Trabajo Fin de Grado

Condiciones y requisitos de seguridad para la acreditación de un nodo del Sistema de Información para el Mando y Control de ET (SIMACET V.5)

Autor

Juan Carlos Morales Abdelatif

Directores

Director académico: Dr. D. Carlos Sánchez Tapia

Director militar: Cap. Ricardo Simón Serna

Centro Universitario de la Defensa-Academia General Militar

Año 2018

Resumen

A medida que la tecnología avanza, las organizaciones van cambiando la manera de gestionar su información y datos de usuario. La integridad, fidelidad, disponibilidad y seguridad de estos datos se ha convertido en algo crucial para las empresas y administraciones públicas. Las Fuerzas Armadas y, en este caso, el Ejercito de Tierra no son menos ante estas necesidades. Es por ello que el principal sistema de mando y control con el que cuenta el Ejército de Tierra (SIMACET) se actualiza acorde a estos requerimientos y debe pasar un proceso de acreditación para garantizar la seguridad de esta nueva actualización.

En este proyecto se va a proceder a desglosar todo el proceso de actualización de este sistema a una nueva filosofía de software, la virtualización, así como el de actualización de los requisitos que se han de implementar para que, después de su proceso de acreditación, un nodo de SIMACET sea satisfactoriamente acreditado por el Centro Criptológico Nacional (CCN) o la Jefatura de Apoyo Técnico CIS (JCISAT), que son ambos los organismos competentes de acreditación en el Ejercito de Tierra.

Para alcanzar el objetivo, se ha comenzado por analizar el hardware propuesto para instalar la nueva versión de SIMACET, analizar la electrónica de red propuesta, y estudiar el software de virtualización elegido, su estructura y diferentes tecnologías de supervivencia y optimización. Una vez realizado este paso, se ha procedido a estudiar todo el proceso de acreditación de un sistema de información, solicitudes y documentación que hay que generar.

Debido a esta nueva filosofía de software, de ahora en adelante cada nodo de SIMACET debe ser acreditado cada vez que salga a una maniobra o ejercicio, al contrario que en versiones anteriores donde con una sola acreditación era suficiente para poder utilizar los nodos. Esto es muy importante ya que el proceso de acreditación lleva unos plazos que deben cumplirse y la coordinación a la hora de tramitar el proceso es esencial.

Abstract

As technology advances, organizations are changing the way they manage their information and user data. The integrity, fidelity, availability and security of these data have become essential for companies and public administrations. The Armed Forces and, in this case, the Army are also dealing with these changes. That is why the main command and control system for the Army (SIMACET) is being updated according to these requirements and it must pass an accreditation process to ensure the security of this new update.

In this project we will proceed to develop the whole process of updating this system to a new philosophy of software: virtualization. Furthermore, the requirements to implement the new update of the system in order to make a SIMACET node satisfactorily accredited by the National Cryptologic Centre (CCN) or the CIS Technical Support Headquarters (JCISAT), both competent accreditation units in the Army, will be described.

To achieve the objective, some aspects have been analysed: the proposed hardware to install the new version of SIMACET, the proposed network electronics, and the chosen virtualization software, its structure and different technologies of survival and optimization. Once this step has been made, the whole process of accreditation of a system of information, applications, and documentation has been studied.

Due to this new philosophy of software, from now on each node of SIMACET must be accredited every time it goes out to a manoeuvre or exercise, in contrast with previous versions where only one accreditation was enough to use the nodes. This is very important because the accreditation process has to be fulfilled and coordination when performing the process is a key aspect.

Agradecimientos

No había mejor lugar para realizar las prácticas de mando que en el Bon II del Regimiento de Transmisiones 1 (Madrid), concretamente en la Cia. CTPC donde encuadrado en la sección de Sistemas de Información, para mi SIMACET, donde un día de septiembre de 2010 un joven sargento se incorporaba a esa Cia y ahora volvía allí para realizar sus prácticas como oficial.

He sido acogido por el mejor personal que podría a haber en una unidad de transmisiones, y como no puede ser menos tengo que citar aquí, ya que sin ellos no habría sido posible este TFG destacando lo cómodo que me han hecho sentir en el Regimiento, mi Regimiento.

Especial agradecimiento al Capitán D. Ricardo Simón Serna, jefe de la Cia. de CTPC que desde el primer día me hizo sentir un mando más, un teniente más. A los Tenientes D. Carlos Barquín Portillo y D. Miguel Ángel De la Vega Iges, que me acogieron como uno más y que sin su aporte técnico y humano tampoco hubiera sido posible este trabajo.

A mis Sargentos Primeros D. Ignacio Moliner Tapia, D. Manuel Javier Menes Díaz y mis Sargentos D. Adrián Pacheco Jiménez, D. Jacobo López Roa y D. Antonio Castillo López, antiguos compañeros y excelentes profesionales que espero y deseo tener bajo mi mando algún día, seguro que, con ellos, sea sección o compañía, formarían el mejor grupo de cuadros de mando de transmisiones sin ninguna duda.

Por otro lado, tengo que agradecer especialmente el aporte que Dr. D. Carlos Sánchez Tapia me ha dado, su continua disponibilidad, amplio conocimiento y gran preparación ha hecho posible dar forma a este TFG.

Índice

Listado de Acrónimos

ADA	Autoridad Delegada de Acreditación
AOSTIC	Autoridad Operacional del Sistema de las TIC
APO	Autorización Provisional para Operar
AR	Análisis de Riesgos
ASA	*Adaptative Security Appliance*
ASS	Administrador de Seguridad del Sistema
ASTIC	Autoridad de Seguridad de las TIC
ATPO	Autorización Temporal con Propósitos Operacionales
CCN	Centro Criptológico Nacional
C	Confidencial
CO	Concepto Operacional del Sistema
DC	*Domain Controller*
DL	Difusion Limitada
DLL	*Dynamic-Link Library*
DNS	*Domain Name Server*
DRES	Declaración de Requisitos de Seguridad
DRS	*Distributed Resource Scheduler*
ESXi	*Elastic Sky X*
ET	Ejército de Tierra
EVC	*Enhanced VMotion Compatibility*
EXE	Ejercicio
FT	*Fault Tolerance*
GE	General de Ejército
HA	*High Availability*
HP	*Hewlett Packard*
HPS	Habilitación Personal de Seguridad
IGEOSIT	*Interim Geo-Spatial Intelligence Tool*
IIS	*Internet Information Services*
iSCSI	*Internet Small Computer System Interface*
JCHAT	*Joint Tactical Chat*
JCISAT	Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica
JEDIVOPE	Jefe de la División de Operaciones
JEME	Jefe de Estado Mayor del Ejército de Tierra
JOCWACTH	*Joint Operations Centre Watch*
JOIIS	*Joint Operations/Intelligence Information System*
LAN	*Local Area Network*
LOGFAS	*Logistics Functional Area Services*
LUN	*Logical Unit Number*
OTAN	Organización del Tratador del Atlántico Norte
PBX	Private Branch Exchange
POS	Procedimientos Operativos de Seguridad
RBA	Red Básica de Área
RRC	Red Radio de Combate
SEGINFOPER	Seguridad de la Información en las Personas

SEGINFOSIT	Seguridad de la Información en los Sistemas de Información y Telecomunicación.
SIJE	Sistema de Información del Jefe de Estado Mayor del Ejercito
SIMACET	Sistema de Información para el Mando y Control del ET
SO	Sistema Operativo
SQL	*Structured Query Language*
STIC	Seguridad en las TIC
TIC	Tecnologías de la información y la comunicación
UCO	Unidad Centro u Organismo
UE	Unión Europea
USB	*Universal Serial Bus*
VLAN	Virtual LAN
VM	*Virtual Machine*
VMNIC	*Virtual Machine Network Interface Controller*
VTS	Verificación Técnica de Seguridad

1. Introducción

1.1 Motivación del trabajo.

En la actualidad, los nodos del Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET) tienen una configuración completamente física, es decir, existe un servidor físico para cada servicio. Con el salto a la versión 5 de este sistema, la configuración de hardware y software varía con el objeto de establecer un sistema virtualizado, se transforman los servidores físicos en virtuales y se adapta toda la electrónica de red para que pueda trabajar de esta manera.

Las necesidades tácticas de los puestos de mando y el incremento en la demanda de servicios por parte de los usuarios han motivado el salto hacia una solución de virtualización, de tal manera que, con menos recursos de hardware, se establezcan más servicios, estos se optimicen al máximo y se asiente un sistema completamente escalable.

Hay que añadir que con esta versión de SIMACET ya no se puede solo hablar de las aplicaciones del sistema estrictamente, sino que se añaden diferentes servicios como una herramienta colaborativa (Sharepoint) y diferentes servicios OTAN (JOIIS, IGEOSIT, LOGFAS, JCHAT, JOCWATCH…).

Para llevar a cabo este cambio se ha optado por una suite de software que ofrece la empresa VMware, que incluye: sistemas operativos específicos de virtualización (VMware ESXi) y una serie de aplicaciones y tecnologías que ofrece esta solución (VMware vCenter Server, VMware High Availability (HA), VMware Fault Tolerance (FT)). Con esto y una electrónica de red adaptada a esta suite, se consigue un despliegue de servicios al usuario con una alta fiabilidad y una gestión de estos servicios mucho más sencilla y descentralizada.

Una vez elegida esta solución de virtualización, y con el fin de poder ser utilizada, el Centro Criptológico Nacional (CCN) establece una serie de normas, instrucciones, guías y recomendaciones que se han de aplicar en el sistema para que este organismo o JCISAT acredite el sistema como seguro en función de la clasificación de seguridad que tiene asignada la información que gestiona el sistema. Estas normas vienen recogidas en las CCN-STIC y serán las bases de este TFG.

Las STIC tienen como fin mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas detectadas por el CCN-CERT. La mayor parte de las normas que se publican en la página web del CCN están especialmente dirigidas al personal de las Administraciones Públicas y empresas. Algunas de las series están clasificadas como Difusión Limitada (DL) o Confidencial (C) y, por tanto, es necesaria su solicitud al CCN-CERT.

Otra novedad en lo referente a la parte de acreditación del sistema es que a partir de ahora cada nodo se acreditará cada vez que participe en un ejercicio, con lo cual, ello conllevará un proceso de instalación, trabajo burocrático y proceso de acreditación que intentará desarrollar este TFG.

1.2 Objetivo y alcance del trabajo.

El objetivo principal del siguiente TFG es establecer las condiciones y requisitos de seguridad que requiere SIMACET versión 5, con el fin de conseguir que un nodo con esta versión sea acreditable por el CCN o por JCISAT. Para ello contaremos con un nodo versión 5 que pertenece al Regimiento de Transmisiones 1 (Madrid) y que está siendo preparado para participar en el EXE QUICK LION 18.

Para poder alcanzar este objetivo se van a desarrollar los siguientes puntos:

1) Identificar y aplicar las medidas de seguridad que afectan al hardware, principalmente a la electrónica de red que conforma el nodo.
2) Identificar y aplicar las medidas de seguridad que afectan al software de virtualización, en este caso aquellas que afectan a VMware vSphere versión 6.5.
3) Identificar y aplicar las medidas de seguridad que afectan al software de SIMACET, desde los controladores de dominio, hasta servidores miembros y las aplicaciones del sistema.

Otro objetivo que se pretende alcanzar en este TFG es definir un procedimiento de montaje e instalación de tal manera que al final del proceso quede un nodo de SIMACET versión 5 en condiciones de ser acreditado por el organismo que corresponda.

1.3 Estructura de la memoria.

Esta memoria está estructurada de la siguiente manera:

1. **Introducción**: en este capítulo se explica de manera general cuál es contenido del trabajo y qué es lo que ha motivado este título. Además, incluye los objetivos que quiere abordar y el alcance de este. Por último, se explica la metodología seguida durante este TFG.

2. **Software**: este capítulo introduce al lector en el software de SIMACET, cómo está compuesto, de qué aplicaciones está formado y cómo funcionan sus redes de conexión, y por otro lado, explica la nueva filosofía de servidores virtualizados a la que va a migrar todo el sistema en base a la suite vSphere de la casa VMware.

3. **Acreditación**: en este capítulo se analiza el hardware propuesto para los nuevos nodos v.5, toda su configuración y puesta en funcionamiento de nivel físico de la capa OSI hasta el nivel de aplicación, así como todo el proceso de acreditación por parte del CCN o JCISAT explicando las autoridades y documentación que están implicadas en este proceso.

4. **Conclusiones y posibles trabajos futuros**: Finalmente se exponen las conclusiones del análisis de este proceso de acreditación de los nuevos nodos que van a formar parte del principal sistema de mando y control del ET y se proponen dos posibles trabajos con el objetivo de mejorar tanto la parte de despliegue de un centro de transmisiones como la optimización de un proceso de acreditación.

1.4 Metodología.

Para alcanzar los objetivos anteriormente citados, en este TFG se ha aplicado la siguiente metodología:

1. Estudiar las características del hardware propuesto para instalar la nueva versión de SIMACET y determinar sus capacidades. En particular, identificar y estudiar las CCN-STIC que afecten a este hardware y cómo se deben aplicar.
2. Estudiar el software VMware vSphere que se va a instalar en los servidores físicos, qué recursos y tecnologías de virtualización se van a utilizar y aplicar las CCN-STIC que afecten a esta parte.
3. Estudiar el software que compone SIMACET y aplicar las CCN-STIC que se vayan a aplicar en los servidores del sistema.

2. Software

2.1 Introducción a SIMACET.

- Definición que recoge el manual de la ACING [1]*: "El Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET) permite a los Cuarteles Generales, Estados Mayores de las Divisiones y Brigadas (Grandes Unidades) y a las Planas Mayores de Mando de los escalones de Regimiento, Grupo Táctico, Batallón o Grupo (Pequeñas Unidades),* ***planear, gestionar, controlar y dirigir las operaciones, así como obtener una visión coherente y homogénea del campo de batalla en todos los Puestos de Mando en tiempo operativo"***.

- Este sistema permite explotar la información facilitando la toma de decisiones con funcionalidades de ayuda a la decisión y realización de informes, envío de órdenes y mensajes a los escalones superiores, laterales y subordinados.

- Es un conjunto de hardware, software, personal y procedimientos que pretende conseguir una visión común del campo de batalla, un sistema de mensajería fiable, una alta supervivencia del sistema y una alta movilidad de los usuarios.

- Técnicamente, SIMACET es un **sistema distribuido de redes de área local** (**LAN**) que se comunican entre sí a través de diferentes redes de transmisión (**RBA[1], RRC[2], satélite…**), y que dispone de un sistema de **réplica** de la **base de datos táctica** (para disponer de la misma información en cualquier punto de la red), un sistema de **mensajería** entre los diferentes usuarios y un conjunto de interfaces con otros sistemas de información nacionales y no nacionales.

- Funcionalmente, dispone de un conjunto de aplicaciones administrativas, de gestión táctica, de comunicaciones, de información geográfica y una serie de utilidades que, en conjunto, facilitan las labores de mando y control (ver Figura 1).

[1] Red Básica de Área (RBA): Conjunto de estaciones que conforman la red mallada de un sistema de comunicaciones que permite el acceso a usuarios de diferentes puestos de mando a nivel operacional [2].
[2] Red Radio de Combate (RRC): Conjunto de medios, principalmente radio, que conforman la red de comunicaciones a nivel táctico [2].

Figura 1. Esquema de aplicaciones de SIMACET

- SIMACET está compuesto por un conjunto de nodos. Un **nodo** es un conjunto de hardware y software que se caracteriza por tener una Base de Datos Táctica que intercambia datos con otros nodos (ver Figura 2).


Figura 2. Nodo de SIMACET de GU.

- Los **nodos son autónomos** y, por lo tanto, no dependen de otros nodos para subsistir. La información está replicada en cada nodo y **la caída de un nodo no implica pérdida de información** en el sistema.
- **La red de réplica de SIMACET es el mecanismo que permite que todos los puestos de mando compartan en tiempo operativo una misma situación táctica**. Este sistema de réplica se basa en la

existencia de una Base de Datos en cada nodo, cuyas modificaciones pueden enviarse (réplicas) mediante distintos sistemas de transmisión, de forma que al final las bases de datos de todos los nodos contengan la misma información. El transporte de la información táctica (réplica de bases de datos) se realiza en el orden de minutos y este mecanismo de réplica es único en toda la red.

Se adjunta un Anexo A donde se muestra una configuración de un nodo genérico de SIMACET en versiones anteriores a la versión 5. Estos servidores físicos pasan a ser VMs en la versión 5. Para ello se contará con el software de virtualización vMware vSphere v. 6.5 citado anteriormente.

2.2 Introducción a la virtualización.

2.2.1 Concepto de virtualización

La virtualización es la separación del hardware físico por medio de una capa de software conocida como hipervisor. El hipervisor permite instalar múltiples instancias de un mismo sistema operativo y organiza el acceso al hardware físico de dichos sistemas operativos. En la Figura 3 se puede observar el concepto de capa de virtualización (hipervisor).

2.2.2 Tipos de virtualización

Dentro de los tipos de virtualización existen varios tipos bien diferenciados en función de su modo de instalación en el hardware o el tipo de servicio que ofrecen [3]: *Bare-Metal, Hot-based, Application virtualization, storage virtualización* (almacenamiento virtual).

2.2.2.1 *Bare-metal* (o Hipervisor de tipo 1)

Este tipo de virtualización de sistema operativo instala la capa de software llamada hipervisor o capa de virtualización en el bare metal (este término quiere decir hardware físico o de primer nivel). Ejemplos de hipervisores *Bare-metal*: VMware ESX, VMware ESXi, Microsoft Hyper-V, Citrix XenServer y Oracle VM (ver Figura 3).

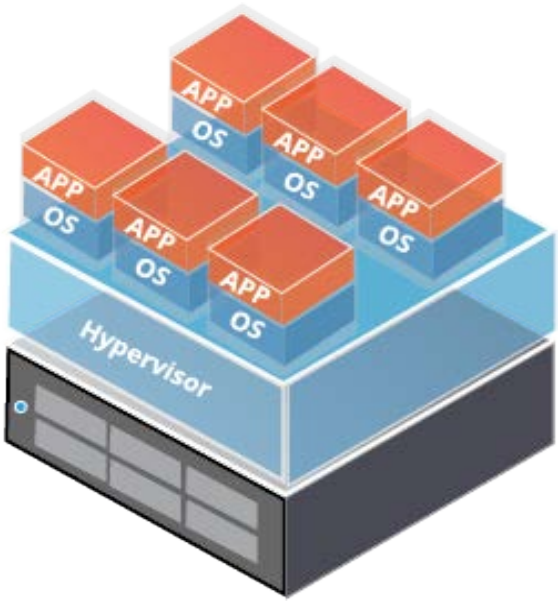


Figura 3. Arquitectura de Hipervisor tipo 1.

2.2.2.2 *Hosted virtualization* (o Hipervisor Tipo 2)

Este tipo de virtualización se utiliza cuando se instala un software de virtualización sobre un sistema operativo nativo. Este software es capaz de lanzar VMs (máquinas virtuales). Algunos ejemplos son: VMware Workstation, VMware Player, Microsoft Virtual PC y Virtual Box.

La diferencia principal entre los dos tipos es que el Tipo 1 accede directamente a los recursos de hardware del host sobre el que está instalado mientras que el Tipo 2 tiene que pasar primeramente por un sistema operativo nativo (ver Figura 4).

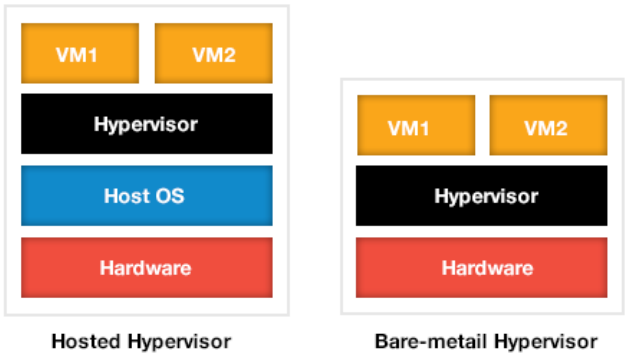


Figura 4. Estructura de los dos tipos de hipervisores.

2.2.2.3 *Application virtualization* (Virtualización de Aplicaciones)

Es el proceso de separar (encapsular) la aplicación que está siendo instalada del sistema operativo. Con este tipo de virtualización evitamos conflictos ya que no se instala la aplicación en el sistema operativo, por lo que no se altera el registro ni las librerías (DLLs).

2.2.2.4 *Storage virtualization* (Almacenamiento Virtual)

Es el proceso de ofrecer almacenamiento virtual a los hosts. El almacenamiento virtual puede ser una combinación de diferentes tecnologías físicas y puede situarse en diferentes lugares de la red, pero aparece en el host como único almacenamiento.

2.2.3 Generalidades de las máquinas virtuales

La única diferencia entre una máquina física y una virtual es que la maquina física instala el sistema operativo sobre un hardware físico, sin embargo, la máquina virtual instala el sistema operativo sobre un hardware virtual desarrollado por software.

Las VMs, ya sean creadas en plataforma x86 o x64, se componen de un conjunto de ficheros, cuyos tipos se describirán a continuación, con todo lo que ello conlleva (backup, moverlos, copiarlos en donde queramos…).

Tipos principales de extensión de ficheros para las VMs:

• .vmx
Este fichero contiene la configuración de las VMs (número de procesadores virtuales, cantidad de memoria reservada, dispositivos, etc.…).

• .log
Este fichero tiene el registro de actividad de la máquina virtual. Es útil para solventar problemas.

• .nvram
Este fichero contiene el estado de la BIOS de la máquina virtual.

• .vmsn y .vmsd
En este tipo de ficheros se almacenan los snapshots realizados de cada máquina virtual.

• .vmdk
Este fichero se corresponde con el disco duro físico (archivos del sistema, sistema operativo y las distintas aplicaciones instaladas en las VMs).

Principales beneficios de las VMs:

a. Aislamiento.
Cada VM instalada en un host es independiente del resto.

b. Encapsulado.
Las VMs están encapsuladas en una serie de ficheros que las hacen muy portables y facilitan trabajar con ellas.

c. Independencia del Hardware.
Las VMs corren en el host sin preocuparse del hardware que hay debajo. La conexión con los recursos físicos del hardware se hace a través de la capa de virtualización.

d. Compatibilidad.
Todas las VMs utilizan la arquitectura de hardware estándar de x86 o x64, por lo que se asegura la correcta compatibilidad entre el hardware virtualizado y el sistema operativo.

2.2.4 VMware vSphere 6.5 suite

Esta suite incluye un número de productos y funcionalidades que, juntas, proporcionan una solución de virtualización en una organización.

2.2.4.1 VMware ESXi

El núcleo de la suite VSphere es el hipervisor. Está compuesto de un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software hipervisor, y los servicios y servidores que permiten la interacción entre software de gestión y administración y las VMs.

2.2.4.2 VMware vCenter Server

Es el componente que permite gestionar de manera centralizada varios hosts con ESXi instalados y VMs. Añade gran parte de las tecnologías que ofrece esta suite como HA, DRS (*Distributed Resource Scheduler*) y FT. Este software consiste en multitud de módulos y servicios, y tiene que ser instalado en un servidor en dominio (virtual o físico) con Windows Server.

Los requerimientos mínimos para vCenter Server 6.5 son 2CPUs de 2Ghz de 64bits, 8GB de memoria RAM y 8GB de espacio en disco duro.

2.2.4.3 VMware Web Client

En las versiones anteriores, para acceder a los ESXi o a vCenter se utilizaba una aplicación cliente que ofrecía vSphere, con la versión 6.5, se accede a través de un navegador web con el plugin de Flash Player habilitado, apuntando a la dirección IP o nombre del servidor si existe un servicio DNS[3] activo (ver Figura 5).

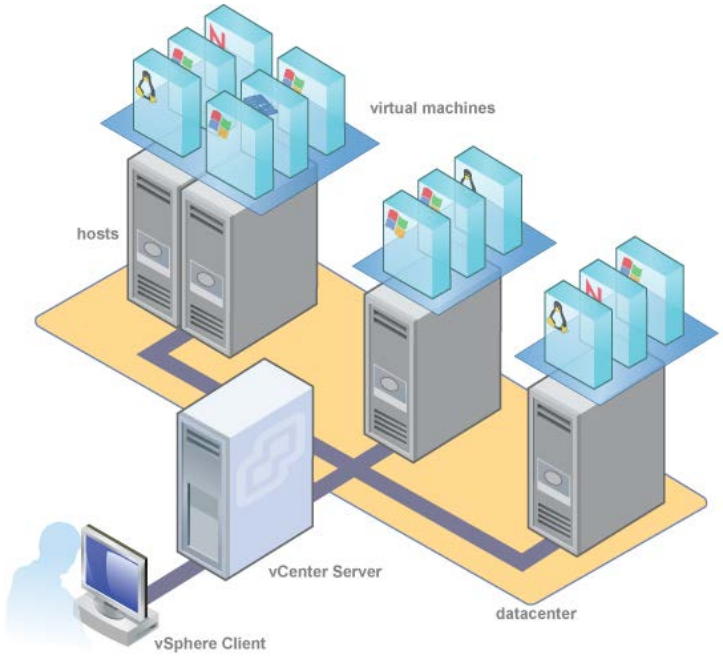


Figura 5. Esquema de la suite vSphere.

[3] Este servicio se encarga de transformar las direcciones IP en nombres de dominio y viceversa, y lo suele albergar el DC.

2.2.4.4 Tecnologías de supervivencia

Una de las características que diferencian a la solución de virtualización de VMware es la alta capacidad de supervivencia gracias a sus tecnologías de HA y FT que, en comparación con otras soluciones de virtualización, son mucho más fiables.

2.2.4.4.1 VMware High Availability (HA)

La alta disponibilidad de VMware proporciona un proceso automático para reiniciar las VMs que estaban corriendo en un determinado host cuando este se viene abajo. HA supervisa continuamente todos los hosts de un pool de recursos y detecta sus errores. Los hosts emiten una señal periódica denominada *heartbeat* hacia los demás host del clúster[4], un agente situado en cada host escucha el *heartbeat* procedente de los demás host del pool de recursos y así sabe si el host está trabajando o esta caído, una pérdida de *heartbeat* inicia el proceso de reinicio de todas las maquinas afectadas de otros hosts. HA asegura que haya suficientes recursos disponibles en el pool de recursos en todo momento para poder reiniciar las VMs en distintos servidores físicos en caso de fallo de un servidor.

2.2.4.4.2 VMware Fault Tolerance (FT)

Al igual que con HA, FT reinicia las VMs en caso de caída de un servidor físico, y, además, elimina el tiempo de caída (*downtime*), de tal manera que la caída de un servidor es transparente para el usuario. Para llevarlo a cabo, lo que hace esta tecnología es generar una máquina en espejo en otro host físico preparada para funcionar en cualquier momento (ver Figura 6).

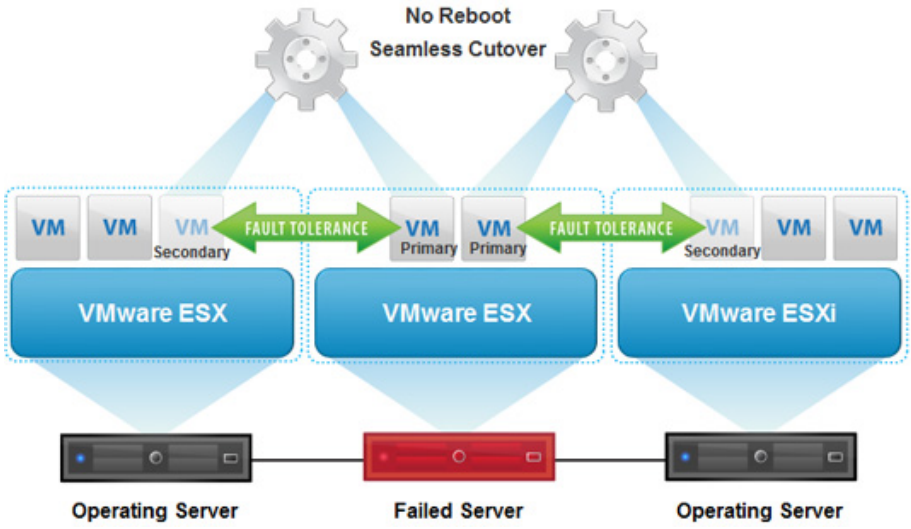


Figura 6. Fault Tolerance trabajando.

2.2.4.5 Tecnologías de optimización

Otras de las tecnologías que contiene la suite de virtualización vSphere son DRS y EVC (*Enhanced VMotion Compatibility*), que están dedicadas a optimizar los recursos de los servidores físicos.

[4] Hay que diferenciar dos tipos de clúster en este documento, el clúster físico que tienen los nodos anteriores a la versión 5, que simplemente se complementan cuando un host falla, y el clúster de virtualización que aúna los recursos de hardware que contienen los hosts que forman el nodo.

2.2.4.5.1 *Distributed Resource Scheduler* (DRS)

Esta tecnología tiene como misión la distribución automática de recursos entre los diferentes hosts ESXi que están configurados dentro del clúster. Clúster en esta suite es una agregación implícita de CPU y memoria entre todos los hosts que componen el clúster. DRS se encarga de situar cada VM en el host físico que mejores prestaciones proporcione en ese momento. DRS comprueba en todo momento que una VM está en su funcionamiento óptimo, y, si no es así, la pasará a otro host o reducirá la carga de trabajo del host que está corriendo la máquina.

2.2.4.5.2 *Enhanced VMotion Compatibility* (EVC)

Esta tecnología es la encargada de facilitar las funcionalidades del hardware de Intel y AMD con una alta compatibilidad de las CPUs entre los servidores agrupados en los clústers con DRS implementados.

3. Acreditación

La acreditación es un procedimiento de obligado cumplimiento para todos los sistemas que manejen información clasificada en la administración. Con este proceso se consigue una autorización otorgada a un sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su CO. Todos los sistemas que requieran manejar información clasificada deberán ser previamente acreditados. SIMACET puede trabajar con cualquier clasificación de seguridad, sea OTAN/UE o nacional[5], y las medidas que se han de aplicar van acordes a esta clasificación, que como novedad en la versión 5, variará dependiendo del ejercicio o maniobra. Para llevar a cabo este TFG se va a realiza toda la instalación.

El hardware sobre el que se va a realizar la acreditación en líneas generales es el siguiente:

- 2 Servidores HP Proliant DL380p GEN8:
  - Procesador INTEL XEON E5-2650 8CORE a 2Ghz
  - Memoria RAM: 384 GB (12 módulos de 16 GB por servidor)
  - Almacenamiento interno: 2 HD de 146 GB
  - 2 Tarjetas de red (Quad-Port)
- Cabina de almacenamiento HP P2000 G3 iSCSI:
  - 24 discos de 900 GB
- Cabina de backup D2D HP StoreOnce 4500 iSCSI:
  - 4 discos de 2 TB
- 2 Switch ALLIED TELESIS AT-x610 24TS
- Firewall CHECKPOINT SB 20.

Esta configuración podrá variar en función del tipo de nodo que se despliegue, pero la estructura de 2 o 3 servidores, 2 Switches de interconexión, 1 servidor iSCSI, una cabina de backup y Firewall siempre se mantendrán (aunque podrán variar en cuanto a marca o modelo y alguna característica de hardware referente a memoria RAM o procesadores). El estudio de los requisitos que se va a realizar en este TFG será sobre este hardware que es el que se encuentra disponible en el RT-1 (Madrid). En el Anexo B se muestra gráficamente la nueva configuración física genérica de un nodo de Brigada como el estudiado en el Regimiento.

[5] Los niveles de seguridad nacional, aunque son de competencia solo nacional tienen su equivalente a nivel OTAN, por ejemplo, el grado de seguridad nacional DIFUSION LIMITADA es equivalente al grado OTAN de seguridad NATO RESTRICTED.

3.1 Procedimiento de configuración y despliegue.

El proceso de despliegue y configuración para conseguir un nodo acreditable se divide en varias partes diferenciadas, en las que se irán aplicando una serie de CCN-STIC que estipula el CCN para que el nodo sea acreditable. Existen dos tipos de STIC, unas son las que aplican las restricciones y otras son denominadas incrementales. Estas últimas sirven para permitir que funcionen las aplicaciones que dan servicio a los usuarios. Un ejemplo sería la CCN-STIC 515 “Incremental de servidor de impresión” que permite abrir los puertos de impresión para que los usuarios puedan imprimir. Estos puertos habían sido cerrados por la CNN-STIC 590 “Orígenes de eventos de servidores”, que entre las medidas que realiza se encuentra la de cerrar todos los puertos del servidor para que no exista ningún agujero de seguridad por donde se pueda acceder.

3.1.1 Conexionado y marcado de los equipos y cableado

En esta fase inicial se realiza el conexionado de los servidores, clientes y equipos de electrónica de red (switches, router y firewall). Además, se tiene que realizar el marcado de todos los cables de interconexión y reflejarlo en el apéndice de TRAZABILIDAD, necesario para la acreditación.

En esta fase también se realiza o verifica el TAMPERING (Colocación de etiquetas anti-manipulación) en todos los equipos que puedan ser susceptibles de ser manipulados por personal ajeno (ver Figura 7).

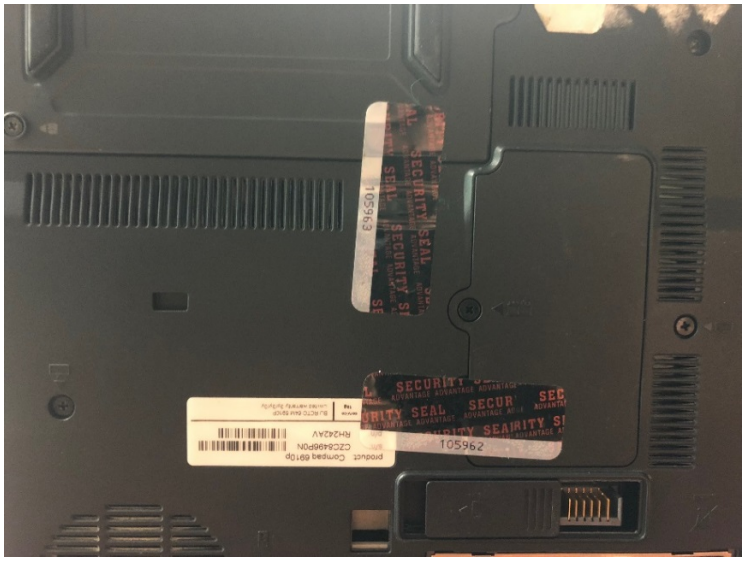


Figura 7. Cliente de SIMACET después del proceso de TAMPERING.

3.1.2 Estructura y asignación de recursos de hardware:

Los nuevos nodos de SIMACET versión 5 se han diseñado con una estructura física de hardware adaptada a virtualización. En este caso se ha diseñado un clúster de virtualización con el hardware anteriormente citado, de tal manera que se utilicen todos los recursos de hardware de todos los hosts como si fueran uno. La asignación de las tarjetas de red físicas a las VLANs que van a gestionar el sistema de virtualización son las siguientes:

- VLAN de **Gestión**: en esta VLAN se encuentran los ESXi, el servidor de vCenter y su controlador de dominio (DC). A esta VLAN deberá acceder el administrador para gestionar la capa de virtualización.
- VLAN de **Producción**: en esta VLAN se encuentran todos los DCs, servidores miembros, y servidores independientes que dan servicio a los usuarios.
- VLAN de **vMotion**: esta VLAN gestiona la supervivencia de las VMs y se encarga de mover una máquina de un servidor físico a otro. En ella actúa la tecnología HA y FT anteriormente descritas.
- VLAN de **Almacenamiento**: debido a que el servidor de almacenamiento es de tipo iSCSI[6] se requiere una red para acceder a este. Se crea esta VLAN con una serie de tarjetas de red dedicadas a ello para poder gestionar la carga y descarga de archivos a las unidades virtuales creadas dentro del servidor iSCSI denominadas LUN.

Estas VLANs serán configuradas en los switches del nodo de tal manera que unos puertos del switch estén destinados a los puertos troncales[7] (*trunks*) entre ambos, y otros puertos estén asignados a una VLAN. A estos switches, aparte de la configuración lógica, se les aplicará la configuración de seguridad que establece la CCN-STIC 643 "Seguridad en Equipos de Comunicaciones de Allied Telesis con Sistema Operativo AW+".

En el servidor iSCSI se guardan todas las máquinas y software necesarios para hacer funcionar el sistema. Este servidor está compuesto por 22 discos duros físicos con una capacidad de 780 GB cada uno y uno de estos discos está configurado como Hot Spare (espera caliente) para entrar a funcionar en caso de que uno de ellos falle. Por otro lado, estos discos están configurados de manera lógica en RAID 5 y 11 unidades lógicas (LUNs) es decir, el software de virtualización detecta 11 unidades de almacenamiento. Para acceder a estas LUNs, el servidor dispone de 4 puertos físicos numerados del 1 al 4.

Se adjunta un Anexo C.1, que muestra un esquema grafico de la VLANs asignadas a los switches y las tarjetas de red físicas de cada servidor ESXi asignadas a cada VLAN, y un Anexo C.2, que muestra una tabla de los puertos asignados a cada VLAN en los switches.

3.1.3 Instalación y configuración de la capa virtual:

Una vez conexionado, cableado y marcado todo el nodo, se procede a la instalación del software de virtualización. En este caso, en cada servidor físico se instala la versión 6.5 de ESXi. Este software detectará todo el hardware del servidor (procesadores, discos duros, tarjetas de red, etc.) y nos pedirá que elijamos qué tarjetas de red queremos utilizar para su gestión (vmnic), que en este caso serán la 1 y la 2. Posteriormente, se designarán las tarjetas de red utilizadas para cada VLAN, como se detalla en el Anexo C.1. Durante la instalación no se aplicarán configuraciones de seguridad que, posteriormente, se realizarán desde vCenter. Para acceder a vCenter y configurar el clúster de virtualización se utilizará un cliente web. Una vez configurado el clúster se procede a aplicar la configuración de seguridad que marca la CCN-STIC 401 "Configuración de seguridad de entornos virtuales VMWare ESX". Se configuran el direccionamiento de los servidores físicos y los usuarios de administración del entorno virtual.

[6] Este tipo de controladora es una evolución del tipo SCSI que utilizaban los anteriores servidores y permitían su conexión mientras el servidor estaba en funcionamiento. En tipo iSCSI la controladora pasa a ser un conector RJ-45 con las mismas funcionalidades y con la capacidad de funcionar a nivel de red (capa 3 del modelo OSI).
[7] Este tipo de puertos no pertenecen a ninguna VLAN y sirven de interconexión entre los dos switches por donde pasa información de todas las VLANs configuradas en ellos.

Esta STIC establece unas medidas que son la parte novedosa de esta acreditación [4]:

- Recomendaciones de instalación de VMWare ESXi.
- Recomendaciones de configuración de VMWare ESXi.
- Recomendaciones de configuración de vCenter.
- Recomendaciones de configuración de las VMs.

Figura 8. Vista servidor ESXi 6.5 de un nodo de SIMACET configurado.

Posteriormente, se procede a instalar vCenter 6.5, para lo que se creará un dominio dedicado a la virtualización. Este dominio será una VM y se encontrará dentro de uno de los host ESXi. Esta utilidad proporciona la capacidad de gestión de los 2 ESXi desde una misma conexión, así como la implementación de las tecnologías de supervivencia y optimización. Para su instalación será necesario instalar y confeccionar un servicio de DNS y una SQL Database.

Una vez configurado el vCenter y confeccionado el clúster desde el que colgarán los servicios que queremos ofrecer, procederemos a configurar las redes que anteriormente hemos configurado con VLANs en los switches. En este punto aparece un concepto nuevo que es el de vSwitch, que consiste en un switch virtual que sirve para diferenciar las redes y al que se le asignan las tarjetas de red físicas de salida de los host ESXi.

Una vez finalizado este proceso, la capa virtual estará configurada para dar servicio de VMs (ver Figura 8).

3.1.4 Despliegue de máquinas virtuales

Una vez terminada la configuración de la capa virtual, se procede al despliegue de VMs de SIMACET que darán servicio a los usuarios. Estas máquinas, en esta prueba, están usando Windows 2008 Server R2 de 64 bits (W2K8R2) como sistema operativo para controladores de dominio y servidores miembro y Windows 7 Profesional de 64 bit (W7) para clientes.

SIMACET V.5 utiliza una estructura de dominio donde cada nodo es independiente y la conectividad entre nodos se realiza a través de relaciones de confianza, de tal manera que cada nodo, independientemente de su entidad, es completamente autónomo, como se ha explicado anteriormente. Para dar servicios a los usuarios, del controlador de domino cuelgan una serie de servidores miembro en el que cada uno ofrece un servicio a los usuarios (correo, chat, SIMACET, aplicaciones de logística, servicios OTAN…).

Una vez configuradas las VMs con todos los servicios, se procede a aplicar las CCN-STICs correspondientes a cada servidor con cada servicio particular. Cabe destacar que el propio CCN adjunta en muchas de ellas una serie de scripts que aplican la configuración de seguridad con solo ejecutar el script. Para un Controlador de Dominio y un servidor miembro se aplicarán las siguientes STICs:

- Controladores de Dominio:
  - Default Domain Controllers Policy
  - CCN-STIC-533 Incremental DC
  - CCN-STIC-522A Inicios de sesiones anteriores - DC
  - CCN-STIC-521A Incremental Dominio
  - CCN-STIC-550 Incremental DC para Exchange Server
  - Incremental Agente Veritas (comunicación BackUp exec)
- Servidores Miembro:
  - CCN-STIC-521A Servidor Miembro
  - Servidor BackUp Exec
    Incremental Taso
  - Servidor ePo
    Incremental Servidor ePO Hercules17
  - Servidor JEMM
    CCN-STIC-524 Incremental Servidores IIS 7.5
  - Servidor LOGFAS
    CCN-STIC-524 Incremental Servidores IIS 7.5
  - Servidor Simacet
    Incremental Permisos Servidor Simacet
  - Servidor de Ficheros
    CCN-STIC-524 Incremental Servidor de Ficheros
  - Servidor de Impresion
    CCN-STIC-515 Incremental Servidor de Impresión
  - Servidor Entidad de Certificación
    CCN-STIC-524 Incremental Servidores IIS 7.5
    CCN-STIC-595 Incremental Entidad de Certificación-fix-Heras
    CCN-STIC-595 Incremental Servidor Entidad de Certificación
  - Servidor Exchange
    CCN-STIC-524 Incremental Servidores IIS 7.5
    CCN-STIC-550 Incremental Servidor Exchange 2010
  - Servidores KMS[8]
    Incremental puertos KMS
  - Servidores SharePoint
    CCN-STIC-533 Incremental Servidor SharePoint 2010
  - Servidores SQL Server
    CCN-STIC-540 Incremental SQL Server 2008 R2

[8] También denominado switch de pantalla, es un dispositivo que permite cambiar el ESXi que queremos visualizar, el servidor de BackUp o el servidor iSCSI.

3.1.5 Configuración de clientes

Se denomina cliente de SIMACET al ordenador portátil que da acceso al usuario a SIMACET. Estos clientes tienen como sistema operativo nativo Windows 7 Profesional, y las aplicaciones cliente de los servicios que da el sistema. Además, a estos clientes también hay que aplicarles las STICs correspondientes a este SO:

- CCN-STIC-522A Windows 7
- Configuraciones de Seguridad según la Guía CCN-STIC-522A
- CCN-STIC-533 Incremental Equipos Windows 7 Autenticación Kerberos
- CCN-STIC-515 Incremental Servidor de Impresión-Clientes Windows
- CCN-STIC-522A Windows 7-Equipos
- CCN-STIC-530 Office 2010-Equipos
- Incremental de puertos KMS

3.1.6 Configuración de firewall Cisco ASA SB-20

Para poder conservar la estabilidad e integridad de los recursos de una red propia, estos se deben de proteger de todo aquello que no pueda controlarse, que en un caso como este son todas las conexiones entrantes que pueda recibir el sistema desde el exterior. La manera más eficiente de implementar un dominio de seguridad es mediante un *firewall*. Este tipo de dispositivos son capaces de implementar una separación física y una separación lógica. Además, son capaces de implementar políticas de seguridad.

Este dispositivo está implementado con el objetivo de filtrar aquellos paquetes de capa nivel 3 y superior del modelo de referencia OSI, así como establecer un sistema de prevención de intrusos de red. [5]

Para ello, a este dispositivo se le aplica la configuración establecida en la CCN-STIC-651 “Seguridad en Cisco ASA”.

3.1.7 Auto auditoría

Una vez que el sistema esté completamente configurado y desplegado, es interesante utilizar las herramientas que utilizará el CCN para auto-evaluar el nodo. Para ello se hace uso de las herramientas CLARA y NESSUS, las cuales evaluarán al completo todos los equipos y máquinas virtuales en busca de posibles errores de configuración, ausencia de aplicación de políticas de seguridad o presencia de software y sistemas operativos desactualizados. De esta forma podremos solventar dichas deficiencias, de cara a pasar dicha acreditación.

Además, es interesante revisar toda la documentación que es necesario remitir a la autoridad acreditadora en busca de posibles errores o incongruencias con la configuración presentada y documentar los diferentes procedimientos que se llevarán a cabo en materia de actualizaciones (cómo se distribuyen las últimas actualizaciones de sistemas operativos o software a los equipos de la red), control de dispositivos USB o renovación de licencias (en caso de finalizar periodo de soporte del software).

3.2 Evaluación por parte del CCN o JCISAT.

Como ya hemos mencionado antes, la acreditación es un procedimiento de obligado cumplimiento para todos los sistemas que manejen información clasificada en la administración. Con este proceso se consigue una autorización otorgada a un sistema para manejar información clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad y disponibilidad, con arreglo a su Concepto de Operación del Sistema (CO).

3.2.1 Documentación y autoridades que intervienen en el proceso de acreditación

Para llevar a cabo el proceso es necesario generar una serie de documentos en arreglo a unas normas que establece el CCN. Esta documentación debe ser confeccionada de manera muy escrupulosa ya que, a la hora de tramitarla, cuando el organismo acreditador evalúe el sistema, si encuentra algo erróneo, parará el proceso y la unidad que solicita la acreditación deberá repetirla. Los principales documentos del proceso son: [6]

- *Concepto de operación del Sistema (CO):*

  Documento en el que se establece el objeto o función del sistema, el tipo de información que va a manejar, cómo se va a conectar a las diferentes redes exteriores, las condiciones de explotación y las amenazas a las que estará sometido [6]. Además, debe incluir una descripción de todo el sistema, con su composición de hardware y software, un listado con los servicios que va a ofrecer al usuario y el plano situacional donde se va a encontrar el sistema a acreditar. Según Norma CCN-STIC-207 “Estructura y contenido del concepto de operación de seguridad”.

- *Análisis de Riesgos (AR):*

  Proceso sistemático para el estudio de las amenazas a las que se verá sometido el sistema. Este documento deberá seguir obligatoriamente un procedimiento formal en aquellos Sistemas de Información que vayan a manejar información clasificada nacional de nivel SECRETO o RESERVADO. Según Normas CCN-STIC-410 “Análisis de riesgos en sistemas de la Administración”, CCN-STIC-470-I1 “Manual de usuario PILAR. Análisis y gestión de riesgos v7”, y CCN-STIC-472G “Manual de usuario PILAR BASIC v7”.

- *Declaración de Requisitos de Seguridad (DRES):*

  Documento en el que se hace una exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implantar, conforme al análisis de riesgos. Se actualiza conforme un sistema evoluciona. Constituye la base para la acreditación. Según Norma CCN-STIC-202 “Estructura y contenido de la declaración de requisitos de seguridad (DRES)”.

- *Procedimientos Operativos de Seguridad (POS)*

  Documento que describe las operaciones concretas a realizar sobre el sistema, para materializar el cumplimiento de las DRES. Se pueden hacer extractos para los usuarios que, en función de su contenido, podrán disponer de una clasificación inferior o carecer de ella. El documento debe recoger la administración y organización de seguridad, la seguridad física, la seguridad ligada al personal, la seguridad documental, la seguridad en las TIC, los planes de continuidad y los procedimientos de gestión de configuración del sistema. Según Norma CCN-STIC-203 “Estructura y contenido de los procedimientos operativos de seguridad (POS)”.

Además, dentro del proceso de acreditación intervienen una serie de autoridades y órganos detallados a continuación:

- *Autoridad Delegada de Acreditación (ADA) en el ámbito del ET.*

  La Autoridad de Acreditación (AA) es la autoridad responsable de conceder la autorización a un sistema para manejar información hasta un grado determinado, o en unas condiciones determinadas. En el ámbito del MINISDEF, esta autoridad recae en el Ministerio de Defensa.

  La AA podrá nombrar autoridades delegadas que en el caso del ET es el GE. JEME, para aquellos sistemas específicos que manejen información clasificada nacional.

  Para el apoyo al JEME en sus funciones como ADA, es nombrada la JCISAT como organismo de Acreditación del ET y tiene como cometidos los siguientes:

  - Gestión, en el ámbito del ET, del proceso de acreditación de los Sistemas.
  - Comprobación de documentación de seguridad (CO, DRES y POS).
  - Comprobación del área SEGINFOPER (Habilitaciones Personales de Seguridad (HPS)).

  Cuando el sistema maneje información de carácter OTAN/UE, será el CCN el órgano acreditador, pero en este caso no existe ningún tipo de estructura delegada ya que es el propio CCN el organismo nombrado.

- *Autoridad de Seguridad de las TIC (ASTIC) del ET.*

  El General jefe de la División de Operaciones del EME (JEDIVOPE), es el jefe de Seguridad de la Información en el ámbito del ET, asume los cometidos de Autoridad de Seguridad de las TIC del ET.
  Algunas de sus misiones principales:

  - Planear y controlar todos los aspectos relacionados con SEGINFOSIT en el ET.
  - Aprobar el CO de todo sistema que deba ser acreditado por la Autoridad Delegada de Acreditación (ADA).
  - Solicitar a la ADA la acreditación o renovación de seguridad de los sistemas.

- *Autoridad Operacional del Sistema de las TIC (AOSTIC).*

  Esta figura está nombrada de acuerdo a varios criterios dependiendo del estado en que se encuentre el sistema:

  1. General Jefe de la JCISAT, para los Sistemas específicos del ET que se encuentran en diferentes Mandos y UCOs.
  2. Jefe de la Oficina de Programas correspondiente, para todos aquellos sistemas específicos del ET que se encuentren en fase de desarrollo, instalación o pruebas.
  3. Jefe de UCO, que podrá delegar en el jefe del Núcleo/Sección de Sistemas de Información o de la G-6/Área CIS, para aquellos Sistemas que afecten a un único Mando o UCO. Este es el caso que afecta a la acreditación del nodo del RT-1 (Madrid) donde es nombrado como AOSTIC la G6 del Cuartel General de la División “Castillejos”.
  4. Jefe de la UCO cuando se dé el caso de que solo existen ordenadores aislados.
  5. En los nodos del SMCM esta figura se nombrará a los estipulados en el documento del Estado Mayor del Ejército “Criterios Operativos. Estructura SEGINFOSIT de los nodos del SMCM en el ámbito del ET”.

Esta es la autoridad encargada de elaborar el CO y elevarlo al Organismo de Acreditación para su aprobación por la ASTIC. Se encarga además del desarrollo, operación y mantenimiento del Sistema durante su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. También se encarga de la aprobación de los Procedimientos Operativos de Seguridad, así como de elaborar la DRES de acuerdo a los resultados del Análisis de Riesgos y de velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).

- *Administrador de Seguridad del Sistema (ASS).*

  El ASS es el responsable de todas las tareas que conciernen la gestión, configuración y actualización de hardware y software en los que se basan los mecanismos y servicios de seguridad. Esta figura será única por sistema, aunque una misma persona puede ser ASS de más de un sistema. También se encarga de informar al AOSTIC de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad del sistema. Se puede nombrar una autoridad delegada de este administrador si fuese necesario (ASS-D).

  El ASS será designado por el AOSTIC, del que dependerán funcionalmente. Su identidad aparecerá reflejada en la documentación de seguridad del Sistema (DRES y POS).

  Para sistemas específicos como SIMACET, que por su complejidad necesita personal agregado para llevar a cabo sus funciones del ASS, se podrá nombrar un solo ASS y en el resto de nodos un Administrador de Seguridad del Sistema local (ASS-L).

En la última parte, dependiendo de si el sistema es nacional u OTAN/UE, se realiza la Verificación Técnica de Seguridad (VTS). El objetivo de esta verificación es comprobar que se han aplicado los requisitos de seguridad definidos en la documentación. Para ello, el Organismo de Acreditación (JCISAT) o en su caso el CCN para los enclaves nacionales con acceso a sistemas OTAN/UE, verificará la implantación de todos los correspondientes certificados de las instalaciones (SEGINFOINS), de personal (SEGINFOPER) y de radiaciones no deseadas (TEMPEST). Otro término que aparece durante el proceso de acreditación es *Zoning* (Zonificación de equipo), que consiste en clasificar por zonas en función de nivel de radiación electromagnética que producen los equipos desplegados. Los procedimientos de evaluación empleados por el CCN están basados en la norma SDIP-28 de OTAN o IASG-7-02 de la UE. [8]

3.3 Proceso de acreditación.

1) AOSTIC remite a la ASTIC del E.T. a través de JCISAT la solicitud de acreditación junto con el CO. Es el inicio formal de la solicitud de acreditación del sistema e incluye la finalidad y alcance del sistema, clasificación de la información que se va a manejar, breve descripción del sistema, y la estructura SEGINFOSIT: AOSTIC y ASS. JCISAT lo envía a JEDIVOPE, quien debe autorizar la implantación del sistema.
2) En paralelo se solicita Zoning, TEMPEST y HPSs, que deben de estar preparados antes de la VTS (Verificación Técnica de Seguridad).
3) JCISAT, tras recibir el COS realiza el AR (Análisis de riesgos), informando al AOSTIC para que resuelva deficiencias.
4) AOSTIC hace el DRES (Declaración de Requisitos Específicos de Seguridad)
5) ASS elabora el POS (Procedimientos Operativos de Seguridad) y lo remite al AOSTIC.
6) AOSTIC eleva DRES y POS a JCISAT.
7) AOSTIC, tras revisar las correcciones del DRES y POS, comunica a JCISAT que está listo para la VTS.
8) VTS: Se comprueba SEGINFOSIT, SEGINFOINS, SEGINFOPER y TEMPEST.
9) JCISAT eleva a la ASS-D (GE JEME) el documento de conformidad y propuesta de acreditación.
10) AAS-D contesta a JCISAT y éste se lo comunica al AOSTIC[9].

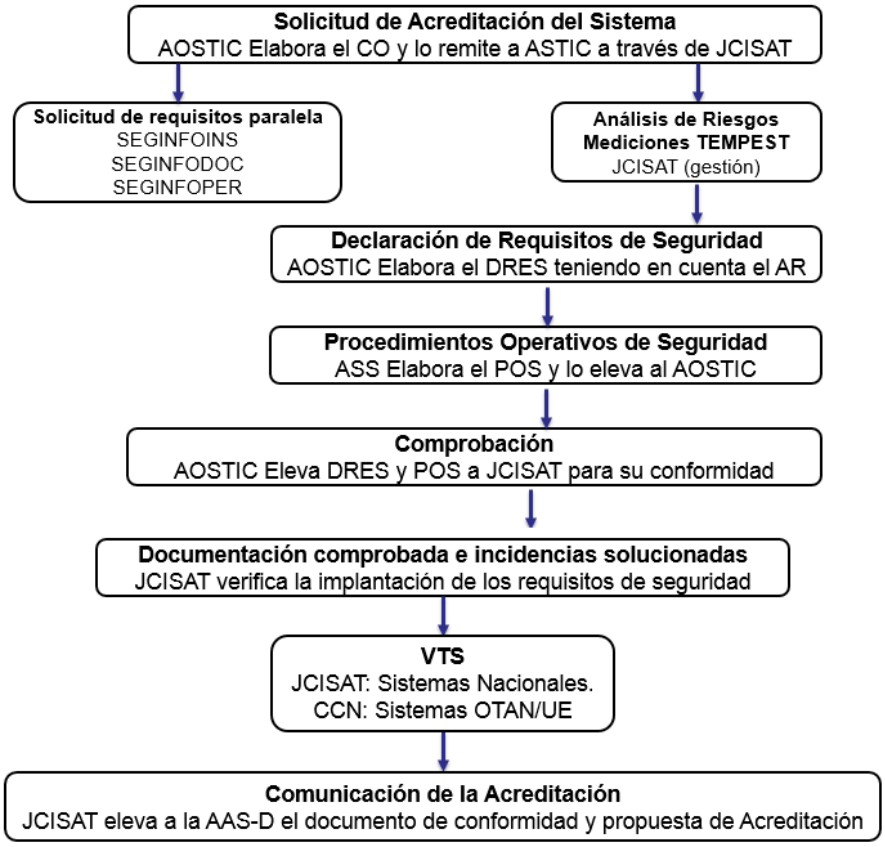


Figura 9. Esquema de acreditación de un sistema.

Es necesario nombrar toda la estructura SEGINFOSIT previamente al inicio del proceso de acreditación. El responsable del nombramiento de dicha estructura es el jefe de la unidad de la que depende el sistema de información. Se adjunta Anexo E con el proceso completo con referencias temporales.

3.4 Problemas comunes durante el proceso de certificación y soluciones planteadas.

- *Errores en la documentación generada*

  La documentación que se genera durante el proceso de acreditación debe ser muy minuciosa, ya que se abordan muchos apartados y es común dejar pasar por alto algún detalle. Por ejemplo, durante el proceso de acreditación del nodo perteneciente al RT-1, en el CO no se habían declarado los puertos troncales entre switches y por ello JCISAT devolvió el documento. Una vez tramitada la modificación, el proceso continúa.

- *SEGINFOPER (HPS)*

  Para que el sistema sea gestionado, tanto los administradores como los operadores deben de tener la HPS en vigor y con una categoría de seguridad igual o superior a la que gestiona el sistema. Por ello es importante revisar que el personal así lo tenga y los periodos de caducidad para que no coincidan en mitad de un ejercicio.

- *Sistemas operativos o software fuera de soporte*

  El sistema contiene un servidor WSUS para actualizaciones. Para que este servidor contenga las últimas actualizaciones tanto de SO server como de cliente hay que introducírselas mediante un proceso minucioso a través de un USB que proporciona el PCMSHS. Debido a la complejidad del proceso, es muy normal que Windows publique parches de seguridad y el sistema no disponga de ellos en la fecha de acreditación.

- *Motores de antivirus no actualizados*

  Al igual que en el caso de los parches de Windows, el antivirus que tiene el sistema es McAfee y los motores de actualización de antivirus y las bases de datos de antivirus las proporciona PCMSHS.

- *Fallos en las aplicaciones de Guías STIC*

  Las guías CCN-STIC son altamente complejas y largas. Algunos documentos contienen más de 600 páginas con recomendaciones de seguridad, con lo cual, es muy complicado aplicar todas las indicaciones de las guías sin ningún fallo.

- *Control de USB*

  Durante un ejercicio solo hay un elemento de la maniobra autorizado a tener los puertos USB habilitados, de tal manera que es el único elemento que puede introducir información en el sistema. Este se denomina TASO. Por ello hay que tener un minucioso control de los equipos clientes y que todos ellos tengan los puertos USB deshabilitados.

Todos estos resultados que se muestran han podido ser extraídos de anteriores acreditaciones de versiones anteriores a SIMACET 5 y se trata de los errores más comunes. Además, también se han extraído resultados después de ejecutar las aplicaciones de auto-auditoria (CLARA y NESSUS). Se ha podido observar, después de hacer funcionar estar aplicaciones, principalmente las deficiencias en la aplicación de las STIC, ya que estos programas auditan los servidores a nivel de software por encima de la virtualización, es decir, la virtualización no se comprueba.

3.5 Situaciones finales posibles después del proceso de acreditación.

En el proceso de acreditación del sistema se pueden dar las siguientes situaciones finales:

- Autorización Temporal con Propósitos Operacionales (ATPO)

  Esta autorización es la adecuada para los sistemas en ejercicios y operaciones, que por sus especiales características no pueden someterse a un procedimiento de acreditación completo. Esta autorización tiene una validez de 6 meses y solo es prorrogable una vez.

- Autorización Provisional para Operar (APO)

  Esta autorización se concede cuando el sistema se encuentra en proceso de acreditación, para los casos en los que no se haya superado completamente el proceso o como paso previo a la concesión definitiva. Su validez es de 6 meses no prorrogables.

- Acreditación

  Situación alcanzada por los sistemas que hayan superado con éxito el proceso de acreditación. Tiene una validez en función de la clasificación de seguridad del sistema:

  - Sistemas clasificados RESERVADO o SECRETO, máximo 3 años.
  - Sistemas clasificados CONFIDENCIAL, máximo 5 años.
  - Sistemas clasificados hasta DIFUSION LIMITADA, máximo 7 años.

  Los plazos para un sistema que vaya a ser utilizado con clasificaciones de seguridad OTAN/UE son equivalentes a los aquí mostrados.

Se adjunta un Anexo E con un diagrama de Gantt con el proceso de instalación, configuración y acreditación del nodo versión 5 sobre el que se ha basado este TFG, para el que se había solicitado un nivel de seguridad CONFIDENCIAL (nacional). Este proceso es una estimación ya que, como se explica en las conclusiones, el EXE QUICK LION 18 ha sido suspendido debido a motivos económicos.

3.6 Re-acreditación de sistemas.

La re-acreditación es la renovación de la autorización para continuar manejando información clasificada una vez que caduca la aprobación concedida. Este proceso será iniciado por la AOSTIC que necesita re-acreditar un sistema con una antelación de tres meses antes de la fecha de expiración.

Una re-acreditación también podría verse solicitada por una variación en el hardware o software que conforman en sistema, siempre y cuando cambien la manera de acceso electrónico o genere alguna vulnerabilidad que deba ser tratada en base a alguna CCN-STIC [10].

4. Conclusiones y propuestas de trabajos futuros

4.1 Principales conclusiones.

El proceso de acreditación de un nodo de SIMACET versión 5 es altamente complejo y meticuloso. En él se añaden dos nuevas disciplinas a dominar por los administradores: la virtualización y la implementación de un firewall. El hecho de que a partir de ahora cada vez que un nodo salga a un ejercicio tenga que ser acreditado hace que el proceso de instalación, configuración y acreditación sea mucho más largo en lo referente a trámites burocráticos.

A nivel de software, la nueva administración desde un sistema virtualizado permite una configuración del sistema mucho más rápida que con las versiones anteriores. En los nodos de la versión 4.2.1 y anteriores se necesitaba clonar los nodos desde el inicio, sin embargo, ahora con los modos de clonación y despliegue de plantillas que incorpora vSphere es mucho más cómodo.

El administrador gana en facilidad de configuración y mantenimiento del sistema debido a que puede acceder al sistema desde cualquier puesto de la maniobra, es decir, no es necesario que se encuentre físicamente en el nodo, y, además, puede descentralizar los servidores y asignar a otro personal la configuración de cada uno, ya que, de nuevo gracias a la virtualización, se puede acceder a los servidores de manera simultánea.

Sin embargo, el administrador debe implementar nuevas medidas de seguridad que afectan a la parte de virtualización. Todas estas medidas son completamente novedosas y complicadas, las cuales requieren de formación específica en este ámbito.

Por otro lado, la autoridad del sistema y la autoridad delegada pierden comodidad en los trámites administrativos ya que deben cumplir plazos para que el nodo llegue a un ejercicio debidamente acreditado. Este proceso descrito requiere la asistencia de personal que tiene que evaluar el nodo físicamente y, en caso de encontrar deficiencias, el personal responsable del sistema debe solventarlas.

El proceso de acreditación y la implementación de esta nueva configuración del sistema con virtualización no van de la mano. El proceso de acreditación está diseñado para un sistema físico de tal manera que con acreditarse una vez sería suficiente, sin embargo, ahora es necesario hacerlo una vez por cada ejercicio. En este aspecto, la autoridad competente debería analizar el proceso de acreditación para adaptarlo a un sistema virtualizado.

Además, el CCN está pendiente de actualizarse en cuanto a requisitos que debe exigir para acreditar un sistema bajo software de virtualización. Buena muestra de ello es que la CCN-STIC 442 “Seguridad en VMWare ESXi” está pendiente de ser publicada y la CCN-STIC 441 “Configuración de seguridad de entornos virtuales VMWare ESX” está publicada en enero de 2010. La configuración de seguridad de esta última STIC está basada en la versión 4 de ESX. Y, aunque toda la configuración de seguridad está incluida en la versión 6.5, esta incluye más opciones de seguridad que podría ser necesario implementar en la actualidad.

Finalmente, el nodo perteneciente al RT-1 no ha podido ser acreditado ya que el EXE QUICK LION 18, para el que estaba solicitado su uso, ha sido suspendido por motivos presupuestarios, se trataba de un ejercicio muy grande donde estaban implicadas muchas unidades y que finalmente se ha reducido a un ejercicio tipo maqueta donde no se requiere la acreditación del nodo. En los plazos anteriores al ejercicio, G6 de la “División Castillejos” había desarrollado el CO del nodo, donde, como ya hemos citado anteriormente, se denegó debido a que no se habían declarado los puertos troncales. No obstante, al nodo se le han aplicado todas las medidas y políticas necesarias para que sea acreditable en un ejercicio futuro. Durante la realización de este TFG se ha podido observar todo este proceso de primera mano. La complejidad a la hora de aplicar las políticas

de seguridad en las VMs, ya que las STICs son altamente complejas, y los manuales explicativos que proporciona el CCN y el PCMSHS, que son muy densos, hacen de esta tarea un proceso arduo y complejo. Además, la implementación de un software Bare Metal de virtualización ha sido un nuevo reto al que los administradores han tenido que enfrentarse, ya que, no solo ha consistido en el proceso de instalación, sino también en el de aplicación de medidas de seguridad a este nivel como establece la CC-STIC.

4.2 Propuestas de trabajos futuros.

- Diseño de un proceso de acreditación de un sistema de información sobre plataforma de virtualización.

Como ya se ha comentado anteriormente, un nuevo sistema de información basado en un software de virtualización y el proceso de acreditación de un sistema no van de la mano. Suponen demasiados plazos y trámites burocráticos que hacen que un nodo pierda eficacia táctica al no estar disponible en un periodo de tiempo corto.

Las unidades han tomado SIMACET como sistema principal de una maniobra o ejercicio para ejercer la acción de mando y control sobre sus unidades desplegadas y para información de estas en un tiempo táctico real, que facilitan la toma de decisiones al mando del ejercicio u operación.

Desarrollar un nuevo sistema de acreditación orientado a certificar un sistema con software basado en virtualización sería un TFG adecuado, siempre y cuando esté orientado a reducir tanto los plazos de tiempo, como el número de veces que se debe acreditar el sistema y los trámites burocráticos, y que, como consecuencia, aumentarían la disponibilidad táctica del sistema garantizando un nivel adecuado de ciberseguridad de SIMACET.

- Integración de todos los servicios de un puesto de mando en un nodo de SIMACET.

La capacidad de poder desplegar cualquier tipo de servidor en cualquier sistema operativo dentro de una VM permite instalar muchos servicios desde los nodos, junto con la separación por VLANs en la parte física y virtual. El propio nodo de SIMACET versión 5 estaría preparado para implementar más servicios a parte del propio sistema SIMACET y de las aplicaciones OTAN, como viene haciendo.

Por ejemplo, desde el propio nodo se podría desplegar un servidor de telefonía IP (PBX) e incluir el servicio de telefonía dentro del nodo. Así se evitaría tener que desplegar un router de Call Manager Cisco, lo cual, no solo mejoraría la administración, sino también se ahorrarían costes al no tener que comprar estos routers.

También se podrían unificar físicamente los sistemas desplegables del ET, como por ejemplo SIJE, ya que utiliza una estructura de cliente-servidor, al igual que SIMACET, y sus controladores de dominio podrían pasar a ser VMs.

Una completa integración de todos los servicios en el mismo servidor físico facilitaría el despliegue de medios en un puesto de mando ya que reduciría la electrónica de red necesaria, la cantidad de personal para hacer el despliegue, así como los costes de hardware. Además, se podría diseñar una nueva estructura de centro de transmisiones ya que la filosofía de despliegue de medio cambiaría radicalmente.

Bibliografía

[1] Academia de Ingenieros, *SIMACET*, Hoyo de Manzanares, 2017.

[2] Mando de Adiestramiento y Doctrina, «Empleo de la Unidad de Transmisiones de la Brigada,» Granada, 2004.

[3] J. V. Sanchez Leandro, Introducción a la Virtualización con VMware ESXi, Valencia, 2010.

[4] Centro Criptológico Nacional, «Configuración de seguridad de entornos virtuales VMWare ESX,» 2010. [En línea]. Available: https://www.ccn-cert.cni.es/.

[5] Centro Criptológico Nacional, «Seguridad en Cortafuegos CISCO ASA,» 2015. [En línea]. Available: https://www.ccn-cert.cni.es/.

[6] Defensa, Estado Mayor de la, Procedimiento de Acreditación de Sistemas CIS Conjuntos v1.0, Madrid, 2007.

[7] C. Barquín Portillo, «Desarrollo de la Politica de Seguridad y Procedimientos de Auditoria para Seguridad en Sistemas de Informacion y Telecomunicaciones en entorno Militar,» Madrid, 2018.

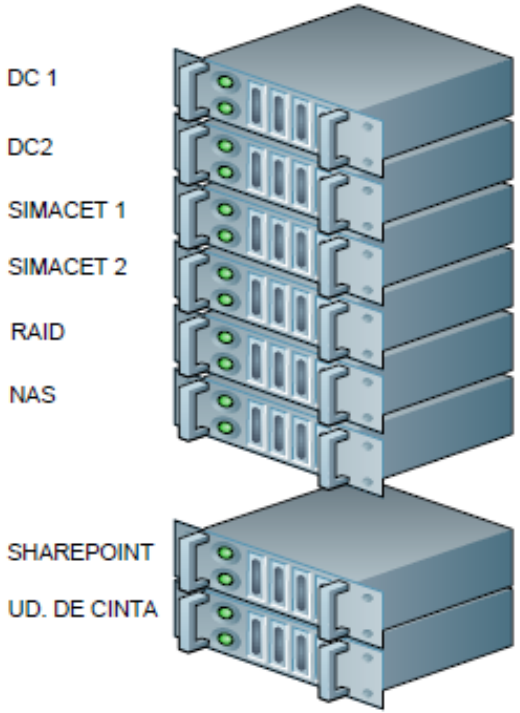
[8] Centro Nacional de Inteligencia, *Normas de la Autoridad Nacional para la proteccion de la Informacion Clasificada*, Madrid, 2016.

[9] M. A. De la Vega Iges, «Informe EXE TRITON 18,» 2018.

[10] Jefatura CIS y AT, «Seguridad de la Información en los Sistemas de Información (SEGINFOSIT) en el ambito del ET,» Madrid, 2011.

ANEXO A

NODO SIMACET VERSION 4.2.1



SIMACET 1 Y 2:
- SIMACET (CANCERBERO)
- XOMAIL

RAID: SERVIDOR DE DISCOS DE ALMACENAMIENTO QUE CONTIENE LA INFORMACIÓN ALMACENADA DE LOS SERVIDORES DE SIMACET 1 Y 2

CLUSTER
PROPORCIONA:
REDUNDANCIA DE MEDIOS
Y
ALTA DISPONIBILIDAD:
MODOS DE FUNCIONAMIENTO:
- ACTIVO-ACTIVO
- ACTIVO-PASIVO

NAS:
- SERVIDOR DE IMPRESIÓN
- SERVIDOR DE FICHEROS
- SERVIDOR DE CORREO EXCHANGE 2003
- SERVIDOR DE BASE DE DATOS SQL 2005
- SERVIDOR JEMM (LLEVA SU PROPIA BASE DE DATOS)
- SERVIDOR JCHAT (LLEVA SU PROPIA BASE DE DATOS – OPENFIRE)
- VERITAS: GESTOR DE COPIAS DE SEGURIDAD

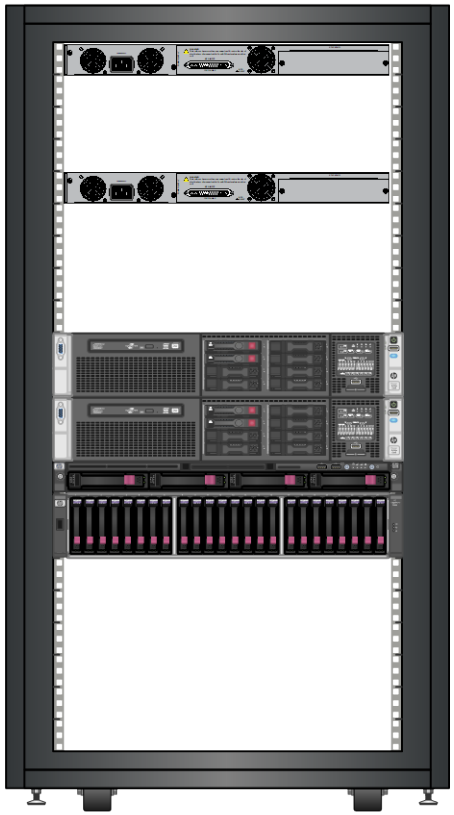
SHAREPOINT:
- SERVIDOR DE WSS 3.0 + (SERVIDOR DE BBDD SQL 2005 EXPRESS EMBEBIDA)

UD. DE CINTA:
- COPIAS DE SEGURIDAD

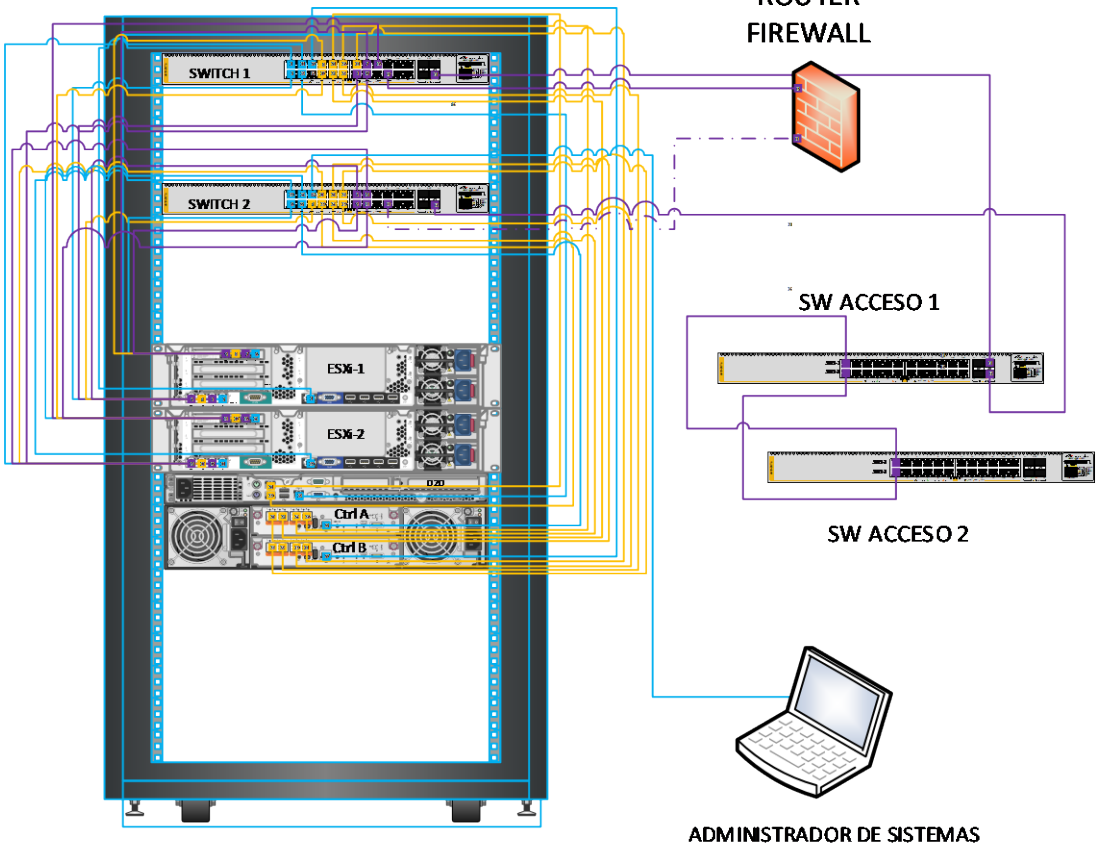
ANEXO B

NODO DE SIMACET VERSION 5

VISTA FRONTAL



VISTA TRASERA



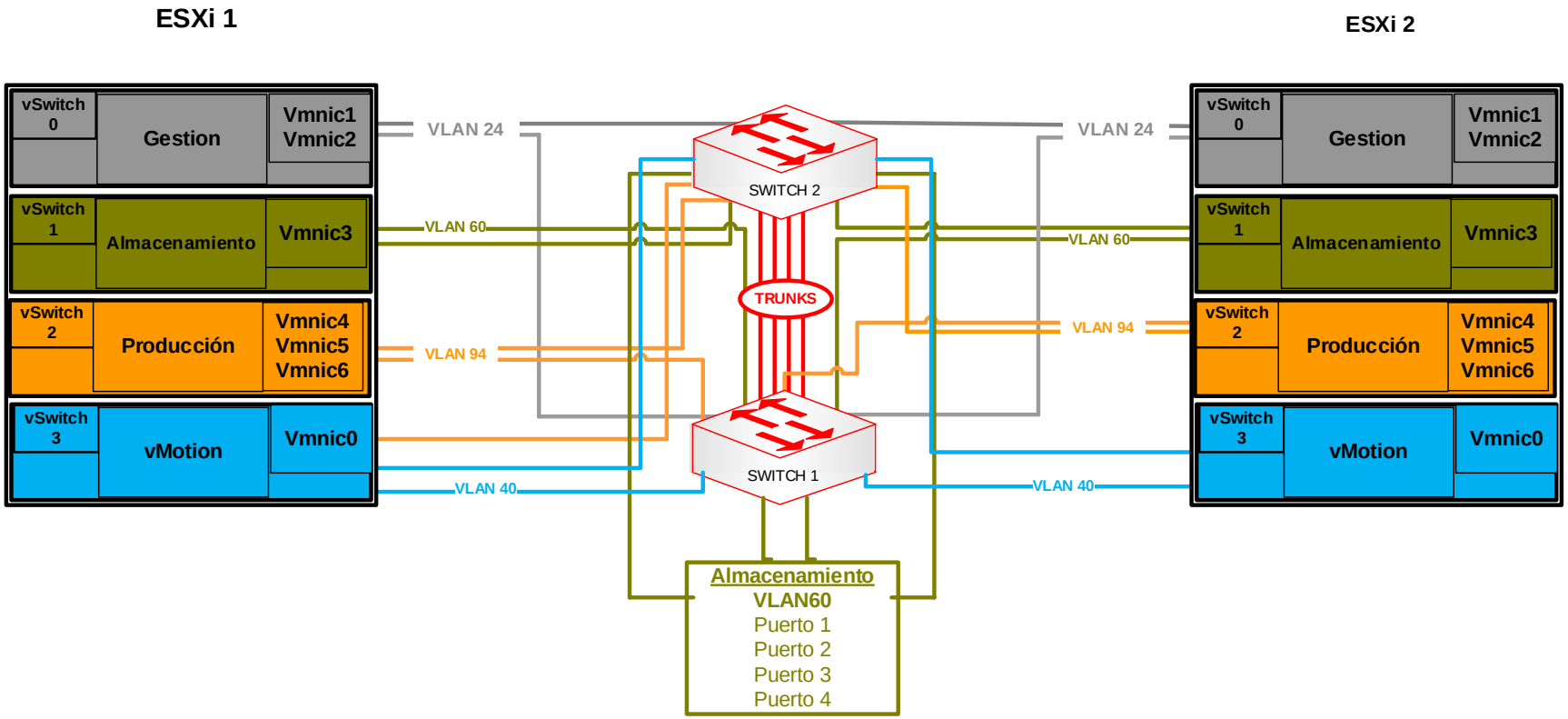
ALMACENAMIENTO – VLAN 60

GESTION – VLAN 24

PRODUCCION – VLAN 94

ANEXO C.1

ESQUEMA DE SWITCHES Y TARJETAS DE RED



ANEXO C.2

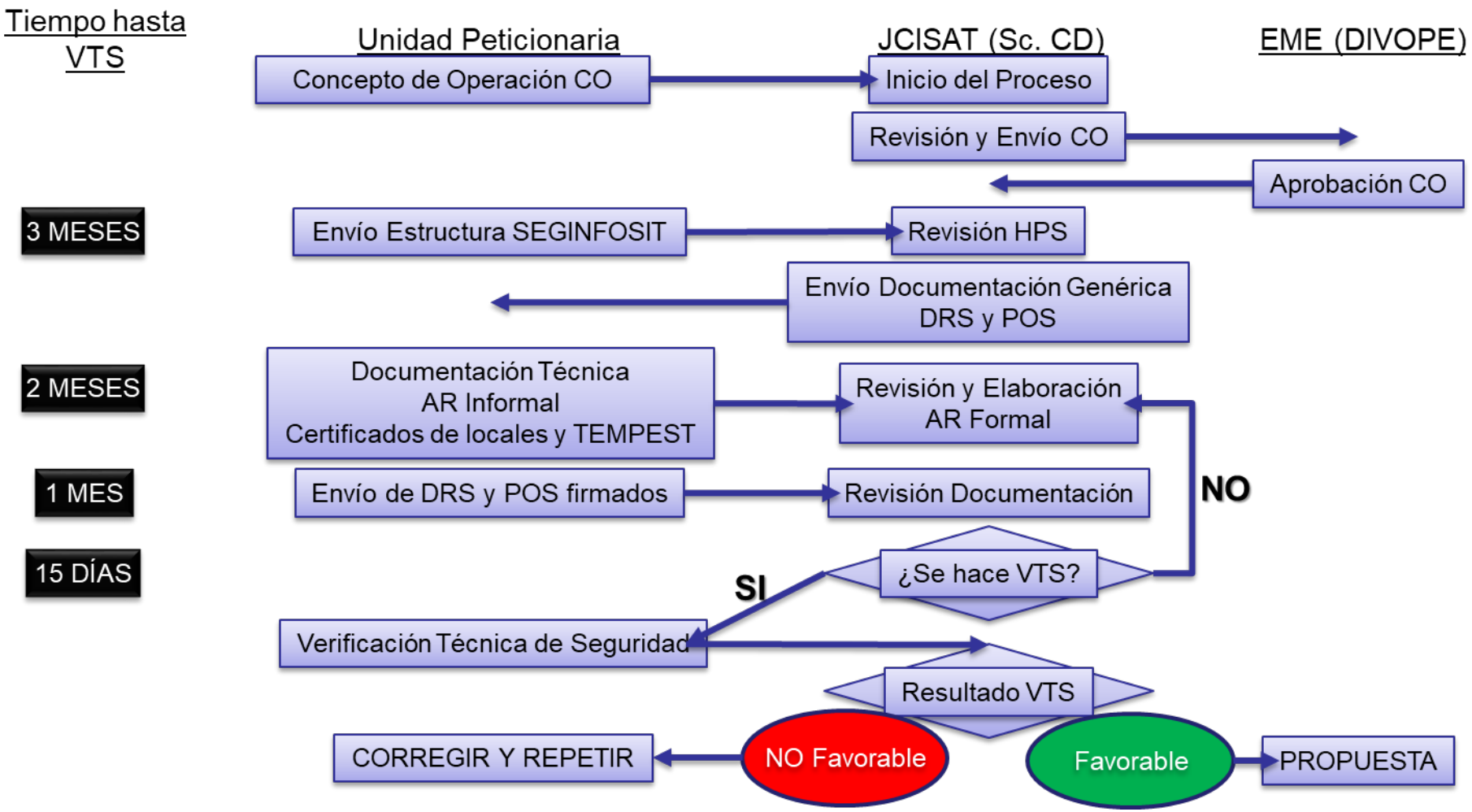
ASIGNACION DE PUERTOS DEL SWITCH

Switch	Red	VLAN	Puerto	Función
1	Gestion	24	1	esxi1-vmnic1
1	Gestion	24	2	esxi2-vmnic1
1	Gestion	24	3	Administrador PC
1	Gestion	24	4	Mngmt ILO ISCSI 0
1	Gestion	24	5	Mngmt ILO esxi1
1	Produccion	94	10	esxi1-vmnic4
1	Produccion	94	11	esxi2-vmnic5
1	Produccion	94	12	esxi2-vmnic7
1	vMotion	80	13	esxi1-vmnic0
1	vMotion	80	15	Switch2 P.15
1	ISCSI	60	17	esxi1-vmnic3
1	ISCSI	60	18	iSCSI-1
1	ISCSI	60	20	iSCSI-2
1	Trunk	Trunk	21	Uplink Switch 2
1	Trunk	Trunk	22	Uplink Switch 2
1	Trunk	Trunk	23	Uplink Switch 2
1	Trunk	Trunk	24	Uplink Switch 2

Switch	Red	VLAN	Puerto	Función
2	Gestion	24	1	esxi2-vmnic2
2	Gestion	24	2	esxi1-vmnic2
2	Gestion	24	3	Auxiliar PC
2	Gestion	24	4	Mngmt ILO ISCSI 1
2	Gestion	24	5	Mngmt ILO esxi2
2	Producción	94	10	esxi2-vmnic4
2	Producción	94	11	esxi1-vmnic5
2	Producción	94	12	esxi1-vmnic7
2	vMotion	81	13	esxi1-vmnic0
2	vMotion	81	15	Switch1 P.15
2	ISCSI	60	17	esxi2-vmnic3
2	ISCSI	60	18	iSCSI-3
2	ISCSI	60	20	iSCSI-4
2	Trunk	Trunk	21	Uplink Switch 1
2	Trunk	Trunk	22	Uplink Switch 1
2	Trunk	Trunk	23	Uplink Switch 1
2	Trunk	Trunk	24	Uplink Switch 1

ANEXO D

DIAGRAMA CON PERIODOS TEMPORALES DE ACREDITACIÓN



ANEXO E

DIAGRAMA DE GANTT CON EL PROCESO DE ACREDITACIÓN.