project Manager* (PM) y el *Chief Technology Officer* (CTO) de la empresa.

5.1.3. Diseño de la arquitectura

Una vez el proyecto está estructurado, se pasa a diseñar la arquitectura del entorno de desarrollo. También se deben extraer unas breves conclusiones que sirven para alinear el objetivo de todo el equipo con el enfoque de este proyecto.

5.2. Montaje del servidor Cloud

Durante esta tarea se realiza una revisión de la arquitectura para obtener la versión final, un análisis del mercado para llevar a cabo la contratación del servidor *Cloud*, y finalmente se instala el sistema operativo y se crea un *firewall* para la máquina.

5.2.1. Análisis del mercado, contratación y licenciamiento

Una vez se dispone de la arquitectura revisada, se procede a investigar distintas empresas que ofrecen *hosting* en *Cloud* mediante un análisis de mercado, y se escoge la opción más conveniente.

En el momento que el servicio está contratado, se adquiere la licencia del *software* que se utilizará para la creación de las máquinas virtuales.

5.2.2. Instalación del sistema operativo y firewall

Cuando se dispone de la infraestructura base, se instala y configura el sistema operativo para poder empezar a crear el *Cloud* que aloja todos los servidores necesarios. Se dota al *Cloud* de un *firewall* para que bloquee los posibles ataques.

5.2.3. Revisión de la arquitectura

El objetivo de esta subtarea consiste en revisar la arquitectura para obtener un esquema más sólido y representativo, el cual permitirá entender el funcionamiento del ambiente de desarrollo en cuanto a intercomunicación e infraestructura.

5.3. Creación e interconexión de máquinas virtuales

Una vez está listo el servidor en la nube, se diseña la infraestructura de red y se comienzan a crear e interconectar las máquinas virtuales. Finalmente, se llevan a cabo distintas pruebas para confirmar el correcto funcionamiento de las máquinas.

5.3.1. Diseño y creación de la infraestructura de red

El objetivo de esta subtarea es diseñar una infraestructura de red que permita satisfacer los requisitos del proyecto. En este caso se crean dos redes privadas virtuales, una para desarrollo y la otra para producción.

5.3.2. Despliegue de máquinas virtuales (MV)

Una vez se dispone de toda la infraestructura *Cloud* y el *software* que nos permite crear y gestionar las máquinas virtuales, se crean, configuran e interconectan todos los servidores que alojan los servicios instalados.

5.3.3. Testeo (fase 1)

Una vez montado el *Cloud* y estén las MV desplegadas, se testea que todas puedan comunicarse debidamente entre ellas, y también que se disponga de los requisitos necesarios para poder alojar los servicios.

5.4. Instalación e integración del Software

Mediante el acceso a las máquinas virtuales debidamente interconectadas, se procede a instalar, configurar e integrar el *software*. Finalmente, se procede a comprobar si la integración de los productos funciona correctamente.

5.4.1. Instalación y configuración del Software

Esta subtarea forma parte del objetivo más importante y costoso de todo el desarrollo del proyecto. Durante su realización, se instala y configura todo el *software* necesario para dotar de las funcionalidades requeridas del entorno de desarrollo.

5.4.2. Integración de los servicios

Cuando el *software* necesario está debidamente instalado, se pasa a integrar los productos entre ellos.

Los servicios por separado son herramientas muy potentes para la gestión de usuarios, accesos, contraseñas y ofrecen seguridad a la hora de almacenar datos de los usuarios.

Aunque por separado sean herramientas útiles, integrarlas ofrece funcionalidades clave para las empresas que quieran introducir doble factor de autenticación, SSO y protección de recursos mediante *Proxy Servers*, entre otras.

5.4.3. Testeo (fase 2)

Con todos los servicios ya integrados, se deben testear conjuntamente para más adelante proceder a configurar los servidores *Proxy* e introducir autenticación multi factor y SSO.

5.5. Configuración

Cuando el *software* está debidamente integrado, se proporcionan mejoras de seguridad al entorno utilizando autenticación multi factor, servidores *Proxy* y *Single Sign On*. Finalmente, se comprueba que el funcionamiento conjunto de todo el entorno es el adecuado.

5.5.1. Mejoras de seguridad

Durante esta subtarea se introduce la autenticación multi factor en el ambiente de desarrollo a través de la herramienta NetIQ Advanced Authentication, y también se crean servidores *Proxy* que protegen todos los recursos internos del laboratorio a través del *software* NetIQ Access Manager.

5.5.2. Single Sign On (SSO)

Mediante el desarrollo de esta subtarea se dota al entorno de un método de inicio de sesión único, mayormente conocido como *Single Sign On* (SSO), para lograr este propósito se crean federaciones por vía del protocolo SAML2.0. Con esta funcionalidad podemos acceder a todos los servicios, autenticando solamente una vez.

5.5.3. Testeo (fase 3)

Con la realización de todas las subtareas mencionadas anteriormente, se dispone del ambiente de desarrollo creado en su plenitud. En esta fase de testeo se prueban todas las funcionalidades añadidas y se crea una demo que muestra el correcto funcionamiento del conjunto de servicios.

5.6. Documentación final

Esta tarea se realiza cuando el desarrollo del proyecto ha finalizado. Se termina toda la documentación, se crea la presentación y se confecciona el póster.

5.6.1. Informe final

Con el desarrollo del proyecto finalizado, se procede a confeccionar la primera versión del informe final.

5.6.2. Entrega final

Esta subtarea consiste en preparar y revisar todos los documentos adjuntos al dosier de la entrega final.

5.6.3. Presentación

Durante esta subtarea se dedican esfuerzos a crear la presentación que se utilice para exponer el proyecto delante del jurado evaluador.

5.6.4. Póster

Esta tarea consiste en diseñar un póster que plasme todo el desarrollo del proyecto.

6 DESARROLLO

Este apartado plasma el desarrollo del proyecto a través de la explicación de las tareas previamente planificadas que se han llevado a cabo.

6.1. Estudio preliminar

La intención de esta primera etapa fue asentar una base para tener las ideas claras, y avanzar de una manera productiva. Se realizó una primera recolección de información, un análisis técnico, y por último se diseñó la arquitectura del entorno a través de toda la información recolectada.

6.1.1. Recolección de información

Durante esta subtarea se indagó en la red en búsqueda de información para ampliar el conocimiento en el ámbito de las estructuras *Cloud*, y de las buenas prácticas a la hora de crear un entorno de desarrollo para empresas.

6.1.2. Análisis técnico

Mediante reuniones con el equipo y los responsables técnicos de la empresa, se extrajeron los requisitos que debía satisfacer la realización de este proyecto y se marcaron puntos críticos que se debían resolver durante el desarrollo de etapas más maduras.

6.1.3. Diseño de la arquitectura

Una vez realizado el análisis técnico, se diseñó la arquitectura del proyecto y se definió que servicios del catálogo de la empresa debían estar presentes en el ambiente de desarrollo. También se definió en el diagrama los servicios migrados del antiguo ambiente de producción al nuevo.

Debido a que la realización de este proyecto se enfoca solamente en el entorno de desarrollo, a continuación se explican únicamente los componentes de este en orden de importancia.

VPN: Servidor que actúa como puerta de enlace a las redes privadas. Autentica a los usuarios internos del

entorno de desarrollo a través de certificados y claves privadas, previamente generadas.

NetIQ Access Manager (NAM): Herramienta que permite gestionar accesos, proteger recursos mediante servidores *Proxy*, asignar políticas de riesgo, crear federaciones y otras múltiples tareas relacionadas con la gestión y control de accesos.

NetIQ eDirectory: Directorio de usuarios dónde se almacenan de forma segura los datos y credenciales de estos. Es una base de datos orientada a objetos organizada en un árbol jerárquico [15] la cual se comunica a través del protocolo LDAP [16].

NetIQ iManager: Consola web de administración del directorio que proporciona acceso seguro a todas las configuraciones. También sirve como herramienta de monitorización de los drivers utilizados para sincronizar con aplicaciones externas.

NetIQ Advanced Authentication Factors (NAAF): Herramienta que permite asignar métodos de autenticación a grupos de usuarios. A partir de estos métodos se crearon políticas para utilizar autenticación multi factor.

NetIQ Self Service Password Reset (SSPR): Servicio web de gestor de contraseñas. Elimina la necesidad de los usuarios de depender de un administrador para cambiar o recuperar sus contraseñas.

Micro Focus GroupWise: Plataforma de mensajería y servicios de correo. Es la solución corporativa de la empresa para comunicarse.

Micro Focus Filr: *Software* dedicado a la compartición de archivos a nivel empresarial, permite almacenar y acceder de forma simultánea a los documentos necesarios.

Rancher Cluster: Cluster dedicado a la gestión de Kubernetes. En el entorno de desarrollo se dispone de tres nodos creados para alojar contenedores.

SUSE Manager: *Software* dedicado a la gestión y actualización del *software* de todo el entorno de desarrollo. Permite lanzar actualizaciones automáticas, instalar paquetes remotamente, otorgar licencias y monitorizar todos los servidores del entorno.

La *figura 1* muestra la arquitectura de la infraestructura de servidores y aplicaciones englobada en un servidor *Cloud*. Dentro de este se fraccionó la red en dos partes, pública y privada. El único servidor que tiene un dominio público es el de VPN, debido a que cualquier usuario que quiera acceder a los entornos tanto de desarrollo como producción, debe encontrarse dentro de la red privada.

El servidor VPN actúa como puerta de enlace para toda la infraestructura, y conjuntamente con la creación del servidor NAM se logra proporcionar un nivel de seguridad alto, ya que este actúa como servidor *Proxy* de todas las máquinas que se encuentran tanto en la VLAN de desarrollo como en la de producción. Es importante destacar que

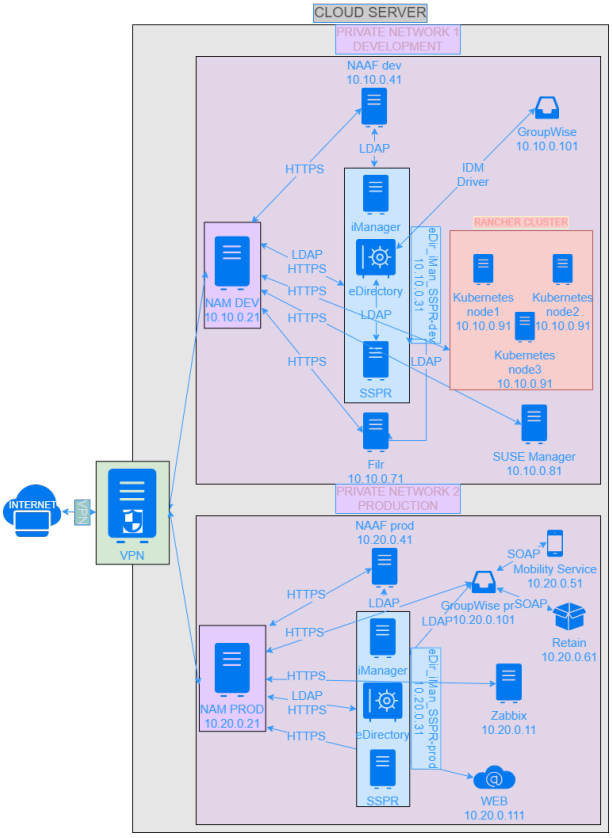

Fig. 1: Arquitectura del entorno

iManager, eDirectory y SSPR están situados en un mismo servidor, debido a que la herramienta de gestión (iManager) y el directorio forman parte del mismo *software*. Por otro lado, SSPR solamente requiere de la instalación de un servidor web Tomcat. Debido a que consume pocos recursos, se decidió alojar en el mismo servidor que los otros dos servicios mencionados.

Los servicios de las redes internas se comunican mediante el protocolo HTTPS con el servidor NAM a través del puerto 443. Todas las comunicaciones que transporten datos de los usuarios mediante consultas al directorio (eDirectory) son realizadas a través del protocolo LDAP/LDAPS (puertos 389 y 636 respectivamente).

Por último, los servicios externos con los que eDirectory se sincroniza proporcionan una protección extra a los datos de los usuarios que estos servicios almacenan localmente. La sincronización se realizó mediante drivers que utilizan políticas de gestión de identidades (IDM) que se programaron en código C++. Esto proporciona una gran profundidad a la gestión de credenciales, debido a que a través de las políticas se puede personalizar totalmente el comportamiento de la comunicación entre el directorio y aplicaciones externas.

6.2. Montaje del servidor Cloud

La siguiente tarea que se ejecutó fue el montaje del servidor, a partir de esta tarea se dispuso de la base en la cual cimentar todo el proyecto. Una vez contratado el servicio de *hosting* que aloja nuestro servidor en la nube, se procedió a instalar el sistema operativo que incluyó todas las máquinas virtuales necesarias para alojar los servicios posteriormente instalados.

En esta etapa se llevó a cabo un análisis de mercado con el cual se decidió que proveedor era el más adecuado, se instalaron el sistema operativo y el firewall, y finalmente se realizó una revisión de la arquitectura.

6.2.1. Análisis de mercado, contratación y licenciamiento

El objetivo de esta tarea fue investigar y contratar el servicio más adecuado para que alojase toda la infraestructura de este proyecto. A través de una búsqueda intensiva comparando distintos proveedores de servicios *Cloud*, se extrajo que la opción más adecuada para alojar la infraestructura de la empresa era *OVHCloud* [17]. Se escogió esta opción debido a que ofrece unos precios competentes y permite tener disponible el servidor cuanto antes debido a su reducido tiempo de entrega.

Aparte de la contratación del proveedor de servicio *Cloud*, se analizó cuál sería el sistema operativo (SO) adecuado para esta máquina, y se extrajo que *VMware ESXI 7.0* [18] sería el elegido. Esto es debido a su gran versatilidad, la buena documentación y el precio razonable que tiene.

VMWare ESXI es un *software* que recoge las funcionalidades de hipervisor, SO, y *software* de virtualización. Esto es una gran ventaja, debido a que con la adquisición de este producto se dispone de todas las herramientas necesarias para el host *Cloud*.

6.2.2. Instalación del sistema operativo y firewall

Una vez se dispuso de la infraestructura *Cloud*, se utilizó la interfaz web que *OVHCloud* provee para gestionar los servidores dedicados. Se instaló *VMware ESXI* y se configuró la estructura de almacenamiento de forma que se pudo satisfacer todos los requerimientos.

Específicamente se crearon dos *datastores* (*datastore1, datastore2*), en el cual el primero se utilizó como partición reservada para el sistema operativo y los servicios internos del *VMware kernel*, y la segunda partición se creó de manera que tuviese espacio suficiente para alojar todas las máquinas virtuales, ISOs, archivos de backup, etc.

6.2.3. Revisión de la arquitectura

Finalmente, se realizó una revisión de la arquitectura. Fruto de este análisis, se identificó una posibilidad de migrar el entorno de producción existente a la infraestructura *Cloud* inicialmente creada para desarrollo.

6.3. Creación e interconexión de máquinas virtuales

La fase de creación e interconexión fue crucial para el desarrollo del proyecto, ya que las máquinas virtuales creadas tenían que satisfacer todos los requisitos de sistema del *software* que más tarde se instaló. Durante esta tarea llevó a cabo el diseño y la creación de la infraestructura de la red, y se realizó el despliegue de las máquinas. Finalmente, se comprobó el correcto funcionamiento de las conexiones.

6.3.1. Diseño y creación de la infraestructura de red

Para dotar al entorno de las interconexiones necesarias para lograr el comportamiento adecuado de las redes, se diseñó toda una infraestructura de red que tenía como objetivo cumplir el planteamiento realizado durante la creación de la arquitectura del *Cloud*. Esta infraestructura consta de los siguientes elementos:

Rack virtual (vRack): Un vRack [19] es un rack virtual que permite agrupar virtualmente varios servidores, permitiendo que se puedan comunicar entre ellos de manera privada mediante VLANs. En el caso de este proyecto, surgió la necesidad de tener un paquete de direcciones IP públicas añadidas en el vRack, esto es debido a que a partir de estas direcciones podemos fraccionar las VLANs que se consideraron durante el diseño de la arquitectura.

Conmutadores virtuales (vSwitch): En este proyecto se crearon dos conmutadores virtuales, el primero (vSwitch0) se utiliza para servicios internos del propio kernel del sistema operativo, p.e. auditoría, tolerancia a fallos, etc. El segundo (vRackSwitch), es el que conecta todas las máquinas virtuales que coexisten en nuestro servidor. En este caso, las máquinas virtuales de desarrollo, las de producción, y también la máquina VPN que tiene asignada una dirección IP pública.

NICs físicos: Nuestra máquina *Cloud* dispone de cuatro adaptadores de red físicos (NICs físicos), vmnic0-3. Estos NICs están clasificados según su utilidad, los vmnic0 y vmnic1 están dedicados al tráfico de redes privadas, y los vmnic2 y vmnic3 se dedican al tráfico de las redes públicas.

IP pública del host ESXI: *OVH Cloud* nos proporcionó por defecto un par de direcciones IPs públicas. Una de ellas es donde se aloja el host que contiene el propio *VMware*, y la otra dirección IP es la puerta de enlace que utiliza esta máquina para salir hacia internet. Debido al diseño de nuestra arquitectura, redirigimos el tráfico saliente a través de la máquina VPN y la IP de la puerta de enlace proporcionada por defecto no será utilizada.

Redes privadas: En este proyecto existen dos redes virtuales privadas, una de ellas se dedicará al entorno de desarrollo y la otra al entorno de producción.

Grupos de puertos: La creación de grupos de puertos es la herramienta que ofrece *VMware ESXI* para poder tener varias redes conectadas a un mismo *switch*, pero estando aisladas entre ellas.

En este proyecto se crearon tres grupos de puertos, que corresponden a las tres redes mencionadas. El primero está dedicado a la red privada de desarrollo, el segundo dedicado a de producción, y el último está dedicado a las máquinas que necesiten tener una interfaz de red pública, en este caso solamente se incluye la máquina VPN.

6.3.2. Despliegue de máquinas virtuales (MV)

Una vez se dispuso de la infraestructura de red, se crearon y configuraron las máquinas virtuales necesarias para poder empezar a instalar el *software* en ellas (*fig. 4 en el anexo*).

VPN: Se trata de un *appliance* [20]. Los *virtual appliance* son sistemas pre-integrados, que contienen todo lo necesario en cuanto a SO y *software* para desplegar la aplicación. Esto garantiza un aislamiento completo de la aplicación, y facilita mucho la tarea de despliegue.

Esta MV actuará como router, debido a que todos los servicios alojados en las redes privadas utilizarán el *gateway* público de esta máquina para salir a internet. Esto nos proporciona una mejora de la seguridad de toda la infraestructura, ya que para acceder a cualquier servicio de la empresa, se deberá autenticar primero mediante doble factor. Consta de tres interfaces de red. Dos privadas, una para cada VLAN, y una pública que se trata de la puerta de enlace.

NAM DEV: Esta máquina es el *appliance* encargado de realizar la función de servidor *proxy* a todas las MV del *Cloud* contenidas en el entorno de desarrollo. Cabe destacar que cada entorno dispone de su servidor NAM correspondiente, encargado de actuar como *proxy* a sus servicios. La máquina está conectada al eDirectory a través del protocolo LDAP para poder leer datos de usuarios y realizar autenticaciones.

En cuanto a red se refiere, tiene dos interfaces de red, esto es debido a que debe tener conexión a la VLAN y la puerta de enlace (VPN) para así poder ejercer de servidor *Proxy* para todos los servicios.

eDirectory/iManager/SSPR: Esta máquina aloja tres servicios, esto es debido a que todos ellos son muy ligeros, y se puede ahorrar capacidad de memoria y cómputo englobándolos todos en una misma máquina virtual.

Los servicios que se encuentran en esta máquina permiten almacenar y gestionar las credenciales de los usuarios a través del directorio y el iManager. SSPR proporciona un portal de autoservicio, donde los usuarios podrán modificar y recuperar sus contraseñas, entre otras funcionalidades.

La red está configurada mediante una sola interfaz, la cual corresponde a la red privada.

NAAF: Esta máquina es el *appliance* donde se configura y gestiona todas las autenticaciones multi factor del entorno. Se aloja en la red privada y solamente tiene una interfaz, ya que a través de su *gateway* y el enrutamiento realizado, podrá comunicarse adecuadamente con todas las máquinas de su red y también tendrá acceso a internet, a través del servidor *Proxy* (NAM DEV).

GroupWise: Máquina que contiene el servicio de correo de la empresa.
Debimos dotar a esta máquina de una gran cantidad de almacenamiento y memoria, debido a que será la responsable de gestionar todo el correo corporativo. Consta de una sola interfaz correspondiente a la red privada.

Filr: Esta máquina es un *appliance*. Es la encargada de almacenar todos los archivos compartidos entre los trabajadores de la empresa, que pueden ser accedidos a través de un front-end web. Solamente tiene una interfaz de red, que corresponde a la red privada.

Rancher cluster: Este servidor engloba tres nodos dedicados a la creación de Kubernetes, estos serán los encargados de alojar todos los contenedores que se deseen crear. A través de otra máquina virtual, la cual contendrá el *software* denominado Rancher, se gestionarán los contenedores. Tanto los nodos de Kubernetes como la máquina que contiene Rancher, solamente tienen una interfaz de red perteneciente a la red privada.

SUSE Manager: Esta máquina servirá para gestionar todas las operaciones relacionadas con la actualización de *software*, configuración, supervisión del rendimiento y las auditorías de toda la red. Solamente constará de una interfaz, la cual pertenece a la red privada.

6.3.3. Testeo (fase 1)

Una vez realizadas todas las tareas comentadas, se procedió a testear que todas las máquinas tuviesen las conexiones adecuadas, respetando las redes privadas creadas y utilizando la máquina VPN como router hacia internet.

6.4. Instalación e integración del Software

Durante el desarrollo de esta fase, se instaló todo el *software* necesario en las máquinas virtuales (MV). Una vez se dispuso del *software* instalado en las máquinas, se procedió a integrarlo.

La integración de estas herramientas ofrece un conjunto de funcionalidades muy amplio. Estas funcionalidades se enfocan en la gestión de credenciales, accesos, permisos, contraseñas y autenticaciones.

6.4.1. Instalación y configuración del Software

En primer lugar, en esta subtarea se llevó a cabo la instalación basada en dotar a las MV del *software* necesario para que realicen las funciones que se han descrito anteriormente. Una vez se instaló el *software*, se configuraron los parámetros necesarios: dominios, estructura del árbol del directorio, interconexiones, grupos de usuarios y roles.

Se debe tener en cuenta que en las MV que son *virtual appliances*, solamente se llevó a cabo la configuración de sus servicios.

6.4.2. Integración de los servicios

Durante la integración de los servicios, se llevó a cabo un proceso de configuración de las herramientas, con la finalidad de que actuasen en conjunto.

En primer lugar, se procedió a integrar el directorio (eDirectory) con la herramienta de gestión web (iManager), la integración de estas dos herramientas permite tener un control total de las operaciones que se deseen realizar dentro del directorio a través de una interfaz web.

Seguidamente, se procedió a integrar el portal de autoservicio de contraseñas (SSPR) con el directorio. De esta manera se unificó en un servicio la creación de políticas de contraseña, gestión de autenticación de los usuarios, y la recuperación de la contraseña.

La siguiente integración que se llevó a cabo fue la de NetIQ Advanced Authentication (NAAF). Este paso fue crucial para el posterior propósito de otorgar autenticación multi factor a los servicios deseados.

En penúltimo lugar, se integró la herramienta de gestión del sistema operativo de todos las máquinas del entorno (SUSE Manager). Mediante la integración de este servicio con los demás servidores, se pudo registrar el sistema operativo de todos ellos al mismo tiempo, facilitando así esta tarea.

Por último, se integró el servidor de correo de pruebas de la empresa (GroupWise) con el directorio para poder obtener todos los usuarios de este, y autenticar mediante LDAP cuando se acceda al servicio web de mail.

6.4.3. Testeo (fase 2)

Durante esta fase de testeo se comprobó que todos los servicios fuesen capaces de comunicarse con el directorio, y que pudiesen autenticar a los usuarios mediante el protocolo LDAP.

6.5. Configuración

La fase de configuración de los servicios fue una de las más complicadas de llevar a cabo, debido a que se utilizaron varios protocolos para dotar al entorno de autenticación multi factor y SSO a través de servidores *Proxy*. En primera instancia se crearon federaciones entre servicios mediante el protocolo SAML 2.0, y se utilizó el servicio NetIQ Access Manager (NAM) para que actuase como *reverse proxy server* a todos los servicios del entorno. Esto proporciona una gran seguridad a los servicios internos, debido a que todas las conexiones del exterior (en este caso la propia VPN) conectan directamente con NAM a través de su interfaz externa y este redirigirá el tráfico a los servicios adecuados, con su dirección y puerto correspondiente, dependiendo del tipo de conexión.

6.5.1. Mejoras de seguridad

Para mejorar la seguridad de los servicios, se configuraron todos los servidores a través de NetIQ Access Manager (NAM) y se crearon servidores *proxy*, los cuales dotan de una protección extra a todos los servidores internos del entorno de desarrollo.

A través de esta estructura, se puede definir cuáles serán los recursos protegidos de los servicios. En el caso de este proyecto, se protegieron todos los servicios de administración reservados a los usuarios privilegiados que se dedican a administrar las distintas actividades que los usuarios realizan dentro del entorno.

Una vez se tuvieron los servicios protegidos, se procedió a configurar la autenticación multi factor para estos. Este propósito se logró gracias a la integración entre NetIQ Advanced Authentication (NAAF) y NAM. Fruto de esta dupla de productos, se definieron métodos de autenticación asociados a clases y contratos, que posteriormente se asignaron directamente a recursos protegidos, definidos anteriormente en los servidores *proxy*.

6.5.2. Single Sign On (SSO)

Como segundo objetivo se logró dotar de inicio de sesión único a todos los servicios, se introdujo *Single Sign On* (SSO) mediante la federación de servicios utilizando el protocolo SAML2. Este hito es muy beneficioso para el entorno, debido a que los usuarios una vez autenticados en el *Identity Provider* (IP), NetIQ Access Manager en nuestro caso, pueden acceder a todos los servicios del entorno, *Service Provider* (SP), sin tener que volver a identificarse. Esto funciona estableciendo una relación de confianza entre el IP y el SP mediante un intercambio de archivos de metadatos. Estos archivos contienen la información necesaria para realizar traspasos de información de forma segura. Entre estos datos se encuentran certificados, URIs de redireccionamiento e internas, y datos de la entidad certificadora que ha emitido dichos certificados.

Cabe destacar, que en el servidor dedicado a eDirectory, iManager y SSPR, se llevó a cabo la creación de un framework dedicado a los usuarios finales (*figura 2*). Dentro de este framework web, los usuarios logran acceder a todos los servicios que se encuentran en el entorno de desarrollo. Este framework funciona a través del servicio One SSO Provider (OSP) [21] mediante el cual logra comunicarse con el directorio y las aplicaciones integradas.

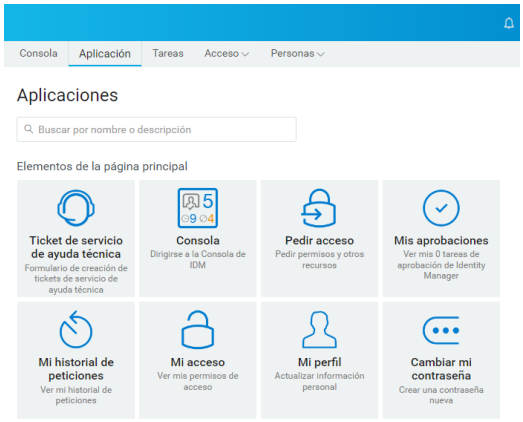

Fig. 2: Framework de los usuarios

No obstante, se quiso ir un paso más allá, y se logró integrar el framework con el servicio de gestión de accesos (NAM). Para lograrlo, se hizo uso del protocolo de SSO SAML2. En primer lugar, se estableció una relación de confianza entre el proveedor de servicio (OSP) y el proveedor de identidades (NAM) para relegar la autenticación al servidor encargado de gestionar los accesos.

Una vez se obtuvo esta relación de confianza, se procedió a configurar el servidor *proxy* para que funcionase adecuadamente con SSO. Esto dio bastantes problemas, debido a que OSP es bastante delicado con las redirecciones de las cabeceras, y al estar protegido por un servidor *proxy*, las conexiones entrantes se traducen de un dominio público (idapps.itechgrup.com) a un dominio privado (it-idvdev.itechgrup.local).

Aparte, también se debía realizar una traducción de puertos, debido a que las peticiones externas llegan al puerto 443 del NAM y estas deben ser redirigidas al puerto 8543, que es el encargado de alojar todas las aplicaciones del servicio OSP.

Finalmente, mediante configuraciones de redirección en el *Firewall* del servidor proveedor de servicio, se logró el hito deseado. El *framework* se logró proteger mediante un *Proxy*, y tenía SSO a todas sus aplicaciones.

6.5.3. Testeo (fase 3)

Durante esta última fase de testeo, se realizaron las pruebas pertinentes para asegurar que las funcionalidades introducidas tuviesen el comportamiento deseado. Se creó un circuito de pruebas para el usuario, de modo que se comprobó que todos los posibles casos de uso del entorno no presentasen ningún error.

Fue realmente útil realizar esta subtarea, debido a que surgieron algunos resultados no deseados, y a través de esta fase final de testeo se pudo retocar los pequeños errores que había.

7 Discusión

Mediante la realización de este proyecto, se obtuvo un entorno de desarrollo que ofrece un servicio de calidad. Este entorno contiene todas las funcionalidades necesarias para llevar a cabo diferentes testeos previos a puestas en marcha, de una forma colaborativa, productiva y eficiente. El entorno de desarrollo creado es una herramienta muy potente, que facilita la realización de tareas previas a la puesta en marcha en los entornos de producción de los clientes, mejorando así la metodología de trabajo de la empresa.

Tal y como se observa, los objetivos iniciales de este proyecto han sido cumplidos. A través de un correcto montaje de la estructura *Cloud* en la cual se ha basado este proyecto, se dota a este entorno de una alta disponibilidad, escalabilidad y acceso múltiple. Mediante la creación de máquinas virtuales y su correcta interconexión a través de un buen diseño de la arquitectura de red, se realizó la instalación y configuración de todos los productos de Ciberseguridad necesarios enfocados a la gestión de identidad y accesos. Finalmente, se configuraron servidores *Proxy* y se introdujeron las tecnologías de *Single Sign On* y autenticación multi factor. Gracias a todos estos hitos, se ha obtenido un sistema robusto en el cual basar todas las implementaciones y pruebas preliminares, ya que es un entorno seguro y totalmente aislado del entorno de producción.

A través de la utilización de este entorno, se han agilizado las puestas en marcha de los proyectos de la empresa, ya que la posibilidad de tener el entorno de desarrollo operativo, permite investigar de manera colaborativa entre trabajadores experimentados con otros que no lo son tanto, fomentando así la cooperación dentro de la empresa. El entorno de desarrollo, junto al traspaso de conocimiento entre trabajadores, introduce un nuevo método de formación para futuras incorporaciones, ya que estas dispondrán de un entorno dónde realizar todas las pruebas que deseen, y tendrán una alta cantidad de proyectos en los cuales inspirarse.

Fruto de esta colaboración que el entorno de desarrollo brinda, se ha logrado acortar significativamente los tiempos de entrega de los proyectos, debido a que el entorno permite generar experiencias previas sobre distintos puntos críticos, que se deben tener en cuenta durante la realización de las puestas en marcha en las empresas cliente.

La implementación de este proyecto dentro de la empresa en la cual ha sido realizado, logra mejorar la calidad final de los productos y servicios entregados, y por ende, mejora la satisfacción de los clientes respecto a la contratación de los mismos. Esto es debido a que la utilización de este entorno, descarta la necesidad de estar conectados al sistema de la empresa cliente durante las actividades previas a puestas en marcha, de esta manera se evita una posible afectación a los servicios dedicados a usuarios finales.

La utilización de este entorno de desarrollo, no solamente consigue afianzar las relaciones entre los clientes para los cuales se trabaja, sino que también proporciona herramientas para crear *demos* que permitan abrir nuevas líneas de negocio, promoviendo así la captación de clientes.

Se puede afirmar que los resultados obtenidos son asequibles para un ingeniero informático, debido a que se han logrado alcanzar todos los objetivos propuestos inicialmente. Cabe destacar que sin la posibilidad de realizar este proyecto en una empresa, habría sido mucho más difícil la ejecución del mismo, ya que la contratación del servidor *Cloud* y las distintas licencias del *Software* tienen un elevado coste.

En líneas generales, la realización de este proyecto aporta un valor añadido a los servicios que la empresa provee, debido a que introduce mejoras significativas en el ciclo de desarrollo de los servicios entregados a los clientes.

8 Conclusiones

La necesidad de disponer de un entorno de desarrollo dentro de las empresas relacionadas con las Tecnologías de la Información (TI), es un hecho.

Este proyecto tiene como objetivo principal la creación de un entorno de desarrollo, en el cual llevar a cabo tareas previas a futuras implantaciones en entornos de producción de los clientes, mejorando así la metodología de trabajo utilizada por la empresa.

Este objetivo ha sido logrado a través de la creación de una infraestructura en *Cloud* que dota al sistema de una alta disponibilidad y escalabilidad, y que contiene una red privada virtual (VPN) que aloja todas las máquinas virtuales requeridas para instalar y configurar los productos necesarios para realizar las implantaciones previas a puestas en marcha.

Gracias a la integración del *software* que la empresa ofrece, se dispone de un entorno de desarrollo que dota a los trabadores de las herramientas necesarias para llevar a cabo tareas previas a puestas en marcha relacionadas con la ciberseguridad, más concretamente a la gestión de identidades y accesos (IAM).

Paralelamente, se introdujeron mejoras en la seguridad del entorno de desarrollo creado a través de la utilización de *Proxy Servers*, y las tecnologías *Single Sign On* y autenticación multi factor.

Tecnologías como autenticación multi factor (MFA) y *Single Sign On* (SSO) son realmente influyentes hoy en día, debido a que está demostrado que el eslabón más frágil de un sistema de seguridad en cualquier empresa del mundo, es el factor humano. Implementar soluciones de autenticación multi factor mejora potencialmente la seguridad dentro de cualquier infraestructura. Se puede observar también que la utilización de protocolos tales como LDAP y SAML2.0 son realmente beneficiosos a la hora de securizar usuarios, datos, conexiones y traspasos de información.

El proyecto ha comenzado a dar sus frutos en las pocas semanas que lleva implantado. Los resultados obtenidos llevan a pensar que la realización de este proyecto mejora la metodología de trabajo, y por ende, el resultado final de las implantaciones.

Cabe destacar, que al ser un servicio nuevo introducido en el ámbito de una empresa, los trabajadores se irán familiarizando cada vez más con el entorno a medida que pase el tiempo. Esto dará paso a un crecimiento de la empresa y a la adaptación a nuevos métodos de trabajo.

El entorno de desarrollo creado, no solamente afectará a los resultados finales, sino que también el trabajo previo de futuras incorporaciones en la empresa será llevado a cabo de una manera mucho más productiva. Es decir, se abre una nueva posibilidad de crear una línea formativa interna en la nube, en la cual basar el aprendizaje de los servicios más importantes e interesantes que se ofrecen por parte de la empresa.

Se considera que el entorno de desarrollo obtenido nunca estará cerrado, debido a que en el ámbito de la Ciberseguridad, día a día surgen nuevas amenazas, oportunidades y servicios.

Este entorno de desarrollo se encontrará en constante evolución fruto de su propia existencia. De hecho, se plantea una nueva expansión del servicio, a través de la creación de un sistema de *backup* distribuido en la nube, que permita almacenar de manera segura los datos y que proporcione una alta disponibilidad de estos.

9 Agradecimientos

Para finalizar la realización de este proyecto me gustaría agradecer a todo mi ambiente cercano, familia, pareja y amigos por apoyarme en este camino.

Dar las gracias también a ITechGrup. Empresa en la cual ha sido realizado este proyecto.

Por último, pero no menos importante, agradecer a Ramon Martí por tutorizar este trabajo de final de grado, ayudándome siempre y proveyéndome de consejos útiles en todas las etapas de la realización de este proyecto.

Referencias

[1] Medium. 2016. The Importance of Having a Unified Development Environment. Available at: https://medium.com/@vincentius/the-importance-of-having-a-unified-development-environment-844b22865f9e.

[2] Itechgrup. 2015. Itechgrup — Profesionales en IT, ciberseguridad, riesgos, gobernanza. Available at: https://www.itechgrup.com/.

[3] T. Erl, Z. Mahmood and R. Puttini, Cloud computing. Noida: Dorling Kindersley (India), 2018.

[4] Intelequia. 2020. Ventajas del cloud computing. Available at: https://intelequia.com/blog/post/2055/ventajas-del-cloud-computing.

[5] Ibm.com. n.d. Identity and Access Management (IAM) Solutions — IBM. Available at: https://www.ibm.com/security/identity-access-management.

[6] Okta.com. 2022. Okta UK — The Identity Standard. Available at: https://www.okta.com/uk/.

[7] Microfocus.com. 2019. Strengthen Your Cyber Resilience — CyberRes. Available at: https://www.microfocus.com/es-es/cyberres.

[8] Yubico. 2022. Micro Focus — Yubico. Available at: https://www.yubico.com/es/works-with-yubikey/catalog/micro-focus/.

[9] Suse.com. 2019. SUSE: Soluciones de código abierto para servidores empresariales y la nube. Available at: https://www.suse.com/es-es/.

[10] OVHcloud. 2020. Servidores dedicados Scale-1. Available at: https://www.ovhcloud.com/es-es/bare-metal/scale/scale-1/.

[11] G. Blokdyk, Single sign-on: Beginner's Guide. CreateSpace Independent Publishing Platform, 2017.

[12] Sotomayor, S., 2021. Las metodologías ágiles más utilizadas y sus ventajas dentro de la empresa. Thinking for Innovation. Available at: https://www.iebschool.com/blog/que-son-metodologias-agiles-agile-scrum/.

[13] Hodge, M., 2016. The Snowball Effect: Why Software Testing Can't Afford to Be Passive — Lighthouse Technologies. Lighthouse Technologies. Available at: https://lighthousetechnologies.com/2016/10/19/the-snowball-effect-why-software-testing-cant-afford-to-be-passive/.

[14] Atlassian. n.d. Jira — Software de seguimiento de proyectos e incidencias. Available at: https://www.atlassian.com/es/software/jira.

[15] Microfocus.com. 2021. Lightweight Directory Access Protocol — NetIQ eDirectory — Micro Focus. Available at: https://www.microfocus.com/es-es/products/netiq-edirectory/overview.

[16] LDAP.com. n.d. LDAP.com. Available at: https://ldap.com/.

[17] OVHcloud, OVHcloud. Available: https://www.ovhcloud.com/es-es/.

[18] Gillis, A., 2021. What is VMware ESXi? - Definition from WhatIs.com. SearchVMware. Available at: https://www.techtarget.com/searchvmware/definition/VMware-ESXi.

[19] Ovh.es. 2022. vRack: Cree VLAN privadas para sus servidores. Available at: https://www.ovh.es/soluciones/vrack.

[20] Turnkeylinux.org. 2018. What is a virtual appliance? — TurnKey GNU/Linux. Available at: https://www.turnkeylinux.org/virtual-appliance.

[21] NetIQ Identity Manager Administrator's Guide to the Identity Applications. NetIQ, 2018, pp. 601-608.

APÉNDICE

A.1. Diagrama de Gantt

En la siguiente figura se muestra el diagrama de Gantt utilizado para plasmar la planificación que se ha llevado a cabo durante la realización de este proyecto.

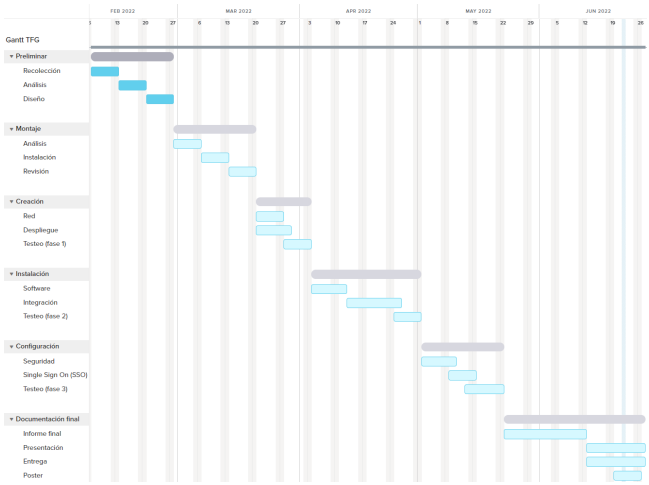

Fig. 3: Diagrama de Gantt

A.2. Esquema de máquinas virtuales

En la siguiente figura se muestran las máquinas virtuales creadas, interconectadas en su respectiva red privada.

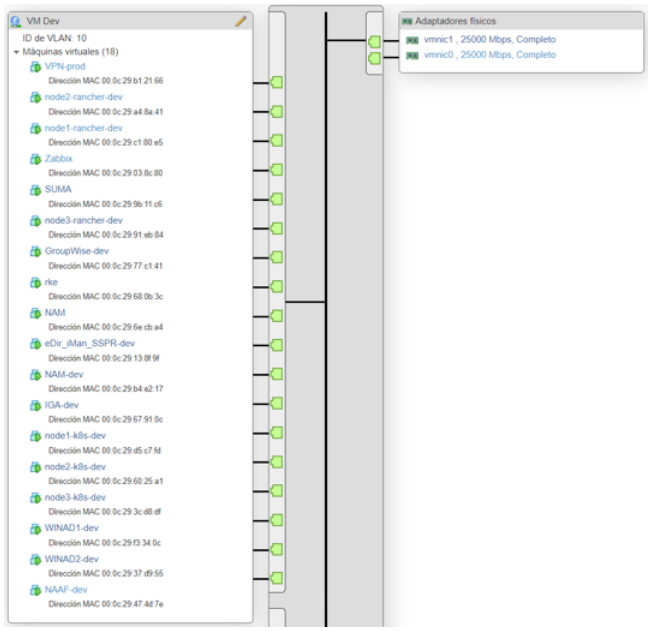

Fig. 4: Esquema máquinas virtuales

A.3. Manual VPN y servicios internos

Previamente a la puesta en marcha del entorno de producción creado, también se confeccionó un manual que explica todos los pasos que se deben llevar a cabo para conectarse a la VPN de la empresa.

Consultar enlace: `https://drive.google.com/file/d/1Vlq-NhaL_PevKd5us7vLBkwYul48xP8F/view`

A.4. Manual de inscripción a métodos multi factor

Para que los usuarios pudiesen acceder a los servicios de producción migrados al nuevo servidor *Cloud*, se creó un manual estilo *Dummies* para que los usuarios especificasen su nueva contraseña y se inscribiesen los métodos de autenticación multi factor deseados.

Consultar enlace: `https://drive.google.com/file/d/1rLklgCAa775a-e9FqvYa_XzoUuMIxDAX/view`