Creación y Gestión de un NOC (Network Operations Center)

Antonio José Pérez Galán
Grado de Ingeniería Informática
Administración de redes y Sistemas Operativos

Consultor: **Joaquín López Sánchez-Montañés**

18 de junio de 2023

Dedicatoria y agradecimientos

A mis abuelos, que ya no se encuentran entre nosotros. Por la educación y valores que siempre me han inculcado ofreciéndome su apoyo de forma incondicional y todo lo que han hecho por mí todos estos años sin dudarlo un momento, ya que, por ellos hoy día soy la persona que soy. Gracias abuelos.

A mi esposa, porque después de tantos años a mi lado, nunca ha dejado de apoyarme y valorarme, viendo cómo luchaba cada día por lograr mi sueño. Dejando de realizar infinidad de cosas para realizar otras que de una u otra forma encaminaría y mejoraría nuestro futuro. Ella siempre me ha dado las fuerzas, incluso en los peores momentos ha estado ahí siempre con una sonrisa. Gracias por estar siempre a mi lado, Irene.

A mi tutor de TFG, Joaquín López Sánchez-Montañés por su trabajo revisando las ideas que se me ocurrían para plasmarlas en el trabajo y orientándome sobre el camino a seguir.

A mi tutor de la UOC, Mario Pareja Nieto que siempre ha estado ahí para resolver cualquier problema que me haya surgido. Y a todos los profesores que me han acompañado en este camino.

Este trabajo es la culminación de años de formación, una formación que me ha ayudado a crecer como persona, aprendiendo e intentando ser mejor cada día. Algo que considero una vocación y que por fin puede verse reflejado.

Ficha del trabajo final

Título del trabajo:	*Creación y Gestión de un NOC (Network Operations Center)*
Nombre del autor:	*Antonio José Pérez Galán*
Nombre del consultor/a:	*Joaquín López Sánchez-Montañés*
Nombre del PRA:	*David Bañeres Besora*
Fecha de entrega:	*Junio 2023*
Titulación:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Administración de redes y sistemas operativos*
Idioma del trabajo:	*Español*
Palabras clave	*NOC, CCR, Operaciones, Control, Monitorización, Red*

Resumen del Trabajo

Los sistemas informáticos cobran una gran importancia hoy en día, tanta que estos sistemas deben ofrecer un servicio de forma ininterrumpida, y por ello surge la necesidad de crear un centro o departamento especializado, que de una forma centralizada ofrezca la posibilidad de solventar cualquier incidencia que pueda surgir, además de gestionar configuraciones y procedimientos.

Para solventar la problemática planteada surge el concepto de NOC (Network Operations Center) o CCR (Centro de Control de Red) en español, que se trata de un departamento especializado formado por personal cualificado principalmente en tareas de administración de sistemas informáticos. Por lo tanto, el objetivo principal de este trabajo es conocer en profundidad el funcionamiento de un NOC para poder gestionarlo de forma conveniente y crear una versión esencial que ofrezca funciones predeterminadas fácilmente ampliables.

Tras conocer el funcionamiento del NOC, se profundizará un poco más en la definición de requisitos que necesita para ofrecer servicio, así como su jerarquía, las funciones que realizará, la documentación e instrucciones que necesitará y la forma de generarla, la definición de procedimientos, la definición de protocolo de actuación, entre otras cosas.

Se configurarán los sistemas y herramientas necesarios para ofrecer el servicio de una forma óptima, además de explicar cómo se desarrolla la actividad dentro de dicho departamento incluyendo comunicación con el personal peticionario.

Para concluir, se creará un piloto cuya función es demostrar el funcionamiento de un NOC en el que se podrá observar el uso de las herramientas y gestión peticiones.

Abstract

Computer systems are of great importance nowadays, so much so that these systems must offer an uninterrupted service and therefore the need arises to create a specialised centre or department, which in a centralised way offers the possibility of resolving any incident that may arise, as well as managing configurations or procedures.

In order to solve this problem, the concept of NOC (Network Operations Center) or CCR (Centro de Control de Red) in Spanish language arises, which is a specialised department made up of personnel qualified mainly in computer system administration tasks. Therefore, the main objective of this work is to gain an in-depth understanding of how a NOC works in order to manage it conveniently and to create an essential version that offers easily extendable default functions.

After getting to know how the NOC works, the definition of the requirements needed to offer the service, as well as its hierarchy, the functions it will perform, the documentation and instructions it will need and how to generate them, the definition of procedures, the definition of protocols for action, among other things, will be discussed in greater depth.

The systems and tools necessary to offer the service in an optimal way will be configured, as well as explaining how the activity is developed within the department, including communication with the requesting personnel.

To conclude, a pilot will be created to demonstrate the operation of a NOC in which the use of the tools and management requests can be observed.

Índice

Índice de Figuras

Índice de Tablas

1. Introducción

1.1. Contexto y justificación del trabajo

En la actualidad, las organizaciones más que nunca necesitan monitorizar sus sistemas y controlar sus recursos para asegurar un buen funcionamiento que les permita evitar pérdidas de servicio, sobre todo en los momentos más críticos.

Para ello existen multitud de herramientas que facilitan la monitorización de estos sistemas y ayudan a catalogar las posibles incidencias que vayan surgiendo con suficiente antelación para ser tratadas y resueltas. Estas herramientas, junto a personal competente en la materia, son el equipo responsable de garantizar que los sistemas funcionen de forma adecuada, además de proveer un entorno totalmente confiable y con la mínima pérdida de servicio.

La combinación anterior de herramientas y personal cualificado da nombre al Centro de Control de Red (CCR), en inglés denominado Network Operations Center (NOC), responsable de diseñar soluciones, realizar instalaciones, ofrecer mantenimiento preventivo y correctivo a las operaciones de soporte, gestionar y monitorizar sistemas informáticos, entre otras muchas tareas.

Ya que la labor principal del NOC es garantizar un servicio ininterrumpido y un funcionamiento correcto de los sistemas, este se está convirtiendo en una prioridad y cada vez más una necesidad para la gran mayoría de las organizaciones que invierten altas sumas de dinero, tanto para el mantenimiento y actualización de los sistemas, como para evitar incidencias con el servicio, las cuales le producirían una mala reputación, además de grandes pérdidas en distintos ámbitos, como puede ser el financiero o económico (bancos, tiendas online, etc.), el de la salud (hospitales, farmacias, etc.), el de las organizaciones gubernamentales (ministerios, prestaciones, etc.), el de los trasportes (metro, tren, etc.), entre otros.

La implantación de un NOC o la subcontratación de estos servicios en una organización, nos asegurarán un desempeño de actividad 24/7 los 365 días del año o durante la mayor parte de este tiempo, cumpliendo con la normativa de seguridad, resolviendo los problemas surgidos y aportando confiabilidad en el sistema.

En este trabajo se describirá el funcionamiento de un NOC y todas las posibilidades que este puede llegar a ofrecer. También se creará un piloto de un NOC, que pueda dar servicio a cualquier tipo de organización, independientemente del tamaño de esta, además de ser adaptativo y ofrecer la posibilidad de ampliar de forma sencilla las actividades o tareas que en él se realizan.

1.2. Objetivos del trabajo

Los principales objetivos de este trabajo son:

- Conocer el funcionamiento general de un NOC y todo el potencial que puede llegar a desarrollar.
- Conocer las distintas actividades que se pueden realizar en el NOC y las herramientas básicas necesarias.
- Comprender la estructura interna del NOC, así como su jerarquía y organización del trabajo.
- Conocer los documentos que se utilizan y los distintos tipos de informes que se generan en el NOC.
- Aprender a analizar lo que necesita la organización, partiendo de unas actividades que puedan cubrir los requisitos básicos de cualquier tipo de organización, para posteriormente implementarlo y ofrecer este servicio.

Los objetivos parciales para lograrlo son los siguientes:

- Comprender cómo funciona un NOC y lo que este puede llegar a ofrecer para entender dónde están los límites.
- Aprender los procedimientos para la resolución de incidencias u otras actividades que se llevan a cabo en el NOC y que nos servirán para conocer cómo se realiza el desempeño de la actividad.
- Comprender las competencias de cada uno de los distintos niveles que existen en el NOC.
- Conocer las distintas herramientas y posibilidades existentes que permitan realizar las diversas actividades desarrolladas en el NOC.

1.3. Enfoque y metodología seguida

Para llevar a cabo este proyecto, debemos entender el funcionamiento de un NOC general, sus características y todos los criterios que permiten el desarrollo de las distintas actividades. También es necesario conocer los distintos documentos, así como las herramientas disponibles para este propósito y analizar la que mejor se adapte a las necesidades de la organización.

Una vez conozcamos en detalle lo descrito anteriormente, procederemos a analizar los requisitos necesarios para la creación del piloto de un NOC, que sea capaz de cubrir las necesidades mínimas de cualquier tipo de organización y con posibilidad de agregar nuevas actividades fácilmente.

1.4. Planificación del trabajo

Para realizar la planificación del trabajo debemos tener en cuenta la fecha de inicio del curso que está fijada el 1 de marzo de 2023 y la fecha de entrega final máxima fijada para el 18 de junio de 2023, por lo que la planificación deberá estar comprendida entre ambas fechas.

Teniendo en cuenta los datos descritos anteriormente y ajustándonos al periodo temporal, se realiza una planificación de actividades para la realización del Trabajo de Fin de Grado que podemos observar en la siguiente tabla:

ACTIVIDAD	COMIENZO	FIN	DURACIÓN
TFG - Creación y Gestión de un NOC	***01/03/2023***	***18/06/2023***	***110 días***
Inicio del Trabajo de Fin de Grado	15/03/2023	15/03/2023	0 días
PEC 1: Plan de trabajo	***01/03/2023***	***15/03/2023***	***15 días***
Planteamiento del proyecto	01/03/2023	01/03/2023	1 día
Búsqueda de información y organización de ideas	02/03/2023	03/03/2023	2 días
Estudio planificación	04/03/2023	05/03/2023	2 días
Estudio propuesta de índice	06/03/2023	07/03/2023	2 días
Elaboración del plan de trabajo	08/03/2023	15/03/2023	8 días
Revisión y entrega PEC 1	15/03/2023	15/03/2023	0 días
PEC 2: TFG entre 40% y 60%	***16/03/2023***	***19/04/2023***	***35 días***
Creación de la estructura del documento de la memoria	16/03/2023	17/03/2023	2 días
Estudio de las herramientas necesarias	18/03/2023	19/03/2023	2 días
Creación máq. virtuales e instalación sistema operativo	20/03/2023	21/03/2023	2 días
Preparación del entorno para la creación del piloto NOC	22/03/2023	23/03/2023	2 días
Instalación y configuración de las herramientas	24/03/2023	03/04/2023	11 días
Avance en la creación de la memoria y revisión	04/04/2023	19/04/2023	16 días
Revisión y entrega PEC 2	19/04/2023	19/04/2023	0 días
PEC 3: TFG entre 80% y 90%	***19/04/2023***	***25/05/2023***	***37 días***
Preparación ejemplos del piloto NOC	19/04/2023	25/04/2023	7 días
Finalización del piloto NOC	26/04/2023	01/05/2023	6 días
Avance en la creación de la memoria y revisión	02/05/2023	25/05/2023	24 días
Revisión y entrega PEC 3	25/05/2023	25/05/2023	0 días
PEC 4: Entrega final del TFG	***26/05/2023***	***18/06/2023***	***24 días***
Acabar la memoria, revisar y realizar correcciones finales	26/05/2023	01/06/2023	7 días
Realizar presentación diapositivas	02/06/2023	09/06/2023	8 días
Realizar vídeo e informe de autoevaluación	10/06/2023	18/06/2023	9 días
Revisión y entrega PEC 4	18/06/2023	18/06/2023	0 días

Tabla 1: Planificación del Trabajo de Fin de Grado

En las siguiente imagen podemos observar el diagrama de Gantt correspondiente a la planificación anterior:

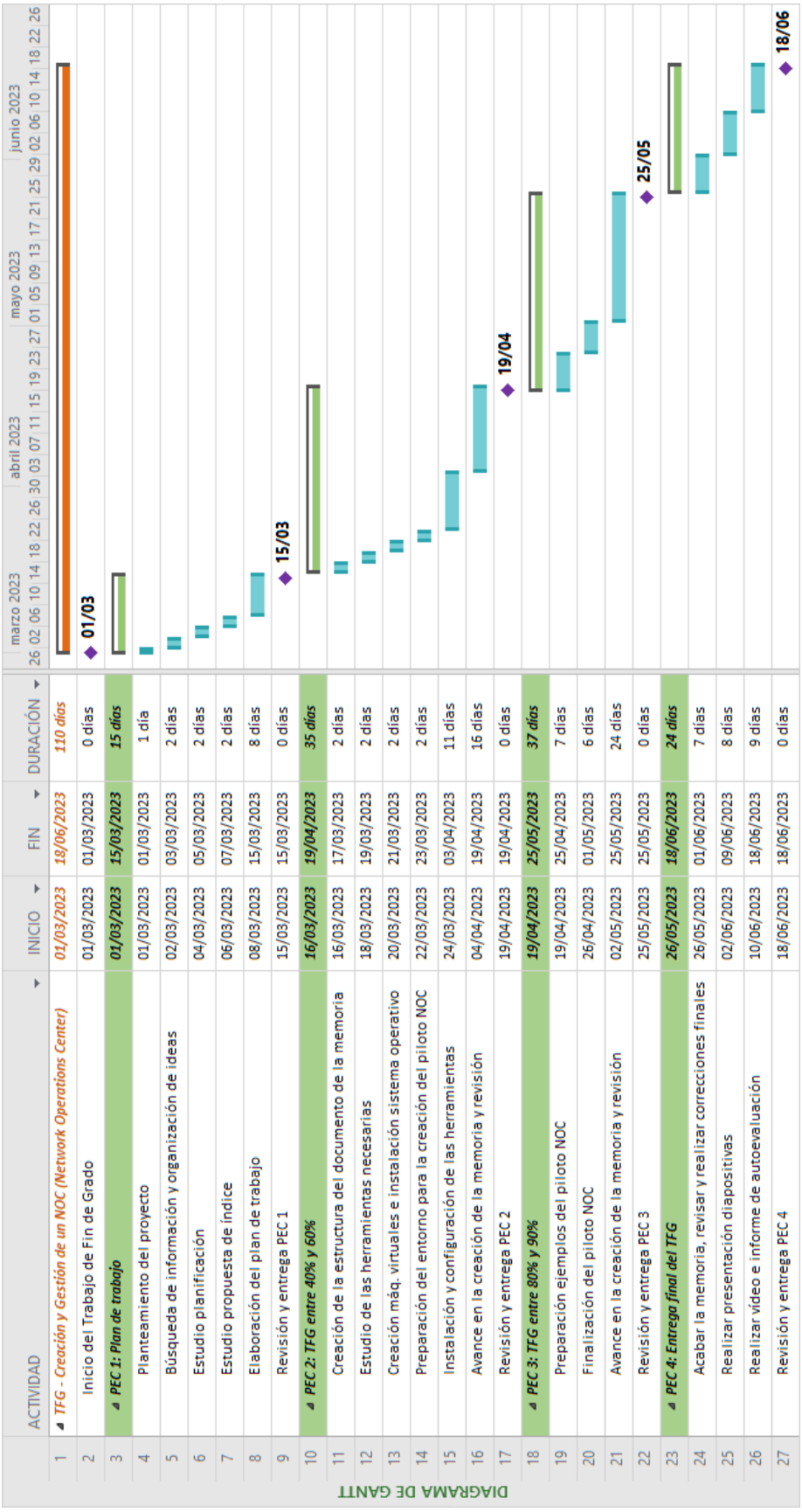


Figura 1: Diagrama de Gantt

1.5. Breve sumario de productos obtenidos

El objetivo de este trabajo es adquirir los conocimientos necesarios para entender el funcionamiento de un NOC, las actividades que puede realizar y los beneficios que puede proporcionar a la organización.

Una vez conocemos el funcionamiento del NOC, tendremos la posibilidad de adaptarlo a las necesidades que demande la organización y para ponerlo en práctica crearemos un piloto de un NOC, cuya finalidad es demostrar lo que en esta memoria se describe.

Teniendo en cuenta lo anterior, el producto obtenido queda incluido en esta memoria como una guía de recomendaciones para el entendimiento, así como la creación y gestión de un NOC, aplicable a cualquier tipo de organización independientemente de su tamaño y actividad realizada.

1.6. Breve descripción de los otros capítulos de la memoria

En este apartado describiremos de forma breve los tres capítulos principales en los que está basado este trabajo:

- **Capítulo 2. Descripción y funcionamiento general de un NOC**

  En este capítulo se define el concepto de NOC, así como las principales características que debe poseer y las actividades que puede llegar a realizar de una forma general, que nos brindará los conocimientos necesarios para su comprensión.

- **Capítulo 3. Definición de requisitos para la creación de un NOC**

  En este capítulo se definen los requisitos mínimos que cualquier NOC debe poseer, los cuales nos darán una idea y nos ayudarán a comenzar con su diseño, para posteriormente realizar la creación de un piloto de un NOC, que cubrirá todas las necesidades básicas de cualquier tipo de organización.

  También, definiremos y normalizaremos los documentos necesarios que deben estar alojados en la base de conocimientos y a los que todo el personal del departamento deberá poder acceder para la realización de sus respectivas tareas o actividades.

- **Capítulo 4. Creación de un piloto de un NOC**

  En este capítulo crearemos el piloto de un NOC para poner en práctica lo explicado en los dos capítulos anteriores, mostrando las distintas instalaciones y configuraciones necesarias para la ejecución de las herramientas, que permitirán el desempeño de la actividad en el NOC.

2. Descripción y funcionamiento general de un NOC

En este capítulo se explica en detalle el concepto de NOC (Network Operations Center), así como sus funciones principales, los beneficios que proporciona a la organización, donde está ubicado, su organización interna y jerarquía en niveles. También, veremos que nos podemos encontrar dentro de dicho departamento y las herramientas que se utilizan, para finalizar con una descripción general de su funcionamiento.

2.1. ¿Qué es un NOC?

Un NOC (Network Operations Center) o CCR (Centro de Control de Red) en español, es un centro o departamento especializado en tareas de administración de sistemas, donde casi la totalidad del personal que lo compone son administradores TI.

La necesidad de crear un NOC surgió por varias razones principales. Una de estas razones era la de centralizar todas las tareas de administración de sistemas y proporcionar así un lugar para situar a todos los profesionales de este ámbito, en lugar de tenerlos de un lado para otro solucionando las incidencias que iban surgiendo o realizando tareas de mantenimiento como la actualización de los sistemas, entre otras. Otra de estas razones es la de poder supervisar de forma constante una red de computadores y detectar fallas en su funcionamiento, ya sea por un tema de seguridad, fallo en el hardware de algún equipo o cualquier otra cosa que pueda surgir.

De forma general, este departamento se emplaza dentro de una sala amplia, que posee una instalación centralizada, donde los profesionales ya sean internos o de terceros pueden monitorizar, supervisar, resolver incidencias y mantener una red de computadores de manera constante, fácil y rápida para asegurar una alta disponibilidad de todos los servicios, sobre todo los de carácter crítico. Para poder realizar las operaciones mencionadas, es imprescindible que el NOC disponga de toda la tecnología necesaria para apoyar dichas operaciones como pantallas o monitores de gran tamaño, ordenadores, equipos de comunicación y una buena conexión a los recursos de la red.

Las grandes corporaciones con extensas redes, recursos y servicios que deban proporcionar un servicio ininterrumpido de cualquier forma, suelen tener un NOC de forma interna, dentro de la propia organización. Para organizaciones de menor tamaño existe la posibilidad de subcontratar el NOC a empresas del sector tecnológico, que se dedican a ofrecerlo como un servicio y que operan por norma general desde una sede o ubicación externa a la organización que la contrata. No por ser un servicio externalizado debe existir una degradación del servicio sino todo lo contrario, aunque el coste puede ser algo más elevado.

La figura del NOC hoy día, no solo se limita a ofrecer las funciones mencionadas, sino que, debido a la gran versatilidad y amplio horario, puede asumir casi cualquier tarea.

2.2. ¿Qué encontramos dentro de un NOC?

Dentro de la ubicación del NOC encontramos grandes pantallas que muestran información de los equipos que se están monitorizando en todo momento y el estado en el que se encuentran, además de monitores de menor tamaño que nos muestran información de elementos más específicos o de carácter crítico. La necesidad de estas pantallas viene dada para que una gran cantidad de personas tengan la posibilidad de visualizar de forma rápida la información que en ellas se muestran.

El acceso a este lugar debe estar fuertemente restringido y solo permitido a personal autorizado, ya que puede mostrarse información sensible o estratégica respecto a los datos o seguridad de los sistemas.

También, nos encontramos con personal coordinador y técnico, donde la mayoría pertenecen al primer nivel. Este personal se encarga del buen funcionamiento del NOC, que comprende desde su coordinación, hasta la gestión de las distintas tareas repartidas en los distintos niveles según su complejidad de resolución. Las actividades principales desarrolladas consisten en procesar incidencias de cualquier tipo, gestionar alertas, ejecutar procedimientos programados, entre otras tareas.

Otros recursos que podemos encontrar son teléfonos para gestionar las alertas e incidencias, equipos informáticos para el personal, herramientas para la gestión de acceso remoto, bases de conocimientos y otros monitores dedicados a mostrar información de gran interés.

Figura 2: Lo que podemos encontrarnos dentro de un NOC

2.3. Actividades que se desarrollan en un NOC

Las actividades principales que se desarrollan en un NOC están dedicadas en su gran mayoría a mantener el correcto funcionamiento de los sistemas y resolver las incidencias que puedan surgir, siendo el departamento responsable. Pero hay muchas más actividades que pueden implementarse de forma adicional, debido a la facilidad que posee para asumir tareas repetitivas o que deban realizarse fuera de horario laboral, pudiendo seguir hasta el final la trayectoria de la tarea.

A continuación, se muestra una tabla con las actividades principales o básicas que como mínimo deben poder ser ejecutadas y otras actividades secundarias o adicionales que también pueden ser encomendadas al NOC:

ACTIVIDADES PRINCIPALES / BÁSICAS	ACTIVIDADES SECUNDARIAS / ADICIONALES
Monitorización de sistemas	Gestión de actualizaciones y parcheado
Gestión y resolución de incidencias	Gestión del cortafuegos
Ejecución de procedimientos	Gestión del software de seguridad
Gestión de perfiles de usuario y acceso	Gestión del antivirus
Gestión de dispositivos	Bastionado de equipos (*Hardening*)
Creación de informes	Scripting para resolución de problemas y automatizaciones
Ejecución de peticiones de servicio	Gestión de la implementación para traslado a entorno activo
	Gestión del directorio activo
	Aplicación de políticas
	Gestión de certificados
	Gestión de recursos virtualizados
	Gestión de aplicaciones remotas
	Control de inventarios
	Administración de bases de datos
	Gestión de comunicaciones
	Gestión de correo electrónico
	Gestión de almacenamiento y copias de seguridad
	Optimización de los sistemas y la red
	Gestión de sistemas de energía
	Gestión de la nube

Tabla 2: Actividades que se pueden realizar en un NOC

Para ver la descripción detallada de cada actividad, consultar Anexo I de este documento.

2.4. Beneficios que proporciona a la organización

Las ventajas de poseer un NOC especializado supone enormes beneficios para la organización, sobre todo cuando necesita alta disponibilidad de los sistemas y un alto rendimiento en todo momento, que sin duda mejorará la experiencia del usuario final.

A continuación, se muestran algunos de estos beneficios tras la implantación de un NOC:

- Disminución del tiempo de inactividad de los sistemas y servicios.
- Mejora en la disponibilidad de la red y rendimiento.
- Automatización de tareas repetitivas y por lo tanto aumento de productividad.
- Mejoras en la seguridad y detección precoz de amenazas.
- Aumento de la eficiencia y por lo tanto optimización de recursos.
- Sistemas siempre actualizados y revisados.

2.5. Ubicación y disponibilidad

Un NOC puede ubicarse en una sala acondicionada y administrada de forma interna por la propia organización como un departamento más, o por una empresa externa fuera de la organización como un servicio gestionado.

Todas las actividades desarrolladas en el NOC se llevan a cabo las 24 horas del día, los 7 días de la semana y los 365 días de año.

2.6. Organización interna y jerarquía en distintos niveles

Dentro del departamento que constituye el NOC existe una jerarquía en varios niveles, que demarcan la responsabilidad y especialización de cada grupo de técnicos pertenecientes a cada nivel, además de la figura del coordinador como persona responsable de dicho departamento y cuyos perfiles detallaremos a continuación:

- Coordinador NOC
    - Es la persona responsable y encargada de organizar las tareas del departamento.
    - Se encarga de gestionar de la mejor forma posible los recursos del departamento, tanto materiales como personales, solicitando personal en caso necesario para cubrir una alta demanda puntual de servicio.
    - Organiza reuniones para el seguimiento de las actividades que se están desarrollando o están planificadas para su desarrollo.

- Personal técnico de primer nivel (L1)
    - Los técnicos de primer nivel son los encargados de gestionar y solventar incidencias de complejidad media o baja que pueden llegar por distintas vías como la telefónica, correo electrónico, peticiones directas o generación a través de alertas del sistema de monitorización.
    - Son la primera línea para la detección de anomalías en los sistemas y los encargados de comenzar su resolución de forma inmediata.
    - Realizan procedimientos que son complejos de automatizar o requieren de varios pasos como actualizaciones de aplicaciones o sistemas, creación de informes, gestión de llamadas y consulta de correo electrónico para procesar incidencias, gestión de usuarios o cualquier otra tarea dentro del ámbito de la administración de sistemas.
    - Se encargan de la gestión de permisos básicos de usuarios para que puedan acceder al sistema o desbloquearlos en caso necesario.
    - Es el perfil más numeroso dentro del departamento.
    - Su horario de trabajo es 24/7 los 365 días del año, organizado en turnos rotativos.

- Personal técnico de segundo nivel (L2)
    - Los técnicos de segundo nivel son los encargados de gestionar tickets escalados por el primer nivel y que tienen algo más de complejidad para su resolución, requiriendo personal con un nivel más alto de experiencia.
    - Pueden plantear modificaciones y cambios que crean oportunos en el departamento ante el coordinador, personal especialista del tercer nivel o directamente al nivel inferior siempre que mejoren la ejecución de los procesos.
    - Poseen un rango más alto de permisos dentro de la organización respecto a utilización de herramientas, gestión accesos y control sobre otros usuarios del sistema, que les permite poder realizar acciones que el primer nivel no puede por la falta de estos permisos.
    - Dado a su nivel de permisos son los encargados de dar de alta los nuevos sistemas, instalarlos, configurarlos y realizar pruebas antes de que estos sistemas entren en producción.
    - Pueden delegar tareas nuevas o tareas existentes y que puedan automatizarse al nivel inferior, para que se realicen como si de un procedimiento más se tratase.
    - Su horario de trabajo suele ser normal y pueden tener asignadas guardias, en las que deben ofrecer servicio fuera del horario laboral.

- Personal técnico de tercer nivel (L3)
    - Los técnicos de tercer nivel son los que poseen el nivel más alto de conocimientos de la jerarquía y suele estar formado por personas con un nivel de estudios de ingeniería o con muchos años de experiencia en el sector.
    - En este nivel pueden existir especialistas en distintas áreas como expertos en sistemas Windows y Linux o especialistas en sistemas y aplicaciones concretas como son los sistemas de sistemas IBM, VMware, aplicaciones específicas, actualizaciones, bases de datos, integraciones, etc.
    - Se encargan de resolver problemas muy complejos o que aún no tienen solución documentada, teniendo que crear una solución personalizada para ello.
    - Gestionan los tickets escalados por el segundo nivel y deben proporcionar una solución válida al problema de cualquier forma, teniendo para ello distintos recursos a su disposición, como personal de otros departamentos especializados, empresas externas, soporte técnico de las marcas del mercado y cualquier recurso que desee consultar puede serle aprobado previa autorización del coordinador.
    - Pueden plantear modificaciones y cambios que crean oportunos en el departamento ante el coordinador o directamente a los niveles inferiores sin ningún tipo de objeciones.
    - Poseen un rango casi ilimitado permisos dentro de la organización y en casi todos los ámbitos, que le permite hacer casi cualquier configuración o procedimiento.
    - Pueden delegar tareas que estén bien documentadas o de carácter repetitivo a los niveles inferiores.
    - Pueden crear nuevos procedimientos que serán agregados a lista de tareas de los niveles inferiores junto con la correspondiente documentación de dicho procedimiento.
    - Son los encargados de revisar las propuestas de mejora o modificaciones de los documentos existentes y aprobarlas para que pueda ser utilizadas y normalizadas dentro de la base de conocimientos.
    - Es el perfil menos numeroso y más difícil de encontrar para una organización, debido al nivel de conocimientos que se requiere.
    - Su horario de trabajo suele ser normal y pueden tener asignadas guardias, en las que deben ofrecer servicio fuera del horario laboral para la resolución de problemas críticos.

2.7. Herramientas para el desarrollo de la actividad

Las herramientas utilizadas en un NOC dependerán de las actividades que este desarrolle, pero hay un software mínimo que debe poseer y que le permitirá detectar irregularidades en los sistemas, así como gestionar de forma correcta los problemas que puedan surgir, llevar un control de lo que se realiza en todo momento y abrir, crear o modificar todo tipo de documentos.

En las siguientes tablas se muestran las herramientas básicas y algunas otras que ofrecerán la posibilidad de realizar actividades adicionales:

HERRAMIENTAS BÁSICAS	
Software de monitorización	Software que permite la monitorización de los sistemas y alerta cuando algún parámetro no cumple con las reglas definidas. Ej. *Zabbix, SCOM,* etc.
Software de ticketing	Software que facilita la gestión de soporte, además de ofrecer una trazabilidad de las tareas realizadas y del personal que interviene. Ej. *GLPI.*
Software ofimático	Software para la gestión de los documentos necesarios que permiten el desarrollo de la actividad. Ej. *Microsoft 365, LibreOffice, Acrobat Reader,* etc.
Navegador web	Software que permite el acceso a la web e interfaces de herramientas. Ej. *Google Chrome, Firefox,* etc.
Gestor de correo electrónico	Software que permite gestionar múltiples buzones de correo electrónico. Ej. *Microsoft Outlook*.
Software de acceso remoto	Software que permite el acceso remoto a otros equipos para realizar intervenciones, configuraciones o resolver alguna incidencia.
Permisos de administración para los distintos niveles de la jerarquía.	Permisos necesarios para la correcta ejecución de tareas en los distintos sistemas y dispositivos. Estos permisos dependerán del nivel al que pertenezca el técnico y son más restrictivos en niveles inferiores.
Plantillas para informes u otros documentos	Plantillas normalizadas para creación de documentos.
Base de conocimientos	Lugar donde se encuentra la documentación necesaria para el correcto desarrollo de la actividad.
Equipos informáticos para los técnicos	Pueden ser equipos físicos (equipo portátil, PC o tableta) o equipos virtuales (mediante acceso remoto), con todos sus periféricos (ratón, teclado, …).
Teléfonos móviles	Terminales que se usarán para la comunicación del personal técnico en el desarrollo de sus tareas, así como la recepción de nuevas incidencias.
Pantallas o monitores de gran tamaño	Las pantallas de gran tamaño se usan para mostrar información importante, como las alertas del sistema de monitorización u otro tipo de indicadores que debe ser visibles por todo el personal de la sala.
Pantallas o monitores de menor tamaño	Se usan para monitorizar otros sistemas específicos.

Tabla 3: Herramientas para el desarrollo de actividades primarias o básicas

HERRAMIENTAS PARA EL DESARROLLO DE ACTIVIDADES ADICIONALES	
Software de monitorización de red	Software especializado en la monitorización de la red.
Software para actualización de sistemas	Herramientas que facilitan la actualización y parcheado de sistemas de la red. Ej. *WSUS*, *SCCM* para Windows. *Red Hat Satellite* para Linux.
Software de gestión del cortafuegos	Herramientas que permiten la configuración del cortafuegos o firewall.
Software de gestión de la seguridad	Software o conjunto de herramientas que se encargan de proteger de ataques indeseados.
Software o consola centralizada de gestión del antivirus	Software que protege la red de virus informáticos bloqueando o eliminando del sistema la amenaza. Varias compañías permiten la gestión centralizada de todos los dispositivos de la red. Ej. *McAfee*.
Guías de bastionado (*Hardening*)	Documentos que detallan los pasos a realizar para que un sistema sea seguro, reduciendo sus vulnerabilidades. Normalmente estas guías suelen estar adaptadas a los sistemas de la organización.
Software para la gestión de directorio activo	Herramientas que permiten la configuración del directorio activo para gestionar permisos, GPO, etc.
Consolas de gestión de recursos virtualizados	Software que facilita la administración de los recursos virtuales y su interacción con el hardware físico. Ej. *vCenter* de VMware.
Software de gestión de aplicaciones remotas	Herramientas que permiten la publicación de aplicaciones y asignación de permisos a usuarios para que puedan hacer el uso de aplicaciones remotas. Ej. *RemoteApp* de Windows Server.
Software de control de inventario	Software que facilita la gestión del inventario de la organización como los equipos que posee, monitores, periféricos, impresoras, teléfonos, licencias, software, etc. Ej. *GLPI* tiene esta la funcionalidad.
Software de administración de bases de datos	Software que permite administrar la creación, mantenimiento y uso de las bases de datos, además de los permisos de los usuarios que accederán a ellas.
Software de gestión de comunicaciones	Software que permite gestionar dispositivos de comunicaciones como centralitas telefónicas, para poder asignar números, modificar asignaciones, restringir llamadas o resolver incidencias.
Software de administración de correo electrónico	Software que permite administrar cuentas de correo existentes, así como la creación de nuevas cuentas corporativas, grupos de correo, etc.
Software de copias de seguridad	Software encargado de la gestión de copias de seguridad que permitirá la recuperación de estas réplicas en caso de desastre. Ej. *Veeam Backup*.
Software de gestión de sistemas de energía	Software que ofrece información del estado del sistema o estado de las baterías en el caso de un SAI.
Software de gestión de sistemas en la nube	Herramientas que facilitan la gestión de los sistemas en la nube.

Tabla 4: Herramientas para el desarrollo de actividades secundarias o adicionales

2.8. Tipos de informes

La generación de informes es una actividad básica y muy importante dentro de un NOC, ya que proporciona información valiosa sobre el funcionamiento de este y las actividades que allí se realizan.

Esta información puede ser muy útil a la hora de valorar y justificar el trabajo realizado, mejorar procedimientos, ofrecer a los clientes datos sobre qué acciones se han tomado en sus sistemas, cambiar procedimientos para ahorrar costos en recursos y personal, entre otras ventajas.

Entre los distintos informes que se pueden realizar, se mencionan algunos de ellos y más importantes:

- Informes sobre las incidencias que se han gestionado.
- Informes sobre los procedimientos realizados.
- Informes sobre la resolución de una incidencia concreta.
- Informes de los sistemas afectados por incidencias concretas o de forma general.
- Informes de los equipos o los sistemas que se han actualizado.
- Informes de los equipos que se han bastionado.
- Informes sobre el control del inventario.
- Informes relacionados con cualquier actividad que se realice en el NOC.

2.9. Descripción general del funcionamiento

El funcionamiento interno de un NOC puede diferir un poco dependiendo de la organización donde se desarrolle su actividad, pero no deben existir grandes diferencias respecto a un funcionamiento general del mismo.

Básicamente casi cualquier actividad desarrollada en el NOC debe tener un ticket creado, que permitirá conocer en detalle de que trata la actividad, los pasos necesarios para llegar a su resolución, las herramientas que han sido utilizadas, los recursos materiales y personales que se han empleado, la persona responsable, las personas intervinientes, el tiempo de resolución, el tiempo dedicado por cada uno de los técnicos que han intervenido en su resolución y todos los datos que se consideren relevantes.

Basándonos en algunas de sus actividades principales como son la resolución eficiente de problemas que pueden surgir en cualquier momento y la ejecución de procedimientos programados, detallaremos el procedimiento para la gestión y control de estas actividades mediante tickets.

A continuación, se procederá a explicar el proceso para la creación, gestión, resolución y cierre de un ticket, así como los posibles impedimentos que pueden surgir:

- En primer lugar, debemos conocer los datos del procedimiento a realizar, que puede ser planificado con antelación o puede generarse sobre la marcha. En el caso de las incidencias, pueden producirse en cualquier momento y suelen tener una prioridad más alta.

  Los datos de las incidencias se obtienen principalmente a través de una comunicación por correo electrónico, teléfono o alertas generadas por el sistema de monitorización y pueden ser gestionadas en horario 24/7, los 365 días del año.

- Con los datos anteriores creamos un nuevo ticket, en que hay que introducir un título representativo de la tarea a realizar y una descripción detallada.

  El título para los procedimientos se corresponderá con el procedimiento que se va a realizar. Para las incidencias basta con una breve descripción de esta.

  La descripción para procedimientos será un breve texto que detallará el procedimiento a realizar y la documentación necesaria para realizarla. Para incidencias es necesario detallar minuciosamente todos los datos que tengamos sobre dicha incidencia, primeras impresiones, posibles soluciones, documentos de consulta y toda información útil que nos pueda ser de ayuda para facilitar las tareas de resolución.

  Los tickets creados se ubican en un espacio común donde los técnicos pueden verlos y ser asignados a cualquiera de ellos por cualquier otro técnico.

- Una vez creado el ticket es necesario asignarlo a un técnico de primer nivel que será el encargado de gestionarlo y priorizarlo dentro de sus tareas.

  Como ya se ha mencionado anteriormente, las incidencias tienen más prioridad que los procedimientos programados por norma general, pero en el caso de que un procedimiento haya comenzado su ejecución, no siempre puede detenerse para gestionarse una incidencia. Por lo que siempre debe haber uno o varios técnicos disponibles para atender tareas con una alta prioridad.

- Una vez asignado el ticket y llegado el momento de comenzar, se procede con su resolución, agregando todas las tareas que se van realizando al ticket.

  En el caso de un procedimiento, casi siempre hay que seguir unas guías que nos ayudarán a ejecutar dicho procedimiento y agregar información al ticket en caso de que surja algún inconveniente. En el caso de una incidencia, es necesario agregar información al ticket de cada uno de los pasos que se realizan, como consultas de documentos o instrucciones técnicas que solucionen el problema en cuestión o uno similar, ensayos en un entorno de pruebas, cambios realizados o cualquier otra información relevante.

Si el contenido de la documentación o instrucción disponible difiere mucho respecto a la realización del procedimiento o resolución de la incidencia, se puede proponer para crear una adaptación del documento que resuelva este nuevo problema. Las adaptaciones y nuevos documentos solo pueden ser validados y normalizados por personal técnico de tercer nivel o el coordinador.

En caso de que no sea posible su resolución por el técnico de primer nivel debido a que no encuentra la información que le ayude a solucionar el problema o no pueda avanzar de ninguna forma, el ticket debe ser escalado a un nivel superior, en este caso, el segundo nivel. El técnico de segundo nivel responsable se hará cargo del ticket y comenzará con su resolución, pudiendo ser escalado a un tercer nivel en caso de bloqueo por falta de recursos o conocimientos.

Si se produce una incidencia fuera de horario laboral, es de carácter crítico (caída de un servidor que realiza las transacciones en cajero de banco, servicios de emergencias, etc.) y el técnico tiene problemas para su resolución, se puede escalar al servicio de guardia que normalmente está compuesto por personal con gran conocimiento ubicado en el tercer nivel.

Si acaba el turno del técnico responsable del ticket, debe transferirlo para que se pueda continuar con su resolución en un turno posterior, siempre registrando toda la información relativa al cambio de turno dentro del ticket.

También puede ser necesario involucrar a otros departamentos especializados para resolver partes del ticket y que el personal del NOC no posea suficientes privilegios para gestionarlo (p. ej. departamento de RRHH que casi siempre tiene acciones restringidas para el resto de los departamentos de una organización). En este caso el ticket puede asignarse a otro departamento y hasta que este no resuelva la parte correspondiente o tarea encomendada y valide que lo ha resuelto, no se puede continuar con el ticket por parte del NOC.

- Una vez acabado el procedimiento o resuelta la incidencia el ticket queda cerrado y los datos registrados en este, podrán consultarse en el futuro para la realización de informes o cualquier otra información que pueda ser de utilidad.

Una vez explicado de forma general como se realizan dos de las principales actividades desarrolladas en el NOC, podemos extrapolarlo a cualquier otra actividad que se desee implementar, como las actualizaciones de sistemas, desbloqueos de cuentas de usuario, reinicio de un servidor en activo, configuración en el cortafuegos, etc., creando para ello un nuevo ticket que contenga la información, documentación consultada y detalle de las acciones efectuadas para realizar dicha actividad.

También es necesario mencionar, que siempre debe existir un procedimiento de recuperación de desastres o plan de contingencia definido, al que todo el personal del NOC debe tener acceso.

En el siguiente diagrama de flujo se puede observar el procedimiento para la gestión de un ticket descrito anteriormente.

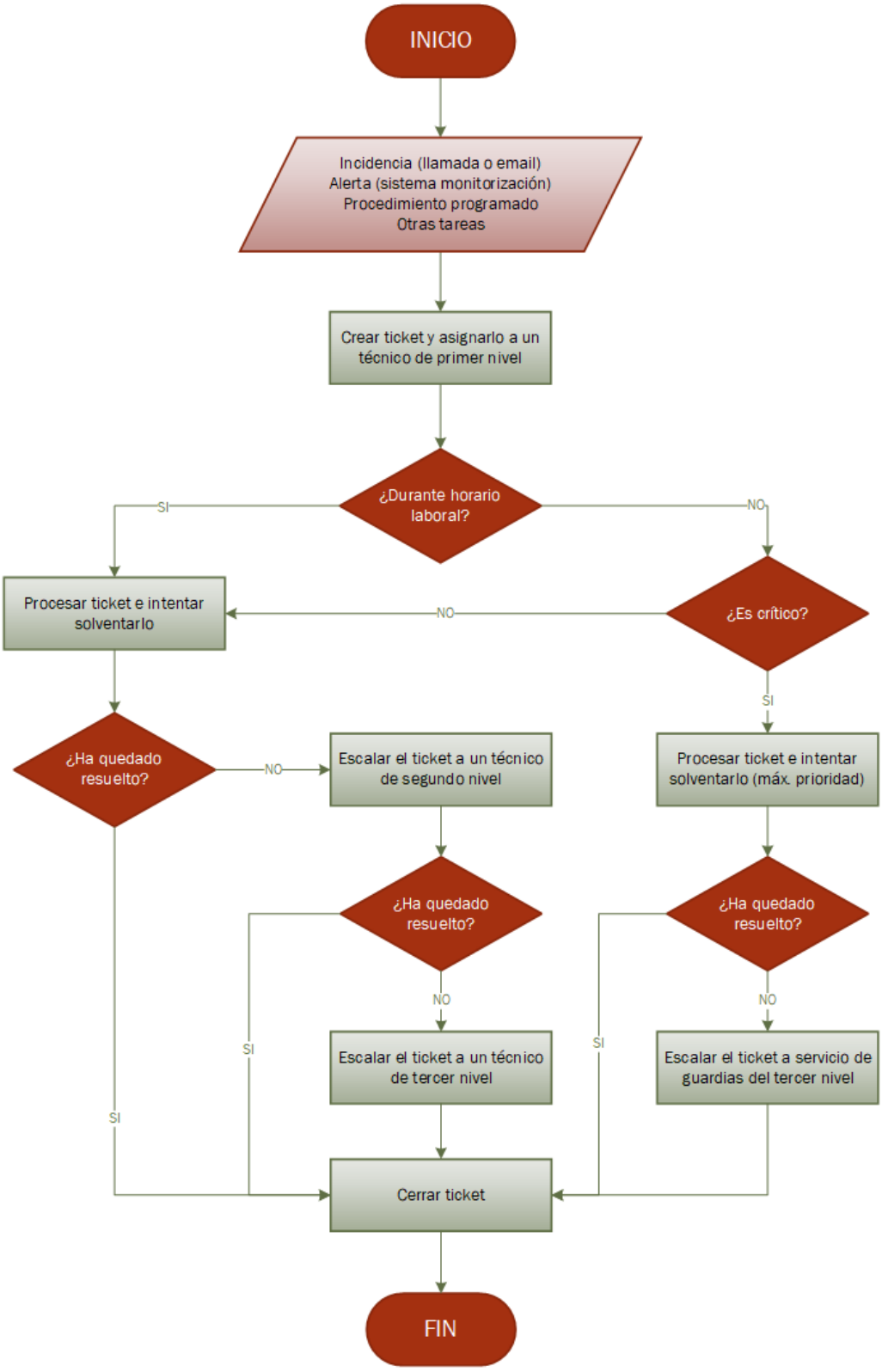


Figura 3: Diagrama de flujo del procedimiento de creación y gestión de tickets

3. Definición de requisitos para la creación de un NOC

En este capítulo se definen las características básicas que cualquier NOC debe tener, las cuales nos ayudarán con su análisis, diseño y posterior implementación de un piloto de un NOC, que cubrirá todas las necesidades básicas de cualquier tipo de organización, independientemente de su tamaño.

3.1. Análisis y definiciones de algunos requisitos necesarios

En este apartado analizaremos y definiremos algunos de los principales requisitos necesarios en un NOC, como las actividades que van a desarrollar, creación de la matriz de contactos y definición del servicio de guardias que son documentos imprescindibles en cualquier NOC, definición de su estructura interna con su jerarquía y el proceso a seguir para la creación de informes.

3.1.1. Análisis y definición de las actividades que se desarrollarán

Un NOC que pueda cubrir las necesidades esenciales de cualquier organización, debe desarrollar como mínimo una serie de actividades, las cuales se listan a continuación:

- **Monitorización de sistemas:** Su función es detectar irregularidades en los sistemas que se están monitorizando, para así poder remediarlas o buscar un plan alternativo que permita la continuidad del servicio.

  Para esta tarea se usa un software de monitorización, encargado de capturar datos del estado de los componentes de los distintos sistemas de la red e interpretarlos conforme a unas reglas definidas y una criticidad asignada.

- **Gestión y resolución de incidencias:** Dentro de las principales actividades que realiza el NOC, la gestión y resolución de incidencias es la que abarca más porcentaje de dedicación por parte del personal técnico, ya que cualquier problema que ocurra en cualquier dispositivo de la red o mal funcionamiento de esta, se convertirá en una incidencia que hay que resolver casi siempre a la mayor brevedad posible.

  Para esta tarea se usa un software de ticketing o gestión de tickets, que se encarga de agrupar toda la información relativa a la descripción del problema y su resolución, que posteriormente será usada como base de consulta para resolver incidencias similares, además de ser la principal fuente de datos para la creación de informes.

- **Ejecución de procedimientos:** Hay ciertos procedimientos que deben ser ejecutados de forma manual, ya que, por su naturaleza no permiten su automatización o poseen algún tipo de dependencia. Estos procedimientos se realizan con regularidad y si no han comenzado su ejecución se pueden aplazar en la mayoría de los casos, siendo menos numerosos que las incidencias.

- **Gestión de perfiles de usuario y acceso:** La gestión de los usuarios abarca las tareas de creación, modificación y eliminación del sistema, así como el desbloqueo de las cuentas y un mantenimiento correcto de los datos. Los perfiles de los usuarios creados en los sistemas también deben ser mantenidos y revisados para evitar consumir recursos innecesarios.

- **Gestión de dispositivos:** Gestionar los dispositivos de la red implica, desde una configuración mínima para que estos puedan estar operativos y utilizados, hasta su mantenimiento en el sistema, teniendo toda la información referente a estos dispositivos correctamente actualizada.

- **Creación de informes:** Los informes brindan información importante de las actividades que se realizan en el NOC, proporcionando datos sobre el trabajo realizado o que permitirán mejorar el servicio ofrecido, entre otra información. La principal fuente de datos para generar estos informes es la herramienta de gestión de tickets, que registra cada una de las acciones realizadas en cualquier actividad y que posea su correspondiente ticket.

- **Ejecución de peticiones de servicio:** Este tipo de peticiones están enfocadas a la realización de procedimientos principalmente, pero pueden ser solicitadas en cualquier momento por cualquier persona autorizada para ello.

Todas estas actividades, permitirán monitorizar los sistemas de la organización para detectar anomalías que puedan derivar en una falta de servicios y que puede perjudicar gravemente a la institución.

Para cada una de las actividades descritas anteriormente se deberá crear un ticket en el sistema, que incluirá todos los datos relevantes hasta llegar a su resolución, ofreciendo así una trazabilidad completa de cada una de las actividades realizadas en el NOC.

3.1.2. Creación de la matriz de contactos

La matriz de contactos es un documento donde se detalla los responsables de cada tecnología, área, departamento o servicio dentro de la organización y su función principal es la de poder contactar con la persona encargada en caso de desastre, que pueda producir una falta de servicio, para que ponga en marcha un protocolo de actuación adecuado que permita resolver el problema.

Por norma general el NOC gestionará e intentará solventar todo lo que esté en su mano para evitar la falta de servicio, pero a veces la enorme complejidad o la falta de documentación hace imposible ejecutar acciones correctoras y por ello siempre debe haber un plan alternativo, en este caso la matriz de contactos realiza esa función.

Los niveles técnicos superiores de la jerarquía no siempre conocen el sistema implementado mejor que el departamento o la persona encargada de montarlo, la cual posee un pleno conocimiento de lo que allí se ha realizado. En este caso, el escalado del ticket a niveles superiores no siempre es la solución óptima, siendo mejor contactar con el responsable del sistema directamente.

La matriz de contactos, también nos ofrece la posibilidad de poder solicitar permisos a los responsables de los sistemas implementados, para poder realizar ciertas acciones o procedimientos en ellos.

En la siguiente tabla, se muestra un ejemplo de una matriz de contactos, que contiene los principales datos de los responsables de cada departamento de la organización, como el nombre del departamento, nombre de la persona, correo electrónico y teléfono, así como algunos contactos para casos de emergencia:

DEPARTAMENTO	NOMBRE	CORREO	TELÉFONO
Servicio de emergencias	**Emergencias**	**-**	**112**
Servicio de guardias	**Guardias NOC**	**guardias@tfg.com**	**699111444**
NOC	Antonio Galán	a.galan@tfg.com	612345678
Microinformática	Sergio Cabello	s.cabello@tfg.com	623456789
Ciberseguridad	Diego Cueto	d.cueto@tfg.com	634567891
Desarrollo (Web)	Laura Gómez	l.gomez@tfg.com	645678912
Desarrollo (General)	Juan Pino	j.pino@tfg.com	656789012
Integraciones	Armando Ruz	a.ruz@tfg.com	667891234
Nuevas tecnologías	Irene Mora	i.mora@tfg.com	678901234
Administración Sistemas (Sistemas Windows)	David Morales	d.morales@tfg.com	689123456
Administración Sistemas (Sistemas Linux)	Andrés Paz	a.paz@tfg.com	690123456
Administración Sistemas (Bases de datos)	Sandra Subires	s.subires@tfg.com	611234567
Administración Sistemas (Redes)	Eva Macias	e.macias@tfg.com	622345678
Administración Sistemas (Otros sistemas)	Ángel Alonso	a.alonso@tfg.com	633456789
Infraestructuras (CPD)	Luis Molina	l.molina@tfg.com	644567891
Infraestructuras	Rafael García	r.garcia@tfg.com	600678912
Instalaciones	Aitor Reina	a.reina@tfg.com	601234567
...	...	...	...

Tabla 5: Matriz de contactos

3.1.3. Definición de los niveles a implementar y su jerarquía

La estructura interna de un NOC está formada por tres niveles compuestos por técnicos especialistas y un coordinador, siendo este último el que posee el rango más alto de la jerarquía en el departamento, siguiéndole los niveles tercero, segundo y primero respectivamente. Esta configuración suele ser la más habitual en casi cualquier NOC, aunque no existe un modelo único y dependiendo de la actividad desarrollada en la organización siempre puede adaptarse.

A continuación, se definirá en detalle los distintos niveles en los que se dividirá el NOC, así como el rol de coordinador y su jerarquía en orden descendente:

- **Coordinador:** Es la persona responsable de dirigir dicho departamento gestionando los recursos de este. Posee el rango más alto en la jerarquía respecto a la toma de decisiones, pero no siempre el nivel más alto de conocimientos.

- **Técnicos de tercer nivel (L3):** Son los técnicos con el nivel más alto de conocimientos y los que más escasean debido a su gran nivel de especialización. Dentro del tercer nivel existirán distintas subáreas que demarcarán las especialidades de cada uno de estos técnicos, como especialistas en sistemas Windows o Linux, especialistas en tecnologías concretas, etc. Su rango en la jerarquía esta justo detrás del coordinador y es el más alto de los tres niveles definidos, pudiendo proponer tareas de forma directa a los niveles inferiores.

- **Técnicos de tercer nivel (L2):** Son los técnicos con un nivel alto de conocimientos que pueden desempeñar tareas de carácter general. Su rango en la jerarquía se encuentra entre el primer y tercer nivel, pudiendo proponer tareas de forma directa al nivel inferior.

- **Técnicos de tercer nivel (L1):** Son los técnicos con el nivel bajo de conocimientos, pero igualmente deben poseer conocimientos profesionales y pueden desempeñar tareas de carácter general. Su rango es el menor de la jerarquía, pero no por ello el menos importante, ya que son la primera barrera en la detección de anomalías y problemas de carácter crítico.

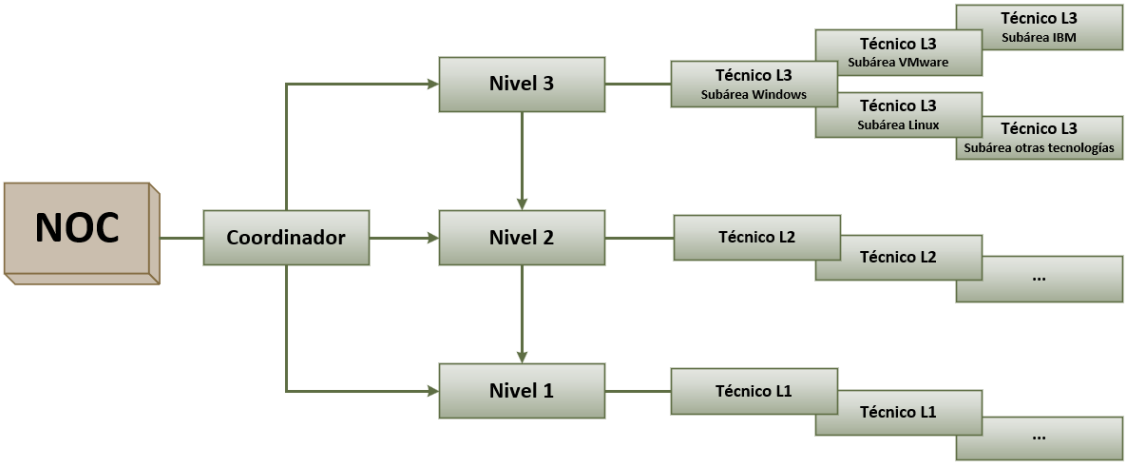


Figura 4: Organigrama NOC

3.1.4. Definición del servicio de guardias

El NOC es un departamento que debe ofrecer su servicio de forma continua y sin interrupción, por ello es necesario definir un sistema de guardias para realizar intervenciones fuera de horario laboral.

Estas guardias están enfocadas solamente a actividades de carácter crítico o pérdida de servicio y serán ofrecidas por personal altamente cualificado, normalmente el tercer nivel. Aunque el tercer nivel posee técnicos especializados en distintas subáreas, todos deben formarse para poder gestionar problemas de cualquier tipo y en cualquier sistema. Las guardias son asignadas de forma individual y serán rotatorias semanalmente entre los técnicos de tercer nivel que estén capacitados para realizarlas.

El personal de primer nivel, aunque desarrolla su actividad las 24 horas, en turnos de 8 horas rotatorios en mañana tarde y noche, no posee servicio de guardias, ya que sus tareas pueden realizarse en cualquier horario y muchos de los procedimientos ejecutados se realizan en horario nocturno, coincidiendo con la menor carga de trabajo de los sistemas. En las ejecuciones de procedimientos nocturnos es donde suelen ocurrir las incidencias más críticas que pueden necesitar el uso del servicio de guardias.

Para que el personal de primer nivel pueda localizar y comunicarse con la persona que ofrece la guardia, existe un documento que recoge la planificación anual de las guardias y que debe de estar actualizado en todo momento. Si por cualquier circunstancia no se tiene claro la persona responsable de esa guardia, se puede llamar a un teléfono habilitado para ello y que se puede localizar en la matriz de contactos, que forzosamente la persona que se encuentre de guardia debe responder.

En la siguiente tabla, se muestra un ejemplo del documento con la planificación de las guardias del departamento, que contiene los datos de las personas encargadas en realizar la guardia, periodo de duración de la guardia, nombre de la persona, correo electrónico y teléfono de contacto, así como el teléfono general:

SEM. #	FECHA DE LA GUARDIA	NOMBRE	CORREO	TELÉFONO
∞	Todo el año	Telf. general	guardias.noc@tfg.com	699111444
≤ 18	≤ 07/05/2023	…	…	…
19	08/05/2023 – 14/05/2023	Camila Beker	c.beker@tfg.com	699123456
20	15/05/2023 – 21/05/2023	Leonardo Prieto	l.prieto@tfg.com	699234567
21	22/05/2023 – 28/05/2023	Teresa Vera	t.vera@tfg.com	699345678
22	29/05/2023 – 04/06/2023	Aurelio Sanz	a.sanz@tfg.com	699456789
23	05/06/2023 – 11/06/2023	Camila Beker	c.beker@tfg.com	699123456
24	12/06/2023 – 18/06/2023	Leonardo Prieto	l.prieto@tfg.com	699234567
≥ 25	≥ 19/06/2023	…	…	…

Tabla 6: Planificación de guardias

3.1.5. Definición del proceso de creación de informes

La necesidad de crear un procedimiento normalizado para la creación de los informes es de vital importancia, de esta forma evitamos que se omita información importante o que se complique en exceso su lectura.

Los informes deben tener reglas, además de plantillas para facilitar y agilizar el trámite de creación. Los apartados que cada informe debe contener dependerán del tipo de informe que se quiera crear y su contenido deben estar muy bien definido.

A continuación, se describirán los distintos apartados que deben contener los informes de actividades básicas desarrolladas en el NOC:

- Parte común que poseerá cualquier tipo de informe realizado por el NOC
    - La primera hoja contiene el título del informe, rango de fechas en las que se basa dicho informe, logotipos de la organización y logotipos del departamento que realiza el informe, que en este caso el NOC.
    - La segunda hoja contiene el nombre del autor de informe, además de una tabla con el nombre del fichero, versión del informe, resumen o cambios que se han producido en el informe desde la versión anterior y fecha de realización del informe.
    - La tercera hoja contiene un índice con todos los apartados y subapartados que contendrá el informe.
    - Las hojas restantes desarrollarán los apartados y subapartados del índice, que dependerá del tipo de informe (ver parte específica a continuación).
    - Las últimas hojas del informe contendrán un apartado final de conclusiones en el que se informará si es posible mejorar el procedimiento actual y la forma propuesta para hacerlo.

- Parte específica para informe sobre las incidencias que se han gestionado
    - Este tipo de informe tendrá un apartado con sus respectivos subapartados, donde se deberá especificar las incidencias que se han gestionado, tipo (p. ej. se producen tras actualizar el sistema o ejecutar algún programa), carácter (p. ej. es crítico o no lo es), recursos empleados, material consultado, personal implicado, datos sobre su resolución, fechas de inicio y finalización, además de cualquier otro dato relevante.
    - Otro apartado, donde se informará de las incidencias más comunes y si es posible buscar una alternativa para solventarlas de forma más eficiente.
    - Otro apartado, donde se indique si ha ocurrido algo fuera de normalidad respecto a la resolución de incidencias, que se deba tener en cuenta.

- Parte específica para informe sobre los procedimientos que se han realizado
    - Este tipo de informe tendrá un apartado con sus respectivos subapartados, donde se deberá especificar los procedimientos realizados, tipo (p. ej. realizar cambios en un software con dependencias), carácter (p. ej. es crítico o no lo es), recursos empleados, material consultado, personal implicado, datos sobre su ejecución, fechas de inicio y finalización, además de cualquier otro dato relevante.
    - Otro apartado, donde se indique si ha ocurrido algo fuera de normalidad al realizar la ejecución de dicho procedimiento.

- Parte específica para informe sobre la resolución de una incidencia concreta
    - Este tipo de informe tendrá un apartado dedicado a una incidencia concreta, donde se deberá especificar el tipo (p. ej. se producen tras actualizar el sistema o al ejecutar algún programa), carácter (p. ej. es crítico o no lo es), recursos empleados, material consultado, personal implicado, datos sobre su resolución, fechas de inicio y finalización, además de cualquier otro dato relevante.
    - Otro apartado, donde se informará los sistemas que han sido afectados por dicha incidencia y si es posible buscar alguna alternativa para solventarlas de forma más eficiente.
    - Otro apartado, donde se indique si ha ocurrido algo fuera de normalidad respecto a la resolución de la incidencia.

- Parte específica para informe de sistemas afectados por incidencias
    - Este tipo de informe tendrá un apartado con sus respectivos subapartados, donde se deberá especificar los sistemas afectados por incidencias ya gestionadas, tipo (p. ej. sistema Windows o Linux), carácter (p. ej. es crítico o no lo es), datos sobre el estado final de los sistemas, fechas de inicio y finalización, además de cualquier otro dato relevante.
    - Otro apartado, donde se informará los sistemas que ha producido más incidencias y si hay alguna forma de evitar que estas se produzcan.

- Parte específica para informe sobre cualquier otra actividad realizada en el NOC
    - Este tipo de informe tendrá un apartado con sus respectivos subapartados, donde se deberá especificar en detalle la actividad realizada.
    - Otros apartados, donde se especifiquen los sistemas afectados, mejoras que pueden realizarse, plan de futuro o cualquier otro dato relevante.

3.2. Análisis de las herramientas principales

En este apartado nos centraremos en estudiar algunas de las herramientas disponibles y las posibilidades que nos pueden ofrecer. También describiremos las herramientas que mejor se adaptan a las necesidades requeridas, para posteriormente implementarlas en el piloto de NOC y que permitirán el correcto desarrollo de las actividades.

3.2.1. Análisis de las distintas herramientas disponibles

Existen multitud de herramientas que permiten la realización de las actividades que se desarrollan en un NOC, facilitando el trabajo y ayudando a conseguir un objetivo final. La elección de estas herramientas dependerá en gran medida de las actividades que se deseen implantar, pero también del equipamiento disponible y del tipo de licencia que se desee adquirir.

Algunas de las herramientas esenciales en un NOC son: software de monitorización, software para la gestión de tickets, software ofimático, navegador web, gestor de correo electrónico, software de acceso remoto, algunos documentos (plantillas, instrucciones técnicas, guías, …) y un sistema que permita construir una base de conocimientos.

Además de las herramientas, también es necesario un equipamiento básico como monitores, equipos completos con sus periféricos, teléfonos, pantallas de distintos tamaños, así como una serie de permisos para que los técnicos puedan realizar las distintas tareas.

Una vez conocemos las necesidades respecto a los tipos de herramientas, equipamiento y permisos, nos centraremos en las principales herramientas que todo NOC debe poseer para poder desarrollar sus actividades, como el software de monitorización de sistemas, software de gestión de tickets y software de ofimática:

- **Software de monitorización:** Este software permite realizar una monitorización exhaustiva de los componentes del sistema y alerta cuando algún parámetro no cumple con las reglas que se han definido.

  Algunas de las herramientas de código abierto que permiten la monitorización de sistemas son: *Prometheus + Grafana*, *Nagios*, *Checkmk* o *Zabbix*, siendo esa última la que mejor se adapta a nuestras necesidades y la seleccionada para implementar en el piloto NOC. Otra herramienta, en este caso de pago es *SCOM* (System Center Operations Manager) desarrollado por Microsoft.

- **Software de ticketing:** Este software facilita la gestión de soporte, permitiendo la creación de un ticket que ofrecerá una trazabilidad completa de las tareas que se han realizado para resolverlo, además de otros datos de interés como el personal que ha intervenido, fecha de apertura, documentos consultados, etc.

Algunas de las herramientas de pago que permiten la gestión de tickets son: *Jira*, *HelpDesk* o *Zendesk*. En nuestro caso para el piloto NOC, usaremos una herramienta de ticketing de código abierto llamada *GLPI* (Gestionnaire Libre de Parc Informatique) o gestión de servicios de tecnología de la información en español.

- **Software de ofimática:** Este software permite trabajar con diversos tipos de documentos permitiendo su creación, lectura y edición.

  Algunas de las principales suites ofimáticas son: *Libre Office* (software de código abierto) y *Microsoft 365* (servicio de suscripción), siendo este último el que implementaremos en el piloto NOC. Otra herramienta complementaria al software anterior es *Acrobat Reader* en su versión gratuita, que nos facilitará la lectura de documentos PDF.

3.2.2. Descripción de las herramientas seleccionadas

Describiremos y estudiaremos los requisitos previos que necesitan las herramientas para poder ser instaladas, enfocándonos en las principales herramientas comentadas en el apartado anterior, así como la configuración del sistema necesaria para su puesta en marcha y que detallamos a continuación:

- **Software de monitorización *(Zabbix)*:** Una de las herramientas que ofrece las funcionalidades necesarias para la monitorización de los sistemas es *Zabbix*. Esta herramienta es de código abierto y está diseñada para monitorizar y registrar el estado de equipos, servidores, servicios y hardware de red.

  Zabbix ofrece monitorización en tiempo real de parámetros que pueden ayudar a determinar el estado de un sistema, permitiendo detectar problemas en sus principales componentes, tanto hardware como software.

  Permite varias opciones de monitorización como chequeos simples para verificar la disponibilidad o el estado de respuesta de servicios y mediante la instalación de un agente en los equipos, se pueden monitorizar sus componentes cuyos datos serán enviados al servidor Zabbix de forma cifrada.

  Los datos enviados a la herramienta de monitorización son almacenados en una base de datos relacional y mediante una interfaz web, permite su consulta, así como la configuración de la propia herramienta Zabbix.

  Para su instalación se requiere un sistema operativo Linux, en nuestro caso usaremos Ubuntu Server, y antes de proceder con la instalación de *Zabbix* es necesario instalar un gestor de bases de datos como *MySQL* o *MariaDB*, un servidor web como *Apache*, configurar *PHP* y abrir puertos en el cortafuegos o firewall.

- **Software de ticketing *(GLPI)*:** Otra de las herramientas, que en este caso ofrece las funcionalidades necesarias para la gestión de tickets en un NOC es *GLPI*. Esta herramienta es de código abierto y tiene multitud de funciones, de las que inicialmente solo usaremos la función de asistencia o soporte y que nos ayudará a gestionar las actividades que se realizan en el NOC, como la gestión de incidencias o la ejecución de procedimientos.

  Los tickets almacenarán datos relevantes sobre el procedimiento utilizado para resolver la tarea y proporcionará un histórico para su posterior consulta.

  Los datos son almacenados en una base de datos relacional y mediante una interfaz web, permite su consulta, así como la configuración de la propia herramienta GLPI.

  Para su instalación es necesario un sistema operativo Linux, en nuestro caso usaremos Ubuntu Server, y antes de proceder con la instalación de *GLPI* es necesario instalar un gestor de bases de datos como *MySQL* o *MariaDB*, un servidor web como *Apache* y configurar e instalar módulos *PHP* necesarios.

- **Software de ofimática *(LibreOffice, Microsoft 365, Acrobat Reader)*:** Otra herramienta básica es una suite ofimática o paquete de aplicaciones de oficina, que permitan crear, modificar y leer cualquier tipo de documento.

  Para la lectura de documentos PDF, se puede usar cualquier navegador que posea esta utilidad o usar un software que permita su visualización, como puede ser *Acrobat Reader* en su versión gratuita u otro similar.

  Tanto *LibreOffice* como *Microsoft 365* tienen varias aplicaciones, las cuales están diseñadas para ser compatibles en su mayor parte entre las dos suites ofimáticas, cuyas aplicaciones más utilizadas son:

  - El procesador de texto (*Writter* en *LibreOffice* y *Microsoft Word* en *Microsoft 365*), facilitará la creación de documentos de texto, así como su visualización y modificación.
  - La hoja de cálculos (*Calc* en *LibreOffice* y *Microsoft Excel* en *Microsoft 365*), facilitará la creación de documentos que nos permitirá el uso de fórmulas matemáticas, así como su visualización y modificación.
  - El programa de presentaciones (*Impress* en *LibreOffice* y *Microsoft Power Point* en *Microsoft 365*), facilitará la creación de presentaciones en diapositivas, así como su visualización y modificación.

  El software ofimático puede ejecutarse en diferentes sistemas operativos y está disponible en multitud de idiomas. Para su instalación, básicamente hay que ejecutar el instalador correspondiente al sistema operativo y seguir sus instrucciones.

3.3. Definición de la base de conocimientos

En este apartado definiremos la estructura de la base de conocimientos, que será un depósito centralizado de información donde los técnicos podrán consultar toda la documentación que puedan necesitar para el correcto desarrollo de la actividad, también veremos la forma de implementarla, así como los documentos que tendrá alojados y el método para agregar nuevos documentos, previamente validados.

Respecto a la creación de una base de conocimientos, existen multitud de herramientas disponibles que permiten su construcción, configuración y mantenimiento de una forma simple. Otras opciones que también nos permitirán crear una base de conocimientos, son las bases de datos con su correspondiente procedimiento para mantenerlas, wikis, intranets, etc., pero una de las más básicas y que además cumple perfectamente con su función es un sistema de archivos compartidos.

El sistema de archivos compartidos permite que el personal técnico pueda disponer de la documentación que necesita desde cualquier ubicación, aunque antes es necesario definir la estructura y algunas reglas de compartición y seguridad para normalizar el uso.

3.3.1. Estructura y reglas

Para crear la base de conocimientos nos basaremos en un sistema de archivos compartidos, cuya estructura se detalla a continuación:

- El sistema de archivos partirá de una carpeta raíz, que se creará en una unidad compartida a la que todo el personal técnico tendrá acceso.
- Dentro de la carpeta raíz, deben existir tantas subcarpetas como actividades se realizan en el NOC, “Instrucciones técnicas” para la gestión de incidencias, “Procedimientos” para la ejecución de procedimientos, “Actualizaciones y parcheado” para los procesos de actualización, “Guías de bastionado” para la segurización de los equipos, etc., y cada una de estas subcarpetas debe contener un directorio al que llamaremos “RETIRADO” y que contendrá los documentos obsoletos de dicha actividad, por ejemplo, “RETIRADO IT / PD / AC / HD / ⋯”.
- Los técnicos de segundo y tercer nivel pueden tener carpetas específicas a las que solo se podrá acceder con el correspondiente rol. Estas carpetas son gestionadas por ellos mismos y por lo tanto no hay estructura definida, por ejemplo, “Técnicos nivel 2” y “Técnicos nivel 3” para los técnicos de segundo y tercer nivel respectivamente.
- El coordinador tendrá acceso completo con permisos de lectura y escritura a todo el sistema de archivos y también puede tener una carpeta específica sin estructura definida que gestionará él mismo, por ejemplo, “Coordinación”.

- Otros documentos, como la matriz de contactos, planificación del servicio de guardias, protocolos de actuación, etc., deben colocarse en una carpeta que también debe ser accesible por todo el personal técnico y que debe contener toda la información importante para situaciones de emergencias o cualquier otro documento relevante y que sea de utilidad. A esta capeta le llamaremos “SOS”.

- Por último, los documentos que se alojan en dichas carpetas deberán tener un identificador único del tipo de documento, sistema al que se refiere, nombre descriptivo de lo que contiene, así como una versión que estará compuesta por la fecha y la revisión del documento, por ejemplo, “IT0002-SW00-Desbloquear usuario v20230328_4.2”.

  En la siguiente tabla se muestran algunos posibles identificadores únicos, que servirán para localizar los documentos en el sistema de archivos:

IDENTIFICADOR	DENOMINACIÓN DEL CÓDIGO
ITxxxx	Este código indica que el documento es una instrucción técnica y por lo tanto sirve para resolver incidencias.
PDxxxx	Este código indica que el documento es un procedimiento programado y por lo tanto sirve para realizar dichos procedimientos.
ACxxxx	Este código indica información relativa a la aplicación de actualizaciones en los sistemas.
HDxxxx	Este código indica que el documento es una guía de bastionado (*Hardening*) y por lo tanto sirve para segurizar los sistemas.
...	...

Tabla 7: Identificadores para localización de documentos en la base de conocimientos

En la siguiente tabla se muestran algunos posibles códigos para sistemas, que servirán para localizar el sistema para el que se ha diseñado el documento:

CÓDIGO	DENOMINACIÓN DEL CÓDIGO
SW00	Sistema Windows en general.
SW10	Sistema Windows 10.
SW11	Sistema Windows 11.
WS16	Sistema Windows Server 2016.
WS19	Sistema Windows Server 2019.
LX00	Sistema Linux en general.
LXUB	Sistema Ubuntu.
LXRH	Sistema Red Hat.
CS00	Cualquier sistema.
OS00	Otros sistemas.
...	...

Tabla 8: Códigos de sistemas para localización de documentos en la base de conocimientos

Una vez definida la estructura, pasamos a concretar reglas que evitarán la duplicación, borrado accidental o modificaciones indeseadas, además del procedimiento para la actualización de los documentos que se encuentran alojados en el sistema de archivos y que describiremos a continuación:

- Para los técnicos de primer y segundo nivel el acceso es de *solo lectura*, a excepción de la carpeta "Técnicos nivel 2" a la accederán solo dichos técnicos.
- El tercer nivel tiene permisos de *lectura* y *escritura* en todo el sistema de archivos, a excepción de la carpeta "Coordinación" a la que no podrán acceder.
- Todos los documentos que se encuentran en el sistema de archivos deben estar en PDF, a excepción de las carpetas "Coordinación", "Técnicos nivel 2", "Técnicos nivel 3" y "SOS" que pueden tener otro tipo de archivos.
- Los documentos del sistema de archivos que conforman la base de conocimientos solo pueden ser modificados por el coordinador y personal de tercer nivel, que serán los encargados de mantener el sistema de archivos actualizado. También son los encargados de verificar, aprobar y agregar los nuevos documentos y mover a la carpeta "RETIRADO" los documentos obsoletos.

A continuación, se muestra un esquema del sistema de archivos compartidos al que llamaremos "Base de conocimientos" y las carpetas restringidas a las que solo podrá acceder con los permisos correspondientes:

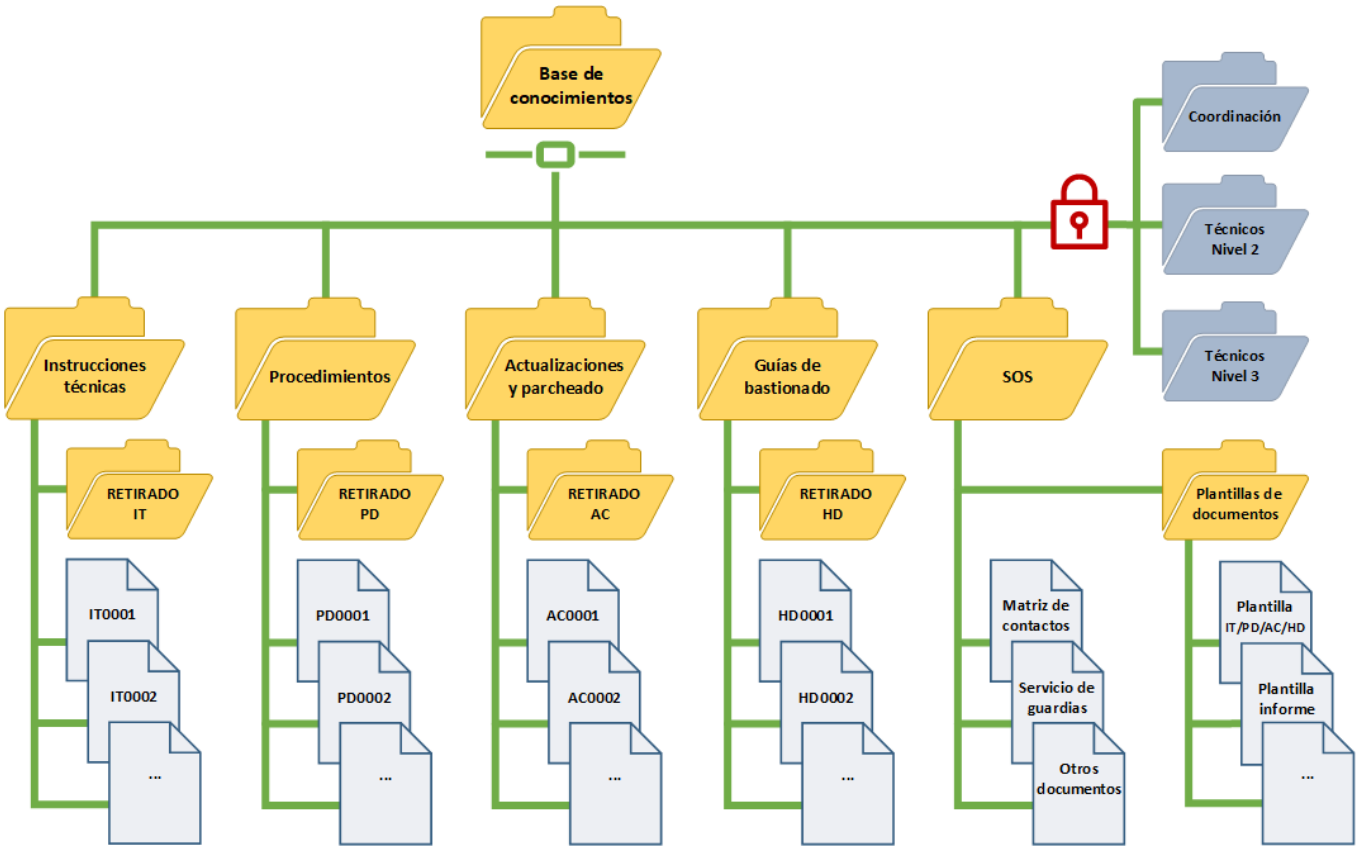


Figura 5: Estructura de la base de conocimientos

3.3.2. Tipos de documentos técnicos

En la base de conocimientos se encuentran distintos tipos de documentos técnicos, como las instrucciones técnicas que ayudan a resolver incidencias, manuales para la ejecución de procedimientos, guías para la aplicación de actualizaciones, guías de bastionado de sistemas, así como cualquier otro documento que pueda ser útil en el desarrollo de las tareas realizadas por el NOC.

Estos documentos deben mostrar un manual sobre la resolución del problema, ejecución de instrucciones, configuración, o cualquier otro tipo de guía adaptada a la tarea a realizar.

Cualquier persona del departamento puede crear un documento, pero siempre deberá ser validado por el coordinador o personal de tercer nivel, que serán los responsables de agregarlo a la base de conocimientos, retirando la versión anterior si la hubiera y colocándola en la carpeta "RETIRADO IT / PD / AC / HD / ⋯".

Cada documento posee una versión, que permite localizarla de forma inequívoca respecto a otras versiones anteriores. La versión posee dos números separados por un punto ***X.Y*** y cada uno de estos números nos indica lo siguiente:

- El primero (X), nos indica si se han producido grandes cambios en el documento que difiere en gran medida con su versión anterior o que ya no se puede ejecutar porque no resuelve el problema.

- El segundo (Y), nos indica si se han producido cambios menores para corregir erratas, modificar opciones que ya no existen u optimizar algunos de los pasos.

Aunque se produzcan cambios en el versionado del documento, el autor original siempre debe aparecer en él, por ejemplo, no se puede modificar una errata que supone un cambio de versión y atribuir la realización completa del documento a la persona que propone el cambio.

En el Anexo II de este documento se puede consultar unas plantillas que facilitan la creación de documentación referente a instrucciones técnicas y procedimientos, así como una descripción de los distintos apartados que deben contener y que nos servirán como base para la creación de nuevos documentos utilizando esta misma estructura.

4. Creación de un piloto de un NOC

En este capítulo crearemos el piloto de un NOC que servirá para poner en práctica lo explicado en los capítulos anteriores, mostrando las distintas instalaciones y configuraciones necesarias, que permitirán el uso de las herramientas para el correcto desarrollo de la actividad, así como unos ejemplos de algunas de sus actividades.

4.1. Requisitos necesarios para la creación del piloto

Equipamiento y software informático

- Hipervisor para la creación de las máquinas virtuales.
- Servidores virtuales para instalar las herramientas necesarias y monitorizarlos.
- Equipos virtuales para monitorizarlos.
- Equipo virtual para el personal técnico con las herramientas necesarias.
- Diferentes versiones de sistemas operativos para ser instalados en los equipos y servidores virtuales.

Herramientas

- Herramienta de monitorización (*Zabbix*).
- Herramienta de ticketing (*GLPI*).
- Herramientas ofimáticas (procesador de textos, hoja de cálculo, lector de PDF o alguna otra aplicación especializada).
- Software de acceso remoto.
- Software de aplicación de actualizaciones de equipos Windows (*WSUS*).

Programación

- Scripts necesarios para generar distintas alertas de forma temporal (alto uso de la CPU, alto uso de la memoria RAM, poco espacio en disco, etc.).

Documentación (Base de conocimientos)

- Matriz de contactos, es una hoja de cálculo con datos importantes sobre responsables de cada tecnología, área, departamento o servicio dentro de la organización.
- Servicio de guardias, es una hoja de cálculo que contiene toda la información relativa al servicio de guardias y como localizar al responsable de la guardia.
- Instrucciones técnicas y procedimientos, son documentos que contienen información útil para la resolución de problemas y ejecución de procedimientos.
- Otro tipo de documentos, guías y manuales (actualización y parcheado de sistemas, guías de bastionado y segurización de equipos, etc.).

4.2. Actividades que se implementarán en el piloto

En la siguiente lista, se puede observar las actividades que serán implementadas o se podrán realizar en nuestro piloto NOC:

- Monitorización de sistemas.
- Gestión y resolución de incidencias.
- Ejecución de procedimientos.
- Creación de informes.
- Ejecución de peticiones de servicio.
- Gestión de perfiles de usuario y acceso.
- Gestión de dispositivos.
- Gestión de actualizaciones y parcheado de equipos Windows.
- Bastionado de equipos (*Hardening*).

Dichas actividades permitirán gestionar los servicios mínimos que todo NOC debería ofrecer. También, se han incluido otras actividades adicionales como la actualización de sistemas Windows y el bastionado de equipos.

4.3. Infraestructura virtual de equipos y servidores

En este apartado se procederá con la creación de nuevos equipos y servidores virtuales, para proceder con la instalación de los sistemas operativos que permitirán el uso de las distintas herramientas que se usarán en el piloto NOC.

4.3.1. Creación de equipos y servidores que contendrán las herramientas

Para la instalación de las herramientas que usaremos en el piloto NOC, es necesario crear algunas máquinas virtuales e instalarles un sistema operativo que dependerá de los requisitos de dicha herramienta.

A continuación, se detalla por cada herramienta, el sistema operativo requerido que permitirá la instalación y configuración de esta, además de un equipo modelo que contendrá todas las aplicaciones que necesitará un técnico del NOC para la realización de las tareas encomendadas:

- **Servidor Windows para la base de conocimientos**

  Un sistema de archivos compartidos formará la base de conocimientos que usará el personal del NOC para el desarrollo de la actividad diaria.

  Para la construcción de la base de conocimientos, crearemos un servidor virtual con sistema operativo Windows Server 2016 que llamaremos “SV-WINSRV-KB” y que nos permitirá implementar un sistema de archivos compartidos. Posteriormente, instalaremos el agente de monitorización y lo agregaremos a la herramienta de monitorización con el nombre “Server KB”.

- **Servidores Linux para las herramientas de monitorización y ticketing**

  Las herramientas de monitorización (Zabbix) y ticketing (GLPI) que utilizaremos para la creación del piloto son de código abierto y se instarán sobre un sistema operativo Ubuntu Server.

  Por lo tanto, crearemos dos servidores virtuales con sistema operativo Ubuntu Server 22.04 LTS, uno para la herramienta de monitorización que llamaremos “SV-UBUSRV-ZBX” y otro para la herramienta de ticketing que llamaremos “SV-UBUSRV-GLPI”. Posteriormente, instalaremos el agente de monitorización y agregaremos ambos servidores a la herramienta de monitorización con los nombres “Server Zabbix” y “Server GLPI” respectivamente.

  En el Anexo III de este documento se puede consultar una guía de instalación del sistema operativo Ubuntu Server 22.04 LTS que contendrá las herramientas mencionadas anteriormente.

- **Servidor Windows para la herramienta de actualización**

  La herramienta de actualización (WSUS) que utilizaremos para la actualización de sistemas Windows, es una característica incluida en Windows Server, por lo que para su instalación usaremos dicho sistema operativo.

  Por lo tanto, crearemos un servidor virtual con sistema operativo Windows Server 2019 que llamaremos “SV-WINSRV-WSUS” y que contendrá la herramienta de actualización. Posteriormente, instalaremos el agente de monitorización y lo agregaremos a la herramienta de monitorización con el nombre “Server WSUS”.

- **Equipo con herramientas para el personal técnico**

  Las herramientas ofimáticas y otro tipo de herramientas que facilitarán la ejecución de tareas al personal técnico se instalarán en un equipo Windows 10, aunque también sería válido un equipo con sistema Linux, p. ej. Ubuntu Desktop.

Por lo tanto, crearemos un equipo virtual con sistema operativo Windows 10 que llamaremos “PC-WIN10” y que contendrá las herramientas necesarias que usará el personal técnico. Posteriormente, instalaremos el agente de monitorización y lo agregaremos a la herramienta de monitorización con el nombre “Desktop 1 Windows 10”.

4.3.2. Creación de equipos para ser monitorizados

Para la configuración y realización de algunos ejemplos referentes a la monitorización de sistemas y generación de alertas, es necesario crear algunos equipos virtuales adicionales, que nos permitirán realizar dichas acciones.

El resto de los equipos que conforman el piloto, también serán monitorizados, aunque no se utilizarán para realizar pruebas de forma activa, ya que ofrecen un servicio que necesitamos para el desarrollo de la actividad.

A continuación, se detallan los equipos virtuales cuyo propósito es poder ejecutar pruebas para generar alertas y así poder ser monitorizados a través de la herramienta de monitorización:

- **Equipos Linux para ser monitorizados**

  Estos equipos se crearán exclusivamente para ser monitorizados y poder generar alertas en la herramienta de monitorización, que nos servirá para verificar que el sistema de monitorización funciona correctamente. Se crearán dos equipos virtuales sobre dos versiones distintas del sistema operativo Ubuntu Desktop.

  Por lo tanto, crearemos dos equipos virtuales. En uno de estos equipos se instalará el sistema operativo Ubuntu Desktop 22.04 LTS que llamaremos “PC-UBUDSK” y en el otro Ubuntu Desktop 22.10 que llamaremos “PC-UBUDSK2”. Posteriormente, instalaremos el agente de monitorización y agregaremos ambos equipos a la herramienta de monitorización con los nombres “Desktop 2 Ubuntu” y “Desktop 3 Ubuntu” respectivamente.

- **Equipo Windows para ser monitorizado**

  En el apartado anterior, ya se ha creado este mismo equipo, por lo que no es necesario realizar ninguna acción de creación.

  Este equipo llamado “PC-WIN10” además de contener las herramientas para el personal técnico, también se utilizará para realizar pruebas referentes a la monitorización y generación de alertas, en este caso de un sistema operativo Windows.

4.3.3. Resumen de equipos y servidores creados

FUNCIÓN	HERRAMIENTA	SISTEMA OPERATIVO	NOMBRE EQUIPO/SERVIDOR	NOMBRE EN ZABBIX
Base de conocimientos	Sistema de archivos compartidos	Windows Server 2016	SV-WINSRV-KB	Server KB
Herramienta de monitorización	*Zabbix*	Ubuntu Server 22.04 LTS	SV-UBUSRV-ZBX	Server Zabbix
Herramienta de ticketing	*GLPI*	Ubuntu Server 22.04 LTS	SV-UBUSRV-GLPI	Server GLPI
Herramienta de actualización	*WSUS*	Windows Server 2019	SV-WINSRV-WSUS	Server WSUS
Herramientas personal técnico	*Office 365*, *Acrobat Reader*, …	Windows 10	PC-WIN10	Desktop 1 Windows 10
Equipo para ser monitorizado	Scripts generación alertas			
Equipo para ser monitorizado	Scripts generación alertas	Ubuntu Desktop 22.04 LTS	PC-UBUDSK	Desktop 2 Ubuntu
Equipo para ser monitorizado	Scripts generación alertas	Ubuntu Desktop 22.10	PC-UBUDSK2	Desktop 3 Ubuntu

Tabla 9: Piloto NOC - Resumen de equipos y servidores virtuales creados

En el Anexo XIII de este documento se pueden ver imágenes de la infraestructura completa de máquinas virtuales, que incluyen los equipos y servidores creados.

4.4. Construcción de la base de conocimientos

En este apartado se procederá con la construcción de la base de conocimientos para la que usaremos un sistema de archivos compartidos, cuya estructura y reglas se detallan en el apartado 3.3.1. Estructura y reglas de este documento.

Comenzamos creando una carpeta raíz en la unidad “C:” del servidor creado para este propósito, al cual hemos llamado “SV-WINSRV-KB”.

La carpeta raíz contendrá toda la base de conocimientos completa, además de otras carpetas con acceso restringido, a las que solo se puede acceder si el usuario tiene el rol con los correspondientes permisos asignados. Las carpetas restringidas “Coordinación”, “Técnicos nivel 2” y “Técnicos nivel 3”, tendrán establecidos unos permisos y una configuración de seguridad más restrictiva que el resto de las carpetas y documentos.

Una vez creada la carpeta raíz, le aplicaremos configuraciones de seguridad y modificaremos algunos permisos específicos, que permitirán la correcta compartición de esta, como un recurso compartido.

Una vez creado el recurso compartido, crearemos la subestructura de carpetas y documentos, completando así la construcción de la base de conocimientos.

A continuación, se muestran los distintos documentos que contendrá la base de conocimientos y el directorio donde localizarlo, así como un esquema final de la estructura completa:

- **Documentos informativos agregados a la base de conocimientos**

  Organigrama y jerarquía del departamento (carpeta "/SOS"): Este documento indica la forma en la que se encuentra estructurado el departamento y ayuda a comprender, cuál es su jerarquía.

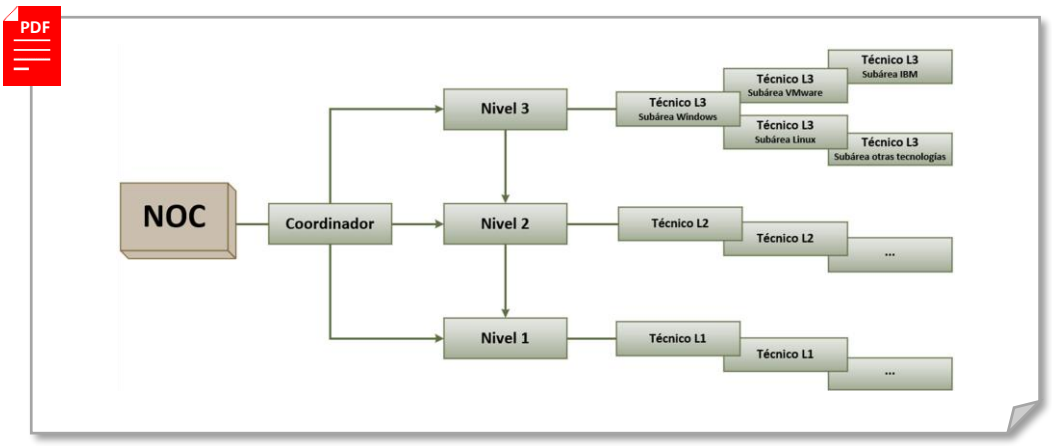
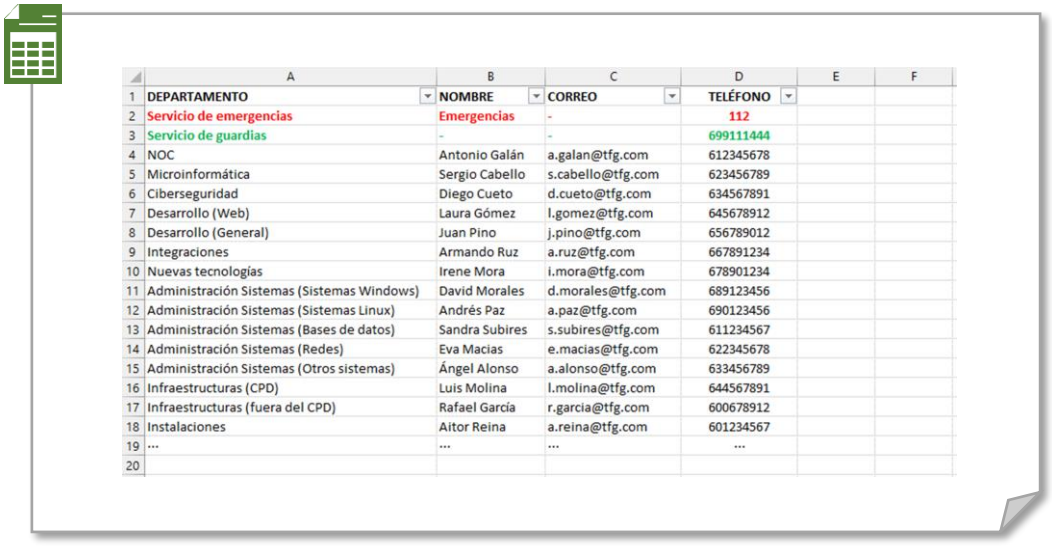


Figura 6: Piloto NOC - Organigrama y jerarquía del departamento

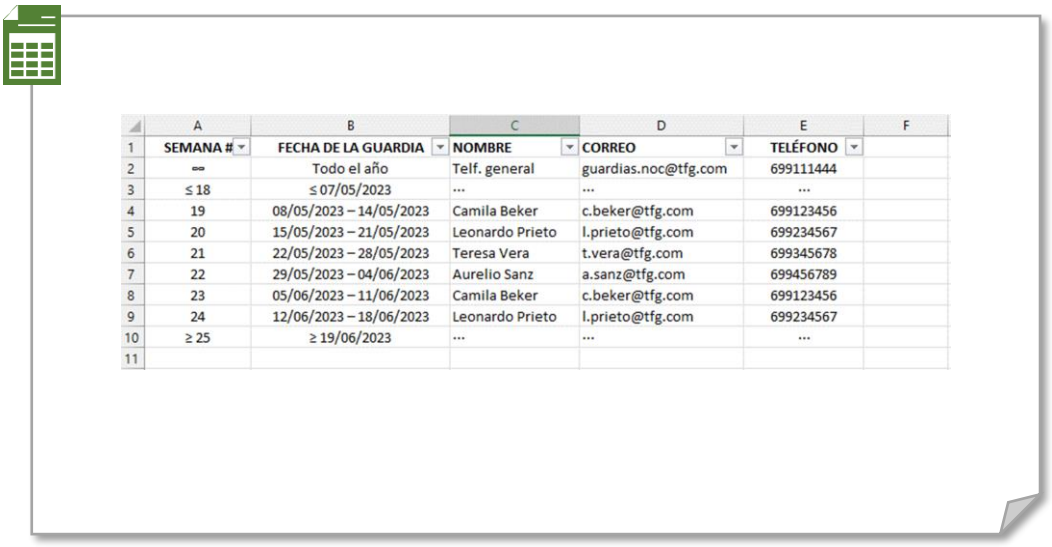
Matriz de contactos (carpeta "/SOS"): Este documento detalla los responsables de cada tecnología, área, departamento o servicio dentro de la organización y su función principal es facilitar el contacto con ellos en caso de desastre.



	A	B	C	D	E	F
1	DEPARTAMENTO	NOMBRE	CORREO	TELÉFONO		
2	Servicio de emergencias	Emergencias	-	112		
3	Servicio de guardias	-	-	699111444		
4	NOC	Antonio Galán	a.galan@tfg.com	612345678		
5	Microinformática	Sergio Cabello	s.cabello@tfg.com	623456789		
6	Ciberseguridad	Diego Cueto	d.cueto@tfg.com	634567891		
7	Desarrollo (Web)	Laura Gómez	l.gomez@tfg.com	645678912		
8	Desarrollo (General)	Juan Pino	j.pino@tfg.com	656789012		
9	Integraciones	Armando Ruz	a.ruz@tfg.com	667891234		
10	Nuevas tecnologías	Irene Mora	i.mora@tfg.com	678901234		
11	Administración Sistemas (Sistemas Windows)	David Morales	d.morales@tfg.com	689123456		
12	Administración Sistemas (Sistemas Linux)	Andrés Paz	a.paz@tfg.com	690123456		
13	Administración Sistemas (Bases de datos)	Sandra Subires	s.subires@tfg.com	611234567		
14	Administración Sistemas (Redes)	Eva Macias	e.macias@tfg.com	622345678		
15	Administración Sistemas (Otros sistemas)	Ángel Alonso	a.alonso@tfg.com	633456789		
16	Infraestructuras (CPD)	Luis Molina	l.molina@tfg.com	644567891		
17	Infraestructuras (fuera del CPD)	Rafael García	r.garcia@tfg.com	600678912		
18	Instalaciones	Aitor Reina	a.reina@tfg.com	601234567		
19	...	...	...	...		
20						

Figura 7: Piloto NOC - Matriz de contactos

Servicio de guardias (carpeta "/SOS"): Este documento contiene la planificación de las guardias para todo el año y ofrece información para contactar con la persona encargada de realizar dicha guardia.



	A	B	C	D	E	F
1	SEMANA #	FECHA DE LA GUARDIA	NOMBRE	CORREO	TELÉFONO	
2	∞	Todo el año	Telf. general	guardias.noc@tfg.com	699111444	
3	≤ 18	≤ 07/05/2023	...	...	...	
4	19	08/05/2023 – 14/05/2023	Camila Beker	c.beker@tfg.com	699123456	
5	20	15/05/2023 – 21/05/2023	Leonardo Prieto	l.prieto@tfg.com	699234567	
6	21	22/05/2023 – 28/05/2023	Teresa Vera	t.vera@tfg.com	699345678	
7	22	29/05/2023 – 04/06/2023	Aurelio Sanz	a.sanz@tfg.com	699456789	
8	23	05/06/2023 – 11/06/2023	Camila Beker	c.beker@tfg.com	699123456	
9	24	12/06/2023 – 18/06/2023	Leonardo Prieto	l.prieto@tfg.com	699234567	
10	≥ 25	≥ 19/06/2023	...	...	...	
11						

Figura 8: Piloto NOC - Servicio de guardias

Proceso de creación de informes (carpeta "/SOS"): Este documento es una guía donde se detalla el proceso de creación de informes y las normas establecidas.

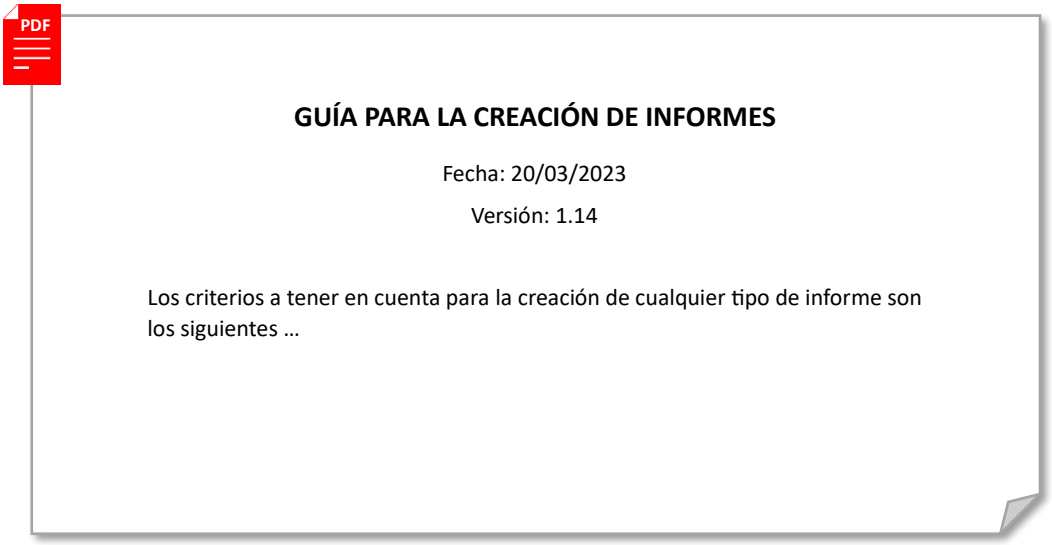
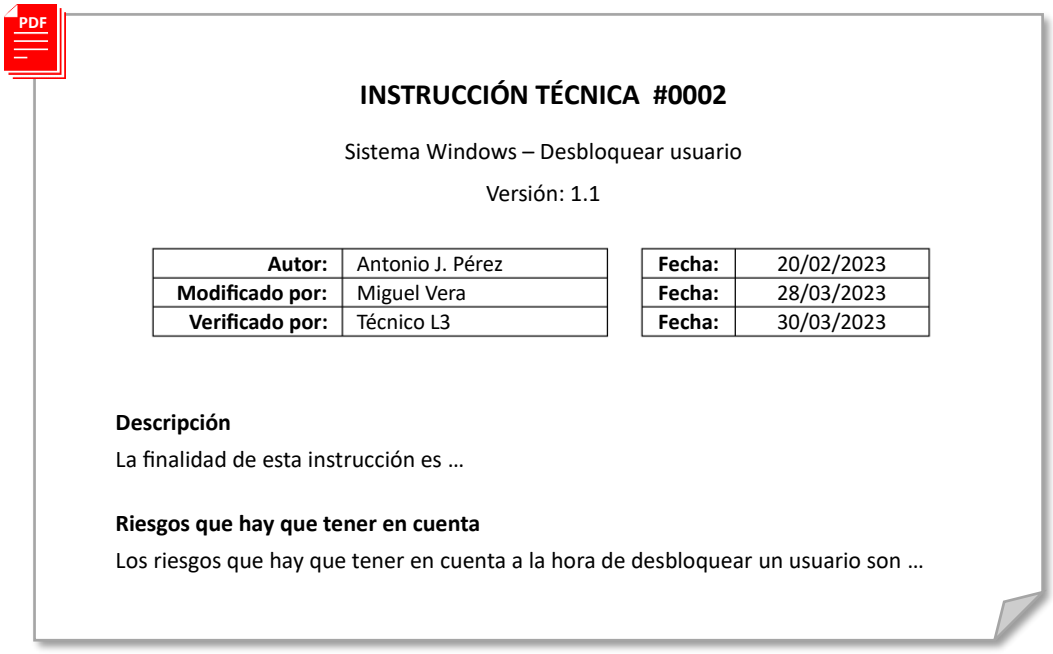


Figura 9: Piloto NOC - Proceso de creación de informes

Plantillas para la creación de documentos normalizados (carpeta "/SOS/Plantillas de documentos"): Esta carpeta contendrá todas las plantillas de los documentos más usuales que se utilizarán en el departamento. Las plantillas permitirán la creación de distintos tipos de documentos como instrucciones técnicas o procedimientos (ver Anexo II).

- **Documentos técnicos agregados a la base de conocimientos**

  Instrucciones técnicas (carpeta "/Instrucciones técnicas"): Estos documentos son unas guías que detallan las tareas a realizar para resolver un problema concreto. En la siguiente imagen, se muestra un fragmento de una instrucción técnica:



INSTRUCCIÓN TÉCNICA #0002

Sistema Windows – Desbloquear usuario

Versión: 1.1

Autor:	Antonio J. Pérez	**Fecha:**	20/02/2023
Modificado por:	Miguel Vera	**Fecha:**	28/03/2023
Verificado por:	Técnico L3	**Fecha:**	30/03/2023

Descripción

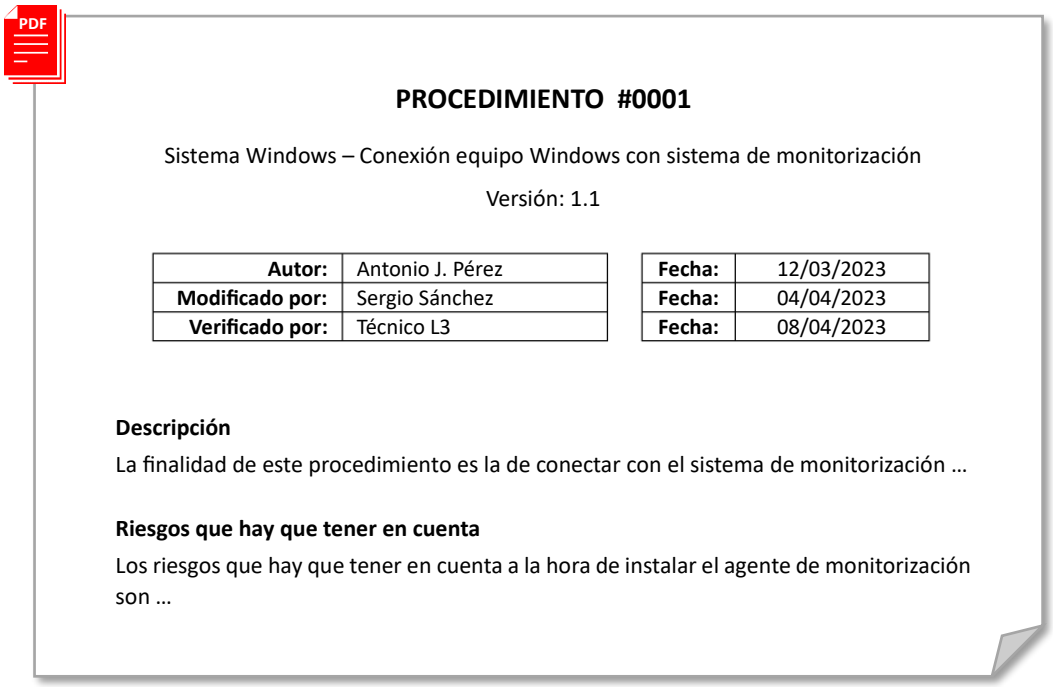
La finalidad de esta instrucción es …

Riesgos que hay que tener en cuenta

Los riesgos que hay que tener en cuenta a la hora de desbloquear un usuario son …

Figura 10: Piloto NOC - Fragmento instrucción técnica IT0002

Procedimientos programados (carpeta "/Procedimientos"): Estos documentos son unas guías que detallan las tareas a realizar para la ejecución de un procedimiento programado. En la siguiente imagen, se muestra un fragmento de una guía para la ejecución de un procedimiento:



PROCEDIMIENTO #0001

Sistema Windows – Conexión equipo Windows con sistema de monitorización

Versión: 1.1

Autor:	Antonio J. Pérez	**Fecha:**	12/03/2023
Modificado por:	Sergio Sánchez	**Fecha:**	04/04/2023
Verificado por:	Técnico L3	**Fecha:**	08/04/2023

Descripción

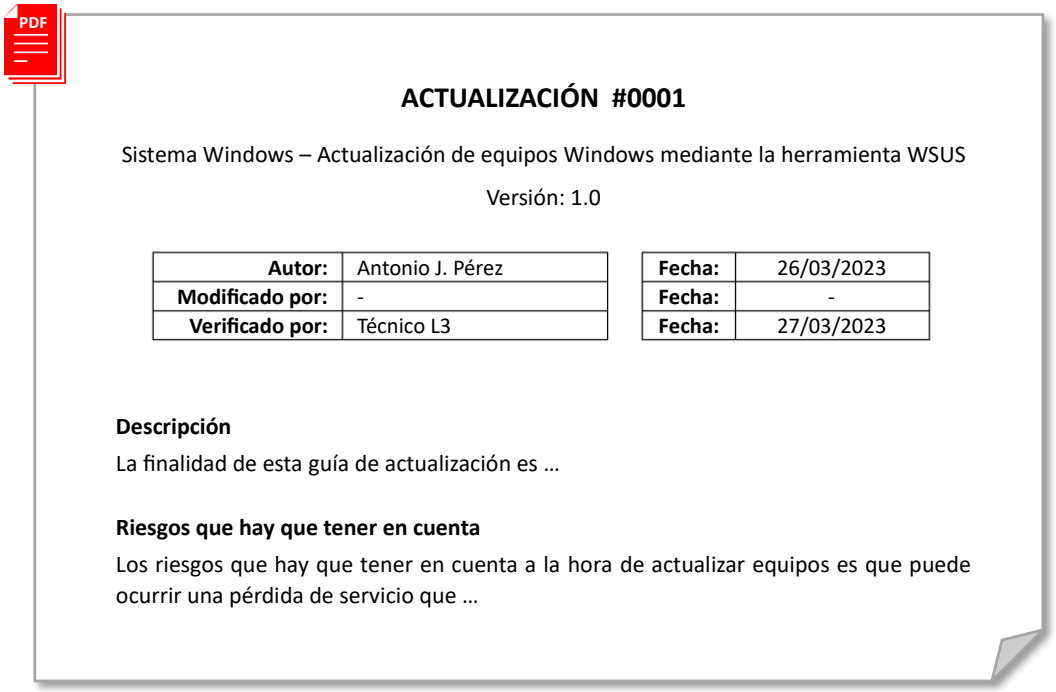
La finalidad de este procedimiento es la de conectar con el sistema de monitorización …

Riesgos que hay que tener en cuenta

Los riesgos que hay que tener en cuenta a la hora de instalar el agente de monitorización son …

Figura 11: Piloto NOC - Fragmento procedimiento PD0001

Guías de actualizaciones de sistemas (carpeta "/Actualizaciones y parcheado"): Estos documentos son unas guías que detallan las tareas a realizar para la actualización de algún sistema. En la siguiente imagen, se muestra un fragmento de una guía de actualización:



ACTUALIZACIÓN #0001

Sistema Windows – Actualización de equipos Windows mediante la herramienta WSUS

Versión: 1.0

Autor:	Antonio J. Pérez	**Fecha:**	26/03/2023
Modificado por:	-	**Fecha:**	-
Verificado por:	Técnico L3	**Fecha:**	27/03/2023

Descripción

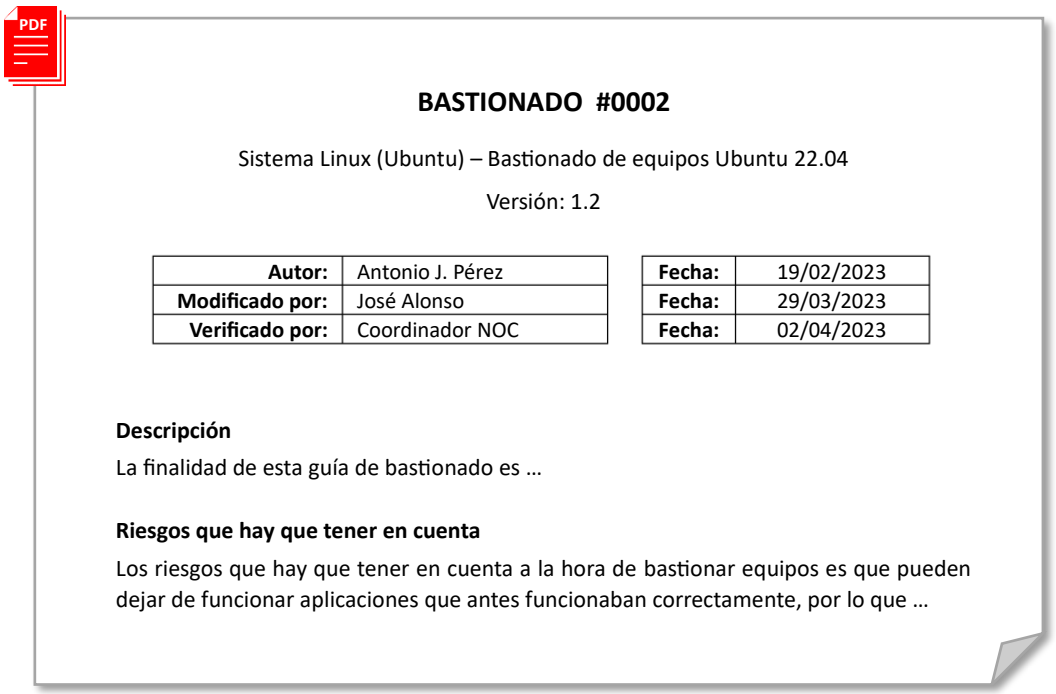
La finalidad de esta guía de actualización es …

Riesgos que hay que tener en cuenta

Los riesgos que hay que tener en cuenta a la hora de actualizar equipos es que puede ocurrir una pérdida de servicio que …

Figura 12: Piloto NOC - Fragmento guía de actualización AC0001

Guías de bastionado de equipos (carpeta "/Guías de bastionado"): Estos documentos son unas guías que detallan las tareas a realizar para el bastionado de un sistema. En la siguiente imagen, se muestra un fragmento de una guía de bastionado:



BASTIONADO #0002

Sistema Linux (Ubuntu) – Bastionado de equipos Ubuntu 22.04

Versión: 1.2

Autor:	Antonio J. Pérez	**Fecha:**	19/02/2023
Modificado por:	José Alonso	**Fecha:**	29/03/2023
Verificado por:	Coordinador NOC	**Fecha:**	02/04/2023

Descripción

La finalidad de esta guía de bastionado es …

Riesgos que hay que tener en cuenta

Los riesgos que hay que tener en cuenta a la hora de bastionar equipos es que pueden dejar de funcionar aplicaciones que antes funcionaban correctamente, por lo que …

Figura 13: Piloto NOC - Fragmento guía de bastionado HD0002

- **Diagrama completo del sistema de archivos que compone la base de conocimientos**

  A continuación, se mostrará una imagen donde se puede observar el sistema de archivos completo que conformará la base de conocimientos del piloto NOC:

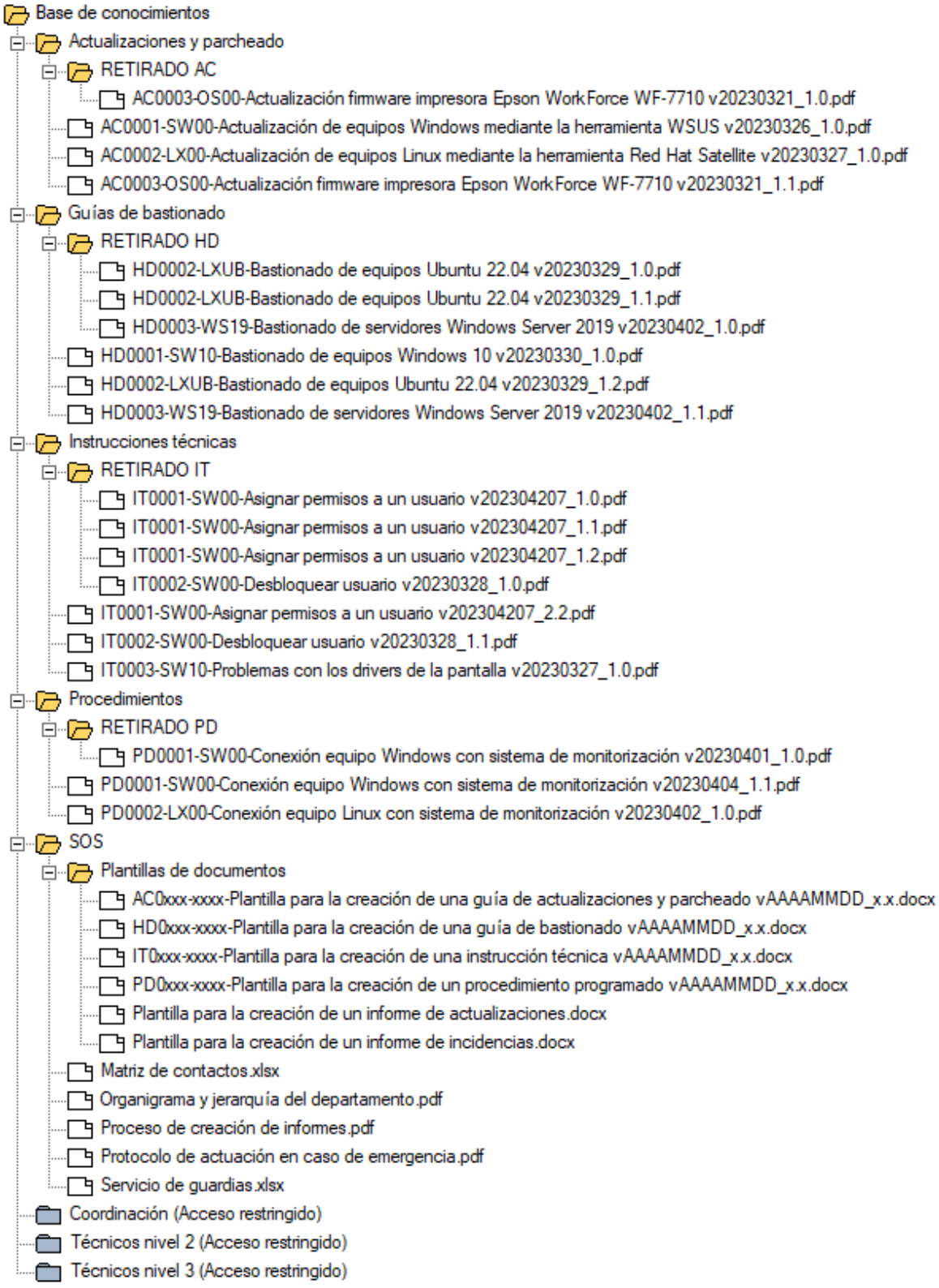


Figura 14: Piloto NOC - Sistema de archivos completo de la base de conocimientos

4.5. Montaje del sistema de monitorización

En este apartado se procederá con el montaje del sistema de monitorización, que nos permitirá conocer el estado de los sistemas, así como los posibles problemas que puedan surgir mediante la generación de alertas.

La herramienta que usaremos para la monitorización es Zabbix. Esta herramienta nos permitirá obtener datos del estado de los sistemas mediante su monitorización a través de un agente y generará alertas cuando alguno de los parámetros no cumpla los requisitos definidos.

4.5.1. Instalación de la herramienta de monitorización

La instalación de la herramienta de monitorización Zabbix, se realizará en un sistema Ubuntu Server y los datos proporcionados por esta aplicación serán accesibles en cada uno de los equipos del personal técnico.

En un NOC la información proporcionada por Zabbix también puede ser expuesta en grandes pantallas para que todo el personal del departamento pueda observarlos fácilmente.

El acceso a Zabbix se realiza mediante una URL y autenticación, siendo necesario disponer de un usuario autorizado.

En el Anexo IV de este documento se puede consultar la guía de instalación del software de monitorización Zabbix que se instalará en el servidor “SV-UBUSRV-ZBX” creado para este propósito, sobre un sistema operativo Ubuntu Server 22.04 LTS.

4.5.2. Configuración de la herramienta de monitorización

Una vez instalada la herramienta Zabbix y accediendo con un usuario administrador, pasamos a la configuración, que nos permitirá su uso de forma adecuada.

En el Anexo V de este documento se puede consultar la guía que nos permitirá la correcta configuración y adaptación del software de monitorización a nuestro sistema piloto.

4.5.3. Instalación y configuración del agente de monitorización

El agente de monitorización o en este caso el agente de Zabbix es el encargado de recopilar en intervalos regulares o programados, todos los datos del equipo donde se encuentra instalado. Posteriormente, estos datos serán analizados y se generará la alerta correspondiente en caso de que sea necesaria.

A continuación, se muestra el procedimiento de instalación del agente Zabbix, que está disponible para múltiples plataformas, siendo las más usuales Linux y Windows:

- **Instalación de agente Zabbix para monitorización en un sistema Linux.**

  El piloto de NOC que crearemos contendrá varios sistemas Ubuntu distintos (Ubuntu Server 22.04 LTS, Ubuntu Desktop 22.04 LTS y Ubuntu Desktop 22.10), los cuales serán monitorizados mediante la herramienta de monitorización.

  En el Anexo VI de este documento se puede consultar una guía de instalación del agente de Zabbix en un sistema operativo Ubuntu, realizado mediante línea de comandos.

- **Instalación de agente Zabbix para monitorización en un sistema Windows.**

  El piloto de NOC que crearemos contendrá varios sistemas Windows (Windows Server 2016, Windows Server 2019 y Windows 10), los cuales serán monitorizados mediante la herramienta de monitorización.

  Para la instalación del agente en los sistemas mencionados anteriormente, usaremos un paquete de instalación desde MSI que podremos obtener desde la web oficial de Zabbix[9] y que podrá ser instalado en ambos sistemas.

  En el Anexo VII de este documento se puede consultar una guía de instalación del agente de Zabbix en un sistema operativo Windows.

4.5.4. Scripts para la generación de alertas

Los scripts para la generación de alertas se pueden considerar como una herramienta más, encargada de sobrecargar los diversos componentes del sistema donde se ejecuta, para así poder generar alertas que nos ayudarán a configurar mejor herramienta de monitorización, pero no solo eso, sino que también nos servirá para comprobar comportamientos anómalos en sistemas ya monitorizados que, por algún motivo, no proporcionan datos de forma correcta.

En el Anexo VIII de este documento se crean dos scripts, los cuales utilizaremos para sobrecargar algunos de los componentes de los equipos que se han creado con el propósito de ser monitorizados, para así poder generar la alerta correspondiente y en el Anexo XIV. Ejemplo se puede ver un caso práctico de ejecución de ambos scripts.

4.6. Montaje de la herramienta de ticketing

En este apartado se procederá con el montaje del sistema de ticketing, que nos permitirá realizar una gestión eficiente de las distintas tareas que se realizan dentro del NOC.

La herramienta que usaremos para la gestión de tickets es GLPI (Gestionnaire Libre de Parc Informatique) o gestión de servicios de tecnología de la información en español. Esta herramienta nos permitirá crear y gestionar tickets con información sobre las tareas finalizadas o pendientes, así como la consulta de datos para la realización de informes o algún otro procedimiento.

4.6.1. Instalación de la herramienta de ticketing

La instalación de la herramienta de ticketing GLPI, se realizará en un sistema Ubuntu Server y nos proporcionará multitud de funciones de las que inicialmente solo usaremos la función de asistencia o soporte, la cual nos ayudará a gestionar las actividades que se realizan en el NOC, como la gestión de incidencias o la ejecución de procedimientos, entre otras.

El acceso a Zabbix se realiza mediante una URL y autenticación, siendo necesario disponer de un usuario con un perfil asignado que, dependiendo del tipo de este perfil, tendrá más o menos privilegios dentro de la herramienta.

En el Anexo IX de este documento se puede consultar la guía de instalación del software GLPI que se instalará en el servidor “SV-UBUSRV-GLPI” creado para este propósito, sobre un sistema operativo Ubuntu Server 22.04 LTS.

4.6.2. Configuración de la herramienta de ticketing

Una vez instalada la herramienta GLPI y accediendo con un usuario administrador, pasamos a la configuración, que nos permitirá su uso de forma adecuada.

En el Anexo X de este documento se puede consultar la guía que nos permitirá la correcta configuración y adaptación del software de ticketing a nuestro sistema piloto.

4.7. Montaje de la herramienta de actualización

En este apartado se procederá con el montaje de la herramienta de actualización, que nos permitirá tener actualizados todos los sistemas Windows de la organización.

La herramienta que usaremos para actualizar los sistemas Windows es WSUS (Windows Server Update Services). Esta herramienta permitirá gestionar la actualizaciones de los diferentes sistemas, evitando saturar la red con la descarga por los distintos equipos de la organización de forma individualizada.

WSUS es una función incluida en el sistema operativo Windows Server, por lo que necesita una licencia válida para ser utilizado.

4.7.1. Instalación de la herramienta de actualización

La instalación de la herramienta de actualización WSUS, se realizará en un sistema Windows Server, esta nos proporcionará una gestión centralizada para aplicar actualizaciones de seguridad previamente descargadas en su repositorio, a todos los equipos Windows de la organización, así como a otro tipo de productos desarrollados por Microsoft.

El acceso a WSUS se realiza mediante una consola que se encuentra en el servidor donde está instalada la herramienta, o de forma remota en cualquier sistema Windows, al que necesitaremos instalar las herramientas de administración remota de servidores o RSAT (Remote Server Administration Tools).

En el Anexo XI de este documento se puede consultar la guía de instalación de la herramienta WSUS que se instalará en el servidor “SV-WINSRV-WSUS” creado para este propósito, sobre un sistema operativo Windows Server 2019.

4.7.2. Configuración de la herramienta de actualización

Una vez instalada la herramienta WSUS, pasaremos a realizar una serie de configuraciones que nos permitirá su uso de forma adecuada.

En el Anexo XII de este documento se puede consultar la guía que nos permitirá la correcta configuración y adaptación de la herramienta de actualización a nuestro sistema piloto.

4.8. Preparación del equipo para el personal técnico

En este apartado realizaremos la preparación de un equipo, que contendrá todas las herramientas que el personal técnico necesitará para el correcto desempeño de las actividades implementadas en el piloto NOC.

Las herramientas se instalarán en el equipo "PC-WIN10" creado para este propósito, sobre un sistema Windows 10.

Aunque el equipo técnico se implementará sobre un sistema operativo Windows 10, también puede realizarse desde cualquier otro sistema operativo siempre que ofrezca la posibilidad de ejecución de las herramientas necesarias.

A continuación, listamos algunas de las herramientas que se instalarán en el equipo técnico:

- **Software ofimático y lector de PDF**

  Estas aplicaciones hacen posible la gestión de los documentos necesarios para poder desarrollar la actividad, además de permitir la creación de otros documentos nuevos, así como la generación de informes.

  Instalaremos *Microsoft 365,* que nos proporcionará aplicaciones como *Microsoft Word, Microsoft Excel,* entre otras y nos ayudará con creación de nuevos documentos y modificación de documentos ya existentes. Para la lectura de PDF instalaremos *Acrobat Reader*.

Figura 15: Piloto NOC - Iconos de las aplicaciones Microsoft Word, Excel y Acrobat Reader

- **Navegador web**

  El navegador web permitirá el acceso a páginas web para buscar información o realizar configuraciones, además de poder ejecutar aplicaciones cuya interfaz solamente es accesible a través de un navegador.

  Instalaremos *Google Chrome*, aunque cualquier navegador actual es igualmente válido.

Figura 16: Piloto NOC - Icono del navegador web Google Chrome

- **Correo electrónico**

  El gestor de correo electrónico permitirá administrar los buzones de incidencias, solicitudes y servicios, así como el correo del propio técnico, que poseerá una dirección de correo electrónico corporativa.

  La suite ofimática ya instalada *Microsoft 365,* nos proporcionará un gestor de correo electrónico llamado *Microsoft Outlook*, compatible con multitud de plataformas de correo, aunque hay otros gestores que ofrecen la misma funcionalidad.

Outlook

Figura 17: Piloto NOC - Icono del gestor de correo electrónico

- **Software de acceso remoto**

  Dado que la actividad del NOC se realiza desde un lugar centralizado, es necesario que el técnico pueda realizar intervenciones de forma remota para poder ejecutar instrucciones técnicas, procedimientos, bastionado de equipos, entre otras cosas.

  Mientras que en equipos Linux la forma más habitual para realizar operaciones en las máquinas es a través de *SSH*, en equipos Windows se usa la herramienta de *Escritorio Remoto* incluida en el propio sistema operativo.

Conexión a
Escritorio remoto

Figura 18: Piloto NOC - Icono de la herramienta de Conexión a Escritorio remoto

- **Acceso a la base de conocimientos**

  La base de conocimientos es un sistema de archivos compartidos que tendremos que mapear en el equipo técnico y nos proporcionará un depósito centralizado de información necesaria para la realización de las actividades del NOC.

Mapearemos en una unidad de red, la carpeta compartida donde se aloja la base de conocimientos "\\192.168.0.191\Base de conocimientos" y crearemos un acceso directo en el escritorio para facilitar su localización.

Base de conocimientos

Figura 19: Piloto NOC - Icono acceso a la Base de conocimientos

- **Acceso a la consola de aplicación de actualizaciones (WSUS)**

  El acceso a la consola de WSUS en el equipo, facilitará enormemente al técnico la gestión de actualizaciones, ya que le evitará tener que conectarse de forma frecuente al servidor que ofrece el servicio y donde se encuentra la consola principal.

  Para ejecutar la consola de WSUS desde cualquier equipo de forma remota, debemos instalar las herramientas de administración remota de servidores RSAT.

Windows Server Update Services

Figura 20: Piloto NOC - Icono acceso a WSUS

- **Acceso a través del navegador web al software de monitorización (Zabbix) y ticketing (GLPI)**

  El acceso tanto al software de monitorización, como al software de gestión de tickets se realizan a través de un navegador web mediante una URL.

  La URL "http://192.168.0.180/zabbix" nos permite el acceso al software de monitorización Zabbix y la URL "http://192.168.0.190" al software de gestión de tickets GLPI.

Además de las herramientas mencionadas, también se puede instalar cualquier otra herramienta de utilidad que facilite el trabajo al técnico o que debido a el desarrollo de una actividad distinta a la que se realiza en este piloto NOC lo requiera.

4.9. Algunos ejemplos de ejecución de actividades del NOC

En este apartado se mostrarán algunos ejemplos de monitorización y ejecución de actividades que nos ayudarán a comprender el funcionamiento y el trabajo que se realiza en un NOC, así como el uso de las herramientas configuradas en apartados anteriores.

A continuación, se muestran varios ejemplos de monitorización de sistemas, gestión de incidencias, ejecución de procedimientos y aplicación de actualizaciones:

- **Ejemplo de monitorización de sistemas e inconvenientes que pueden surgir**

  La monitorización de sistemas es una tarea muy importante en un NOC, ya que nos proporcionará información del estado de los equipos de forma rápida y fiable, sin tener que desplazarnos, ni solicitar autorizaciones para acceder a los sistemas.

  En el Anexo XIV de este documento se puede consultar un ejemplo de monitorización de varios sistemas, además de los principales inconvenientes que pueden surgir al realizar la monitorización.

- **Ejemplos de resolución de incidencias e inconvenientes que pueden surgir**

  La resolución de incidencias es una de las principales tareas realizadas dentro de un NOC y las que más porcentaje de dedicación requiere.

  En el Anexo XV de este documento se pueden consultar dos ejemplos de resolución de incidencias producidas de diferente forma, además de los principales inconvenientes que pueden surgir al resolver los tickets relativos a incidencias.

- **Ejemplo de ejecución de procedimientos e inconvenientes que pueden surgir**

  La ejecución de procedimientos es otra de las principales tareas realizadas dentro de un NOC junto a la resolución de incidencias.

  En el Anexo XVI de este documento se puede consultar un ejemplo de ejecución de un procedimiento programado, además de los principales inconvenientes que pueden surgir al resolver los tickets relativos a procedimientos.

- **Ejemplo de aplicación de actualizaciones e inconvenientes que pueden surgir**

  La aplicación de actualizaciones de forma periódica es uno de los muchos servicios que puede ofrecer un NOC como parte de sus actividades, además de proporcionar a la organización un entorno más seguro y menos vulnerable.

  En el Anexo XVII de este documento se puede consultar un ejemplo de aplicación de actualizaciones a sistemas Windows mediante la herramienta WSUS, además de los principales inconvenientes que pueden surgir al aplicar actualizaciones.

5. Conclusiones

A lo largo de este trabajo se ha definido el concepto de NOC, así como sus principales características, estudiando las distintas actividades que pueden realizarse y las herramientas necesarias para poder desarrollarlas. También se ha definido su jerarquía y estructura interna, la documentación necesaria para poder desarrollar las distintas tareas, la documentación que puede ser generada como son los informes o documentos técnicos, así como el funcionamiento general de este departamento.

Todo lo anterior, nos capacita para poder entender y analizar los requisitos que necesita una organización y así poder ofrecer soluciones que se adapten al modo de trabajo de esta, partiendo de un NOC con unas actividades básicas y adaptándolo a las necesidades de dicha organización, que finalmente se ha representado con la creación de un piloto NOC en un entorno virtualizado.

Por lo que, con la realización de este trabajo se ha aprendido a buscar información sobre un tema concreto, para posteriormente interpretarla y definir cada una de las partes necesarias para poder llevarlo a cabo. Una vez definidas cada una de las partes o características del NOC, hemos aprendido a analizar los requisitos básicos que este debe cubrir, lo que nos ha permitido seleccionar la mejor configuración de equipos y software para la implantación de un NOC en un entorno virtual, permitiendo lograr todos los objetivos planteados al inicio de este trabajo.

El desarrollo de este trabajo ha transcurrido conforme a la plantificación realizada inicialmente, aunque con algunas modificaciones mínimas en la realización de algunos ejemplos que se han adaptado para realizarlos durante el proceso de configuración de los sistemas y herramientas del piloto, rectificando la planificación inicial en consecuencia. La metodología utilizada ha sido la adecuada y no se han introducido grandes cambios, a excepción de algunas partes que ayudan con la comprensión de este trabajo y que no estaban planificadas al inicio porque se consideraban triviales.

Para finalizar, las líneas futuras del trabajo que quedan pendientes se enfocan principalmente en el potencial y la versatilidad que tiene un NOC, pues como se ha comentado en capítulos anteriores, el NOC puede desarrollar muchas más actividades de las que se han comentado en este trabajo, siempre que se adapten a la metodología del departamento y proporcionen un valor añadido a la organización.

Otra mejora que puede ser interesante es la integración del NOC con un SOC (Security Operations Center) o Centro de Operaciones de Seguridad en español, que es un centro o departamento responsable de garantizar la seguridad de la información.

Glosario

Administrador de sistemas: Administrador de las tecnologías de la información o persona encargada del correcto funcionamiento de los sistemas informáticos de una organización.

Administrador de TI: Véase administrador de sistemas.

Alerta: Mensaje que muestra información sobre algún parámetro que no cumple con las reglas definidas, mostrando los datos del sistema que proporciona dicho parámetro.

Alta disponibilidad: Se intenta lograr la máxima disponibilidad de un sistema, mediante la redundancia de este.

Bash: Intérprete de comandos que corre bajo el Shell de Unix.

Bastionado: También denominado endurecimiento, es un proceso de segurización de un sistema, encargado de reducir los agujeros de seguridad o vulnerabilidades.
en.: *Hardening*

CCR (Centro de Control de RED): Véase NOC.

Centralita telefónica: Dispositivo que gestiona y permite las conexiones telefónicas dentro y fuera de la organización.

Ciberseguridad: Área que se enfoca en la protección de la infraestructura informática de la organización.

Copia de seguridad: Método que realiza una copia idéntica de la información y que permitirá una restauración de los datos en caso de que estos se pierdan o se dañen.
en.: *Backup*

Cortafuegos: Sistema de seguridad que gestiona el control de acceso a la red.
en.: *Firewall*

Diagrama de Gantt: Herramienta gráfica cuyo objetivo es mostrar el tiempo de dedicación previsto para diferentes actividades a lo largo del tiempo.

Directorio activo: Conjunto de servicios que gestionan los recursos de una red.

Disparador: Configuración que se ejecuta cuando no se respetan los umbrales programados.
en.: *Trigger*

Equipo virtual: Equipo ejecutado sobre una máquina virtual utilizando recursos de un servidor físico proporcionados y gestionados por un hipervisor.

GPO (Group Policy Object): Grupo de políticas ejecutadas de forma masiva en uno o varios equipos.

Hipervisor: Software que permite realizar una virtualización del hardware para la creación y gestión de máquinas virtuales. Véase también máquina virtual.

Host: Se refiere a un equipo o servidor.

Imagen ISO: Archivo informático donde se almacena una copia de un sistema de archivos.

IoT (Internet of Things): Internet de las cosas, se refiere a una red de dispositivos interconectados y un software que los gestiona.

IP: Significa protocolo de internet y es una dirección única que sirve para identificar un dispositivo en una red de ordenadores.

Mapear: Asignar unidad de red a una carpeta compartida.

Máquina virtual: Es una réplica de un equipo o servidor físico pero definido por software.

NOC (Network Operations Center): Centro o departamento especializado en tareas de administración de sistemas.

Ofimática: Conjunto de herramientas que permiten desarrollar tareas de oficina, como procesamiento de textos, lectura de documentos, etc.

Parche: Cambios que se aplican a un sistema para corregir errores.

Perfil: Colección de permisos y configuraciones que permitirán a un usuario realizar determinadas acciones en el sistema.

Piloto de un NOC: Implementación completa de un NOC en un entorno simulado, que permite la ejecución de las tareas principales desarrolladas en un NOC, adaptadas al entorno para el que se ha creado. Véase también NOC.

Plan de contingencia: Contiene las medidas necesarias para garantizar la continuidad del servicio.

Políticas: Conjunto de reglas que permiten la configuración del sistema operativo.

Powershell: Intérprete de comandos con posibilidad de ejecuta script y que se ejecuta en sistemas Windows.

Recuperación de desastres: Método que permite la restauración de un sistema que ha quedado inutilizado tras ocurrirle algún tipo de percance.

Repositorio: Espacio donde se almacenan los ficheros usados por una aplicación.

Rol: Véase perfil.

RSAT (Remote Server Administration Tools): Conjunto de herramientas que permite la ejecución de la herramienta WSUS desde un equipo remoto.

SAI (Sistema de alimentación ininterrumpida): Componente que estabiliza y suministra energía por unos minutos en el caso que la red principal deje de proporcionarla.

Script: Es un programa que permite la personalización o automatización de instalaciones en un sistema existente.

Segurización: Consiste en reducir las vulnerabilidades de un sistema para conseguir que el sistema sea seguro. Véase también bastionado.

Servidor virtual: Servidor ejecutado sobre una máquina virtual utilizando recursos de un servidor físico proporcionados y gestionados por un hipervisor.

SSH (Secure Shell): Protocolo que permite el acceso remoto a un sistema a través de un canal seguro.

Ticket: Entrada que se genera al momento de proceder con algún tipo de incidencia o solicitud y que documenta todo el proceso hasta su resolución.

Ventana de tiempo: Periodo de tiempo que se reserva para realizar una o varias acciones.

Virtualización: Tecnología que permite imitar el hardware físico para poder crear un sistema informático virtual.

VoIP: Tecnología que permite la transmisión de voz a través de la red a través del protocolo IP.

VPN (Virtual Private Network): Una red privada virtual, permite la creación de una conexión punto a punto entre dos dispositivos a través de internet.

WSUS (Windows Server Update Services): Sistema centralizado que permite la distribución de actualizaciones o parches a sistemas Windows. Véase también parche.

Bibliografía

[1] Instalación GLPI en Ubuntu Server. https://canaltic.pe/2022/10/16/instalacion-glpi-10-0-1-en-ubuntu-server-22-04/ [fecha de consulta: 24/03/2023].

[2] Web oficial de GLPI. https://glpi-project.org/es/ [fecha de consulta: 24/03/2023].

[3] Instalación y configuración de WSUS: https://thesolving.com/es/sala-de-servidores/como-instalar-y-configurar-windows-server-update-services-wsus/ [fecha de consulta: 28/03/2023].

[4] Instalación Zabbix 6.0 en Ubuntu Server. https://bestmonitoringtools.com/how-to-install-zabbix-server-on-ubuntu/ [fecha de consulta: 31/03/2023].

[5] Web oficial de Zabbix. https://www.zabbix.com/ [fecha de consulta: 31/03/2023].

[6] Manual de Zabbix. https://www.zabbix.com/documentation/6.0/es/manual [fecha de consulta: 31/03/2023].

[7] Instalación y configuración del agente de Zabbix en un equipo con Linux. https://help.clouding.io/hc/es/articles/4428725128732-Instalar-y-configurar-Agente-Zabbix-en-Ubuntu-20-04-18-04 [fecha de consulta: 31/03/2023].

[8] Instalación del agente de Zabbix en equipos Windows con paquetes MSI y Linux. https://tutorialesit.com/instalacion-agente-windows-linux-zabbix/ [fecha de consulta: 01/04/2023].

[9] Descarga agente Zabbix MSI Windows. https://www.zabbix.com/download_agents [fecha de consulta: 01/04/2023].

[10] Generar carga de trabajo en CPU y memoria RAM en sistemas Windows. https://www.wellarchitectedlabs.com/performance-efficiency/100_labs/100_monitoring_windows_ec2_cloudwatch/5_generating_load/ [fecha de consulta: 01/04/2023].

[11] Crear menú en Powershell. https://www.jesusninoc.com/03/17/ejercicios-de-powershell-crear-un-menu/ [fecha de consulta: 01/04/2023].

[12] Generar carga de trabajo en CPU y memoria RAM en sistema Linux. https://askubuntu.com/questions/948854/how-do-i-stress-test-cpu-and-ram-at-the-same-time [fecha de consulta: 01/04/2023].

[13] Crear menú en Bash. https://www.baeldung.com/linux/shell-script-simple-select-menu [fecha de consulta: 01/04/2023].

[14] Definición de un NOC. https://www.ciospain.es/movilidad/que-es-un-centro-de-operaciones-de-red-noc [fecha de consulta: 06/04/2023].

[15] Definición y objetivo de un NOC. https://www.manageengine.com/latam/network-monitoring/monitoreo-centro-operaciones-de-red-noc.html [fecha de consulta: 06/04/2023].

[16] Definición, funcionamiento y beneficios de un NOC. https://www-techtarget-com.translate.goog/searchnetworking/definition/network-operations-center?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es [fecha de consulta: 06/04/2023].

[17] Definición de NOC. https://www.internationalit.com/post/centro-de-operaciones-de-red-como-funcionan-los-noc?lang=es [fecha de consulta: 06/04/2023].

[18] Definición de NOC. https://www.stackscale.com/es/blog/noc-centro-operaciones-red/ [fecha de consulta: 06/04/2023].

[19] Gestión en la nube. https://www.unisys.com/es/glossary/what-is-cloud-management/ [fecha de consulta: 08/04/2023].

[20] Software para la monitorización de sistemas. https://geekflare.com/es/best-open-source-monitoring-software/ [fecha de consulta: 14/04/2023].

[21] Software para la gestión de tickets. https://helpdeskpymes.com/herramientas-de-ticketing/ [fecha de consulta: 14/04/2023].

[22] Descripción Zabbix. https://es.wikipedia.org/wiki/Zabbix [fecha de consulta: 14/04/2023].

[23] Descripción Zabbix. https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-zabbix-to-securely-monitor-remote-servers-on-ubuntu-20-04-es [fecha de consulta: 14/04/2023].

[24] Descripción GLPI. https://es.wikipedia.org/wiki/GLPi [fecha de consulta: 14/04/2023].

[25] Descripción herramienta actualización WSUS (Windows Server Update Services). https://es.wikipedia.org/wiki/Windows_Server_Update_Services [fecha de consulta: 12/05/2023].

[26] Definición de SOC. https://www.oracle.com/es/database/security/que-es-un-soc.html [fecha de consulta: 20/05/2023].

[27] Definiciones glosario. https://es.wikipedia.org/ [fecha de consulta: 20/05/2023].

Anexos

Este apartado se compone de 17 anexos que se referencian dentro de los distintos apartados que componen la memoria. Cada uno de los anexos se componen de varias páginas y siempre comienzan en una página nueva.

Los anexos no son completamente necesarios para el entendimiento del trabajo, pero si ayudan a comprender un poco mejor la parte más técnica, como son las instalaciones, configuraciones de los sistemas y herramientas que se mencionan en la memoria, además de proporcionar ejemplos sobre algunas de las tareas y funciones que pueden realizarse dentro de un NOC.

Anexo I: Descripción de las actividades que desarrolla un NOC

Las actividades que pueden desarrollarse en un NOC se dividen en dos tipos, actividades primarias o básicas y actividades secundarias o adicionales. Las actividades primarias deben estar implementadas en cualquier NOC ya que están pensadas para cubrir las necesidades básicas; en cambio, las secundarias son actividades que de forma adicional pueden asumirse dentro de un NOC y su implementación es opcional.

En la siguiente lista se detallan cada una de las actividades principales o básicas que deben desarrollarse en un NOC:

- **Monitorización de sistemas**: La monitorización de sistemas es una de las tareas principales que se realizan dentro de un NOC y una de las más importantes. Su función es detectar anomalías en cualquier dispositivo de la red y tras la generación de una alerta, interpretarla y proceder según su criticidad.

  Para esta tarea se utiliza un software de monitorización, que se encarga de leer los parámetros de los distintos dispositivos de la red e interpretarlos conforme a unas reglas marcadas, que dependerán del dispositivo y su criticidad.

  Las reglas definidas ayudan a identificar o dar una idea de la criticidad de la alerta. Por ejemplo, un equipo servidor se apaga de repente marcando una alerta crítica que puede tener dos interpretaciones. La primera es que, si el servidor ofrece un servicio crítico, la alerta tiene carácter crítico y debe ser resuelta a la mayor brevedad. La segunda es que el servidor ofrece un servicio crítico, pero trabaja como respaldo, por lo que solo funcionaría en caso de que el principal deje de dar servicio, siendo una alerta con un carácter no tan crítico y para la que es posible tomar un poco más de tiempo en su resolución.

- **Gestión y resolución de incidencias:** Tanto la gestión y resolución de incidencias que surgen en los sistemas es otra de las tareas principales que siempre debe realizar un NOC. Las incidencias pueden comunicarse por distintas vías, siendo las prioritarias el teléfono y el correo electrónico, aunque pueden definirse otras alternativas igualmente válidas.

  Para esta tarea se utiliza un software de ticketing, que se encarga de agrupar toda la información relativa a la descripción problema, fecha del problema, sistema afectado, técnicos que participan, departamentos y recursos implicados para su resolución, horas dedicadas a resolverla, entre otros datos. Todos estos datos servirán para crear informes, mejorar los procedimientos, tener un histórico de ciertas incidencias que se repiten con frecuencia o cualquier otra utilidad que se le puedan dar.

- **Ejecución de procedimientos:** La ejecución de ciertos procedimientos de forma manual siempre va a ser necesario en cualquier sistema, bien porque no se pueda

automatizar debido a que requiera configuraciones de distintos tipos en un mismo sistema, como pueden ser modificar políticas, registro, tareas programas, desactivar servicios en otros equipos dependientes o cualquier acción que cada vez se realice de una forma distinta, o bien porque así se requiera para tener un control más exhaustivo sobre el procedimiento y evitar fallos en la ejecución.

Algunos de los procedimientos más comunes suelen ser la actualización y configuración de software de la propia organización, donde se suele requerir distintas acciones sobre varios dispositivos del sistema, configuraciones de equipos dependiendo de su criticidad o servicio que ofrece, bastionado de equipos para su segurización, etc.

- **Gestión de perfiles de usuario y acceso:** La gestión de los usuarios abarca las tareas de creación, modificación, eliminación, desbloqueo de cuentas, permisos de acceso y el mantenimiento de todo esto. Es muy importante mantener toda esta información actualizada para prevenir problemas de seguridad y permitir a los usuarios los accesos que dependiendo de su área o rol deban asignárseles.

  Los perfiles de usuario dentro de servidores que proporcionan terminales remotos también deben ser mantenidos, ya que, si un usuario deja la organización, este perfil debe ser eliminado para liberar los recursos usados y volver a disponer de ellos.

- **Gestión de dispositivos:** La gestión de dispositivos como pueden ser nuevos equipos de usuarios, servidores o cualquier otro que haga uso de la red, también necesitan ser dados de alta e instalarles el agente para la monitorización, asignarles un grupo con ciertos permisos y realizar un mantenimiento periódico para eliminar los que están en desuso.

- **Creación de informes:** La creación de distintos tipos de informes, como pueden ser de incidencias, estado de la red, actualizaciones o cualquier otro que contenga información relevante, son necesarios para dar a conocer a un directivo, personal responsable de algún departamento o un cliente, datos sobre las tareas realizadas o problemas que han surgido en la realización de las actividades. Mediante los informes se pueden realizar estudios que pueden servir de referencia y mejorar el servicio en el futuro, perfeccionando las tareas o procedimientos para aumentar el beneficio de la organización.

- **Ejecución de peticiones de servicio:** Estas peticiones pueden ser realizadas en cualquier momento por cualquier persona autorizada. También pueden ser contratados o pactados en caso de ofrecer un servicio externo y que el cliente decida que, para las tareas desarrolladas en su organización, haya que realizar una modificación, revisión, procedimiento o cambio in situ.

En la siguiente lista se detallan cada una de las actividades secundarias o adicionales que pueden desarrollarse en un NOC:

- **Gestión de actualizaciones y parcheado:** Los sistemas deben estar actualizados y aplicar parches de forma regular, especialmente si se tratan de sistemas de carácter crítico o si la actualización que debe aplicarse tiene esta misma categoría.

  Las actualizaciones ayudan a eliminar vulnerabilidades de seguridad, optimizar y aumentar el rendimiento, mejorar la interfaz, etc. No solo se aplican actualizaciones a sistemas operativos de equipos y servidores o al software que en ellos se ejecutan, también al hardware de red, impresoras, teléfonos móviles, dispositivos IoT o cualquier otro dispositivo que las requieran.

- **Gestión del cortafuegos:** El cortafuegos o firewall es uno de los dispositivos más importantes de nuestra red y mantenerlo es una parte importante de cualquier organización. Las configuraciones que se pueden realizar en estos dispositivos son numerosas, como la apertura de puertos, definición de reglas para gestionar que se permite o restringe, etc.

- **Gestión de software de seguridad:** La gestión de este tipo de software va más enfocada al mantenimiento de cualquier plataforma o servicio de seguridad instalado en la red, haciendo hincapié en su correcta configuración para evitar ataques indeseados y su optimización para evitar ralentizaciones en la red o impedir ejecuciones que comprometan la seguridad de esta.

- **Gestión del antivirus:** El antivirus es otro software que es de vital importancia mantener y tener actualizado en todo momento, debido a que cada vez existen amenazas más avanzadas que intentan burlar esta protección.

  Existen consolas o entornos que facilitan las tareas de gestión, como realizar instalaciones de forma remota, realizar configuraciones, comprobar que el antivirus se está ejecutando correctamente, etc. Estas consolas también facilitan enormemente el trabajo de despliegue masivamente e incluso permite definir las reglas de aplicación dependiendo del dispositivo.

- **Bastionado de equipos (*Hardening*):** Los equipos, tanto de usuarios, como servidores, deben estar segurizados para evitar ataques no deseados. La segurización consta en definir algunas reglas y modificar parámetros dentro de los equipos o sistemas, como puede ser la activación de ciertas políticas, deshabilitar servicios, modificar registros, etc. Para realizar la segurización de un sistema, se siguen guías de bastionado que pueden ser ejecutadas de forma manual, mediante GPO o una mezcla de ambas.

El departamento de ciberseguridad de forma general es el encargado de estudiar y documentar las necesidades de la organización, para posteriormente definir las guías de bastionado que hay que aplicar dependiendo de cada uno de los sistemas.

- **Scripting para resolución de problemas y automatizaciones:** El lenguaje para la creación de scripts es diferente dependiendo del sistema en el que se ejecute, pero la función es la misma, además de ser una herramienta de gran utilidad para resolver automatizaciones de procedimientos e instalaciones y casi cualquier tarea automatizable que nos imaginemos, dentro de un sistema que pueda ejecutarlos.

  Para los niveles inferiores del NOC, no se hace tan necesario el conocimiento y manejo de scripting, aunque si recomendable, normalmente su uso se enfoca más en niveles superiores, ya que para la ejecución de scripts es necesario también poseer permisos de ejecución en determinados entornos.

- **Gestión de la implementación para traslado a entorno activo:** La tarea descrita está enfocada en pasar a producción software que ya ha sido probado en un entorno de pruebas y tiene la aprobación para ejecutarse en un entorno real.

  Normalmente este software necesita de varias configuraciones, instalaciones y permisos de ejecución. Para ello se crean procedimientos específicos puntuales que deben ser ejecutados y que permitirán la puesta en marcha de estos sistemas en el entorno activo.

- **Gestión del directorio activo:** La gestión del directorio activo permite mantener los servicios que conectan a los usuarios con los recursos de la red necesarios para que puedan realizar su trabajo, además de permitir la gestión de permisos, mostrar información de equipos, asignar y crear grupos, desbloquear cuentas, crear GPO, etc.

- **Aplicación de políticas:** En una red deben definirse reglas, tanto para los usuarios o grupos de usuarios, como para los dispositivos que la componen. Las reglas ayudan a optimizar el rendimiento de la red y aseguran que en ella se opere de forma adecuada.

- **Gestión de certificados:** Los certificados permiten autenticar a usuarios en sitios web, redes, aplicaciones de terceros, incluso a nombre de la organización, por lo que la tarea de tener bajo control la disponibilidad y uso de estos certificados es una tarea importante dentro de una organización.

- **Gestión de recursos virtualizados:** La virtualización de recursos va cobrando cada vez más importancia dentro de una organización, ya que esta ofrece muchos beneficios, como la ejecución de varios servidores en un solo equipo físico, fácil monitorización, alta disponibilidad, recuperación de desastres, menor consumo, entre otros.

  Al igual que los recursos físicos, los recursos virtuales como equipos o servidores también necesitan ser gestionados para asegurar su buen funcionamiento, mediante herramientas diseñadas especialmente para la asignación de sus recursos, monitorización y resolución de las incidencias que en ellos puedan surgir.

- **Gestión de aplicaciones remotas:** Una ventaja de la virtualización de aplicaciones es poder ofrecer su ejecución de forma remota.

  Un ejemplo de esta utilidad es la posibilidad de ofrecer a un usuario que se encuentra de viaje, acceso a ciertas aplicaciones (dependiendo de los permisos del usuario) que se ejecutan en un servidor remoto, evitando así el uso de VPN, incluso pudiendo ofrecer servicio desde cualquier terminal o equipo externo.

  Otro ejemplo, puede ser un servidor con una aplicación, a la que los usuarios que deban ejecutarla no tengan permisos de acceso, pudiendo ofrecerles la posibilidad de ejecutar la aplicación de forma remota con los permisos adecuados.

  Por lo tanto, la gestión de aplicaciones remotas consiste en ofrecer la posibilidad de usar aplicaciones virtualizadas a un usuario autorizado, realizando en el servidor de aplicaciones correspondiente, las configuraciones necesarias para la habilitación de la aplicación y gestión de los permisos aplicados al usuario que necesite dicha aplicación.

- **Control de inventarios:** Es necesario conocer los recursos de los que dispone la organización, tanto software, como hardware, además de los que deberá actualizar en breve o necesita adquirir para mejorar ciertos servicios. Todos estos datos permitirán anticiparse a necesidades de la organización y permitirá una mejor gestión de los recursos.

- **Administración de bases de datos:** Las bases de datos deben estar actualizadas y tener un mantenimiento correcto, así como cualquier procedimiento o tarea relacionado con su gestión, dado su gran importancia y criticidad. Por ello, deben prestarse especial atención a las alertas generadas en la herramienta de monitorización por este tipo de servidores.

Respecto a las actualizaciones de los sistemas de bases de datos, son un poco distintos a los demás, teniendo en cuenta que suelen ser sistemas redundantes y completamente idénticos. Un ejemplo referente a la actualización de estos sistemas es que, a la hora de actualizar estos equipos requieren una aplicación de actualizaciones de forma especial, ya que mientras se actualiza uno de estos servidores redundantes, el otro (o los demás sin son varios) está manejando datos y cuando el actualizado se ponga de nuevo en activo, los datos serán distintos, además de sus versiones, lo que puede provocar graves problemas.

- **Gestión de comunicaciones:** La asignación de números telefónicos basados en voz IP, suele realizarse mediante centralitas VoIP (al menos las más modernas), que permiten la gestión mediante una interfaz web y proporciona al usuario una línea telefónica completamente operativa para desarrollar su trabajo.

  En estas centralitas se gestionan los números de teléfonos, permisos, restricciones de llamada (p. ej. al extranjero o a números especiales), cambios de departamento, entre otras cosas y deben ser mantenidas adecuadamente.

- **Gestión de correo electrónico:** La asignación de correo electrónico a un nuevo usuario, así como la creación de grupos de correo, backup, migraciones de tecnología en caso necesario o eliminación de usuarios ya inactivos en el sistema, son algunas de las tareas que se pueden realizar respecto a la gestión del correo electrónico en la organización. El buen funcionamiento de este sistema es primordial en cualquier organización, ya que la inmensa mayoría de comunicaciones se realizan por esta vía.

- **Gestión de almacenamiento y copias de seguridad:** La información es muy valiosa en cualquier organización, por lo que es necesario crear copias de seguridad de esta y asegurar una copia de los datos críticos de forma regular, a largo plazo o fuera de las instalaciones de dicha organización, que nos garantizará su recuperación en caso de desastre y nos asegurará una forma de poder continuar con las operaciones en el futuro.

- **Optimización de los sistemas y la red:** La optimización de los sistemas puede llevarse a cabo de distintas formas, siendo la idea principal, la de utilizar todos los recursos que nos ofrece dicho sistema durante el mayor tiempo posible, sin disminuir su rendimiento y minimizando los costos.

  Hay herramientas que ayudan a conseguir este propósito, evitando cuellos de botella para garantizar un flujo de datos óptimo, así como la saturación de los recursos de un equipo.

En cuanto a la red es importante partir de un buen dimensionamiento inicial, pensando un poco en el futuro y diseñándola de forma escalable, en medida de lo posible, para así aumentar su capacidad en caso de que las técnicas de optimización ya no resuelvan el problema.

- **Gestión de sistemas de energía:** Los sistemas que abastecen de energía a los equipos de la red son de vital importancia y sobre todo, el conocer cuando se produce una falta de servicio que nos permita realizar acciones correctoras a la mayor brevedad posible.

  Uno de los principales sistemas encargados en proporcionar alimentación cuando la fuente principal falla es el SAI (Sistema de Alimentación Ininterrumpida). Este dispositivo protege contra sobretensiones y cortes eléctricos, además de proporcionar tiempo adicional (depende del dimensionamiento del SAI) que permite el funcionamiento de los dispositivos, para así poder evitar que los datos puedan corromperse, perderse o que el hardware se dañe. También ofrece información sobre el estado en el que se encuentra el propio dispositivo SAI y sus baterías, si necesita realizar mantenimiento, si requiere la sustitución de alguna pieza o cualquier otra acción que necesite, por lo que se hace necesario que toda esta información brindada por el dispositivo haya que gestionarla de alguna forma.

- **Gestión de la nube:** Los productos y servicios ejecutados en la nube también necesitan supervisarse, protegerse y gestionarse de manera eficiente, adaptando los recursos de la nube de la mejor forma posible para la organización a través de una gestión eficaz. Para ello existen multitud de herramientas que permiten la supervisión de cualquier tipo de nube sea púbica, privada o híbrida y las actividades que en ella se realiza.

Anexo II: Plantillas documentos técnicos

Plantilla para la elaboración de una instrucción técnica que resuelva una incidencia

INSTRUCCIÓN TÉCNICA #0xxx

Sistema Windows / Linux – Título descriptivo de la Instrucción Técnica

Versión 1.x

Autor:	<Nombre autor>	**Fecha:**	dd/mm/aaaa
Modificado por:	<Nombre modificador>	**Fecha:**	dd/mm/aaaa
Verificado por:	<Técnico L3 o Coordinador>	**Fecha:**	dd/mm/aaaa

Descripción

Describir el objetivo y finalidad de la ejecución de la instrucción técnica.

Riesgos que hay que tener en cuenta

Comentar todos los riesgos derivados de ejecutar la instrucción técnica y cuál sería el plan de contingencia en caso de que falle algo, por ejemplo, si la ejecución de la instrucción técnica implica la parada de un servicio, entonces comentar las repercusiones que puede tener.

Preparación

Operaciones que hay que realizar antes de comenzar con la ejecución de la instrucción técnica.

Pasos a seguir

Lista o índice que indica todas las operaciones a seguir en el siguiente apartado.

Ejecución

Se especifica todas las operaciones a realizar en el mismo orden descrito en el apartado anterior.

Pág. 1

Comprobaciones

Se especifican las comprobaciones que hay que realizar tras acabar la ejecución de la instrucción técnica. Si no hay que realizar ninguna comprobación, escribir “Sin comprobaciones a realizar”.

Acciones posteriores

Se especifican las operaciones posteriores a la ejecución de la instrucción técnica si las hubiera. Si no hay acciones posteriores, escribir “Sin acciones posteriores”.

Comentarios

Espacio reservado para comentar algo relevante y que no aparezca en los apartados anteriores. Si no hay nada que comentar, escribir “Sin comentarios”.

Plan de contingencia

Describir el plan de contingencia de forma detallada o especificar la forma de encontrarlo. Si no existe plan de contingencia o no es necesario, escribir “Sin plan de contingencia” o “No es necesario plan de contingencia”.

Anexos

A partir de aquí pueden agregase anexos que ayuden a la ejecución de la instrucción técnica. Si no hay anexos, escribir “Sin documentación adicional”.

Plantilla para la elaboración de un manual que permita la ejecución de un procedimiento programado

PROCEDIMIENTO #0xxx

Sistema Windows / Linux – Título descriptivo del procedimiento

Versión 1.x

Autor:	<Nombre autor>	**Fecha:**	dd/mm/aaaa
Modificado por:	<Nombre modificador>	**Fecha:**	dd/mm/aaaa
Verificado por:	<Técnico L3 o Coordinador>	**Fecha:**	dd/mm/aaaa

Descripción

Describir el objetivo y finalidad del procedimiento a realizar.

Riesgos que hay que tener en cuenta

Comentar todos los riesgos derivados de ejecutar el procedimiento y cuál sería el plan de contingencia en caso de que falle algo, por ejemplo, actualizar y reiniciar un servicio balanceado que implica configurar el balanceador para derivar todo el tráfico al otro servidor mientras que se realiza la actualización de uno de ellos, para después volverlo a poner en funcionamiento con el riesgo que ello conlleva si no se realiza correctamente.

Preparación

Operaciones que hay que realizar antes de comenzar con la ejecución del procedimiento.

Pasos a seguir

Lista o índice que indica todas las operaciones a seguir en el siguiente apartado.

Ejecución

Se especifica todas las operaciones a realizar en el mismo orden descrito en el apartado anterior.

Pág. 1

Comprobaciones

Se especifican las comprobaciones que hay que realizar tras acabar la ejecución del procedimiento. Si no hay que realizar ninguna comprobación, escribir “Sin comprobaciones a realizar”.

Acciones posteriores

Se especifican las operaciones posteriores a la ejecución del procedimiento si las hubiera. Si no hay acciones posteriores, escribir “Sin acciones posteriores”.

Comentarios

Espacio reservado para comentar algo relevante y que no aparezca en los apartados anteriores. Si no hay nada que comentar, escribir “Sin comentarios”.

Plan de contingencia

Describir el plan de contingencia de forma detallada o especificar la forma de encontrarlo. Si no existe plan de contingencia o no es necesario, escribir “Sin plan de contingencia” o “No es necesario plan de contingencia”.

Anexos

A partir de aquí pueden agregase anexos que ayuden a la ejecución del procedimiento. Si no hay anexos, escribir “Sin documentación adicional”.

Anexo III: Instalación servidor para monitorización y ticketing (Ubuntu Server 22.04)

Pasos a realizar para la instalación de Ubuntu Server 22.04 LTS con la imagen ISO obtenida desde la página web de Ubuntu.

1. Seleccionar idioma del sistema.

   Seleccionamos “English” y pulsamos **Enter** para avanzar.

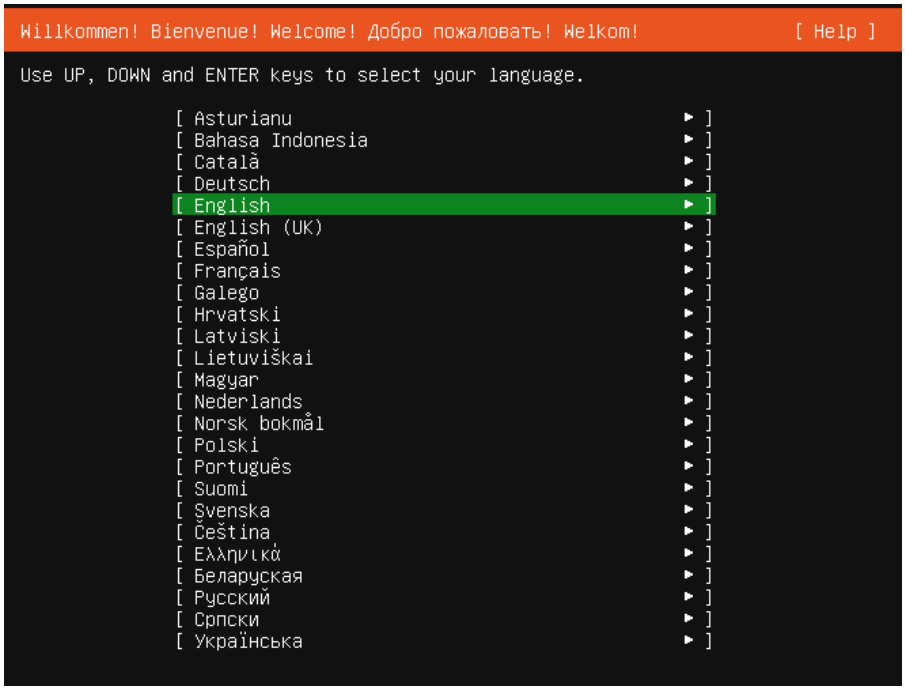


Figura 21: Instalación Ubuntu Server - Idioma del sistema

2. Seleccionar idioma del teclado.

   Modificamos los campos *Layout* y *Variant* seleccionando “Spanish” y una vez seleccionado nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

Figura 22: Instalación Ubuntu Server - Idioma del teclado

3. Seleccionar modo de instalación.

   No tenemos que modificar nada, por lo que dejamos seleccionado “Ubuntu Server”, después nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

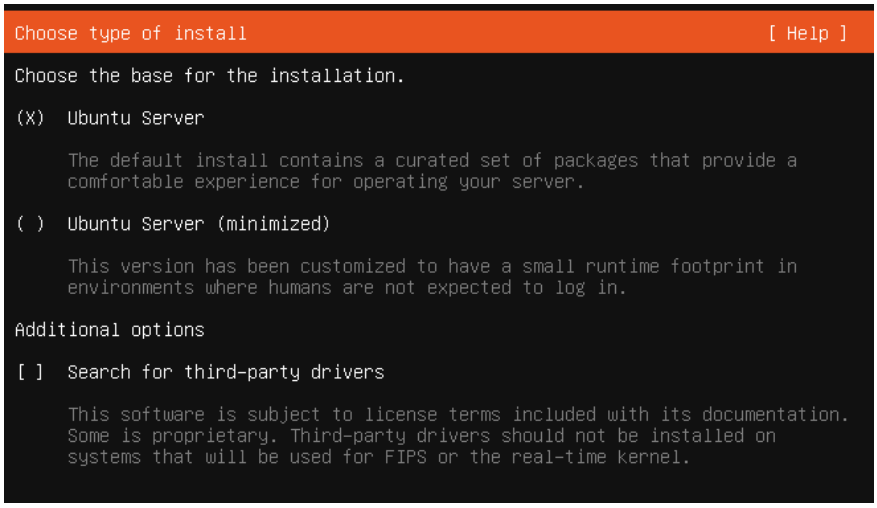


Figura 23: Instalación Ubuntu Server - Modo de instalación

4. Configurar la red.

   No tenemos que modificar nada, solo hay que observar la IP asignada para poder acceder posteriormente al servidor por SSH, después nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

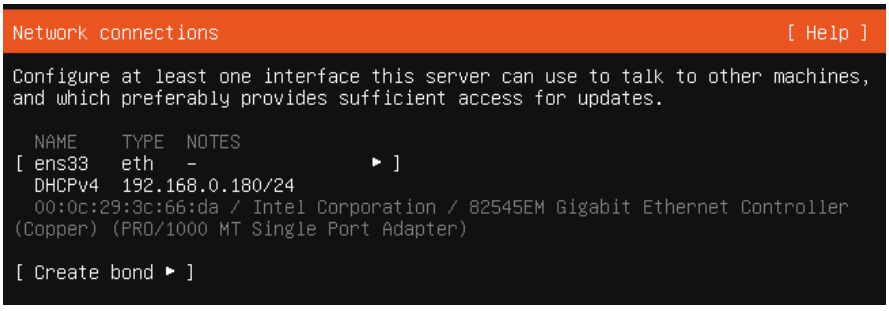


Figura 24: Instalación Ubuntu Server - Configuración de la red

5. Configurar proxy.

   No tenemos que modificar nada, nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

Figura 25: Instalación Ubuntu Server - Configuración del proxy

6. Configurar repositorios de Ubuntu.

   No tenemos que modificar nada, nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

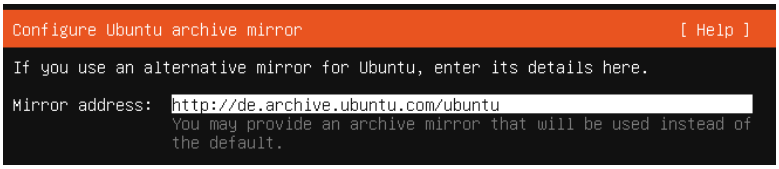


Figura 26: Instalación Ubuntu Server - Repositorios de Ubuntu

7. Configurar almacenamiento.

   No tenemos que modificar nada, por lo que dejamos seleccionado “Use an entire disk”, después nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

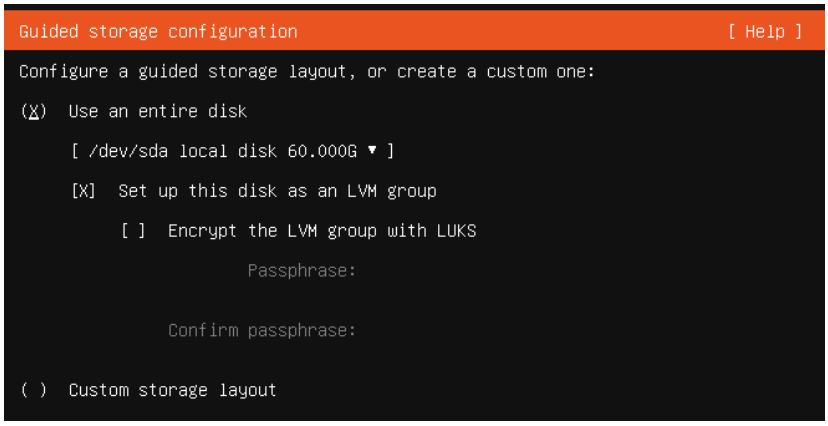


Figura 27: Instalación Ubuntu Server - Elección de almacenamiento

En la configuración del almacenamiento no tenemos que modificar nada, aunque es posible, nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

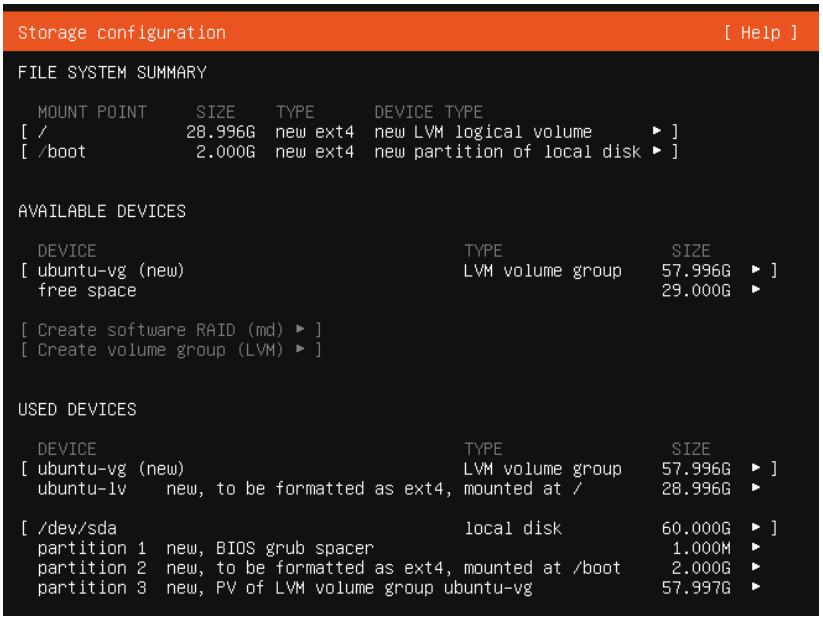


Figura 28: Instalación Ubuntu Server - Configuración del almacenamiento

Se nos informa sobre pérdida de datos la cual vamos a asumir, nos situamos sobre **Continue** y pulsamos **Enter** para avanzar.

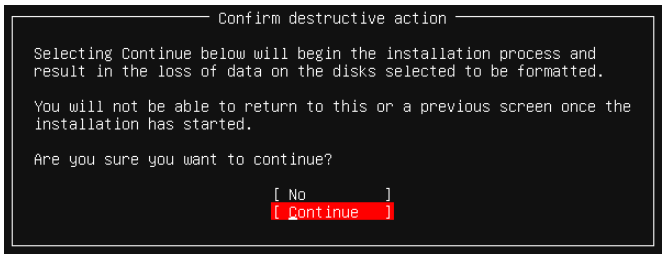


Figura 29: Instalación Ubuntu Server - Información de formateo del disco

8. Configuración del perfil.

   Rellenamos los siguientes datos:

   - *Your server's name*: Escribimos el nombre del servidor, p. ej. "zabbix" o "glpi".
   - *Pick a username*: Escribimos un nombre de usuario, p. ej. "tfg".
   - *Choose a password***:** Escribimos una contraseña, p. ej. "tfg".
   - *Confirm your password*: Volvemos a escribir la contraseña.

   Nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

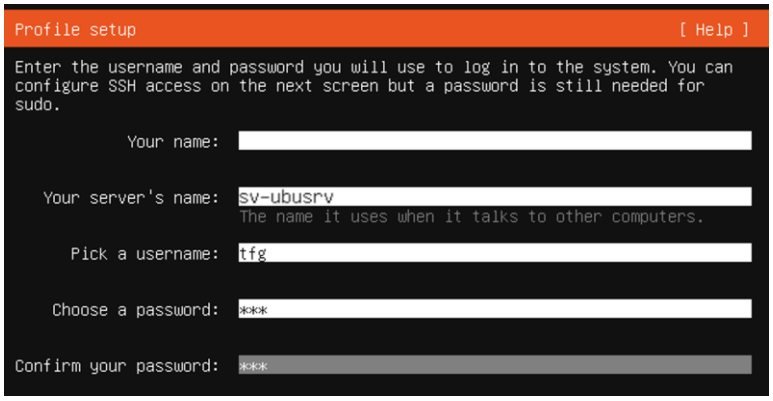


Figura 30: Instalación Ubuntu Server - Configuración del perfil

9. Actualizar a Ubuntu Pro.

   No realizamos ninguna actualización dejando la selección por defecto "Skip for now", después nos situamos sobre **Continue** y pulsamos **Enter** para avanzar.

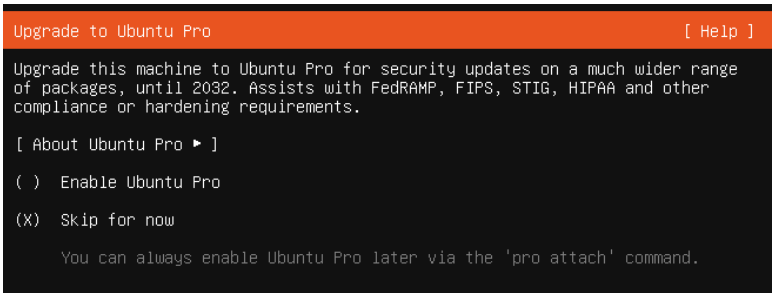


Figura 31: Instalación Ubuntu Server - Actualizar a Ubuntu Pro

10. Habilitar SSH.

    Seleccionamos “Install OpenSSH server” colocándonos encima y pulsando **Enter**, después nos situamos sobre **Done** y pulsamos **Enter** para avanzar.

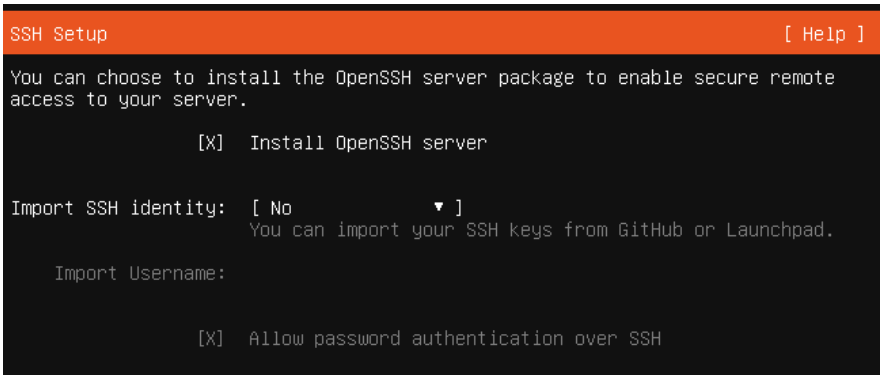


Figura 32: Instalación Ubuntu Server - Habilitar SSH

11. Características adicionales.

    No instalamos características adicionales por lo que dejamos la selección por defecto, nos situamos sobre **Done** y pulsamos **Enter** para instalar.

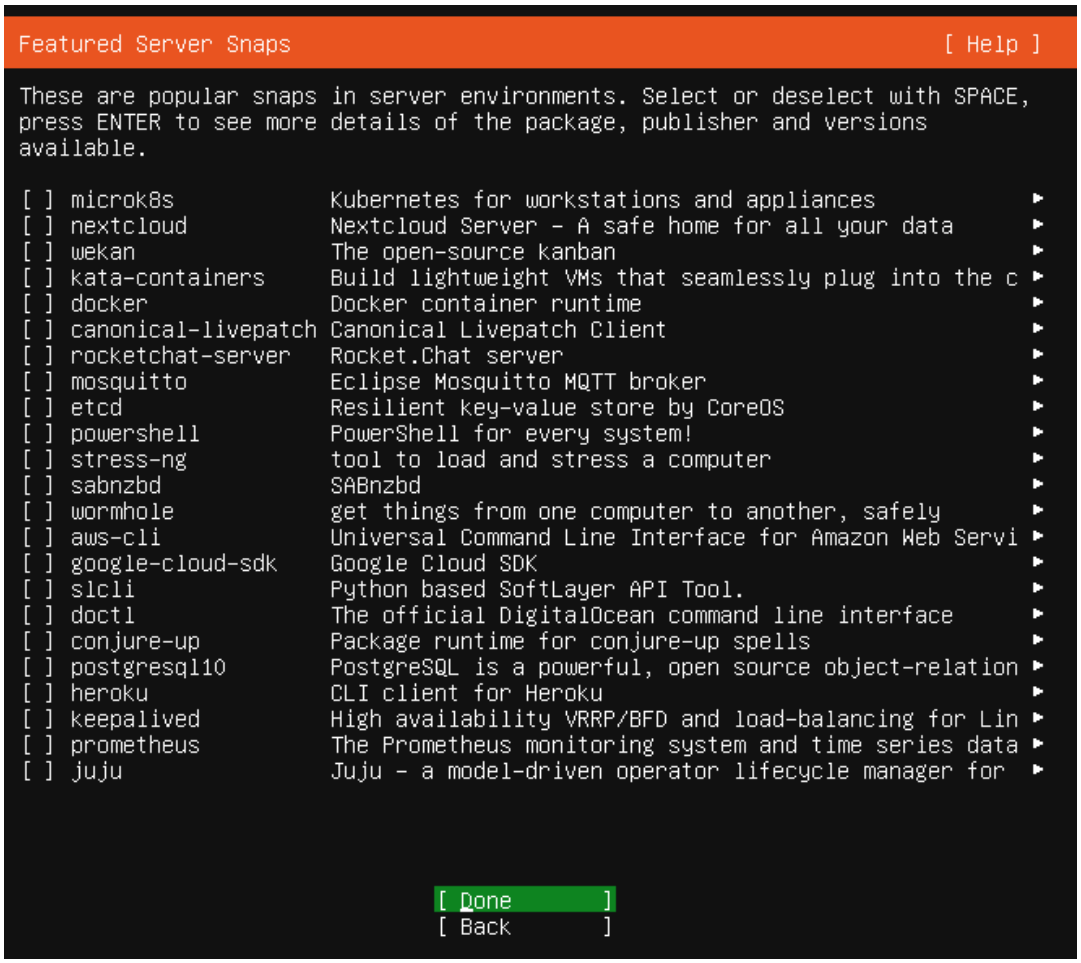


Figura 33: Instalación Ubuntu Server - Habilitar características adicionales

12. Finalizar instalación.

Una vez el proceso de instalación ha finalizado, nos situamos sobre **Reboot Now** y pulsamos **Enter** para reiniciar el servidor.

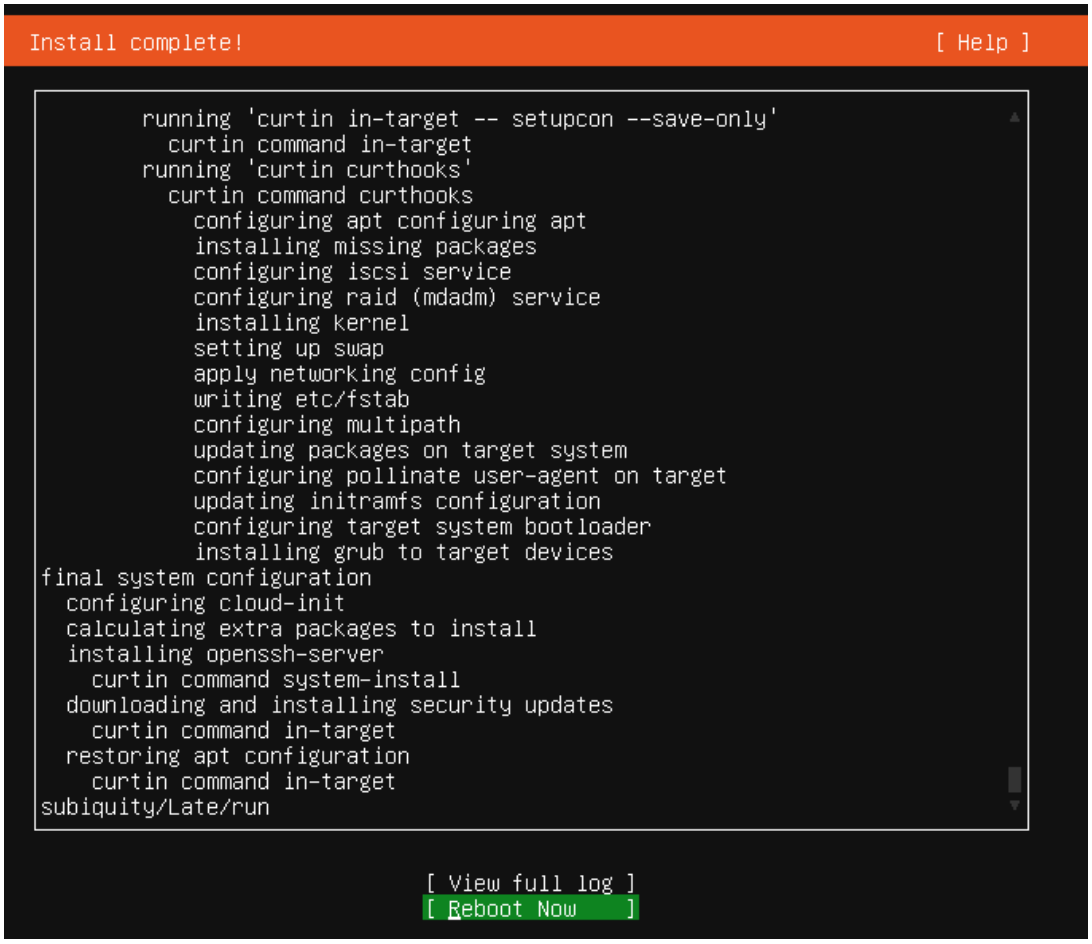


Figura 34: Instalación Ubuntu Server - Fin de la instalación

Anexo IV: Instalación sistema de monitorización (Zabbix 6.0 LTS)

Pasos a realizar para la instalación de Zabbix 6.0 LTS

1. Descargar e instalar los paquetes necesarios para la instalación de Zabbix.

   Descargamos todos los paquetes necesarios para poder realizar la instalación de Zabbix y una vez descargados comenzamos su instalación.

```
sudo su (Para entrar en modo root, realizamos la validación)

wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4+ubuntu$(lsb_release -rs)_all.deb

dpkg -i zabbix-release_6.0-4+ubuntu$(lsb_release -rs)_all.deb

apt update

apt -y install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

2. Configurar la base de datos que usará Zabbix.

   a. Instalamos la base de datos (MariaDB 10.6).

```
apt install software-properties-common -y
```

```
curl -LsS -O https://downloads.mariadb.com/MariaDB/mariadb_repo_setup

bash mariadb_repo_setup --mariadb-server-version=10.6
```

```
apt update

apt -y install mariadb-common mariadb-server-10.6 mariadb-client-10.6
```

   Iniciamos el servicio de MariaDB y habilitamos el inicio al arranque del sistema.

```
systemctl start mariadb

systemctl enable mariadb
```

   b. Restablecemos la contraseña *root* para la base de datos.

   Rellenamos los siguientes datos:

   - *New Password*: Escribimos la nueva contraseña, p. ej. “passDBroot”.
   - *Re-enter new Password*: Volvemos a escribir la contraseña.

```
mysql_secure_installation
```

```
Enter current password for root (enter for none): Pulsar Enter

Switch to unix_socket authentication [Y/n] Y

Change the root password? [Y/n] Y

New password: passDBroot
Re-enter new password: passDBroot

Remove anonymous users? [Y/n] Y

Disallow root login remotely? [Y/n] Y

Remove test database and access to it? [Y/n] Y

Reload privilege tables now? [Y/n] Y
```

c. Creamos la base de datos.

```
mysql -uroot -p'passDBroot' -e "CREATE DATABASE zabbix character set
utf8mb4 collate utf8mb4_bin;"

mysql -uroot -p'passDBroot' -e "GRANT ALL PRIVILEGES ON zabbix.* to
zabbix@localhost identified by 'passDBzabbix';"
```

d. Importamos el esquema inicial de datos.

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --
default-character-set=utf8mb4 -uzabbix -p'passDBzabbix' zabbix
```

e. Agregamos la contraseña de la base de datos en el archivo de configuración de Zabbix.

```
nano /etc/zabbix/zabbix_server.conf
```

Agregamos la siguiente línea en cualquier lugar del archivo de configuración.

```
DBPassword=passDBzabbix
```

Guardamos y salimos del archivo (pulsamos la combinación **ctrl** + **x** para solicitar la salida del archivo, después escribimos la letra **y** para confirmar que se quiere guardar los cambios y finalmente pulsamos **Enter**).

3. Reiniciar procesos de servidor y agente de Zabbix.

   Reiniciamos los procesos tanto del servidor, como del agente de Zabbix y habilitamos el inicio al arranque del sistema.

```
systemctl restart zabbix-server zabbix-agent

systemctl enable zabbix-server zabbix-agent
```

4. Configurar la interfaz de Zabbix.

   a. Configuramos PHP para la interfaz de Zabbix.

```
nano /etc/zabbix/apache.conf
```

   Quitamos el comentario **#** de la línea que contiene el texto "# php_value date.timezone Europa/Riga", y sustituimos la ciudad por la correcta.

```
php_value date.timezone Europa/Madrid
```

   Guardamos y salimos del archivo (pulsamos la combinación **ctrl** + **x** para solicitar la salida del archivo, después escribimos la letra **y** para confirmar que se quiere guardar los cambios y finalmente pulsamos **Enter**).

   b. Reiniciamos el servidor web de Apache y habilitamos el inicio al arranque del sistema.

```
systemctl restart apache2

systemctl enable apache2
```

   c. Configurar interfaz web.

   Nos conectamos a interfaz de Zabbix que acabamos de instalar, usando la URL "http://IP del servidor Zabbix/zabbix" para iniciar el asistente de instalación de Zabbix.

   La IP del servidor Zabbix en este caso es 192.168.0.180, que es la IP asignada al servidor Ubuntu server que contendrá la aplicación de Zabbix, por lo que la URL de acceso será "http://192.168.0.180/zabbix".

En la pantalla de bienvenida seleccionamos el idioma *Default languaje* colocando “English (en_US)”, después pulsamos **Next step** para avanzar.

Figura 35: Instalación Zabbix - Pantalla de inicio de instalación de Zabbix

En la siguiente pantalla simplemente pulsamos **Next step** para avanzar.

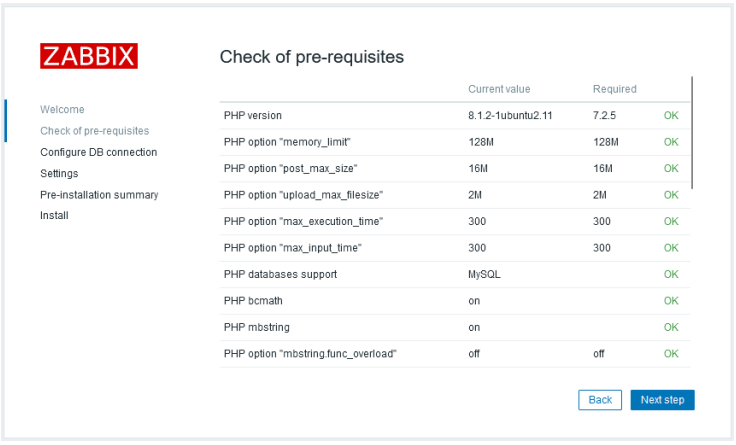


Figura 36: Instalación Zabbix - Verificación de requisitos previos

En la siguiente pantalla configuramos la conexión con la base de datos y como los datos ya están rellenos, solo debemos escribir en el campo *Password*, la contraseña “passDBzabbix”, después pulsamos **Next step** para avanzar.

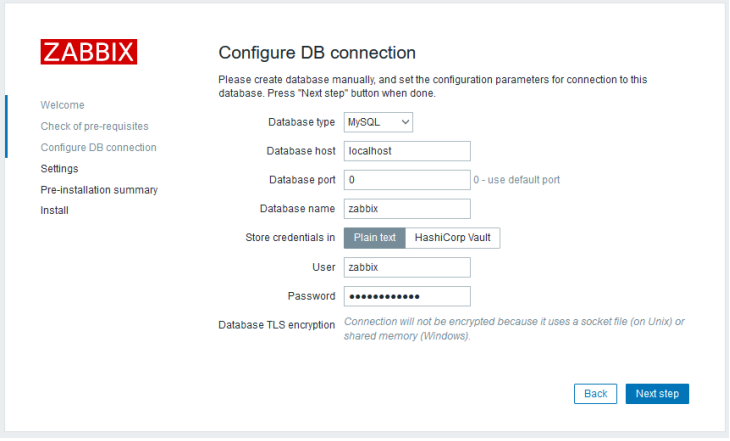


Figura 37: Instalación Zabbix - Configuración de la conexión a la base de datos

En la siguiente pantalla configuramos la zona horaria seleccionando en el campo *Default time zone*, la zona horaria perteneciente a nuestro país "(UTC+01:00) Europe/Madrid", después pulsamos **Next step** para avanzar.

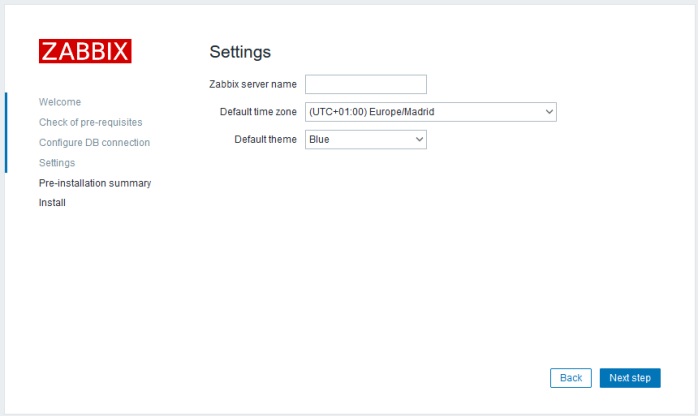


Figura 38: Instalación Zabbix - Configuración de la zona horaria

En la siguiente pantalla se muestra información sobre los parámetros configurados, si todo está correcto pulsamos **Next step** para instalar.

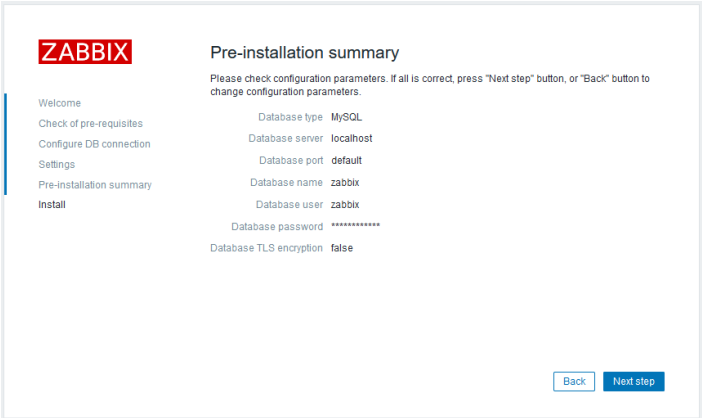


Figura 39: Instalación Zabbix - Resumen previo a la instalación

En la última pantalla podemos observar un mensaje indicando que la instalación de Zabbix ha finalizado correctamente, en este caso pulsamos **Finish** para acabar la instalación.

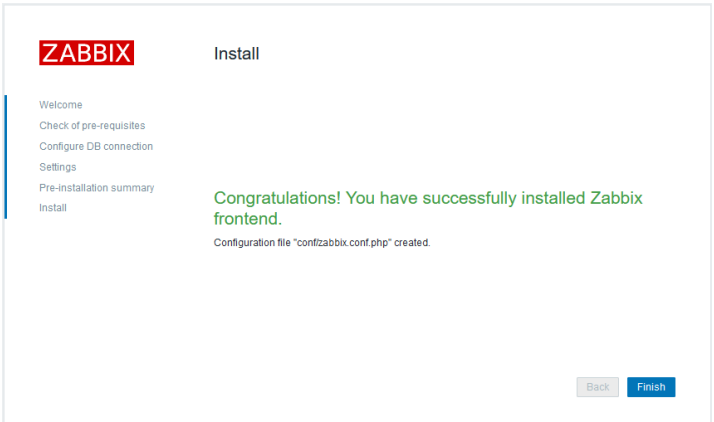


Figura 40: Instalación Zabbix - Fin de la instalación de Zabbix

5. Iniciar sesión en la interfaz de Zabbix utilizando las credenciales de inicio de sesión predeterminadas.

   Para iniciar sesión en Zabbix accedemos a la URL “http://192.168.0.180/zabbix” a través del navegador utilizando el usuario administrador “Admin” y la contraseña “zabbix”.

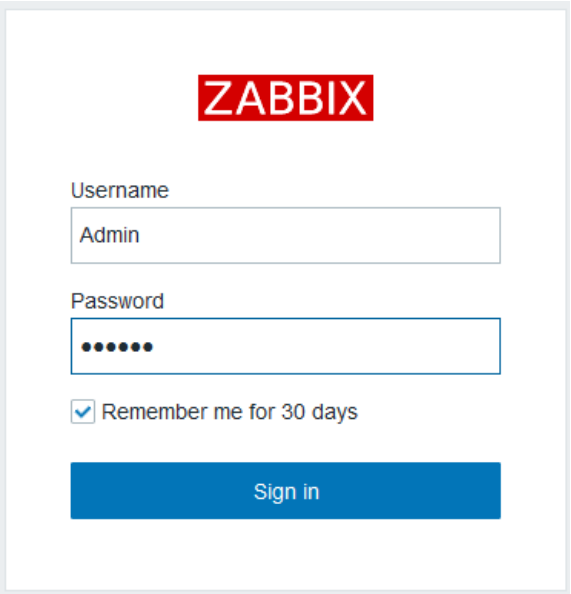


Figura 41: Instalación Zabbix - Inicio de sesión en Zabbix

Una vez accedemos a la URL anterior usando el usuario y contraseña de administrador, podremos ver el tablero de la herramienta de monitorización Zabbix.

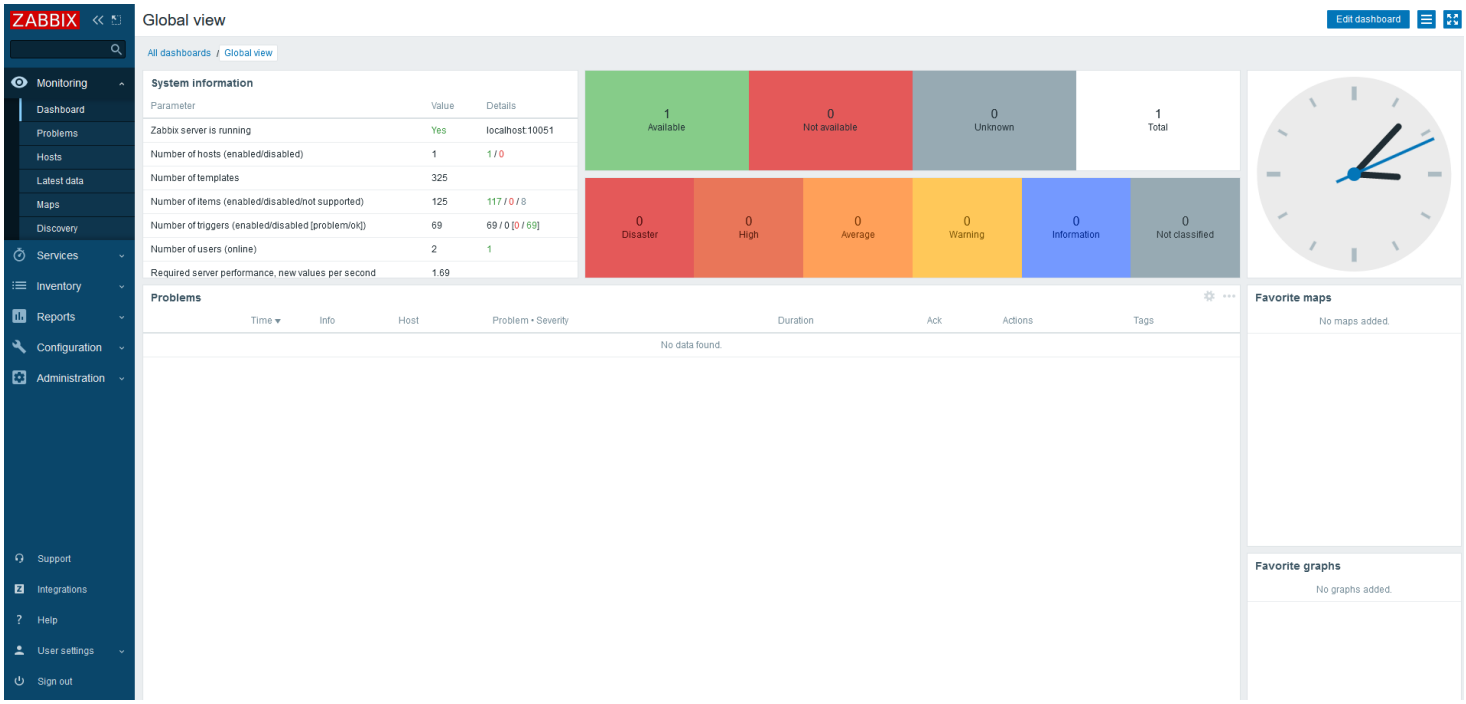


Figura 42: Instalación Zabbix - Tablero de Zabbix

Anexo V: Configuración sistema de monitorización (Zabbix 6.0 LTS)

Pasos a realizar para la configuración del agente de Zabbix en un equipo Ubuntu

A continuación, se muestran los pasos que permitirán la configuración de la herramienta de monitorización:

- **Creación de perfiles**

  Creamos los perfiles con sus respectivos permisos, que permitirán a los distintos tipos de usuarios realizar configuraciones en la herramienta de monitorización Zabbix.

  Para configurar los perfiles de usuario y asignarle sus correspondientes permisos, pulsamos en el menú de la izquierda del tablero de Zabbix "Administration – User roles" y configuramos los siguientes perfiles:

  - *Coordinador:* Es el perfil con menos restricciones y puede ser perfectamente super administrador de Zabbix. Este perfil puede ver y gestionar otros perfiles, grupos o usuarios existentes, además de realizar configuraciones importantes en la herramienta.
  - *Técnico:* Este perfil está pensado para el personal técnico del NOC de cualquier nivel, que tenga autorización para acceder a la herramienta de monitorización. Posee algunas opciones de administración en la herramienta, donde se podrá consultar datos de monitorización detallados y añadir nuevos sistemas o hosts para que sean monitorizados.
  - *Usuario:* Este perfil está pensado para personal autorizado que no pertenezca al NOC, donde se podrá consultar datos de monitorización básicos.
  - *Usuario personalizado:* Este perfil está pensado para personal autorizado que no pertenezca al NOC y que además tenga restringidos los equipos que podrá monitorizar, de los cuales podrá consultar datos de monitorización básicos.

- **Tableros de la herramienta Zabbix correspondientes a los distintos perfiles**

  Una vez configurado el perfil *Coordinador,* tendrá una visión completa del sistema y las gestiones que puede realizar. En la siguiente imagen podemos observar el tablero correspondiente a este perfil:

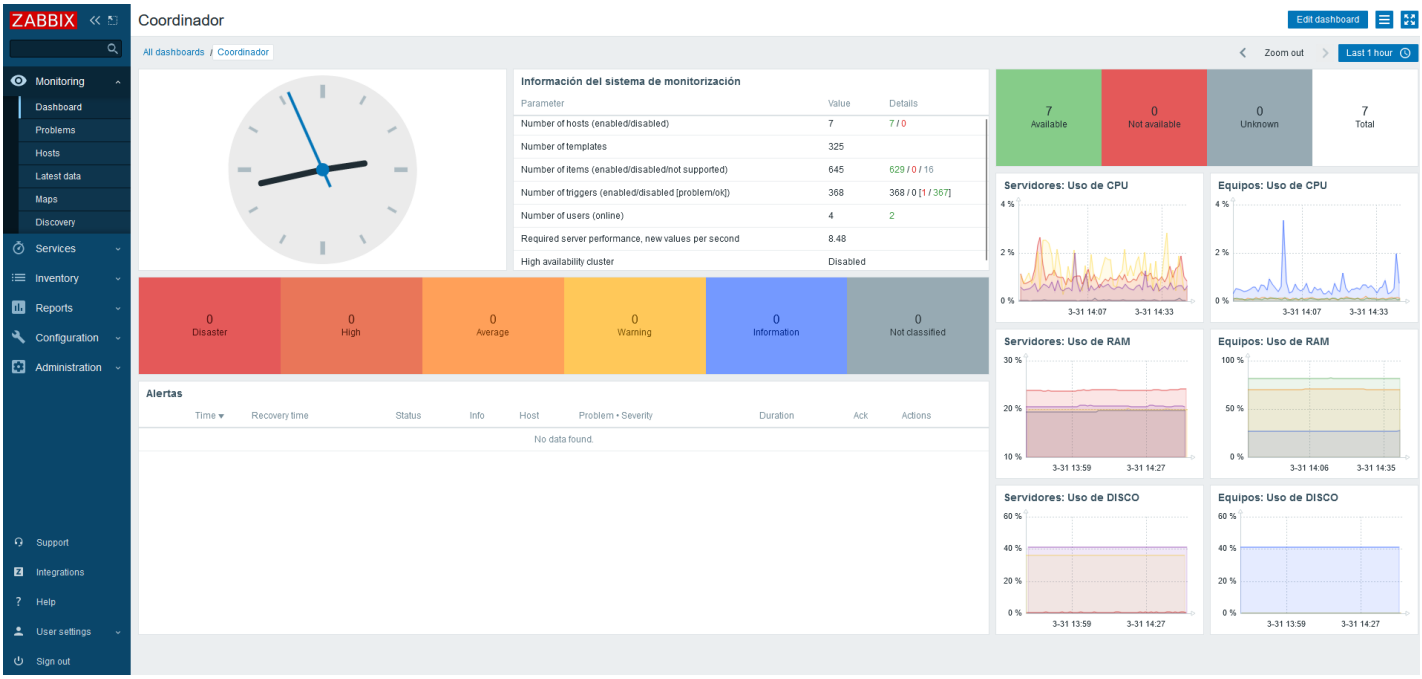


Figura 43: Conf. Zabbix - Tablero Zabbix para el coordinador

El perfil *Técnico* tendrá una visión más reducida que el perfil anterior. En la siguiente imagen podemos observar el tablero correspondiente a este perfil:

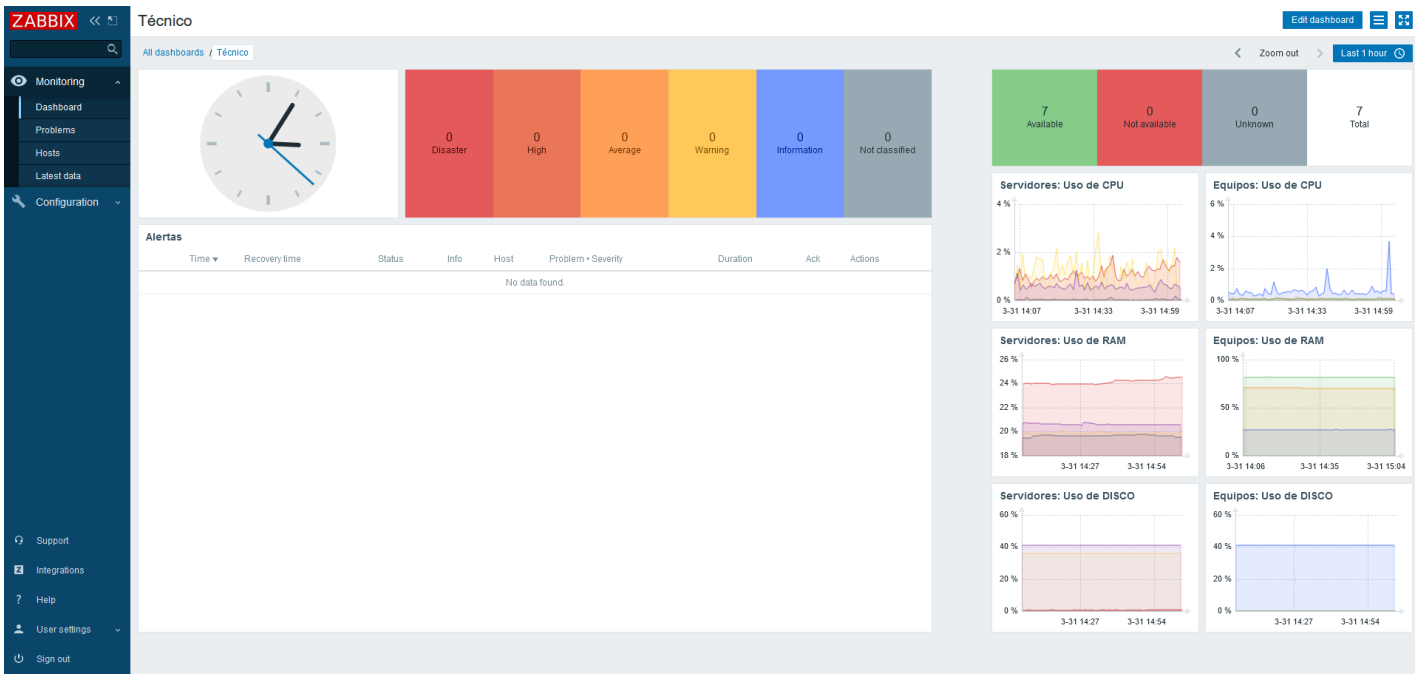


Figura 44: Conf. Zabbix - Tablero Zabbix para los técnicos

Los perfiles *Usuario* y *Usuario personalizado* tendrán una monitorización básica de los equipos a los que se les permita el acceso. En la siguiente imagen podemos observar el tablero correspondiente a este perfil:

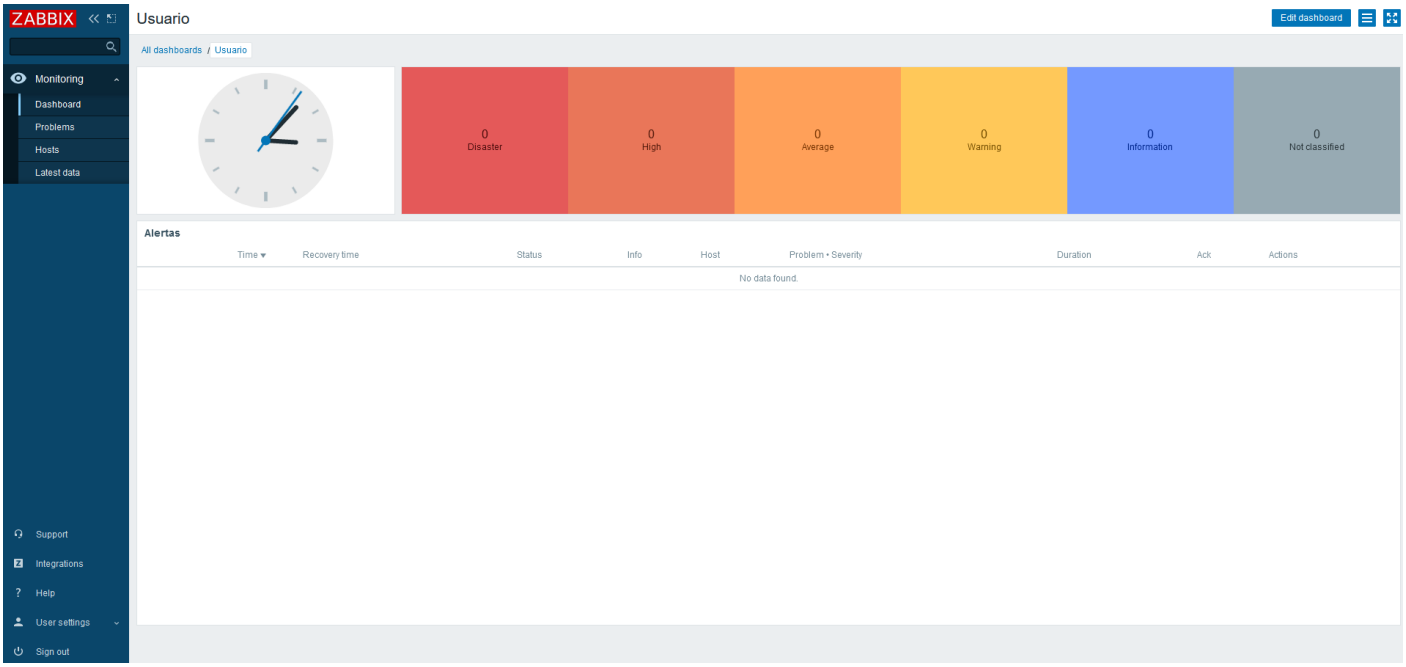


Figura 45: Conf. Zabbix - Tablero Zabbix para los usuarios

- **Asignación de perfiles a usuarios**

  Una vez creados los perfiles y asignados los respectivos permisos a dichos perfiles, pasamos a adjudicárselo a los usuarios. Cada usuario tendrá un perfil asignado y este le habilitará para realizar más o menos acciones en la herramienta de monitorización Zabbix.

  En primer lugar, creamos los usuarios pulsando en el menú de la izquierda del tablero de Zabbix "Administration – Users", para posteriormente mediante el propio menú de creación, asignarle uno de los perfiles configurados desde la pestaña "Permissions".

- **Incorporación de hosts iniciales para su monitorización**

  En el apartado 4 del Anexo VI y en el apartado 3 del Anexo VII para sistemas operativos Linux y Windows respectivamente, se detalla el proceso de agregar un host al servidor Zabbix para su monitorización.

- **Configuración automática de alertas**

  Esta configuración permite asignar a un host una plantilla, que contiene preconfiguradas las principales alertas necesarias para una monitorización completa de un sistema operativo.

En este caso, al agregar el host a la herramienta de monitorización (ver Anexo VI para Linux y Anexo VII para Windows), tendremos la posibilidad de añadir una plantilla (template) mediante una lista desplegable.

Aunque existen multitud de plantillas, las que utilizaremos en el piloto NOC serán "Windows by Zabbix agent" para sistemas Windows y "Linux by Zabbix agent" para sistemas Linux.

Una vez configurada la plantilla, la herramienta de monitorización comenzará a mostrar alertas de ese host, que se podrán ver pulsando en el menú de la izquierda del tablero de Zabbix "Monitoring – Dashboard".

- **Configuración manual de alertas**

  Esta configuración permite un mayor control sobre el componente del sistema monitorizado, ofreciendo la posibilidad de personalizar los parámetros de generación de la alerta y el mensaje que se muestra.

  En este caso, al agregar el host a la herramienta de monitorización (ver Anexo VI para Linux y Anexo VII para Windows), tendremos la posibilidad de añadir una plantilla (template) mediante una lista desplegable, que posteriormente podremos desvincular para crear nuestros propios disparadores que generarán las alertas. También se puede crear la alerta desde cero si se conoce y se está familiarizado con las expresiones o constructores que utiliza la herramienta de monitorización Zabbix.

  Una alerta está compuesta principalmente de un objeto (item) y de un disparador (triggers), los cuales describiremos a continuación:

  - El objeto (item) contiene una llave (key). Esta llave es un comando que nos proporcionará datos del sistema donde se ejecuta dicho comando a través del agente de monitorización.

  - El disparador (trigger) contiene las reglas que se aplicarán sobre el objeto (item) y que generará el mensaje de aviso con la alerta en caso de incumplimiento. Una vez el objeto monitorizado vuelva a proporcionar información que no incumpla las reglas, la alerta se marcará como resuelta quedando archivada para su posterior consulta.

  Una vez conocemos la composición de una alerta, se muestran algunas imágenes de disparadores configurados de forma manual en nuestro piloto NOC, que generarán las alertas que veremos en el tablero principal de Zabbix.

En la siguiente imagen se muestra un disparador llamado “Uso alto de la CPU” y genera una alerta cuando el uso de la CPU es muy alto, durante más de 2 minutos.

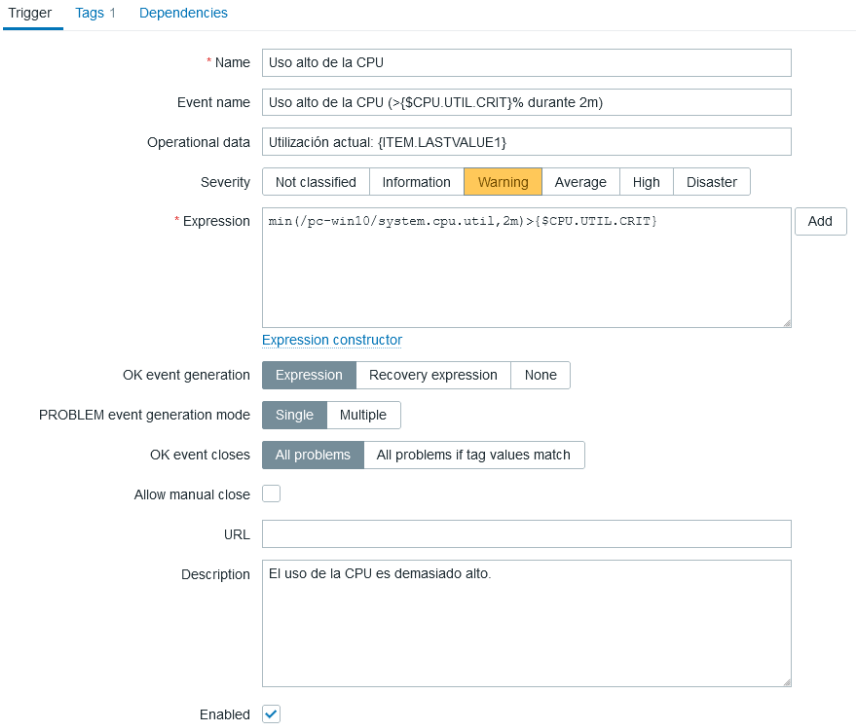


Figura 46: Conf. Zabbix - Configuración disparador por uso alto de la CPU

En la siguiente imagen se muestra un disparador llamado “Uso alto de la memoria RAM” y genera una alerta cuando el uso de la memoria RAM es muy alto, durante más de 2 minutos.

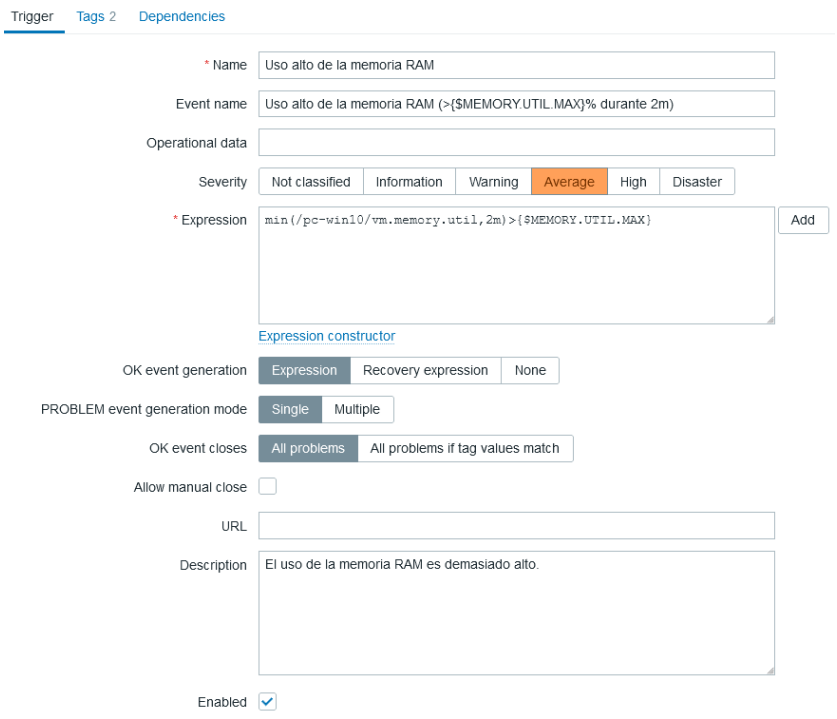


Figura 47: Conf. Zabbix - Configuración disparador por uso alto de la memoria RAM

En la siguiente imagen se muestra un disparador llamado “(C:): Espacio en disco críticamente bajo” y genera una alerta cuando la utilización del espacio en disco es muy alta o queda poco espacio.

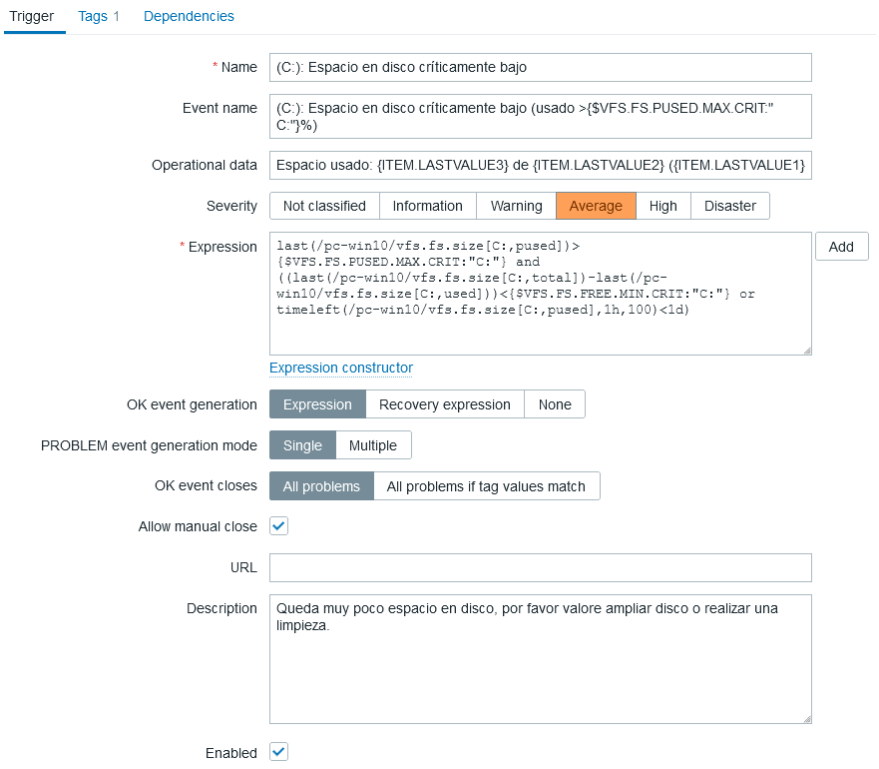


Figura 48: Conf. Zabbix - Configuración disparador cuando hay poco espacio en disco

También se crean disparadores que mostrarán otro tipo de alertas como las siguientes:

- Si el sistema se ha apagado o se ha perdido el contacto con el agente Zabbix, se mostrará “Agente Zabbix no disponible”.
- Si el sistema se ha reiniciado recientemente, se mostrará “El equipo se ha reiniciado”.
- Si el nombre del sistema ha cambiado recientemente, se mostrará “El nombre del sistema ha cambiado”.
- Si la hora del sistema que ejecuta el agente no coincide con la hora del servidor de Zabbix, se mostrará “La hora del sistema no está sincronizada”.

Una vez creados los disparadores, es necesario configurar la gravedad de la alerta. Como se puede observar en las imágenes anteriores, en el disparador hay un campo llamado gravedad (*severity*), que nos permitirá clasificar la alerta generada con seis posibilidades de mayor a menor severidad: Catástrofe (*Disaster*), Alta (*High*), Media (*Average*), Advertencia (*Warning*), Información (*Information*) y No clasificada (*Not Classified*).

Respecto a la configuración de las alertas, es importante destacar que una buena configuración de estas alertas bien sea de forma automática o manual, nos permitirá un mayor control sobre posibles incidencias que puedan surgir en el sistema, permitiéndonos solventarlo en el menor tiempo posible. También nos permitirá descartar falsos positivos, evitando así prestar atención a alertas innecesarias y la pérdida de tiempo que ello conlleva.

Una vez configurados los perfiles, incorporados los hosts que se van a monitorizar, definidas las alertas del sistema y asignado un perfil al usuario, este podrá acceder a la herramienta de monitorización Zabbix mediante un usuario con su correspondiente contraseña y tendrá permisos para realizar las acciones que el sistema le permita conforme a su perfil. Solamente los perfiles *Coordinador* y *Técnico* podrán agregar nuevos hosts a la herramienta para su monitorización.

En el Anexo XIV. Ejemplo de este documento se puede consultar un ejemplo de monitorización de varios sistemas y generación de alertas, tanto en equipos Windows como Linux, que nos ayudarán a comprender mejor el uso de la herramienta.

Anexo VI: Configuración agente Zabbix en equipo Linux para su monitorización

Pasos a realizar para la configuración del agente de Zabbix en un equipo Ubuntu

1. Descargar e instalar los paquetes necesarios para la instalación de agente de Zabbix.

   Descargamos todos los paquetes necesarios para poder realizar la instalación del agente de Zabbix y una vez descargados comenzamos su instalación.

```
sudo su (Para entrar en modo root, realizamos la validación)

wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-
release/zabbix-release_6.0-4+ubuntu$(lsb_release -rs)_all.deb

dpkg -i zabbix-release_6.0-4+ubuntu$(lsb_release -rs)_all.deb

apt update

apt -y install zabbix-agent
```

2. Configurar datos de conexión con el servidor Zabbix.

   Una vez instalado el agente de Zabbix, abrimos el archivo de configuración del agente donde realizaremos unas modificaciones.

```
nano /etc/zabbix/zabbix_agentd.conf
```

   Modificamos las siguientes líneas en el archivo de configuración.

```
### Option: Server (Especificamos la IP del servidor Zabbix)
Server=<Escribir IP del servidor de Zabbix, p. ej. 192.168.0.180>

### Option: ServerActive (Especificamos la IP del servidor Zabbix)
ServerActive=<Escribir IP del servidor de Zabbix, p. ej. 192.168.0.180>

### Option: Hostname (Nombre que tiene que coincidir con el campo "Host name"
cuando agregamos un nuevo host en el servidor Zabbix)
Hostname=<Nombre para el equipo, p. ej. PC-UBUDSK>
```

   Guardamos y salimos del archivo (pulsamos la combinación **ctrl** + **x** para solicitar la salida del archivo, después escribimos la letra **y** para confirmar que se quiere guardar los cambios y finalmente pulsamos **Enter**).

3. Reiniciar el agente de Zabbix

   Reiniciamos el agente de Zabbix y habilitamos el inicio al arranque del sistema.

```
systemctl restart zabbix-agent

systemctl enable zabbix-agent
```

4. Agregar host al servidor Zabbix para su monitorización.

   Nos situamos en el tablero de Zabbix, accediendo desde un navegador web a la URL "http://IP del servidor Zabbix/zabbix". Una vez dentro pulsamos en el menú de la izquierda "Configuration – Hosts" y posteriormente en el botón **Create Host**.

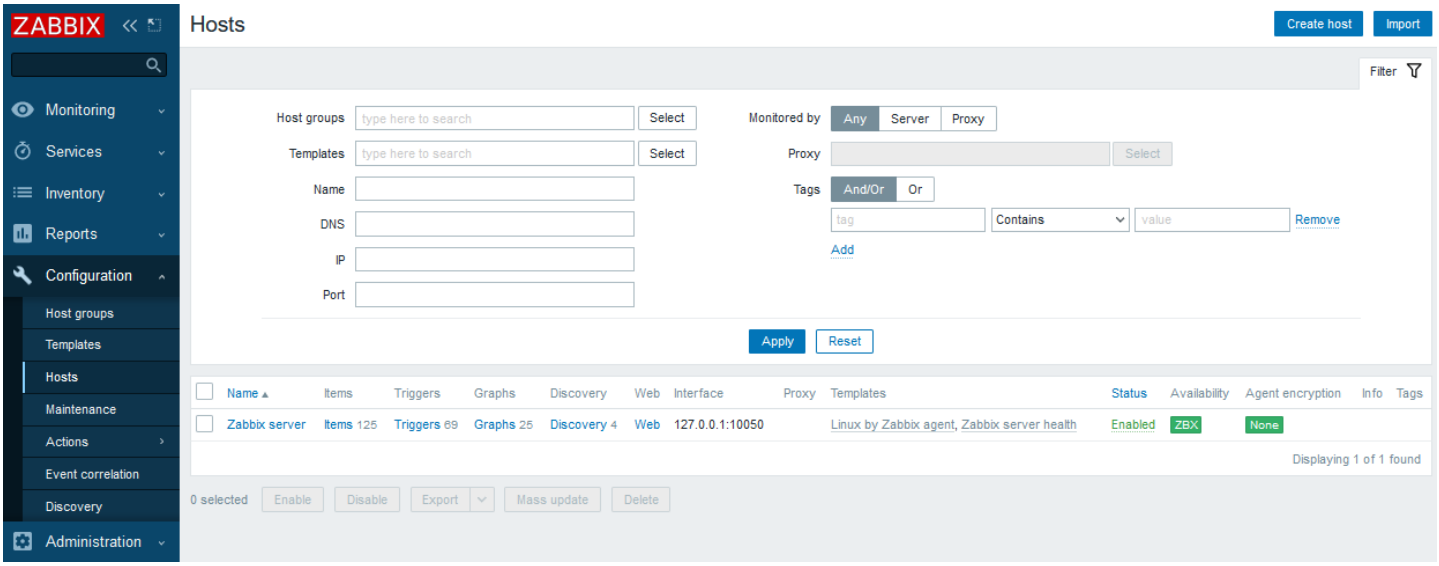


Figura 49: Conf. agente Zabbix Linux - Crear host Linux en el servidor Zabbix

Completamos la siguiente información y pulsamos **Add** para agregar el nuevo host:

- *Host name*: Escribimos el mismo nombre de equipo que se detalló en el campo *Hostname* del fichero de configuración del agente localizado en la máquina que se quiere monitorizar, p. ej. "PC-UBUDSK".
- *Visible name*: Escribimos el nombre que aparecerá en la lista de hosts del servidor Zabbix, p. ej. "Ubuntu desktop".
- *Templates*: Seleccionamos "Linux by Zabbix Agent", que tiene preconfiguradas las principales alertas necesarias para una monitorización completa de un sistema operativo Linux.

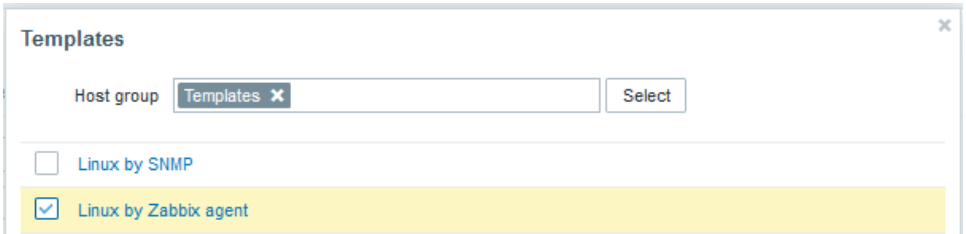


Figura 50: Conf. agente Zabbix Linux - Plantilla (Linux by Zabbix Agent)

- *Groups*: Seleccionamos "Operating systems" (para equipos) o "Linux server" (para servidores).
- *Interfaces*: Seleccionamos "Agent" y escribimos en el campo *IP address*, la dirección IP del equipo que se quiere monitorizar, p. ej. "192.168.0.181".

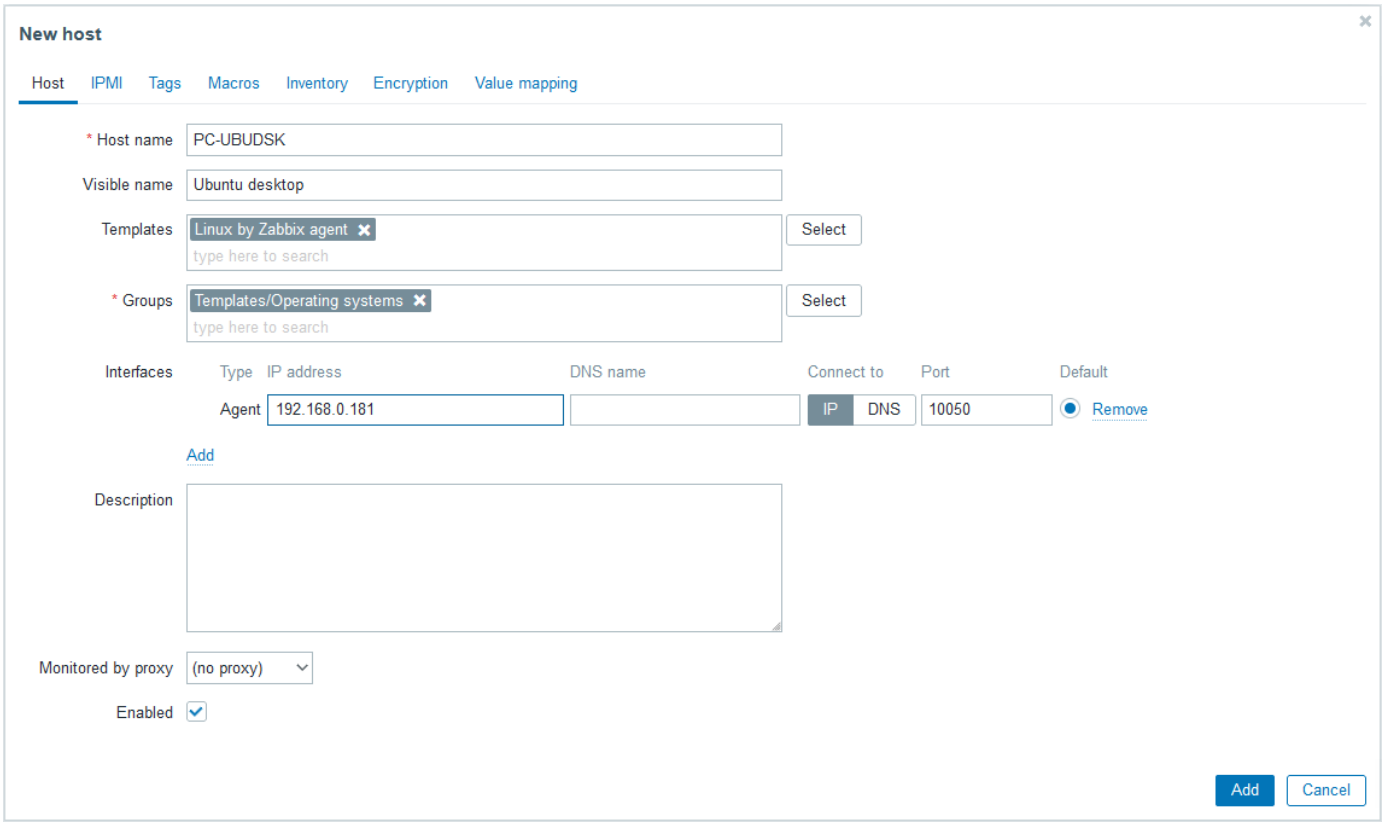


Figura 51: Conf. agente Zabbix Linux - Agregar host Linux al servidor Zabbix

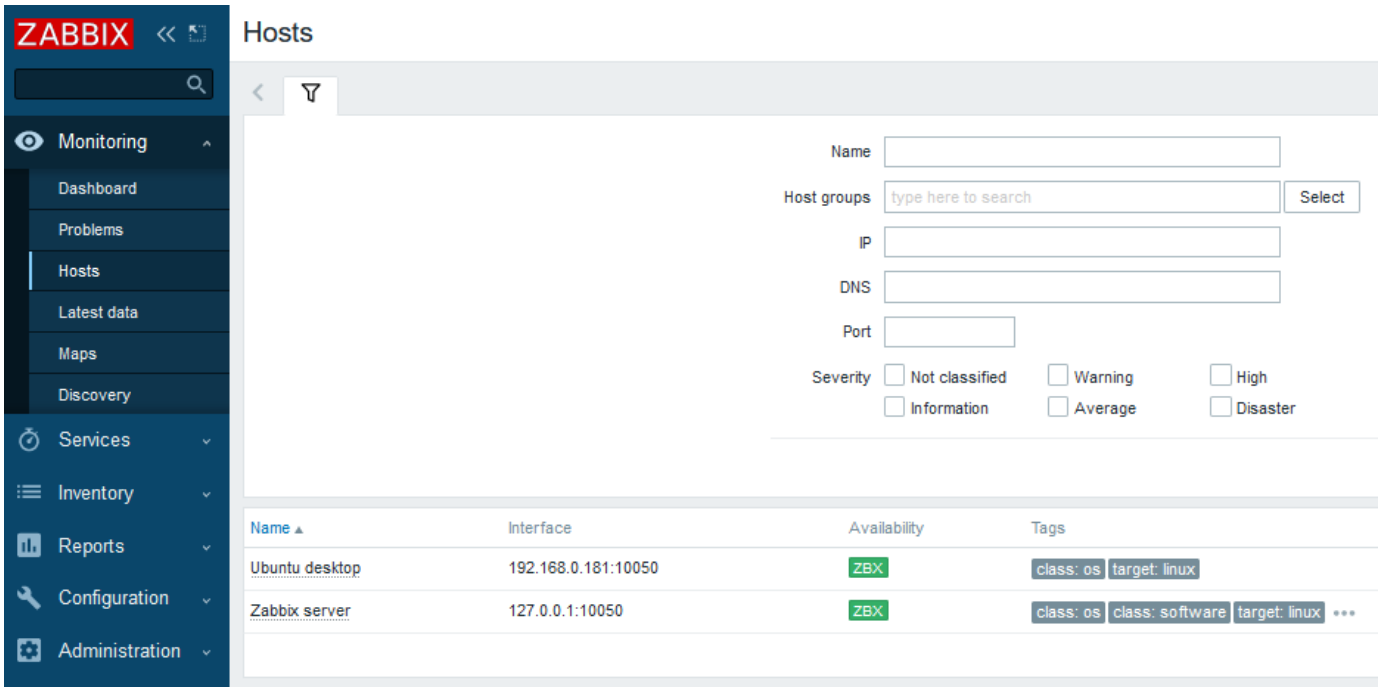


Figura 52: Conf. agente Zabbix Linux - Visualizar host Linux en el servidor Zabbix

Anexo VII: Configuración agente Zabbix en equipo Windows para su monitorización

Pasos a realizar para la configuración del agente de Zabbix en un equipo Windows

1. Descargar instalador MSI del agente Zabbix, el cual podemos obtener desde la web oficial de Zabbix[9]:

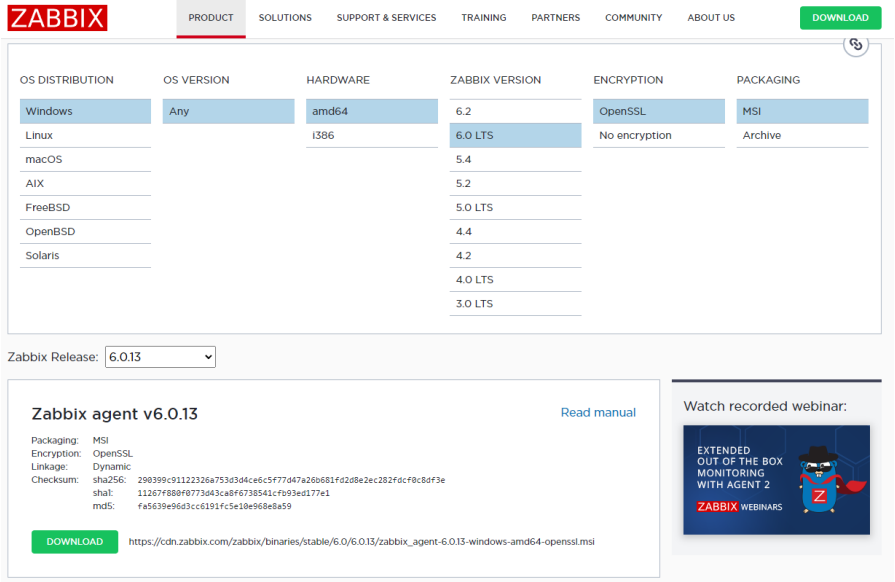


Figura 53: Conf. agente Zabbix Windows - Obtención paquete MSI para instalación

2. Realizar la instalación del agente en un sistema Windows.

   Iniciamos el instalador del agente Zabbix y pulsamos **Next** para avanzar en la instalación.

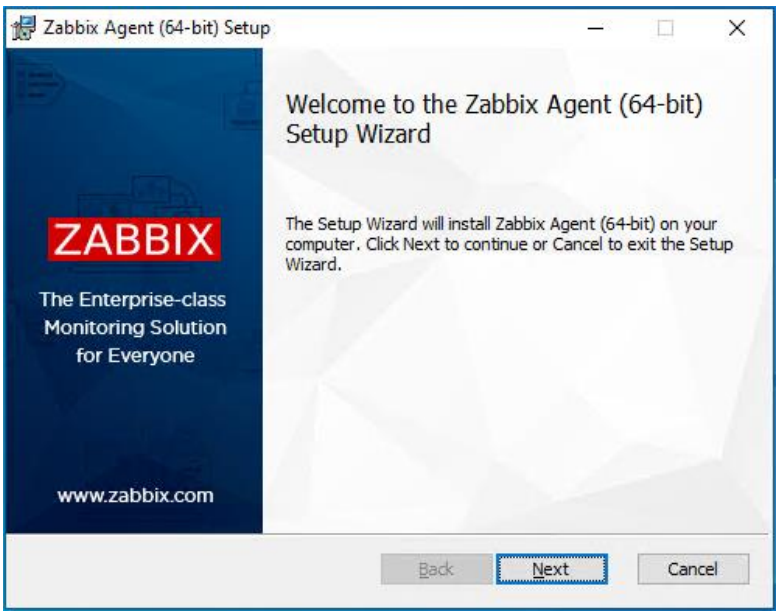


Figura 54: Conf. agente Zabbix Windows - Inicio de instalación del agente Zabbix

Aceptamos los términos del acuerdo de licencia y pulsamos **Next** para avanzar en la instalación.

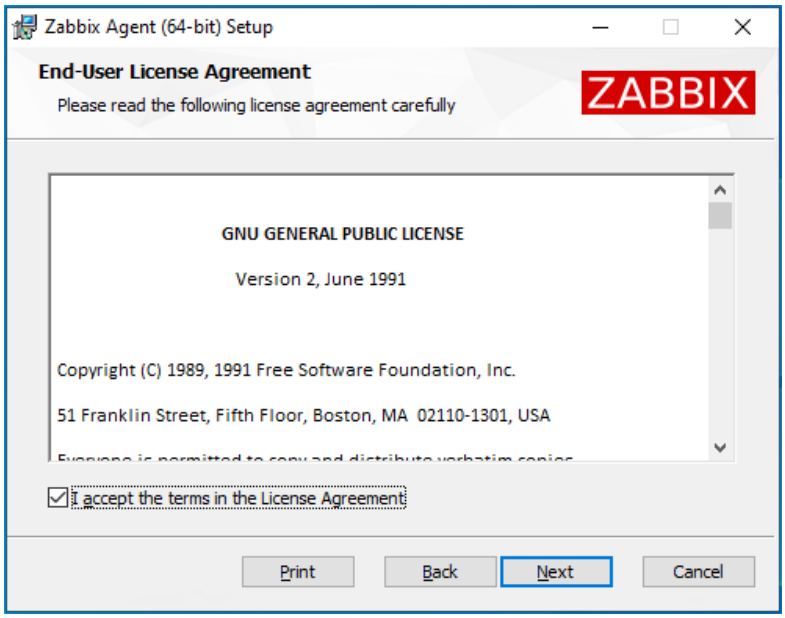


Figura 55: Conf. agente Zabbix Windows - Aceptación de los términos de uso

Dejamos la configuración por defecto de los componentes a instalar y pulsamos **Next** para avanzar en la instalación.

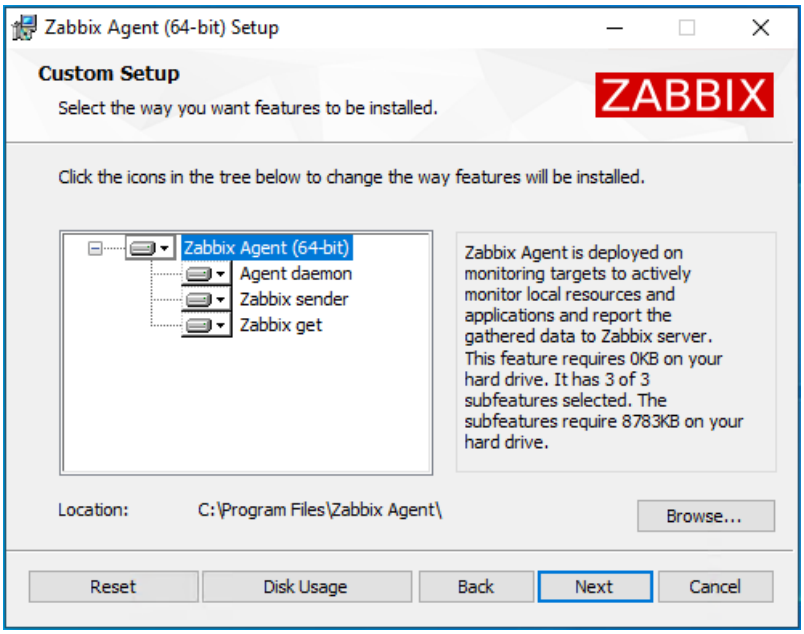


Figura 56: Conf. agente Zabbix Windows - Selección de los componentes a instalar

Completamos la siguiente información y pulsamos el botón **Next** para avanzar:

- *Host name*: Escribimos nombre del equipo a monitorizar, p. ej. “PC-WINDSK”.
- *Zabbix server IP/DNS*: Escribimos IP servidor Zabbix, p. ej. “192.168.0.180”.
- *Agent listen port*: Escribimos el número de puerto tcp, p. ej. “10050”.
- *Server or Proxy for active checks*: Escribimos la IP servidor Zabbix de nuevo.
- Seleccionamos la opción “Add agent location to the PATH”.

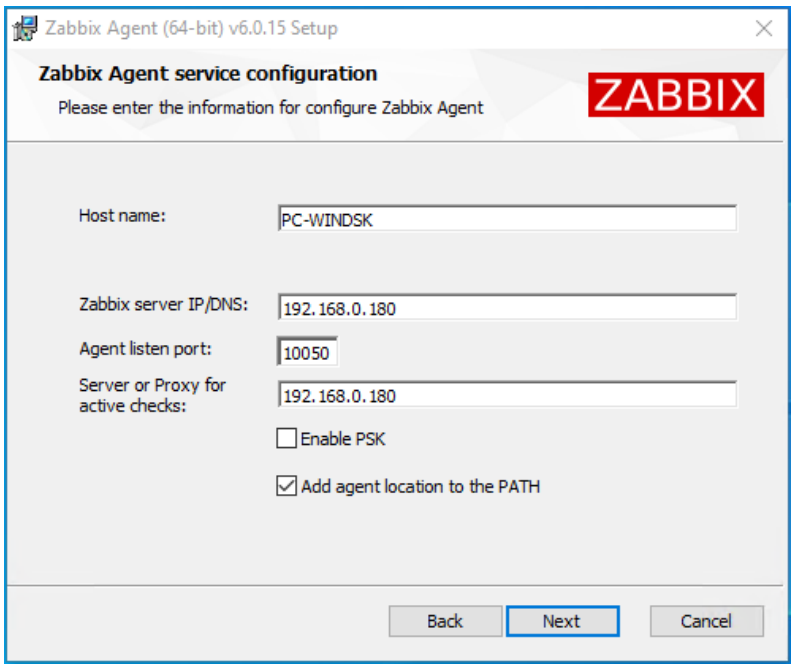


Figura 57: Conf. agente Zabbix Windows - Configuración de conexión al servidor Zabbix

Realizamos la instalación pulsando en **Install**.

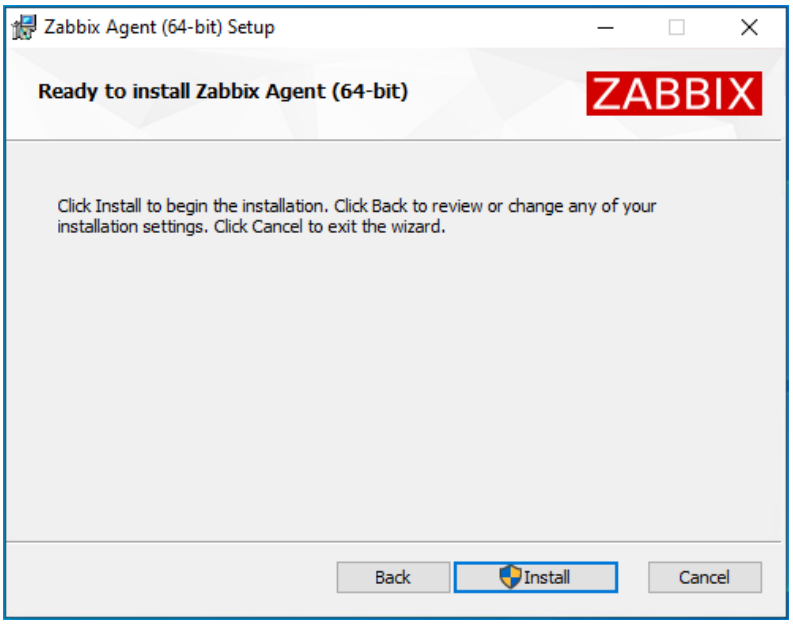


Figura 58: Conf. agente Zabbix Windows - Instalación del agente Zabbix

Finalizamos la instalación pulsando en **Finish**.

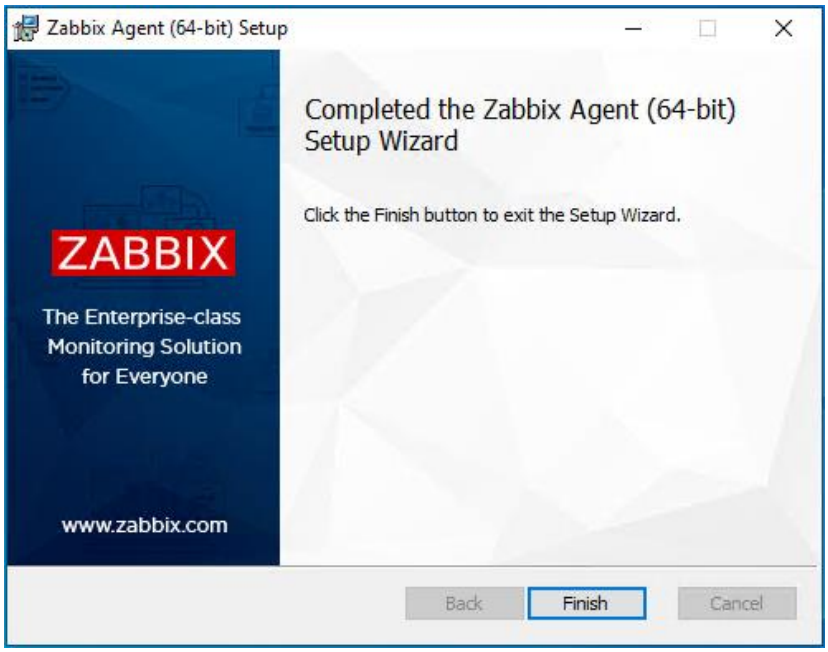


Figura 59: Conf. agente Zabbix Windows - Fin de la instalación del agente Zabbix

3. Agregar host al servidor Zabbix para su monitorización.

   Nos situamos en el tablero de Zabbix, accediendo desde un navegador web a la URL "http://IP del servidor Zabbix/zabbix". Una vez dentro pulsamos en el menú de la izquierda "Configuration – Hosts" y posteriormente en el botón **Create Host**.

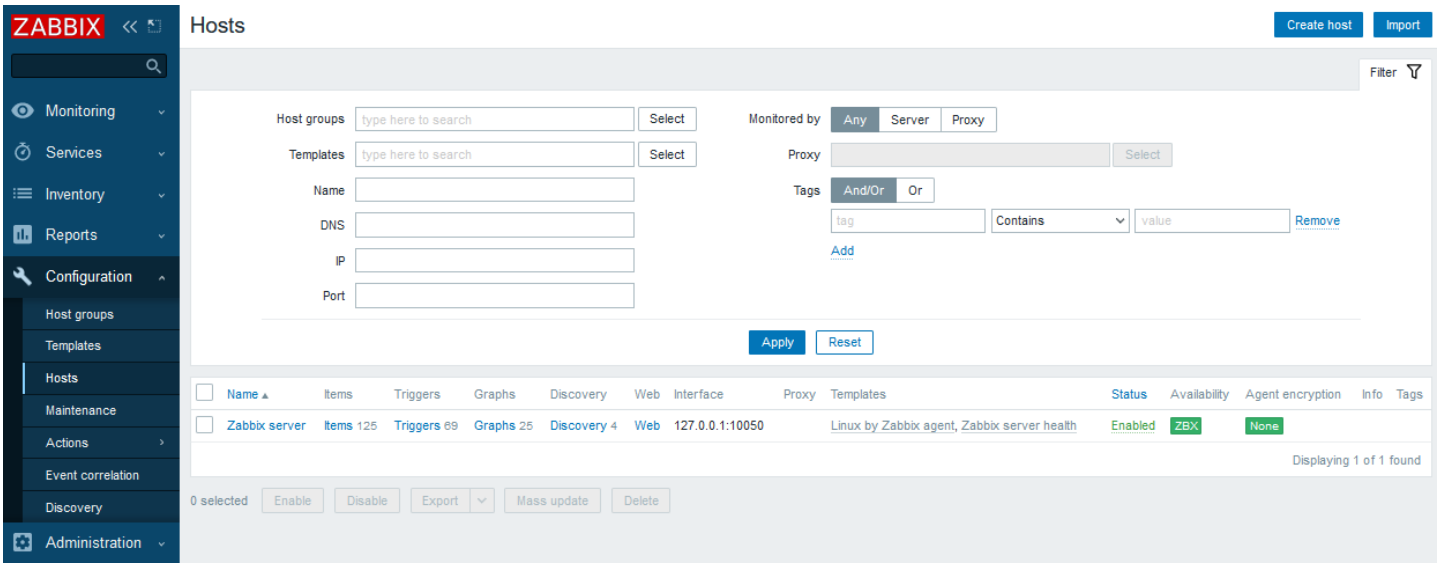


Figura 60: Conf. agente Zabbix Windows - Crear host Windows en el servidor Zabbix

Completamos la siguiente información y pulsamos **Add** para agregar el nuevo host:

- *Host name*: Escribimos el mismo nombre de equipo que se detalló en el campo *Hostname* del fichero de configuración del agente localizado en la máquina que se quiere monitorizar, p. ej. “PC-WINDSK”.
- *Visible name*: Escribimos el nombre que aparecerá en la lista de hosts del servidor Zabbix, p. ej. “Windows desktop”.
- *Templates*: Seleccionamos “Windows by Zabbix Agent”, que tiene preconfiguradas las principales alertas necesarias para una monitorización completa de un sistema operativo Windows.

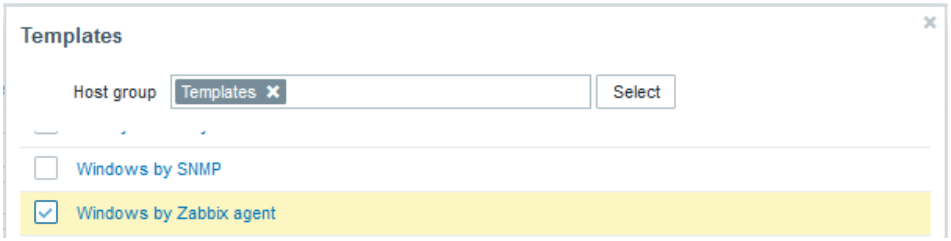


Figura 61: Conf. agente Zabbix Windows - Plantilla (Windows by Zabbix Agent)

- *Groups*: Seleccionamos “Operating systems” (para equipos) o “Linux server” (para servidores).
- *Interfaces*: Seleccionamos “Agent” y escribimos en *IP address*, la dirección IP del equipo que se quiere monitorizar, p. ej. “192.168.0.182”.

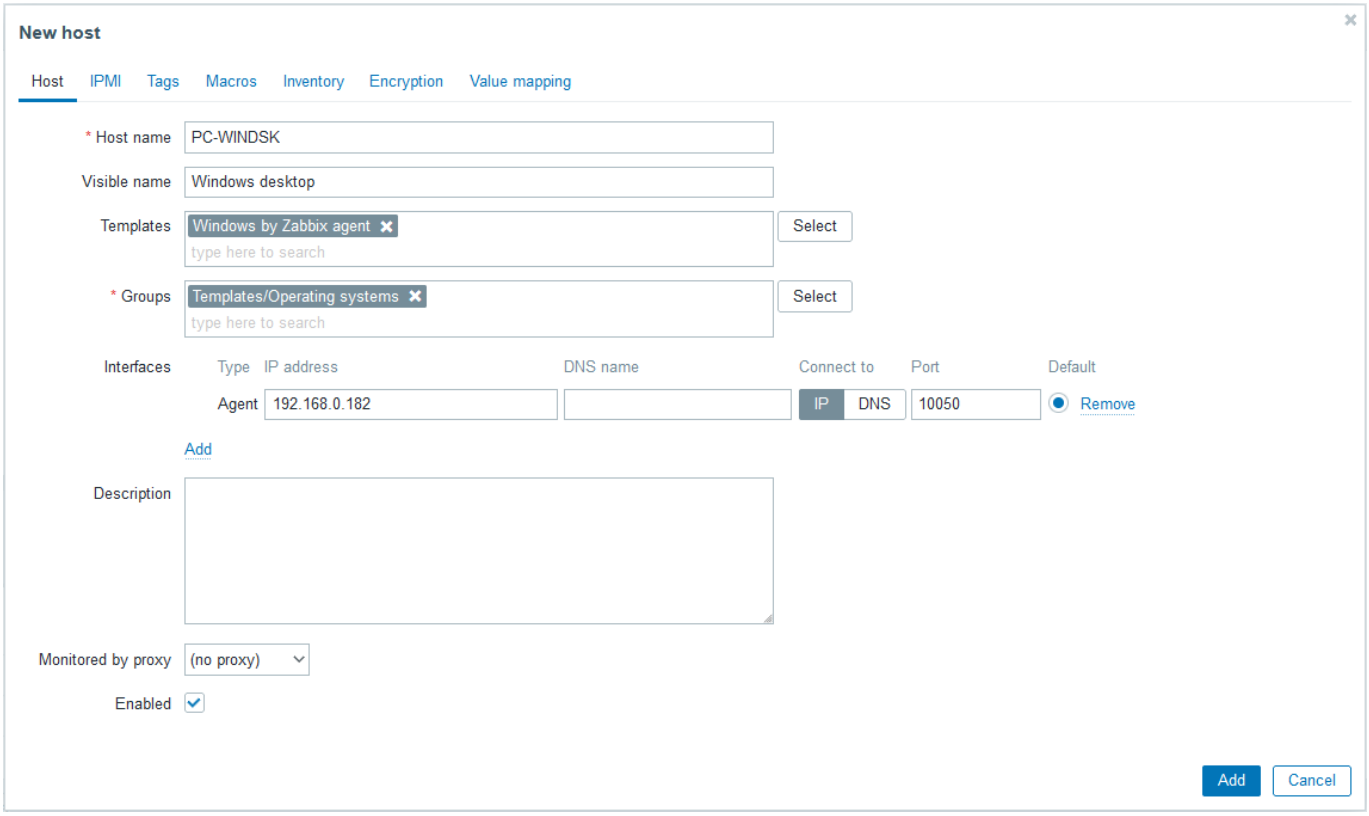


Figura 62: Conf. agente Zabbix Windows - Agregar host Windows al servidor Zabbix

Anexo VIII: Creación de scripts para la generación de alertas

Para la generación de alertas en el sistema de monitorización, se crea un script que se ejecutará sobre sistemas Windows con Powershell y otro sobre sistemas Linux con Bash.

A continuación, se muestra el código de ambos scripts, así como el procedimiento para ejecutarlo:

- **Script para generar alertas en sistemas Windows**

  Al ejecutar este script se muestra un menú donde se puede seleccionar el componente (CPU, RAM o disco) a sobrecargar del sistema Windows donde se ejecuta, que nos permitirá generar la alerta de ese componente específico.

  El nombre del script es "GenerarAlertasWIN.ps1" y para ejecutarlo hay que abrir una ventana de Powershell de Windows, en la que escribiremos la ruta donde se encuentra el archivo que contiene el código del script, por ejemplo, "C:\Scripts\GenerarAlertasWIN.ps1".

```
Function menu {
  Write-Host "1. CargaCPU"
  Write-Host "2. CargaRAM"
  Write-Host "3. LlenaDISCO"
  Write-Host "4. Salir`n"
}

Clear-Host
Write-Host ""
menu

while(($n = Read-Host -Prompt "Seleccione una de las opciones") -ne
"4"){

   switch($n){

      1 {Clear-Host

         Write-Host "`n*********  Carga de la CPU iniciada: $(Get-
         Date -format {dd/MM/yyyy HH:mm:ss})  *********"

         Write-Host "`nAumentando carga de la CPU, por favor espere
         ..."

         foreach ($i in 1..$ENV:NUMBER_OF_PROCESSORS){
            Start-Job -ScriptBlock{
               $res = 1
               foreach ($num in 1..0x1FFFFFFF){ $res *= $num }
            } | Out-Null
         }

         Read-Host -Prompt "`nCarga de la CPU completa, pulse
         cualquier tecla para finalizar y liberar"

         Receive-Job *
         Stop-Job *
         Remove-Job *

         Write-Host "*********  Carga de la CPU finalizada: $(Get-
         Date -format {dd/MM/yyyy HH:mm:ss})  *********`n`n"

         Break
      }
```

```
2 {Clear-Host

    $memSO=512
    $Global:memTotal = ((Get-CimInstance
    Win32_ComputerSystem).TotalPhysicalMemory / 1024) / 1024
    $memMax = $memTotal - $memSO

    $memDisp = new-object
    System.Diagnostics.PerformanceCounter("Memory","Available
    Mbytes")
    $memDisp.NextValue() | Out-Null
    $memRAM = $memTotal - $memDisp.NextValue()

    $avance = ($memRAM / $memMax) * 100
    $completado  = [int]$avance

    Write-Host "`n*********  Carga de la memoria RAM iniciada:
    $(Get-Date -format {dd/MM/yyyy HH:mm:ss})  *********"

    Write-Host "`nAumentando carga de la memoria RAM, por favor
    espere ..."

    $a1 = @()
    $a2 = @()
    $a2 += "a" * 200MB
    $cont = 0
    $ultCompletado = 900

    while ($memRAM -lt $memMax) {
       $a1 += ,@($cont, $a2)
       $a2 += "a" * 200MB
       $cont += 1
       $memRAM = $memTotal - $memDisp.NextValue()
       $avance = ($memRAM / $memMax) * 100
       $completado  = [int]$avance

       if ($completado -ne $ultCompletado) {
          $ultCompletado = $completado
       }
    }

    Read-Host -Prompt "`nCarga de la memoria RAM completa, pulse
    cualquier tecla para finalizar y liberar"

    $a1.clear()
    $a2.clear()
    [System.GC]::Collect()

    Write-Host "*********  Carga de la memoria RAM finalizada:
    $(Get-Date -format {dd/MM/yyyy HH:mm:ss})  *********`n`n"

    break
}

3 {Clear-Host

    $temp = "C:\Scripts\temp"
    $discoSO = 2048
    $discoLibre = ((Get-Volume -DriveLetter C).SizeRemaining /
    1024) / 1024
    $cont = 1

    Write-Host "`n*********  Carga de datos en disco iniciada:
    $(Get-Date -format {dd/MM/yyyy HH:mm:ss})  *********"

    Write-Host "`nCargando datos en disco, por favor espere ..."

    if (Test-Path $temp){
       Remove-item $temp -Recurse
    }
    New-Item $temp -Type Directory | Out-Null
```

```
            while ( $discoSO -lt $discoLibre) {
                fsutil file createnew $temp\archivo$cont 536870912 | Out-
                Null

                $discoLibre = ((Get-Volume -DriveLetter C).SizeRemaining
                / 1024) / 1024

                $cont += 1
            }

            Read-Host -Prompt "`nCarga de datos en disco completa, pulse
            cualquier tecla para finalizar y liberar"

            Remove-item $temp -Recurse

            Write-Host "*********  Carga de datos en disco finalizada:
            $(Get-Date -format {dd/MM/yyyy HH:mm:ss})  *********`n`n"

            break
        }

        default {
            Write-Host -ForegroundColor red "`nOpción no válida`n`n";
        }

    }

    menu

}
```

Figura 63: Creación script - Script para generar alertas en sistemas Windows

- **Script para generar alertas en sistemas Linux**

  Al ejecutar este script se muestra un menú donde se puede seleccionar el componente (CPU, RAM o disco) a sobrecargar del sistema Linux donde se ejecuta, que nos permitirá generar la alerta de ese componente específico.

  El nombre del script es “GenerarAlertasLNX.sh” y para ejecutarlo hay que abrir una ventana de Terminal de Ubuntu, en la que escribiremos la palabra “bash” seguido de la ruta donde se encuentra el archivo que contiene el código del script, por ejemplo, “bash ~/Scripts/GenerarAlertasLNX.sh”.

```
#!/bin/bash

cargaCPU(){
    echo -e
    read -p "Tiempo en segundos que desea que dure la carga de la CPU: " t

    echo -e "\n*********  Carga de la CPU iniciada: $(date +"%d/%m/%Y
    %H:%M:%S")  *********"

    echo -e "\nEl proceso durará $tiempo segundos, pulse CTRL+C para
    finalizar y liberar\n"

    stress --cpu 2 --timeout $t >/dev/null 2>&1

    echo -e "*********  Carga de la CPU finalizada: $(date +"%d/%m/%Y
    %H:%M:%S")  *********\n\n"
}
```

```
cargaRAM(){
   echo -e
   read -p "Tiempo en segundos que desea que dure la carga de la RAM: " t

   echo -e "\n*********  Carga de la memoria RAM iniciada: $(date
   +"%d/%m/%Y %H:%M:%S")  *********"

   echo -e "\nEl proceso durará $tiempo segundos, pulse CTRL+C para
   finalizar y liberar\n"

   stress --vm 4 --vm-bytes 1024M --timeout $t >/dev/null 2>&1

   echo -e "*********  Carga de la memoria RAM finalizada: $(date
   +"%d/%m/%Y %H:%M:%S")  *********\n\n"
}

llenaDISCO(){
   temp="/home/tfg/Scripts/temp"
   discoSO=1024
   discoLibre=$(($(df -kh . -B 1 | tail -n1 | awk '{print $4}') / 1024 /
   1024))
   cont=1

   echo -e "\n*********  Carga de datos en disco iniciada: $(date
   +"%d/%m/%Y %H:%M:%S")  *********"

   echo -e "\nCargando datos en disco, por favor espere ...\n"

   if [ -d $temp ]
   then
      rm -r $temp
   fi

   mkdir $temp
   chmod 777 $temp

   while [ $discoSO -lt $discoLibre ]
   do
      fallocate -l 512M $temp/archivo$cont
      discoLibre=$(($(df -kh . -B 1 | tail -n1 | awk '{print $4}') / 1024
      / 1024))
      cont=$((cont + 1))
   done

   read -p "Carga de datos en disco completa, pulse cualquier tecla para
   finalizar y liberar" -n 1 -s

   rm -r $temp

   echo -e "\n\n*********  Carga de datos en disco finalizada: $(date
   +"%d/%m/%Y %H:%M:%S")  *********\n\n"
}

echo -e
opciones=("CargaCPU" "CargaRAM" "LlenaDISCO" "Salir")

PS3="Seleccione una de las opciones: "

while true; do
   select opcion in "${opciones[@]}"
   do
      case $REPLY in
         1) cargaCPU; break;;
         2) cargaRAM; break;;
         3) llenaDISCO; break;;
         4) echo -e "\n"; exit; break;;
         *) echo "Opción no valida"; break;
      esac
   done
done
```

Figura 64: Creación script - Script para generar alertas en sistemas Linux

Anexo IX: Instalación sistema de ticketing (GLPI 10.0.6)

Pasos a realizar para la instalación de GLPI 10.0.6

1. Instalar los repositorios necesarios para la instalación de GLPI.

   Instalamos y actualizamos los repositorios que posteriormente nos permitirán realizar la instalación de GLPI.

```
sudo su (Para entrar en modo root, realizamos la validación)

apt install -y software-properties-common apt-transport-https

add-apt-repository ppa:ondrej/php -y
apt update && apt upgrade
```

2. Instalar y configurar servidor web Apache.

   Instalamos el servidor web Apache.

```
apt -y install apache2 libapache2-mod-php8.0
```

   Una vez instalado, abrimos el archivo de configuración de Apache donde realizaremos unas modificaciones.

```
nano /etc/apache2/apache2.conf
```

   Tras localizar la sección a modificar sustituimos las palabras “None” por “All”.

```
<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride ~~None~~ All
        Require all granted
</Directory>
```

   Guardamos y salimos del archivo (pulsamos la combinación **ctrl** + **x** para solicitar la salida del archivo, después escribimos la letra **y** para confirmar que se quiere guardar los cambios y finalmente pulsamos **Enter**).

3. Instalar PHP 8.0 para Apache.

   Instalamos PHP 8.0 y reiniciamos el servidor Apache.

```
apt install php8.0 php8.0-common libapache2-mod-php8.0 php8.0-cli
systemctl restart apache2.service
```

Habilitamos PHP-FPM (acrónimo de Fast CGI Process Manager), reiniciamos y recargamos el servidor Apache.

```
apt install php8.0-fpm php8.0-common libapache2-mod-fcgid php8.0-cli

systemctl restart apache2.service

a2enmod proxy_fcgi setenvif && sudo a2enconf php8.0-fpm

systemctl restart apache2.service
systemctl reload apache2.service
```

Instalamos módulos de PHP.

```
apt -y install php8.0 php8.0-{curl,gd,imagick,intl,apcu,memcache,imap}

apt -y install php8.0 php8.0-{mysql,ldap,tidy,xmlrpc,pspell,gettext}

apt -y install php8.0 php8.0-{mbstring,fpm,iconv,xml,gd,xsl,bz2,zip}
```

4. Configurar la base de datos que usará GLPI.

   a. Instalamos la base de datos (MariaDB 10.6).

   ```
   apt install software-properties-common -y
   ```

   ```
   curl -LsS -O https://downloads.mariadb.com/MariaDB/mariadb_repo_setup

   bash mariadb_repo_setup --mariadb-server-version=10.6
   ```

   ```
   apt update

   apt -y install mariadb-common mariadb-server-10.6 mariadb-client-10.6
   ```

   Iniciamos el servicio de MariaDB y habilitamos el inicio al arranque del sistema.

   ```
   systemctl start mariadb

   systemctl enable mariadb
   ```

   b. Restablecemos la contraseña *root* para la base de datos.

   Rellenamos los siguientes datos:

   - *New Password*: Escribimos la nueva contraseña, p. ej. “passDBroot”.
   - *Re-enter new Password*: Volvemos a escribir la contraseña.

```
mysql_secure_installation
```

```
Enter current password for root (enter for none): Pulsar Enter

Switch to unix_socket authentication [Y/n] Y

Change the root password? [Y/n] Y

New password: passDBroot
Re-enter new password: passDBroot

Remove anonymous users? [Y/n] Y

Disallow root login remotely? [Y/n] Y

Remove test database and access to it? [Y/n] Y

Reload privilege tables now? [Y/n] Y
```

c. Creamos la base de datos.

```
mysql -uroot -p'passDBroot' -e "CREATE DATABASE glpi character set
utf8mb4 collate utf8mb4_bin;"

mysql -uroot -p'passDBroot' -e "GRANT ALL PRIVILEGES ON glpi.* TO
glpi@localhost IDENTIFIED BY 'passDBglpi';"
```

5. Preparar la instalación de GLPI.

a. Descargamos la versión de GLPI que queramos instalar, en nuestro caso la última disponible que es la 10.0.6.

```
wget https://github.com/glpi-
project/glpi/releases/download/10.0.6/glpi-10.0.6.tgz
```

Movemos el archivo descargado a la ruta "/var/www/glpi" y lo desempaquetamos.

```
mv glpi-10.0.6.tgz /var/www/
tar -zxvf /var/www/glpi-10.0.6.tgz
```

Tras desempaquetar tendremos una carpeta llamada "glpi" donde estarán los paquetes de instalación.

b. Configurar Apache para que funcione en el navegador y localice la ruta donde se encuentra GLPI.

Conservamos el archivo con la configuración por defecto por si fuera necesario restaurarlo.

```
mv /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-
available/000-default.conf.backup
```

Creamos un nuevo archivo de configuración llamado “glpi.conf”.

```
nano /etc/apache2/sites-available/glpi.conf
```

Agregamos las siguientes líneas al archivo de configuración “glpi.conf”.

```
<VirtualHost *:80>
        ServerAdmin Admin
         DocumentRoot /var/www/glpi/
         ServerName sv-ubusrv-glpi
         ServerAlias sv-ubusrv-glpi

         ErrorLog ${APACHE_LOG_DIR}/error.log
         CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Guardamos y salimos del archivo (pulsamos la combinación **ctrl** + **x** para solicitar la salida del archivo, después escribimos la letra **y** para confirmar que se quiere guardar los cambios y finalmente pulsamos **Enter**).

c. Crear un enlace simbólico.

Una vez creado el archivo de configuración “glpi.conf” es necesario generar un enlace simbólico de este, en la ruta “/etc/apache2/sites-enabled”.

```
ln -s /etc/apache2/sites-available/glpi.conf /etc/apache2/sites-
enabled/glpi.conf
```

d. Modificar permisos sobre el directorio “/var/www/glpi”.

Modificamos los permisos sobre el directorio “/var/www/glpi” y reiniciamos el servidor Apache.

```
chown -R www-data:www-data /var/www/glpi
chmod -R 755 /var/www/glpi

systemctl restart apache2.service
```

6. Realizar la instalación de GLPI desde la interfaz web.

Nos conectamos a la interfaz de GLPI usando la URL “http://IP del servidor GLPI” para iniciar el asistente de instalación de GLPI.

La IP del servidor GLPI en este caso es 192.168.0.190, que es la IP asignada al servidor Ubuntu server que contendrá la aplicación de GLPI, por lo que la URL de acceso será “http://192.168.0.190”.

En la pantalla de bienvenida seleccionamos el idioma por defecto “Español (España)”, después pulsamos **Correcto** para avanzar.

Figura 65: Instalación GLPI - Pantalla de inicio de instalación de GLPI

En la siguiente pantalla simplemente pulsamos **Continuar** para aceptar la licencia.

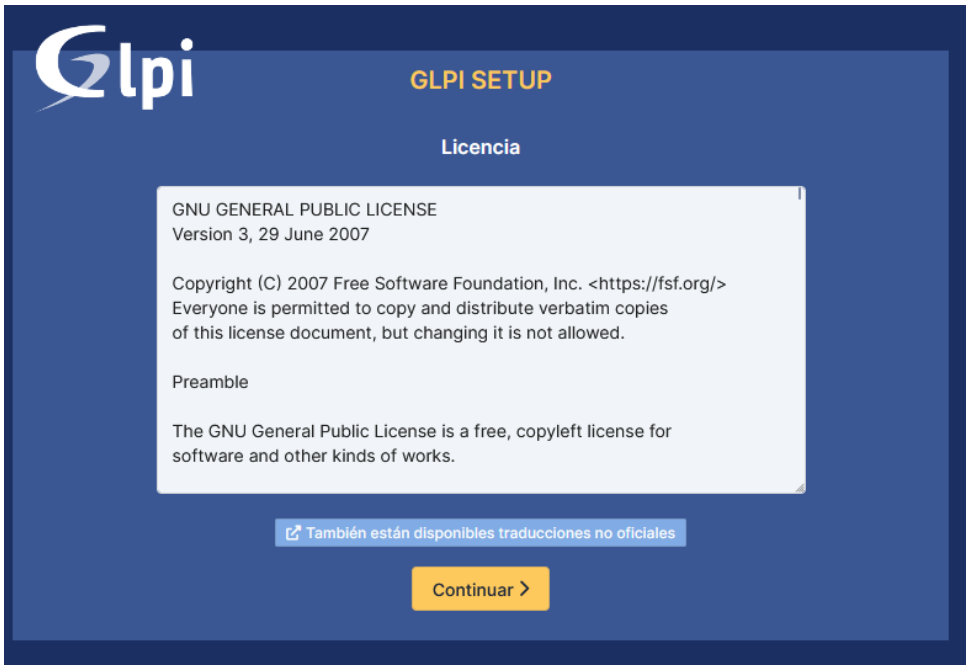


Figura 66: Instalación GLPI - Aceptación de licencia de GLPI

En la siguiente pantalla pulsamos **Instalar** para comenzar la instalación.

Figura 67: Instalación GLPI - Comienzo de la instalación de GLPI

En la siguiente pantalla verificamos que se cumplen todos los requisitos y el entorno es compatible con la ejecución de GLPI. Sí todo está correcto, pulsamos **Continuar** para avanzar.

Figura 68: Instalación GLPI - Paso 0 (Verificación del entorno)

En la siguiente pantalla configuramos la conexión con la base de datos, para ello rellenamos los siguientes datos y pulsamos **Continuar** para avanzar:

- *Servidor SQL (MariaDB o MySQL)*: Escribimos la dirección IP del servidor donde se encuentra la base de datos. En este caso la base de datos se encuentra en el mismo servidor que GLPI, por lo que escribiremos "localhost".
- *Usuario SQL*: Escribimos usuario de la BD de GLPI, p. ej. "glpi".
- *Contraseña SQL*: Escribimos contraseña de la BD de GLPI, p. ej. "passDBglpi".

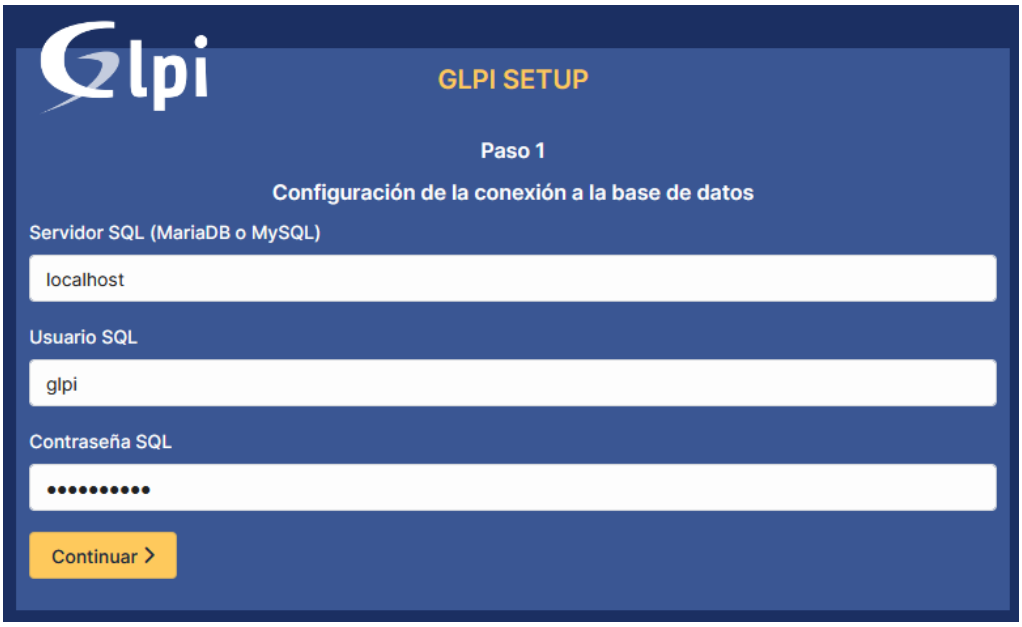


Figura 69: Instalación GLPI - Paso 1 (Datos para la conexión a la base de datos)

En la siguiente pantalla verificamos la conexión a la base de datos, si es correcta seleccionamos la base de datos que creamos anteriormente y pulsamos **Continuar** para avanzar.

Figura 70: Instalación GLPI - Paso 2 (Seleccionar la base de datos para GLPI)

En la siguiente pantalla debemos observar que la inicialización de la base de datos sea correcta. Sí es correcta, pulsamos **Continuar** para avanzar.

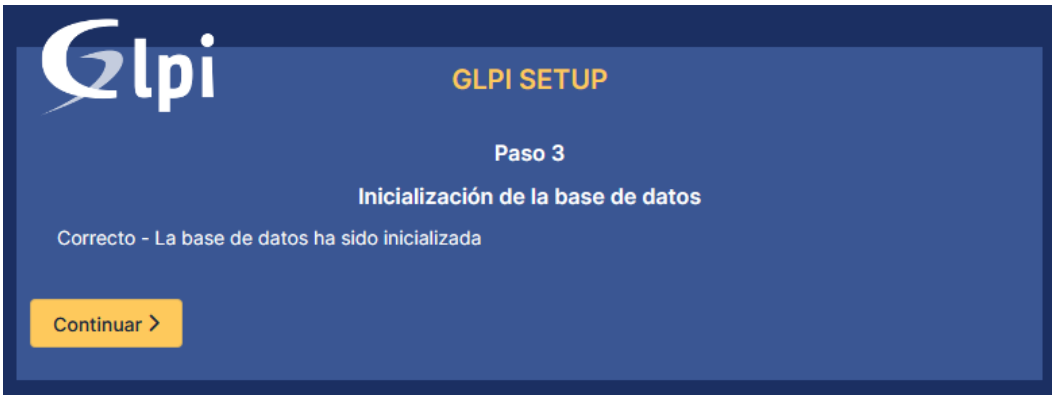


Figura 71: Instalación GLPI - Paso 3 (Inicialización de la base de datos de GLPI)

En la siguiente pantalla debemos valorar si queremos enviar datos estadísticos al sitio web de telemetría de GLPI, marcando la casilla “Enviar estadísticas de uso” en caso afirmativo y dejándola sin marcar en caso negativo, después pulsamos **Continuar** para avanzar.

Figura 72: Instalación GLPI - Paso 4 (Envío de datos estadísticos de uso)

En la siguiente pantalla veremos información sobre un servicio comercial ofrecido por GLPI pero que en este caso no usaremos, así que pulsamos **Continuar** para avanzar.

Figura 73: Instalación GLPI - Paso 5 (Información sobre servicio adicional de pago)

En la última pantalla podemos observar un mensaje indicando que la instalación de GLPI ha acabado correctamente y nos muestra los distintos perfiles con su correspondiente usuario y contraseña creados por defecto al realizar la instalación y que nos permitirá el acceso. Una vez revisada la información anterior pulsamos **Utilizar GLPI** para finalizar.

Figura 74: Instalación GLPI - Paso 6 (Finalización de la instalación de GLPI)

7. Iniciar sesión en la interfaz de GLPI utilizando las credenciales de inicio de sesión predeterminadas.

   Para iniciar sesión en GLPI accedemos a la URL “http://192.168.0.190” a través del navegador utilizando el usuario administrador “glpi” y la contraseña “glpi”.

Figura 75: Instalación GLPI - Inicio de sesión en GLPI

Una vez accedemos a la URL anterior usando el usuario y contraseña de administrador, podremos ver el tablero de la herramienta de ticketing GLPI.

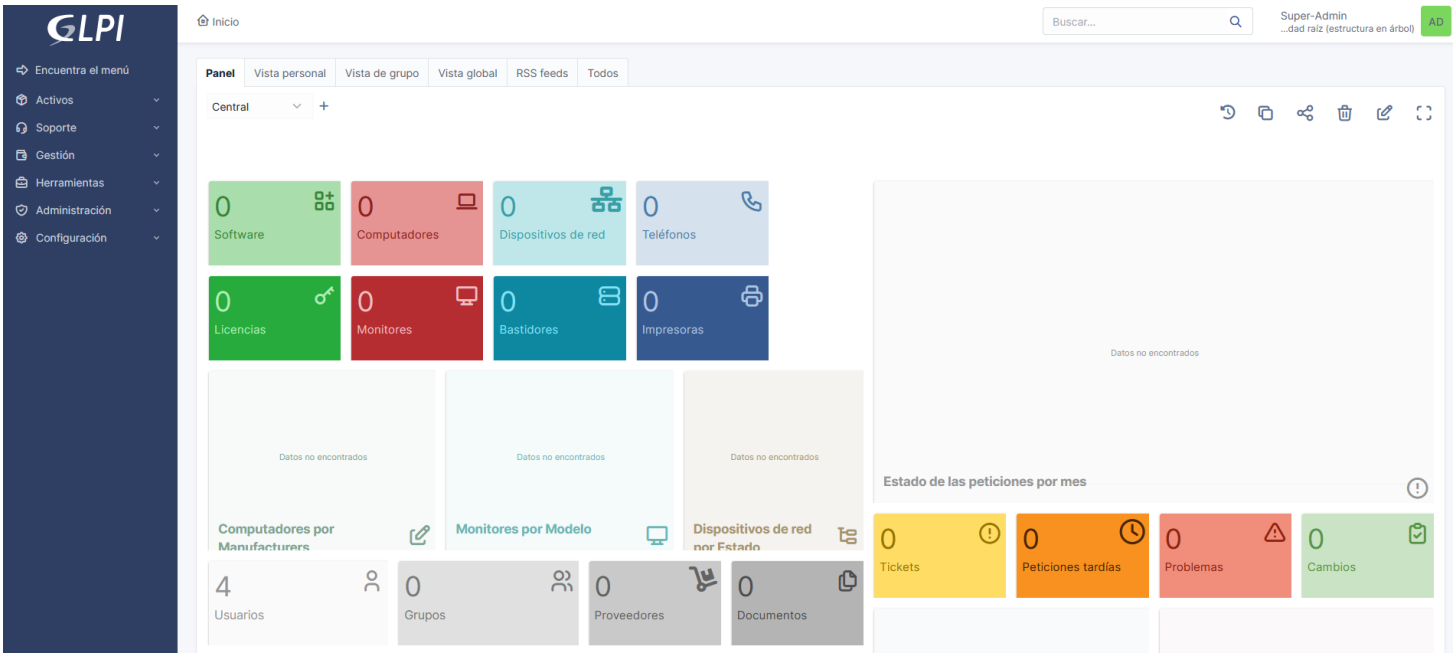


Figura 76: Instalación GLPI - Tablero de GLPI

Anexo X: Configuración sistema de ticketing (GLPI 10.0.6)

Pasos a realizar para la configuración de GLPI 10.0.6

A continuación, se muestran los pasos que permitirán la configuración de la herramienta de ticketing:

- **Creación de perfiles**

  Creamos los perfiles con sus respectivos permisos, que permitirán a los distintos tipos de usuarios realizar configuraciones en la herramienta GLPI.

  Para configurar los perfiles de usuario y asignarle sus correspondientes permisos, pulsamos en el menú de la izquierda del tablero de GLPI "Administración – Perfiles" y configuramos los siguientes perfiles:

  - *Coordinador:* Es el perfil con menos restricciones y puede ser perfectamente super administrador de GLPI. Este perfil puede ver y gestionar otros perfiles, grupos o usuarios existentes, activos e inventario de la organización, estado de las incidencias e indicadores gráficos con datos descriptivos.
  - *Técnico de primer nivel o L3:* Es un perfil también con pocas restricciones, muy parecido al del coordinador y puede ser administrador de GLPI, aunque con algunas opciones restringidas como estadísticas o que estén más enfocadas en la coordinación del departamento y que no necesitan.
  - *Técnico de segundo nivel o L2:* Este perfil puede consultar los usuarios que existen, activos e inventario de la organización, estado de las incidencias y algunos indicadores gráficos con datos importantes.
  - *Técnico de tercer nivel o L3:* Este perfil solo puede consultar y gestionar el estado de las incidencias.
  - *Usuario:* Este perfil con más limitaciones de todos y solo pueden abrir tickets para comunicar incidencias.

- **Tableros de la herramienta GLPI correspondientes a los distintos perfiles**

  Una vez configurado los perfiles, tanto el perfil *Coordinador* como el de *Técnico de tercer nivel,* tendrán una visión completa del sistema y las gestiones que pueden realizar. En la siguiente imagen podemos observar el tablero correspondiente a estos perfiles y solo editable por ellos, pudiendo añadir más tarjetas o pequeñas aplicaciones que facilitarán la visualización de los datos.

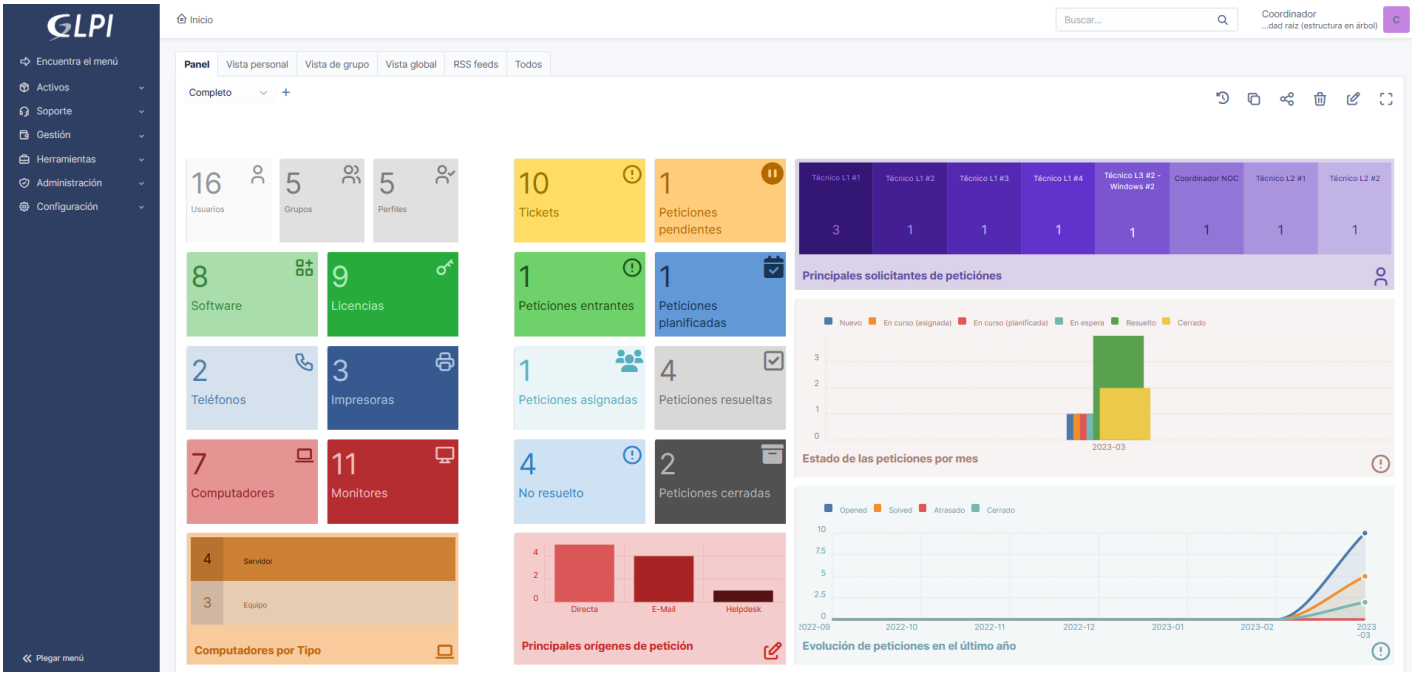


Figura 77: Conf. GLPI - Tablero GLPI para el coordinador y técnicos de tercer nivel

El perfil *Técnico de segundo nivel* tendrá una visión del tablero más reducida que los perfiles anteriores. En la siguiente imagen podemos observar el tablero correspondiente a este perfil.

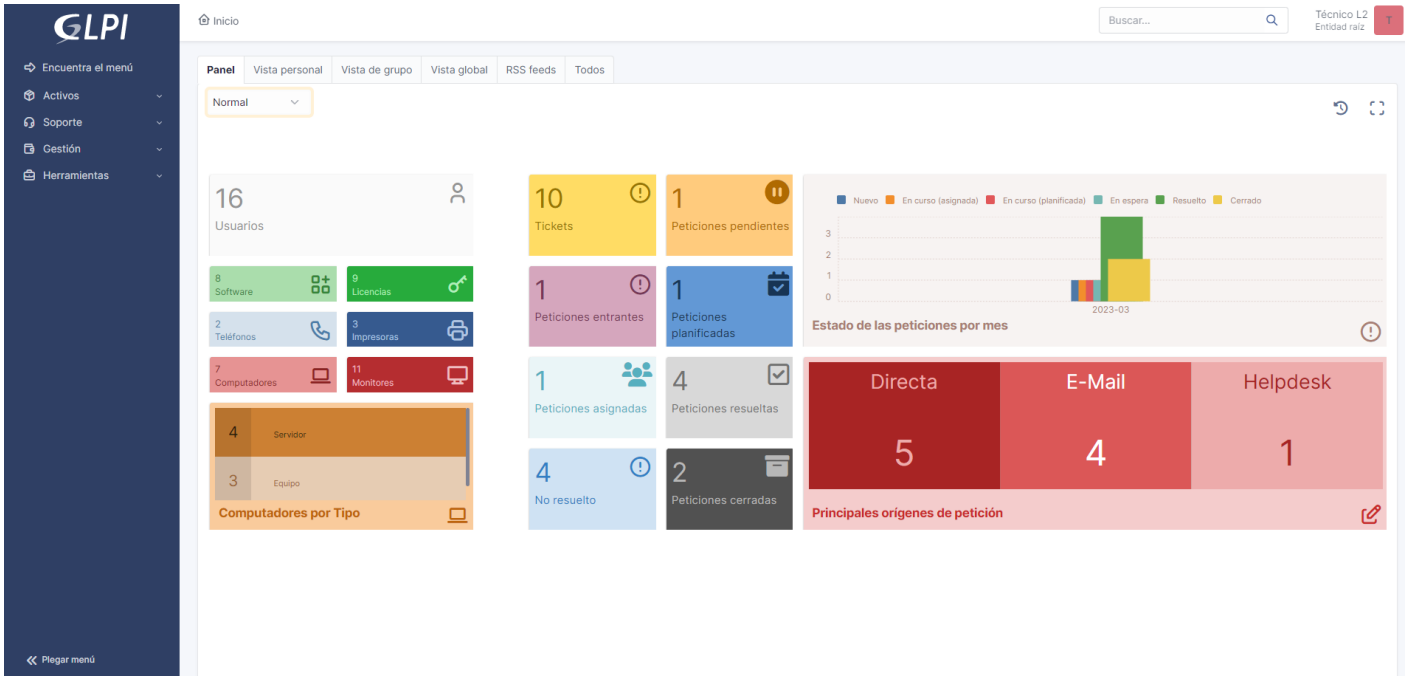


Figura 78: Conf. GLPI - Tablero GLPI para los técnicos de segundo nivel

El perfil *Técnico de primer nivel* tendrá una visión básica que le permitirán la gestión de tickets. En la siguiente imagen podemos observar el tablero correspondiente a este perfil.

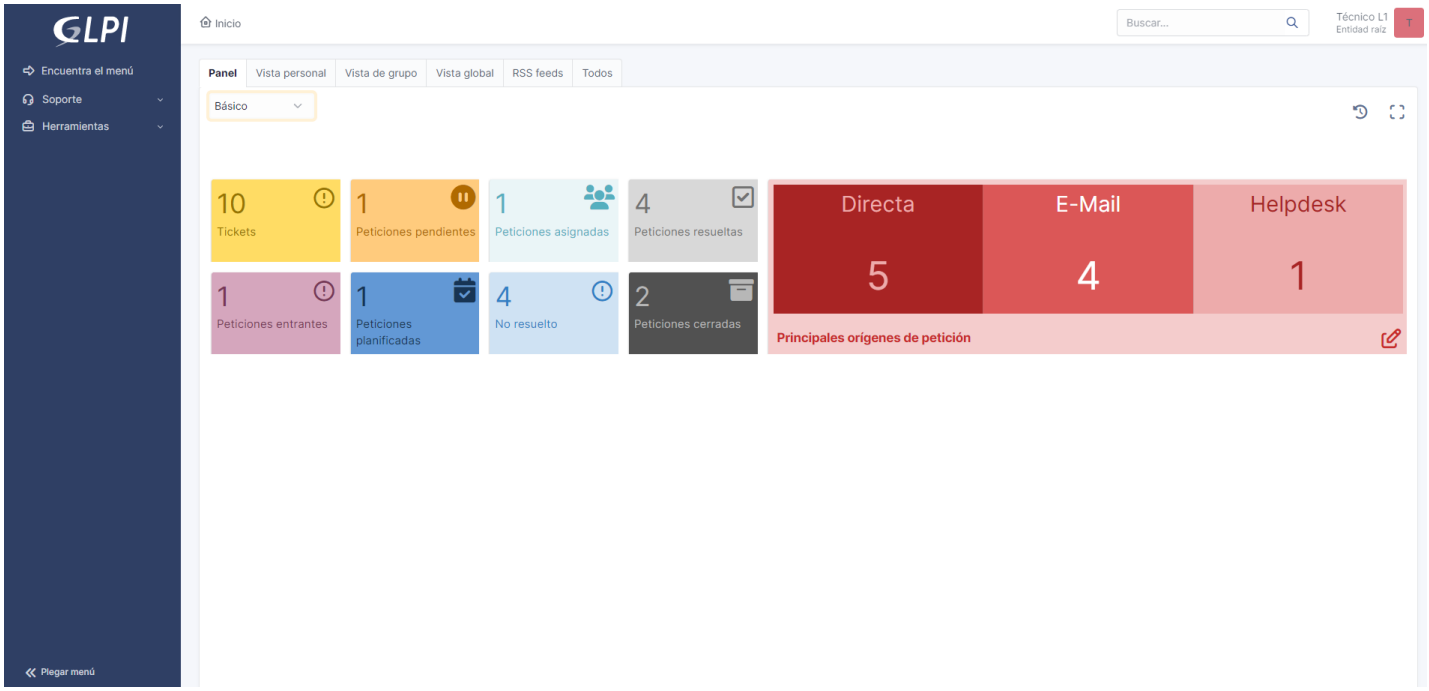


Figura 79: Conf. GLPI - Tablero GLPI para los técnicos de primer nivel

El perfil *Usuario* tendrá solo la opción de poder abrir tickets para comunicar incidencias. En la siguiente imagen podemos observar el tablero correspondiente a este perfil.

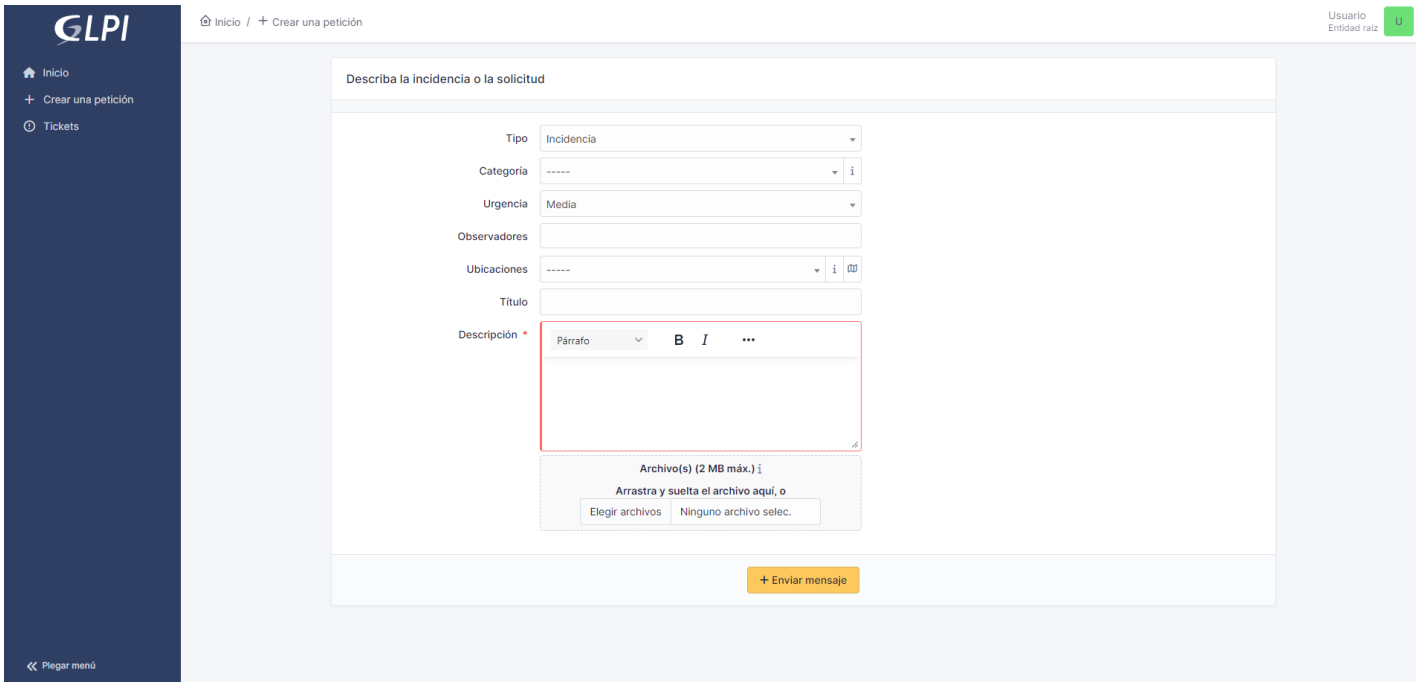


Figura 80: Conf. GLPI - Tablero GLPI para los usuarios

- **Asignación de perfiles a usuarios**

  Una vez creados los perfiles y asignados los respectivos permisos a dichos perfiles, pasamos a adjudicárselo a los usuarios. Cada usuario tendrá un perfil asignado y este le habilitará para realizar más o menos acciones en la herramienta GLPI.

  En primer lugar, creamos los usuarios pulsando en el menú de la izquierda del tablero de GLPI "Administración – Usuarios", para posteriormente mediante el propio menú de creación, asignarle uno de los perfiles ya creados y configurados al usuario que se desee.

- **Inserción de datos iniciales**

  La inserción de datos iniciales en la herramienta no es estrictamente necesario para el proceso de creación de tickets, permitiendo su uso desde que se realiza su instalación y se configura los perfiles de acceso.

  La herramienta GLPI también contiene otras funciones útiles, como es la del control de inventarios, a la que se ha añadido los recursos utilizados para la creación del piloto NOC y que podrá observarse en los niveles más altos de la jerarquía. También permitirá la identificación de algún sistema concreto en caso de incidencia o verificar si es necesario de adquirir algún tipo de componente.

Una vez realizada la inserción de datos principal y asignado un perfil al usuario, este podrá acceder a GLPI mediante un usuario con su correspondiente contraseña y tendrá permisos para realizar las acciones que el sistema le permita conforme a su perfil. Todos los perfiles pueden crear y gestionar tickets para resolver incidencias, ejecutar procedimientos o cualquier otra acción, excepto el perfil *Usuario* que solo tendrá la posibilidad de crear tickets nuevos.

En Anexo XV, Anexo XVI y Anexo XVII de este documento se pueden consultar varios ejemplos, donde se detalla el proceso de creación y gestión de tickets que nos ayudarán a comprender mejor el uso de la herramienta.

Anexo XI: Instalación herramienta de actualización WSUS

Pasos a realizar para la instalación de WSUS en Windows Server

1. Accedemos al servidor con sistema operativo Windows Server donde instalaremos WSUS, una vez dentro iniciamos el *Administrador del servidor* y pulsamos en "Administrar – Agregar roles y características".

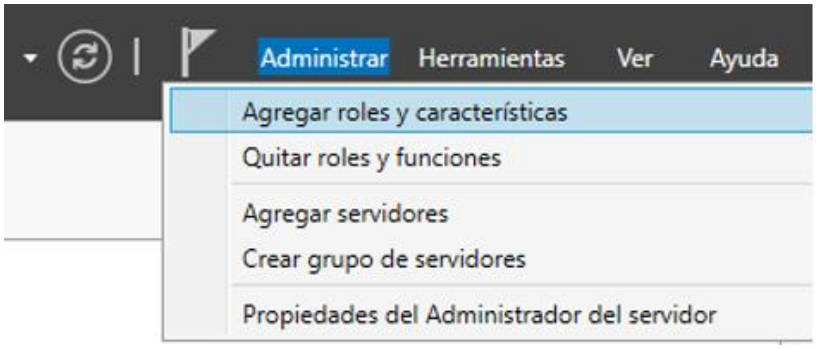


Figura 81: Instalación WSUS - Agregar roles y características

2. Una vez abierto el asistente que nos permitirá agregar roles y características, pulsamos en el botón **Siguiente**, dejando en los primeros pasos las opciones por defecto hasta llegar al paso "Roles de servidor", donde tendremos que seleccionar el rol que queremos instalar, en este caso "Windows Server Update Services".

   Una vez seleccionado el rol, pulsamos **Siguiente** hasta el paso "Contenido", dejando las opciones por defecto en los siguientes pasos.

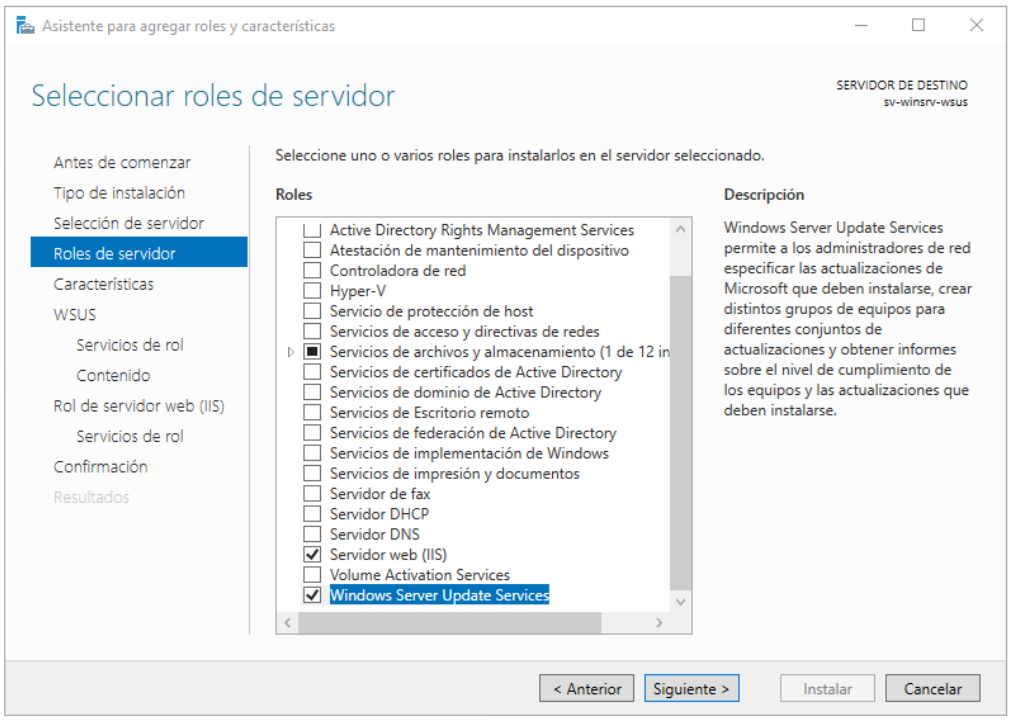


Figura 82: Instalación WSUS - Seleccionar rol Windows Server Update Services

3. Una vez llegamos al paso “Contenido”, escribimos la ubicación donde se descargará el repositorio de actualizaciones, en este caso será “C:\WSUS_repositorio”.

   Una vez escrita la ruta, pulsamos **Siguiente** hasta el paso “Confirmación”, dejando las opciones por defecto en los siguientes pasos.

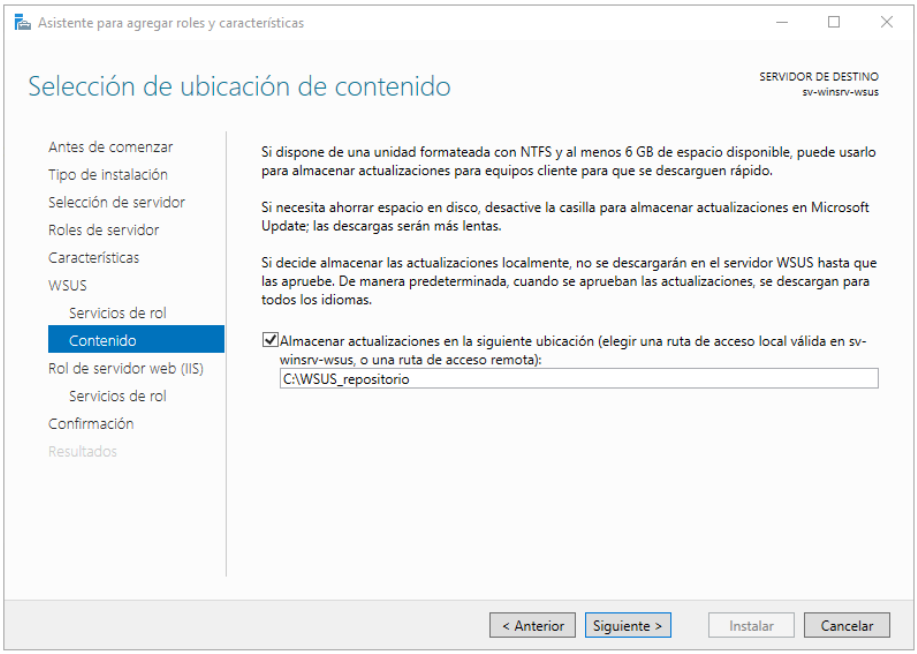


Figura 83: Instalación WSUS - Elegir la ubicación del repositorio de actualizaciones

4. Llegados al paso “Confirmación”, revisamos las selecciones realizadas antes de continuar y si todo es correcto pulsamos **Instalar** para realizar la instalación.

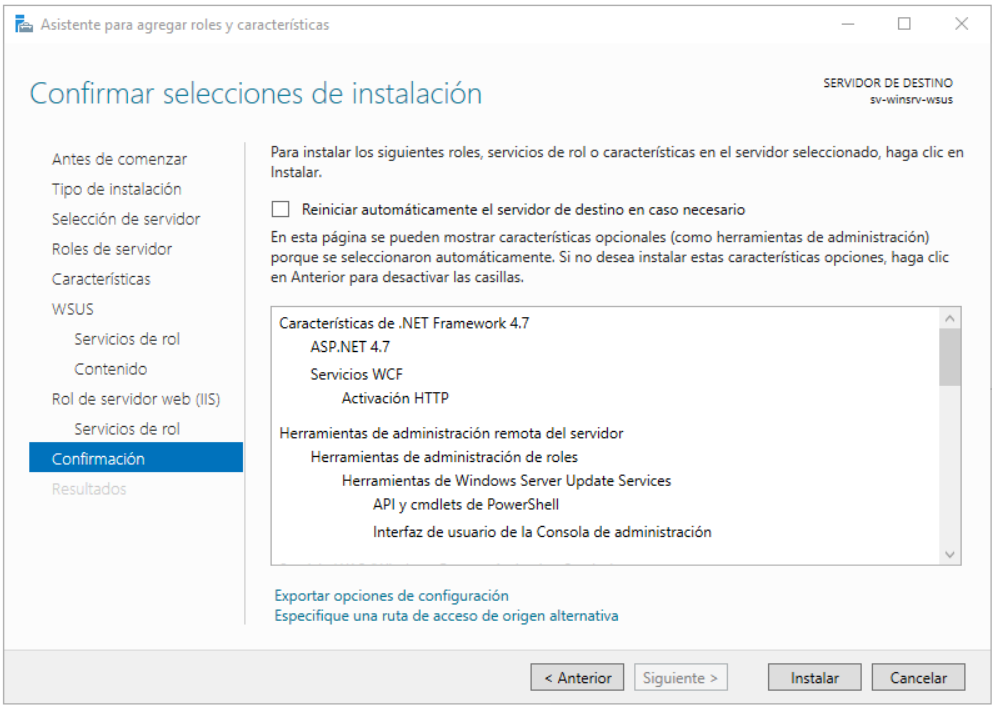


Figura 84: Instalación WSUS - Realizar instalación

Anexo XII: Configuración herramienta de actualización WSUS

Pasos a realizar para la configuración de WSUS en Windows Server

A continuación, se muestran los pasos que permitirán la configuración de la herramienta de actualización:

- **Configuración de WSUS para la descarga automática de actualizaciones**

  Tras abrir la consola de WSUS por primera vez, aparecerá un asistente que nos guiará con la configuración en la herramienta WSUS para la descarga de actualizaciones.

  Para que la descarga de actualizaciones en el repositorio de la herramienta se realice de forma correcta, debemos completar los siguientes pasos que numeraremos a continuación:

  1. Una vez abierto el asistente de configuración de WSUS, pulsamos en el botón **Siguiente**, dejando las opciones por defecto en los primeros pasos, hasta llegar al paso "Elegir idiomas", donde seleccionaremos el/los idioma/s de las actualizaciones que se van a descargar y pulsamos **Siguiente** para avanzar.

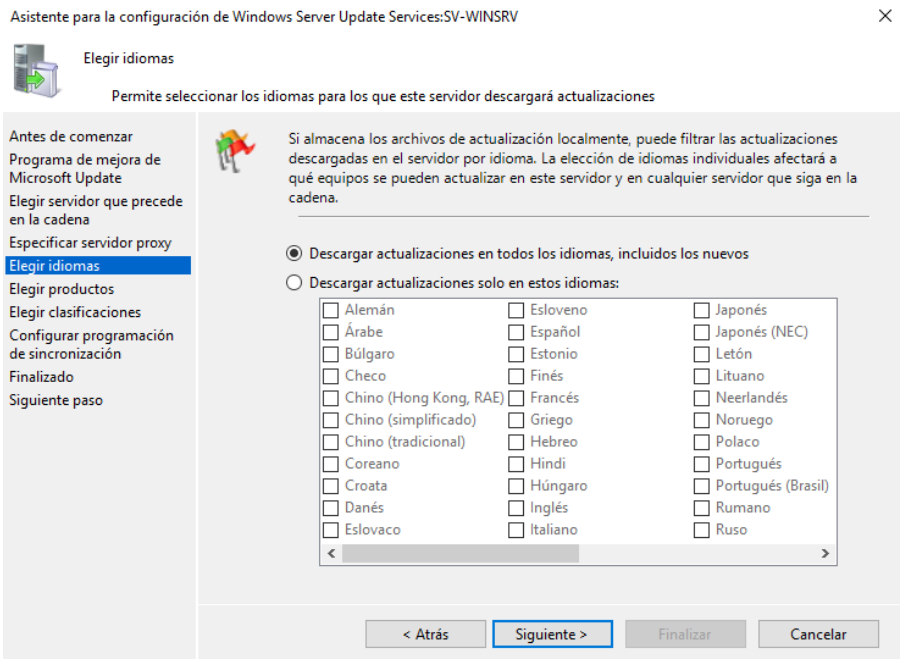


Figura 85: Conf. WSUS - Selección de idioma para la descarga de actualizaciones

2. En el siguiente paso “Elegir productos”, debemos seleccionar los productos que queremos actualizar, de los cuales se descargarán los correspondientes paquetes de actualizaciones y pulsamos **Siguiente** para avanzar.

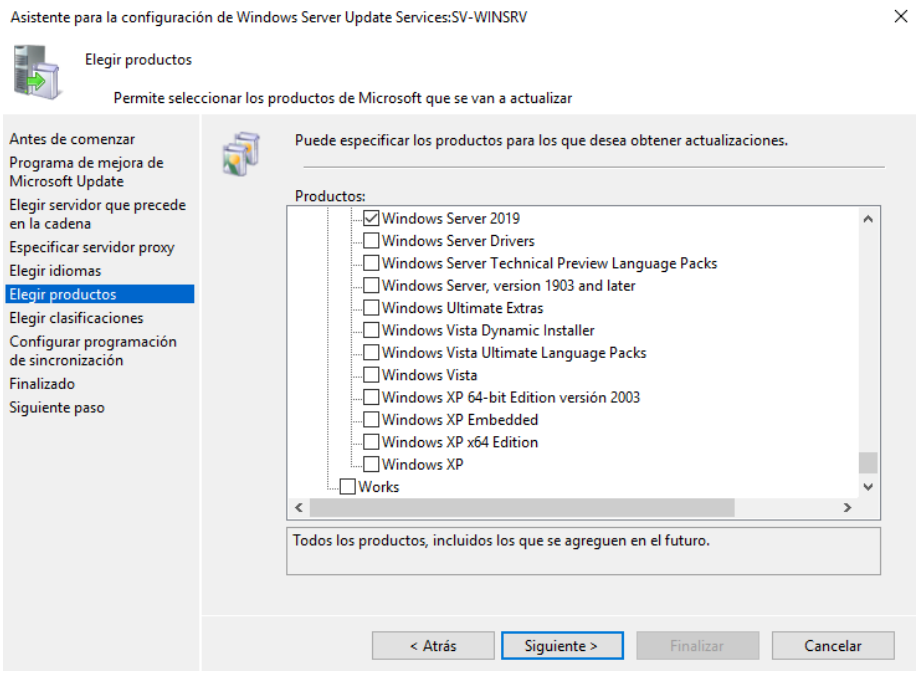


Figura 86: Conf. WSUS - Selección de productos para la descarga de actualizaciones

3. En el siguiente paso “Elegir clasificaciones”, debemos especificar el tipo de actualización que queremos descargar y pulsamos **Siguiente** para avanzar.

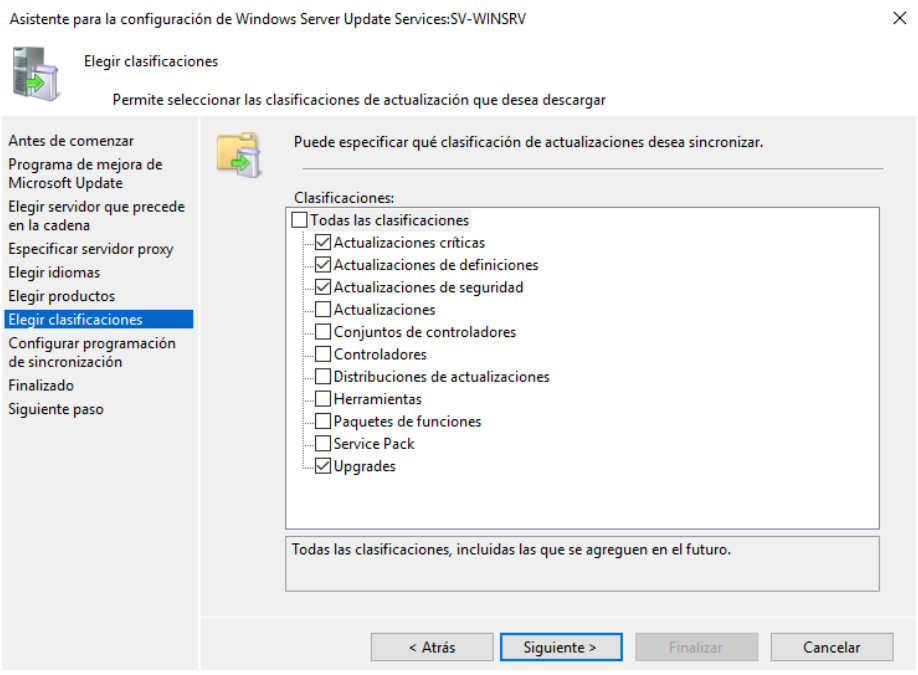


Figura 87: Conf. WSUS - Especificar los tipos de actualizaciones a descargar

4. En el siguiente paso “Configurar programación de sincronización”, debemos especificar el horario de sincronización de WSUS para la descarga de actualizaciones y pulsamos **Siguiente** para avanzar.

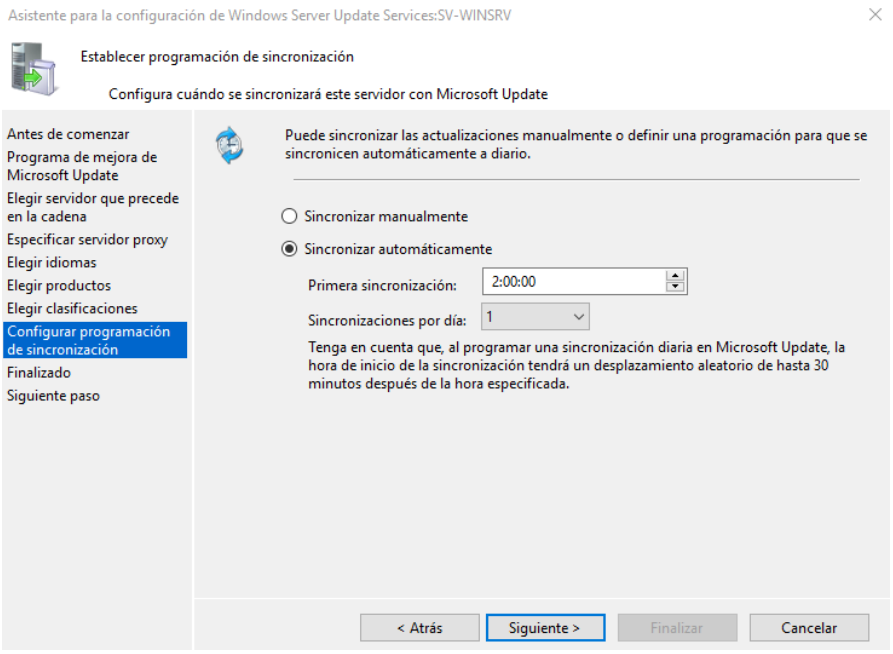


Figura 88: Conf. WSUS - Horario para la sincronización con el servidor de actualizaciones

5. En el siguiente paso “Finalizado”, debemos seleccionar si queremos realizar una primera sincronización de actualizaciones, teniendo en cuenta que la primera descarga de actualizaciones siempre necesita algo más de tiempo que las posteriores y pulsamos **Finalizar** para concluir la configuración.

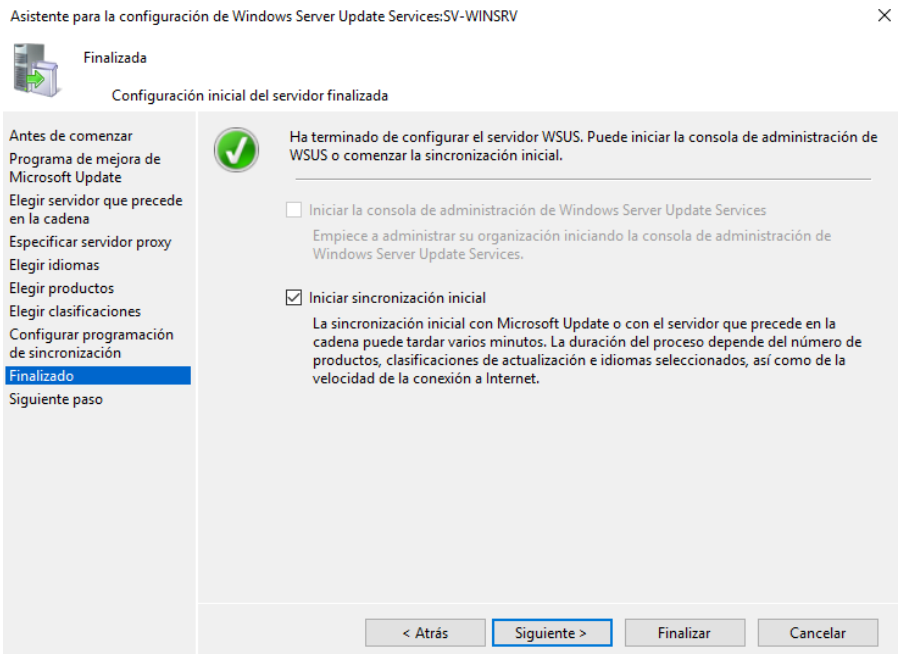


Figura 89: Conf. WSUS - Realizar sinc. inicial de actualizaciones y finalizar configuración

- **Comprobar que se están sincronizando las actualizaciones**

  Una vez configurada la descarga de actualizaciones, comprobamos que la tarea se está realizando.

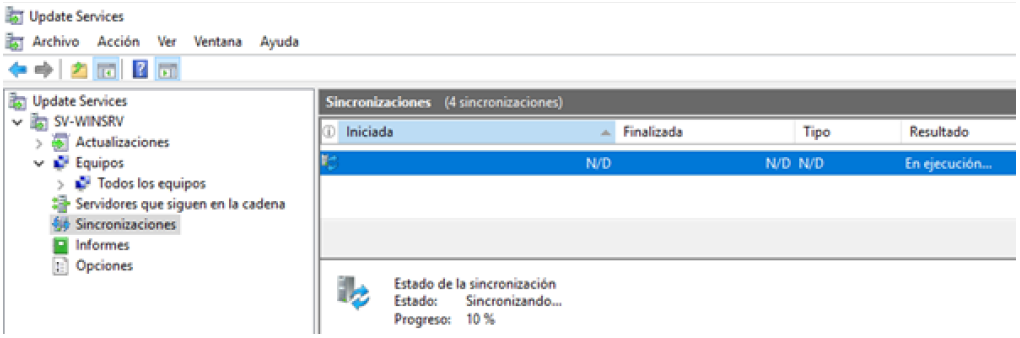


Figura 90: Conf. WSUS - Sincronización de actualizaciones

Tras comprobar que la sincronización se ha realizado, verificamos que finalmente las actualizaciones están descargadas en el repositorio de WSUS, para posteriormente poder ser instaladas.

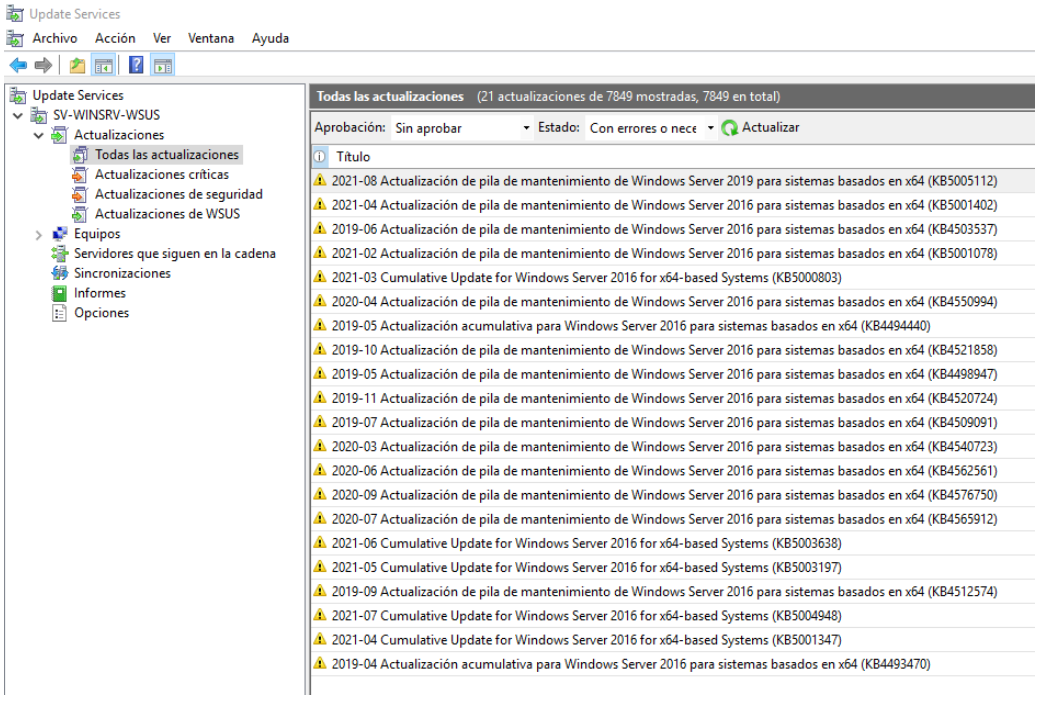


Figura 91: Conf. WSUS - Actualizaciones descargadas y listas para ser aplicadas

- **Configuración de los equipos Windows para que reporten a WSUS**

  Una vez configurada la descarga de actualizaciones y sincronizadas, es necesario que los equipos Windows que van a ser actualizados a través de WSUS, se comuniquen con la herramienta.

  Para que estos equipos se comuniquen con WSUS o reporten, es necesario realizar configuraciones en las políticas de cada equipo, pudiendo automatizar la acción mediante GPO o realizando una configuración inicial de los sistemas mediante un bastionado.

  Para comenzar con la configuración en los equipos, debemos acceder a las políticas del equipo Windows que queremos comunicar con WSUS. Para ello pulsamos **Windows** + **R** y escribimos "gpedit.msc". Una vez abiertas las políticas accedemos a "Configuración del equipo – Plantillas administrativas – Componentes de Windows – Windows Update".

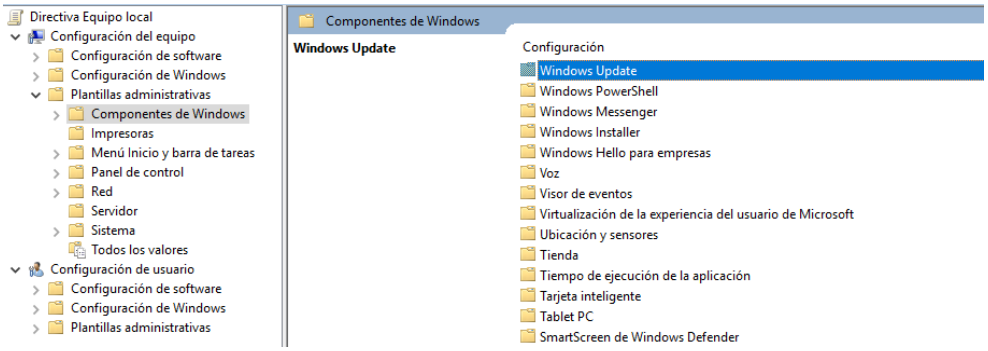


Figura 92: Conf. WSUS - Configuración políticas en equipo para reporte a WSUS

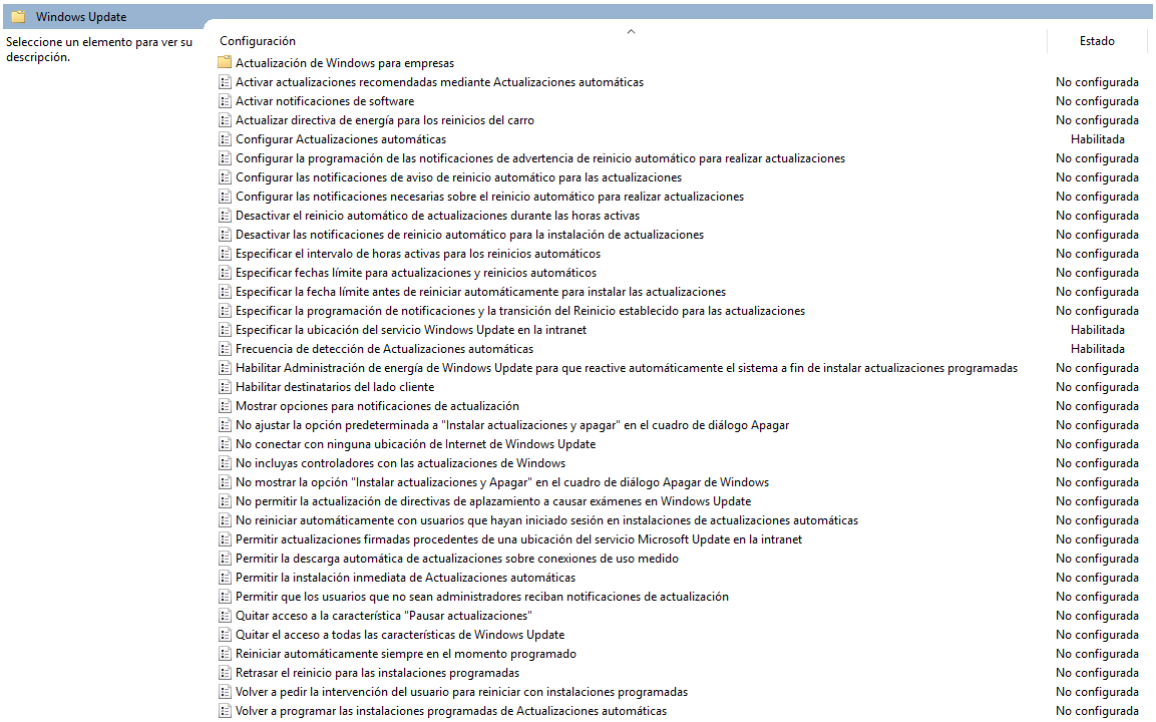


Figura 93: Conf. WSUS - Políticas de Windows Update

A continuación, se enumeran las políticas que son necesarias de modificar para que el equipo se comunique con la herramienta WSUS:

1. *Configurar actualizaciones automáticas*

   Marcamos la política como “Habilitada“ y dejamos las opciones que aparecen por defecto, aunque son modificables y pueden adaptarse a otro tipo de configuración.

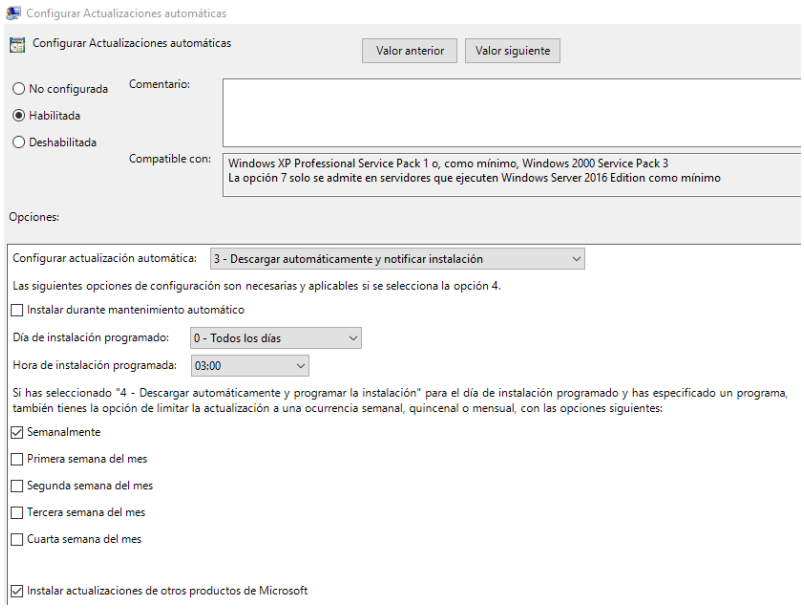


Figura 94: Conf. WSUS - Configurar política para actualizaciones automáticas

2. *Especificar la ubicación del servicio Windows Update en la intranet*

   Marcamos la política como “Habilitada” y en los campos “Establecer el servicio de actualización de la intranet para detectar actualizaciones” y “Establecer el servidor de estadísticas de la intranet”, debemos escribir el servidor y el puerto de WSUS, en este caso “http://sv-winsrv-wsus:8530”.

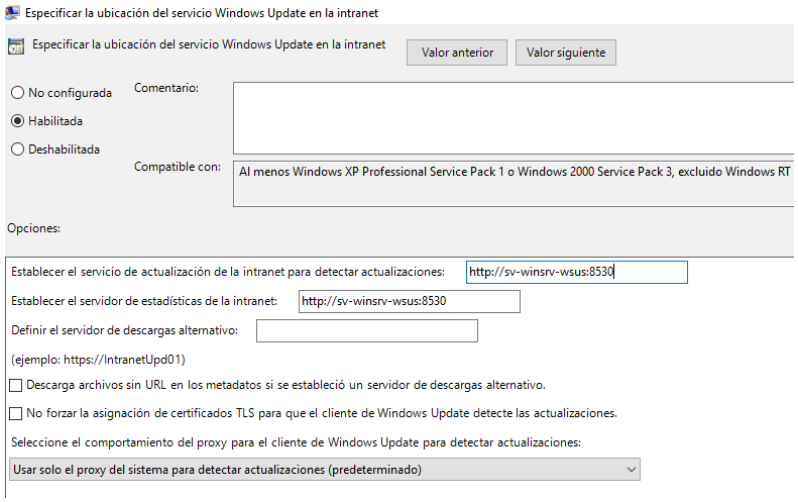


Figura 95: Conf. WSUS - Configurar política para la conexión con el servidor WSUS

3. *Frecuencia de detección de Actualizaciones automáticas*

   Marcamos la política como “Habilitada” y en “Comprobar actualizaciones con el siguiente intervalo (horas)”, debemos especificar la frecuencia de reporte con el servidor de WSUS en horas.

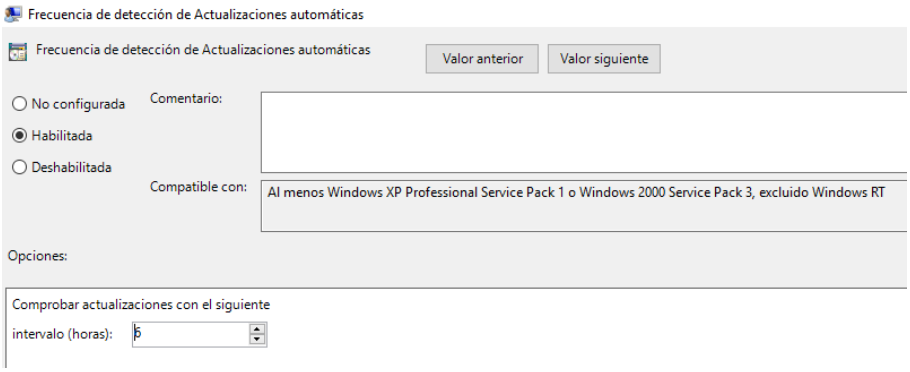


Figura 96: Conf. WSUS - Configurar política para definir la frecuencia de actualizaciones

- **Comprobar que los equipos están reportando**

  Una vez configuradas las políticas en todos los equipos Windows y tras esperar un tiempo para que comiencen las comunicaciones o reportes con WSUS, podemos observar que ya aparecen datos sobre estos equipos en la consola y podemos ver detalles del estado de las actualizaciones que poseen o demandan.

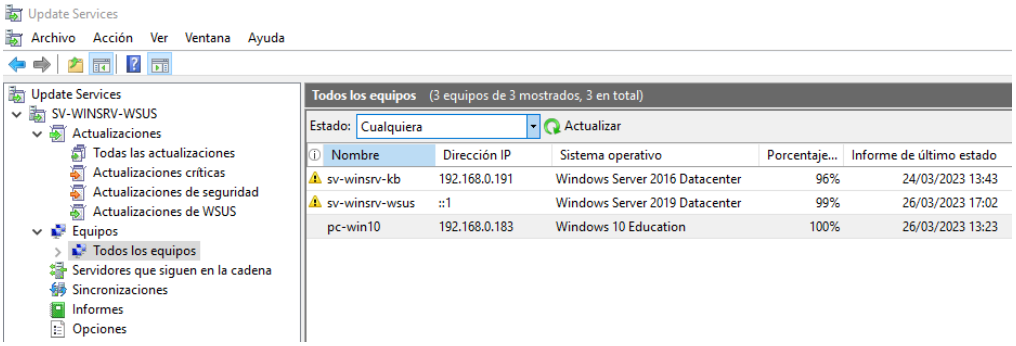


Figura 97: Conf. WSUS - Equipos reportando a WSUS

- **Configuración de la utilidad para la generación de informes a través de WSUS**

  La herramienta WSUS ofrece la posibilidad de crear informes de actualizaciones faltantes en los equipos, actualizaciones aplicadas, actualizaciones pendientes de ser aplicadas, etc.

  Esta utilidad es de gran ayuda a la hora de elaborar los informes del departamento, ya que nos proporciona muchos datos sobre el estado de las actualizaciones y su aplicación, pero para poder utilizarla debemos instalar la aplicación *Microsoft Report Viewer*.

Una vez realizada la configuración de la herramienta WSUS, configurados los equipos para que se comuniquen con la herramienta y habilitada la utilidad para crear informes, ya tenemos operativa la herramienta, a la que los técnico tendrán acceso desde su equipo de trabajo y desde donde podrán gestionar todo lo referente a las actualizaciones de equipos Windows y productos Microsoft de forma centralizada.

En el Anexo XVII. Ejemplo de este documento se puede consultar un ejemplo de aplicación de actualizaciones a través de la herramienta WSUS.

Anexo XIII: Infraestructura completa del piloto NOC

Infraestructura completa de máquinas virtuales necesarias para la creación del piloto

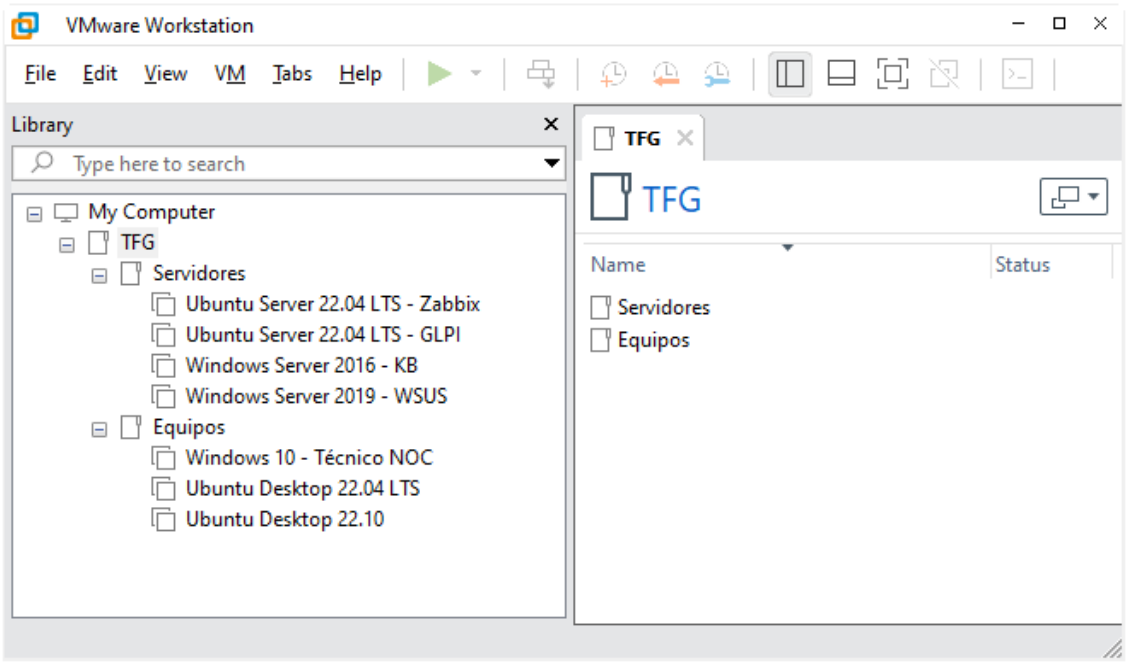


Figura 98: Infraestructura piloto NOC - Máquinas virtuales (infraestructura completa)

Escritorio del servidor que contiene la base de conocimientos (SV-WINSRV-KB)

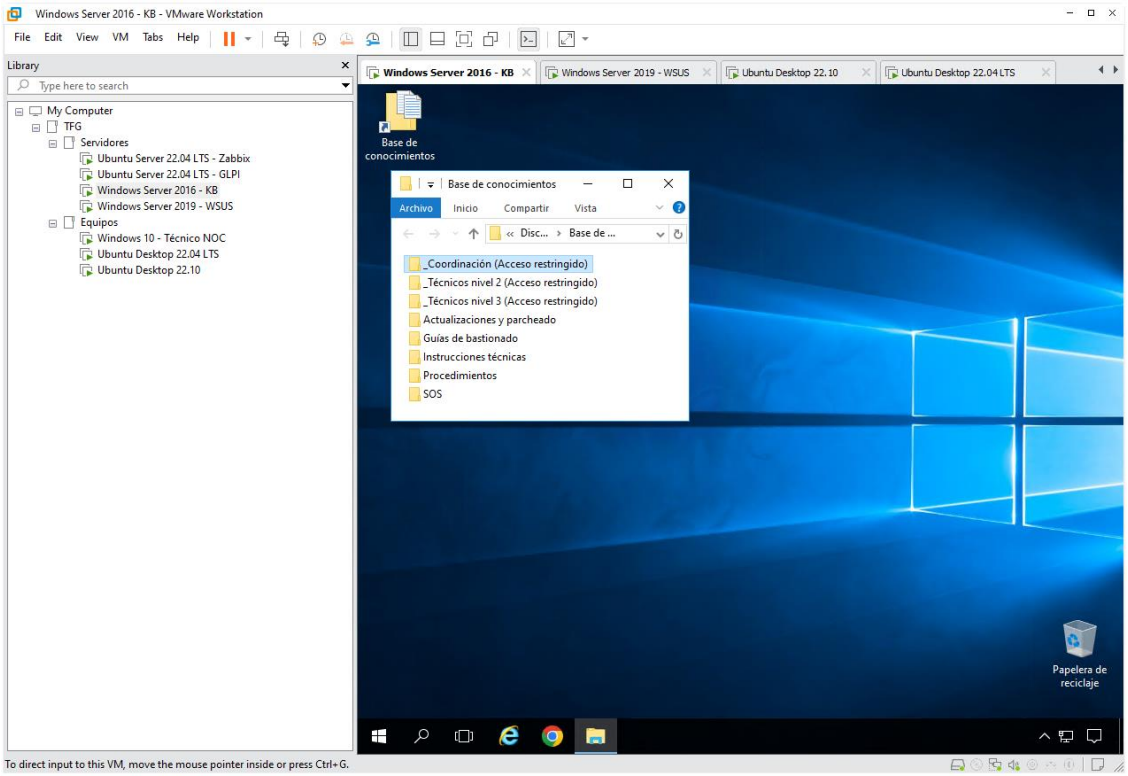


Figura 99: Infraestructura piloto NOC - Servidor con base de conocimientos

Escritorio del servidor que contiene la herramienta WSUS (SV-WINSRV-WSUS)

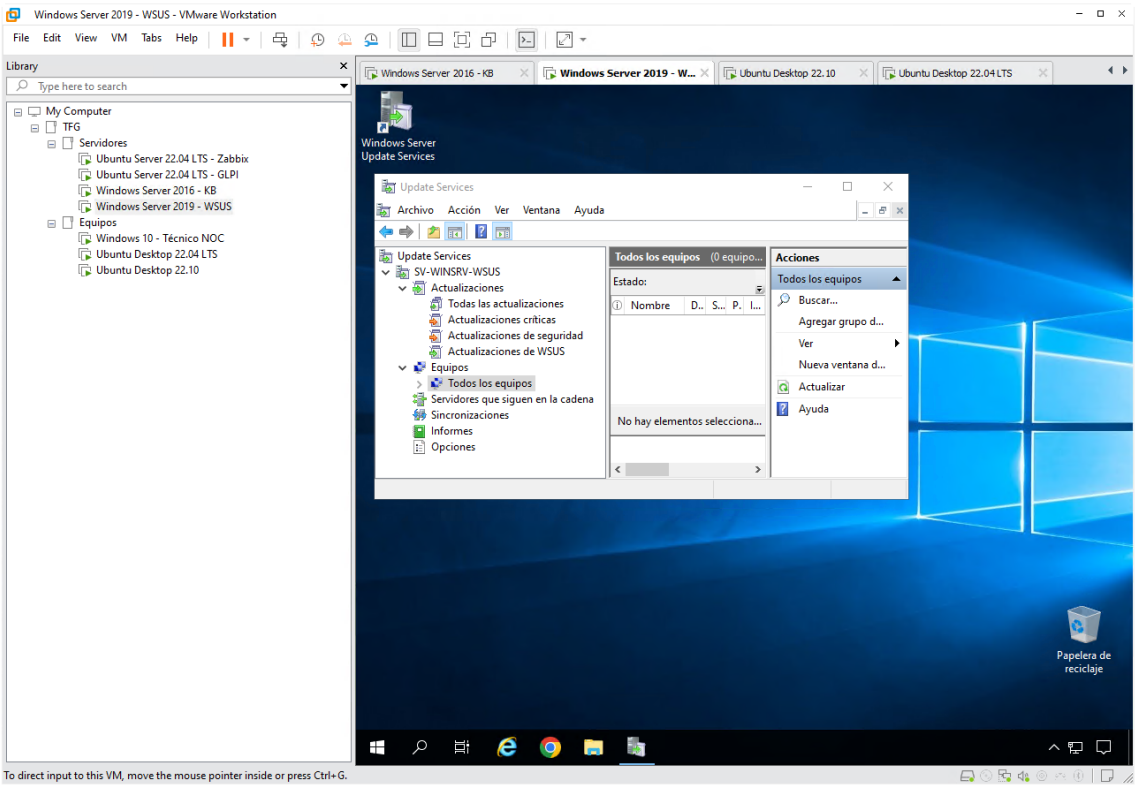


Figura 100: Infraestructura piloto NOC - Servidor con herramienta WSUS

Sistema que contiene la herramienta de monitorización Zabbix (SV-UBUSRV-ZBX)

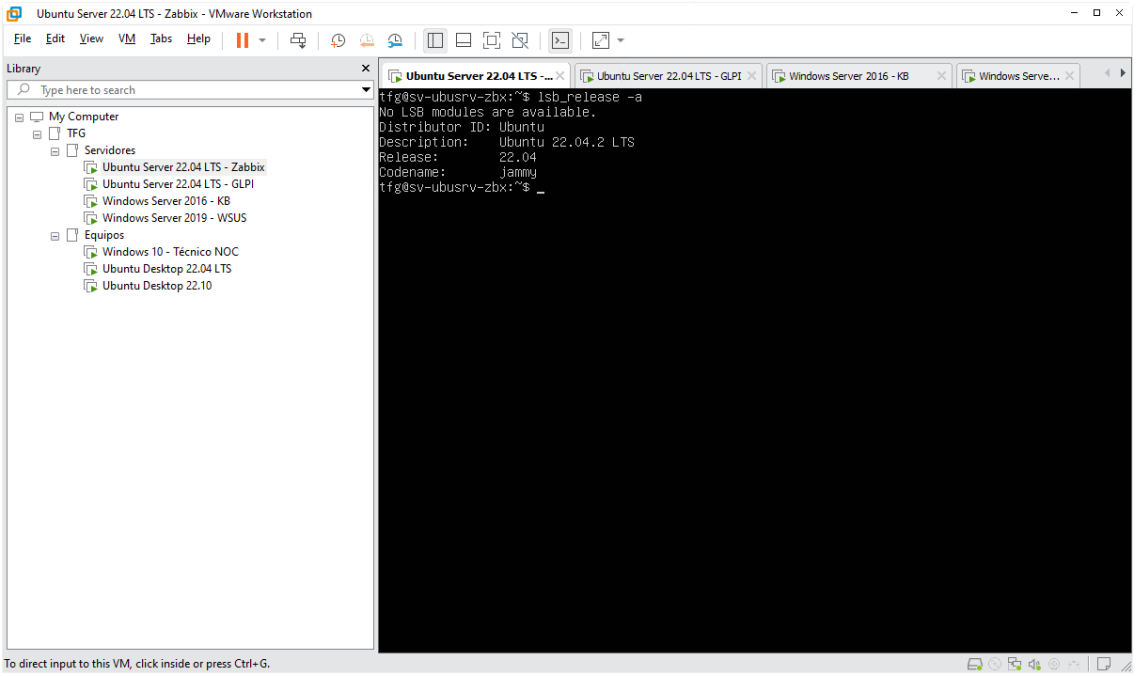


Figura 101: Infraestructura piloto NOC - Servidor con herramienta monitorización Zabbix

Sistema que contiene la herramienta de ticketing GLPI (SV-UBUSRV-GLPI)

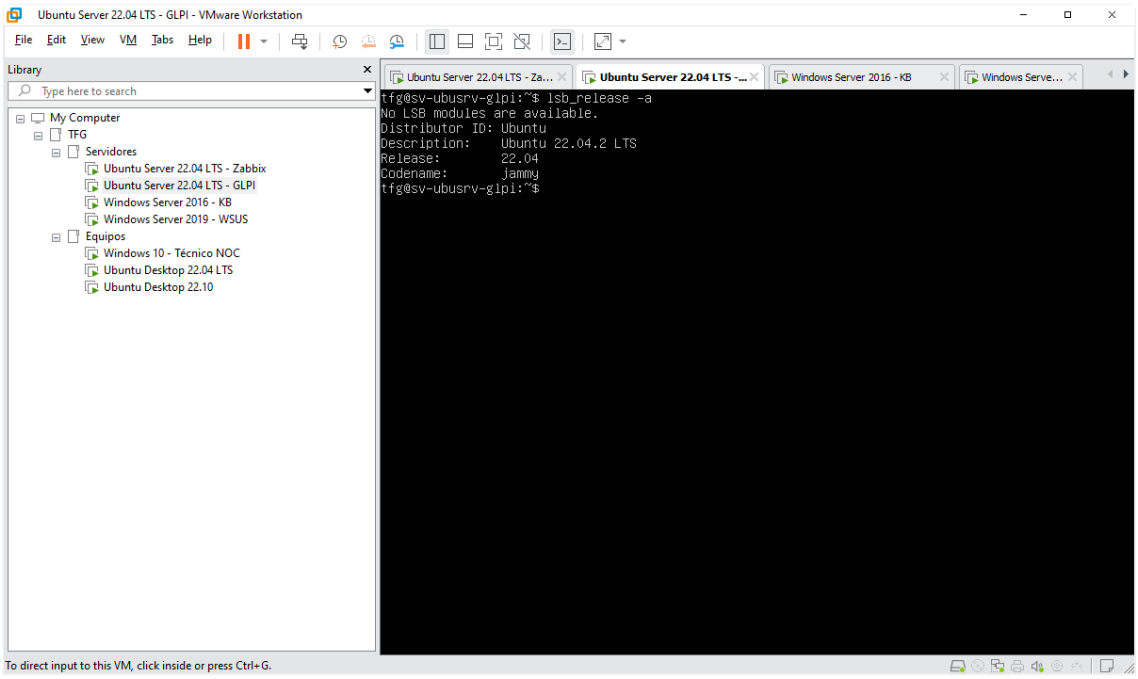


Figura 102: Infraestructura piloto NOC - Servidor con herramienta ticketing GLPI

Escritorio del equipo de trabajo para un técnico del NOC (PC-WIN10)

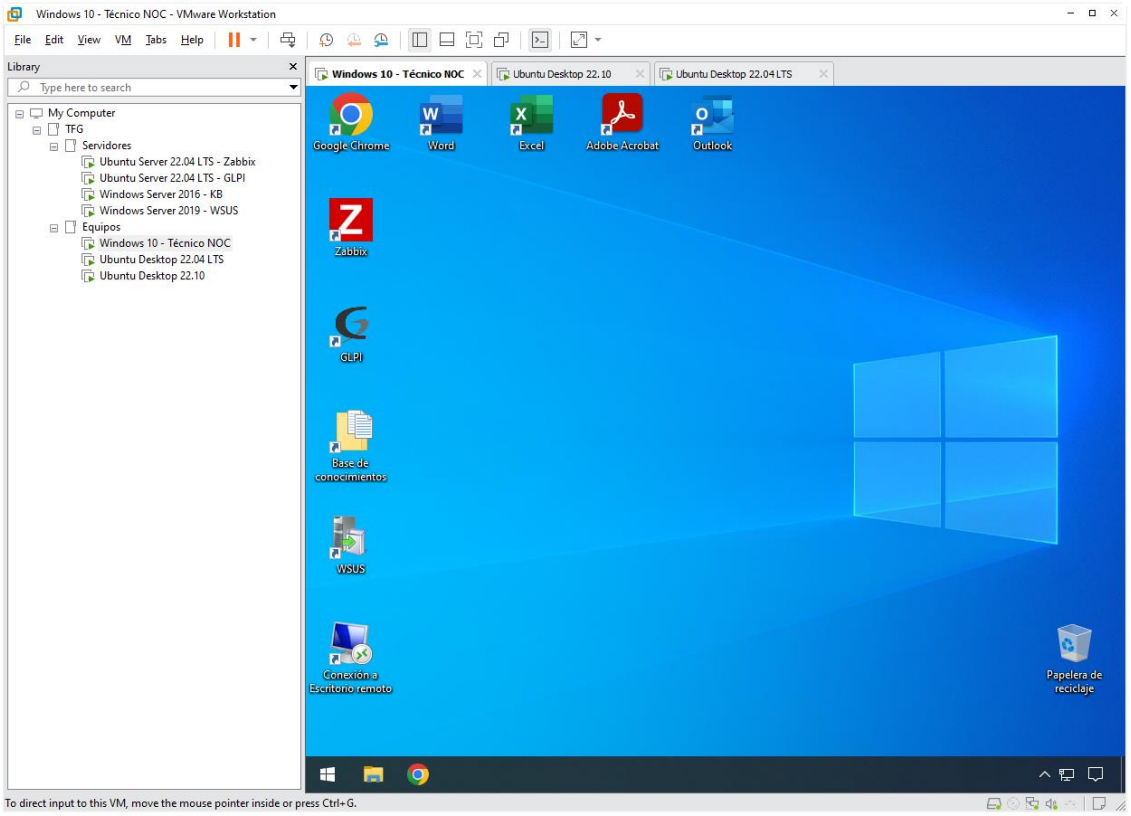


Figura 103: Infraestructura piloto NOC - Equipo de trabajo para un técnico del NOC

Escritorio del equipo creado para su monitorización exclusivamente (PC-UBUDSK)

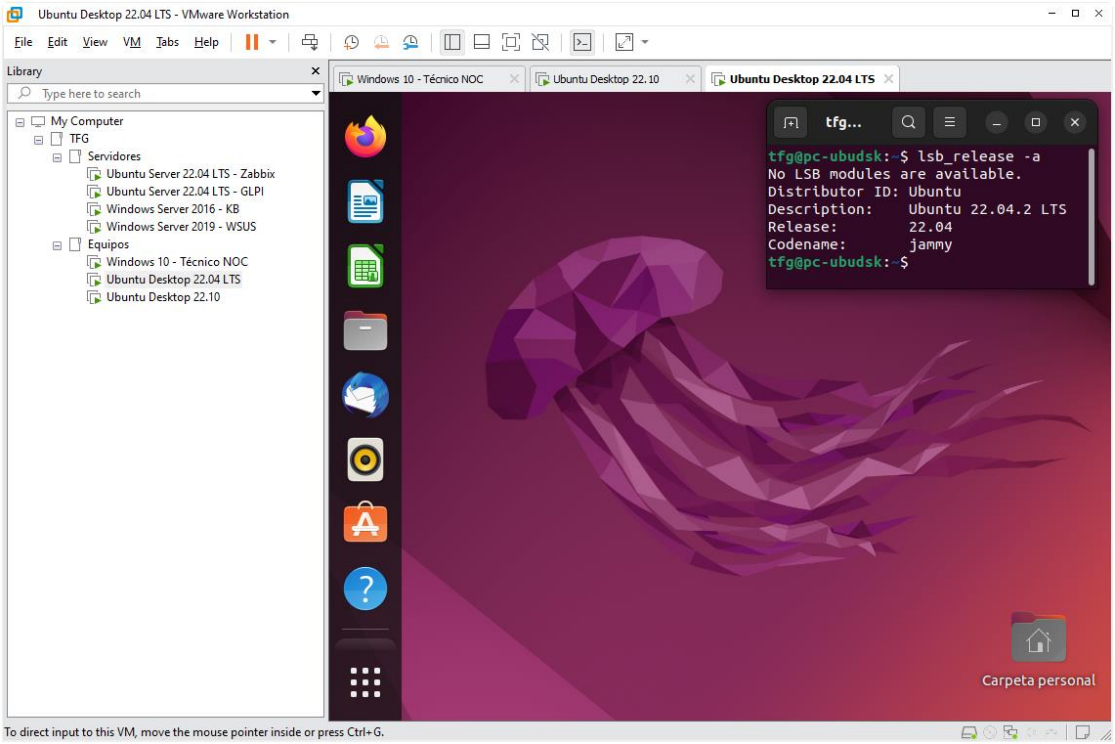


Figura 104: Infraestructura piloto NOC - Equipo 1 creado para ser monitorizado

Escritorio del equipo creado para su monitorización exclusivamente (PC-UBUDSK2)

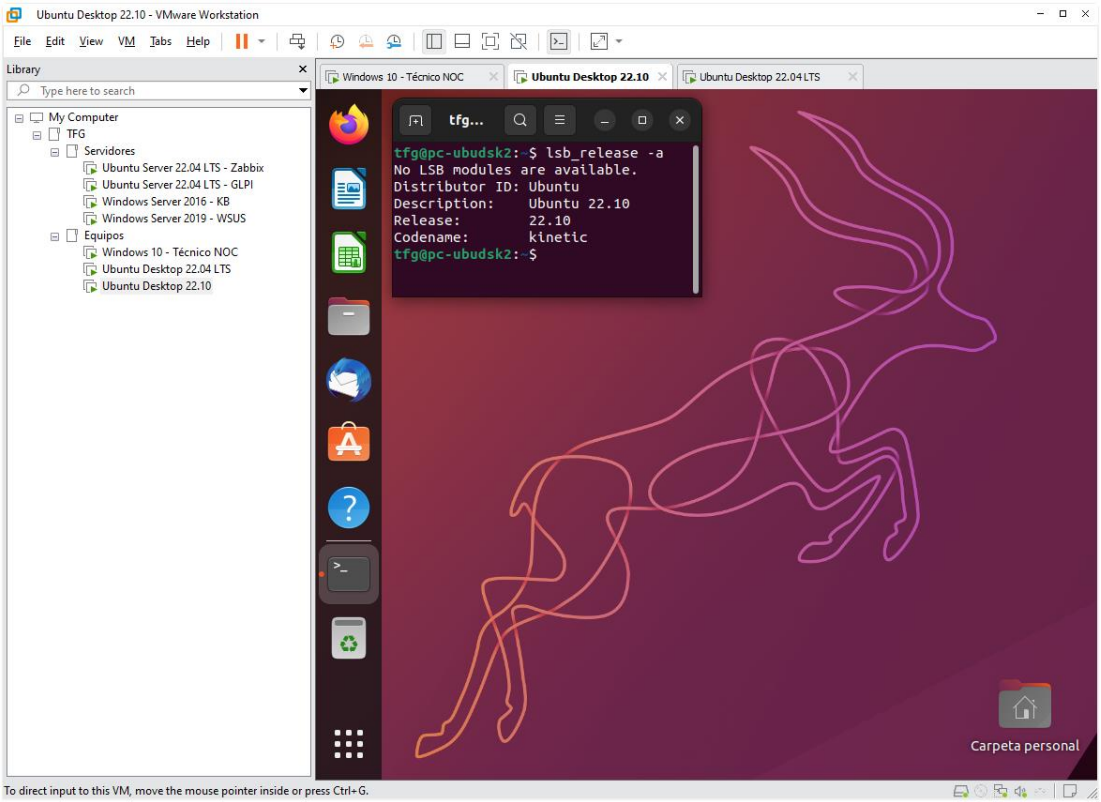


Figura 105: Infraestructura piloto NOC - Equipo 2 creado para ser monitorizado

Anexo XIV: Monitorización de sistemas (ejemplo e inconvenientes)

Ejemplo: Caso práctico de monitorización de sistemas

A continuación, se muestran algunas alertas generadas de forma intencionada, que se podrán ver pulsando el menú de la izquierda del tablero de Zabbix "Monitoring – Dashboard" y que nos permitirá familiarizarnos con el sistema de monitorización, así como comprobar el correcto funcionamiento de la herramienta y verificar los parámetros de configuración para estas alertas:

- **Generación de alertas sobrecargando los componentes de un sistema Windows**

  Al sobrecargar algunos componentes de un sistema Windows, como pueden ser la CPU, memoria RAM o llenar el espacio del disco, se deben generar las alertas correspondientes informando del problema. Para realizar la sobrecarga usaremos un script creado específicamente para esta tarea y que podemos consultar en el Anexo VIII de este documento.

  También generaremos otras alertas, que nos informen si el sistema se ha reiniciado o se ha perdido el contacto con el agente de monitorización, que la mayoría de las veces suele ser porque este se ha apagado o ha quedado bloqueado.

  Para realizar estas pruebas, accedemos al equipo Windows "PC-WIN10" y ejecutamos el script "GenerarAlertasWIN.ps1". Para ejecutarlo hay que abrir una ventana de Powershell, en la que escribiremos la ruta donde se encuentra el archivo que contiene el código del script, en este caso "C:\Scripts\GenerarAlertasWIN.ps1".

  Al ejecutar el script se mostrará un menú con las distintas sobrecargas programadas que se pueden realizar en este sistema.

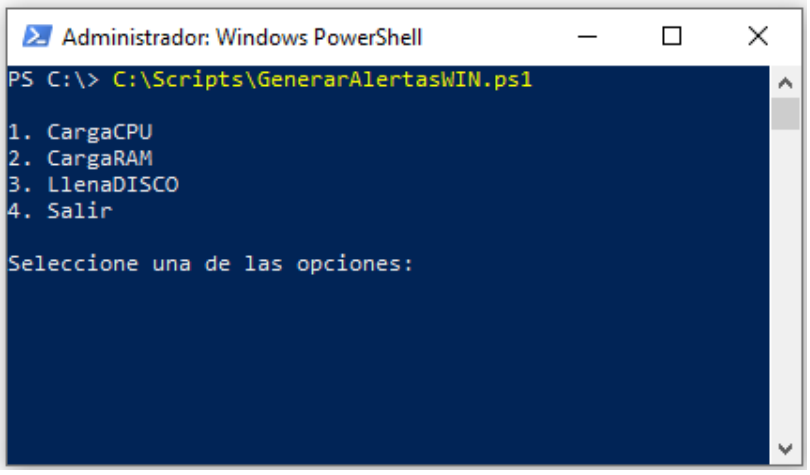


Figura 106: Monitorización. Ejemplo - Script de generación de alertas sistema Windows

Tras ejecutar las distintas sobrecargas de CPU, RAM y disco, se han generado tres alertas producidas por el host “Desktop 1 Windows 10” que se corresponde con el equipo “PC-WIN10”, de las cuales la primera relativa al uso alto de CPU, ha quedado resuelta de forma automática tras volver a la normalidad. La segunda alerta relativa al uso alto de la memoria RAM y la tercera relativa al poco espacio en disco, se han capturado sin resolver, para que se pueda apreciar la forma en la que se muestra en la herramienta de monitorización y que podemos observar en la siguiente imagen.

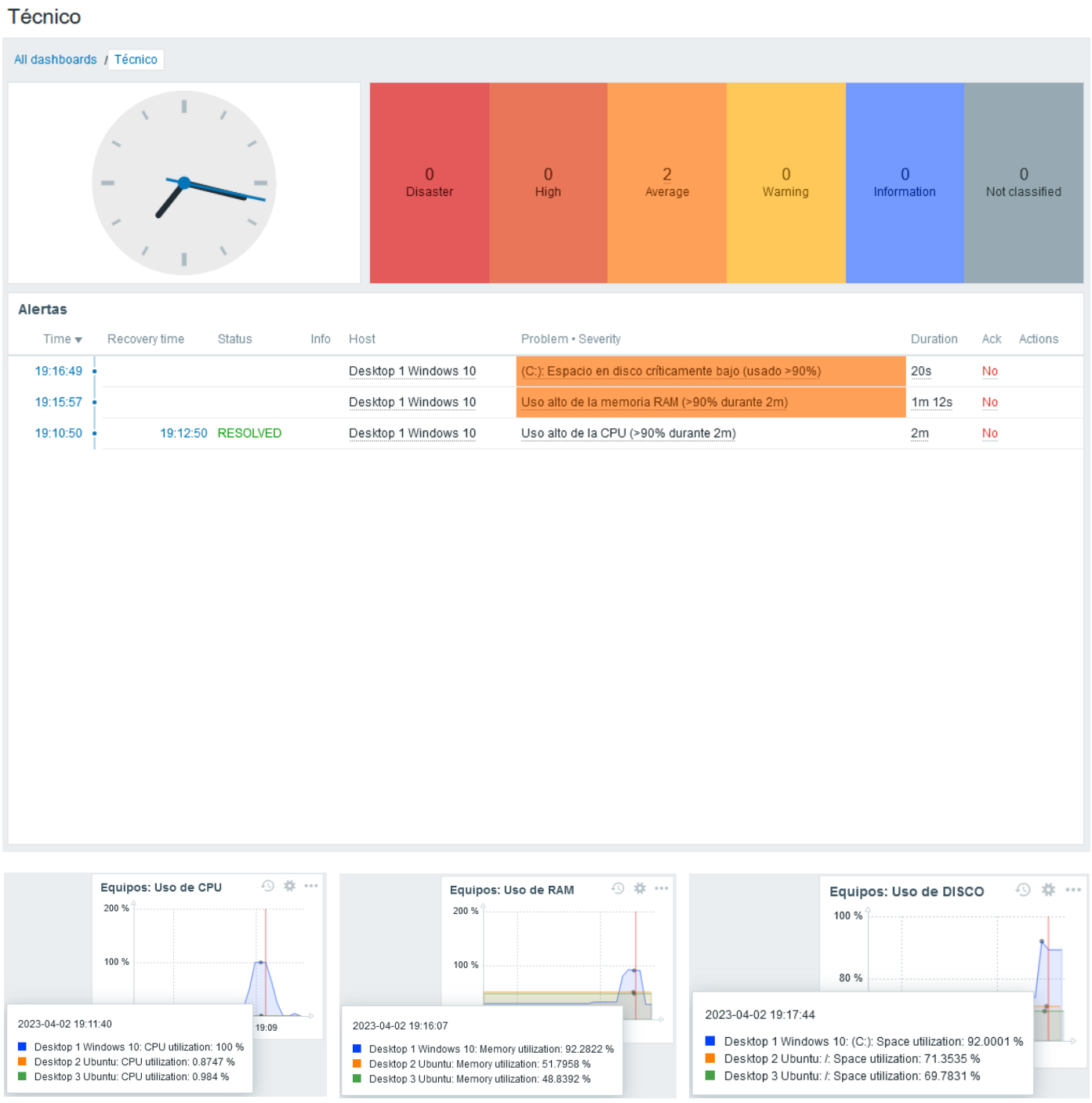


Figura 107: Monitorización. Ejemplo - Alertas CPU, RAM y disco equipo Windows

Una vez generadas las alertas por sobrecarga en algunos componentes del sistema, procedemos a generar otras alertas, que nos avisan del reinicio del equipo, tras reiniciarlo y de la pérdida de conexión con el agente, tras apagarlo.

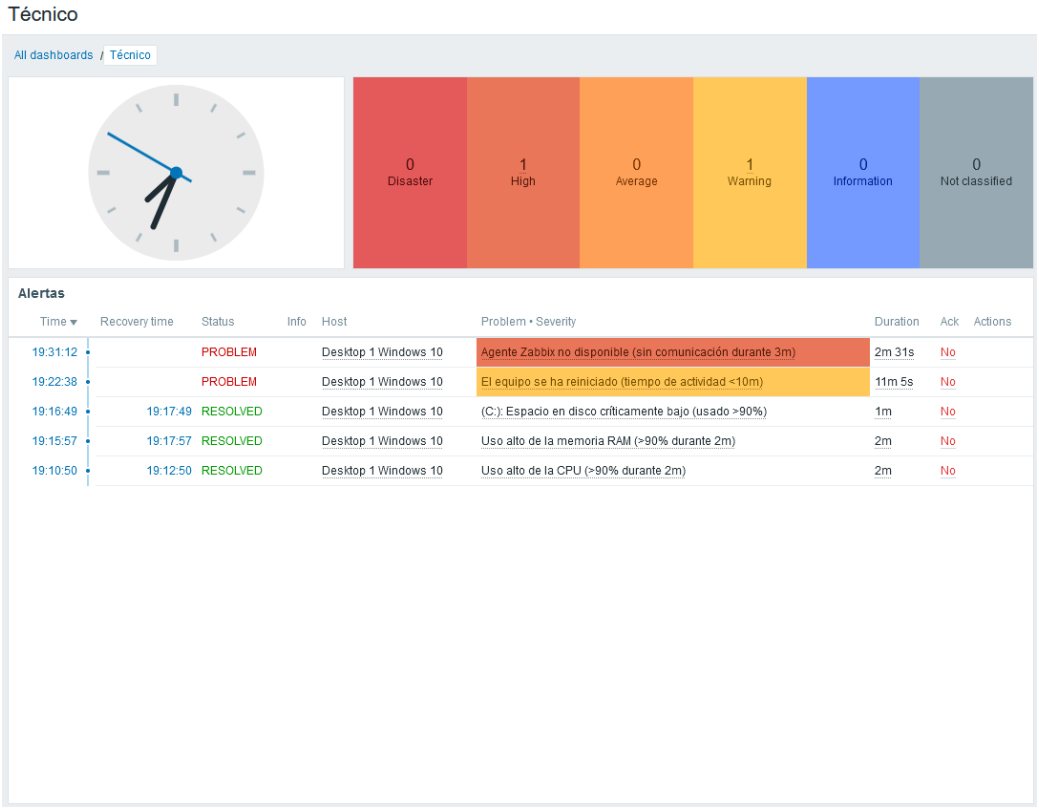


Figura 108: Monitorización. Ejemplo - Alertas reinicio y apagado equipo Windows

- **Generación de alertas sobrecargando los componentes de un sistema Linux**

  Al sobrecargar algunos componentes de un sistema Linux, como pueden ser la CPU, memoria RAM o llenar el espacio del disco, se deben generar las alertas correspondientes informando del problema. Para realizar la sobrecarga usaremos un script creado específicamente para esta tarea y que podemos consultar en el Anexo VIII de este documento.

  También generaremos otras alertas, que nos informen si el sistema se ha reiniciado o se ha perdido el contacto con el agente de monitorización, que la mayoría de las veces suele ser porque este se ha apagado o ha quedado bloqueado.

  Para realizar estas pruebas accedemos a los equipos Ubuntu “PC-UBUDSK” y “PC-UBUDSK2” y ejecutamos el script “GenerarAlertasLNX.sh”. Para ejecutarlo hay que abrir una ventana de Terminal de Ubuntu, en la que escribiremos la palabra “bash” seguido de la ruta donde se encuentra el archivo que contiene el código del script, en este caso, “bash ~/Scripts/GenerarAlertasLNX.sh”.

Al ejecutar el script se mostrará un menú con las distintas sobrecargas programadas que se pueden realizar en este sistema.

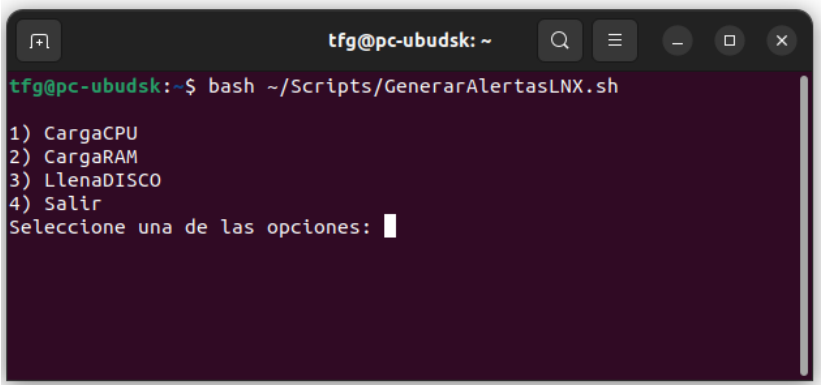


Figura 109: Monitorización. Ejemplo - Script de generación de alertas sistema Linux

Tras ejecutar las distintas sobrecargas de CPU, RAM y disco, se han generado seis alertas producidas por los hosts “Desktop 2 Ubuntu” y “Desktop 3 Ubuntu” que se corresponden con los equipos “PC-UBUDSK” y “PC-UBUDSK2” respectivamente.

El orden de las alertas por orden cronológico de más antiguas a más actuales es: CPU en “Desktop 2”, disco en “Desktop 3”, RAM en “Desktop 2”, CPU en “Desktop 3”, disco en “Desktop 2” y RAM en “Desktop 3”. El motivo de este orden es alternar un poco la generación de las alertas entre varios equipos, las cuales podemos observar en la siguiente imagen.

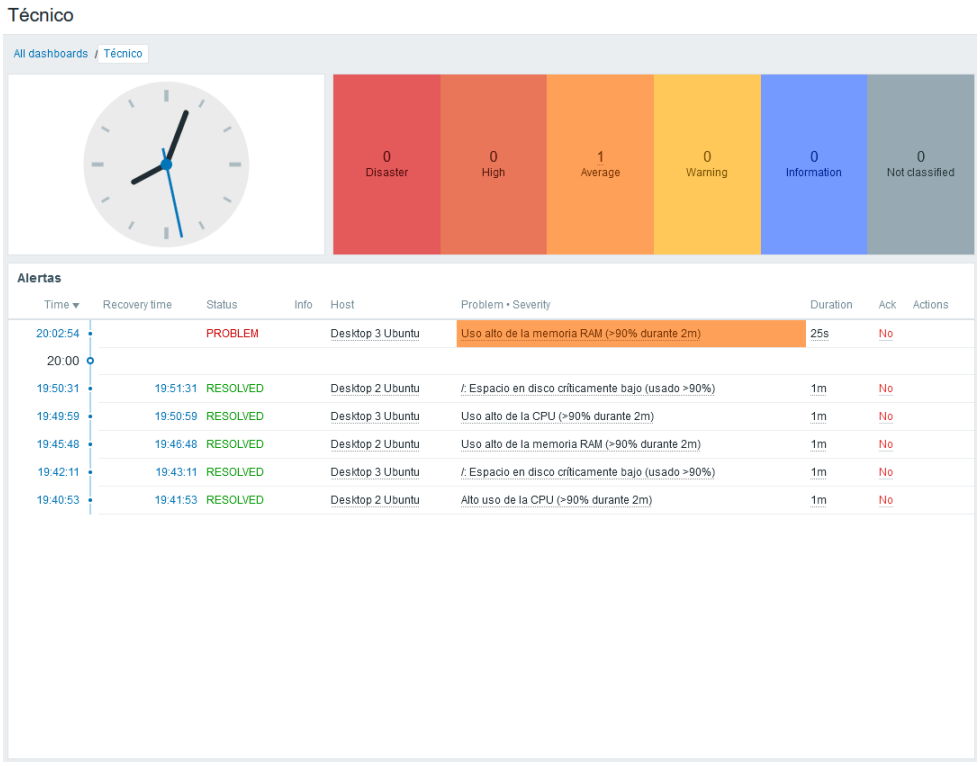


Figura 110: Monitorización. Ejemplo - Alertas CPU, RAM y disco equipo Linux

Una vez generadas las alertas por sobrecarga en algunos componentes de los sistemas anteriores, procedemos a generar otras alertas de forma alternativa entre ambos equipos, que nos avisan del reinicio del equipo, tras reiniciarlo y de la pérdida de conexión con el agente, tras apagarlo.

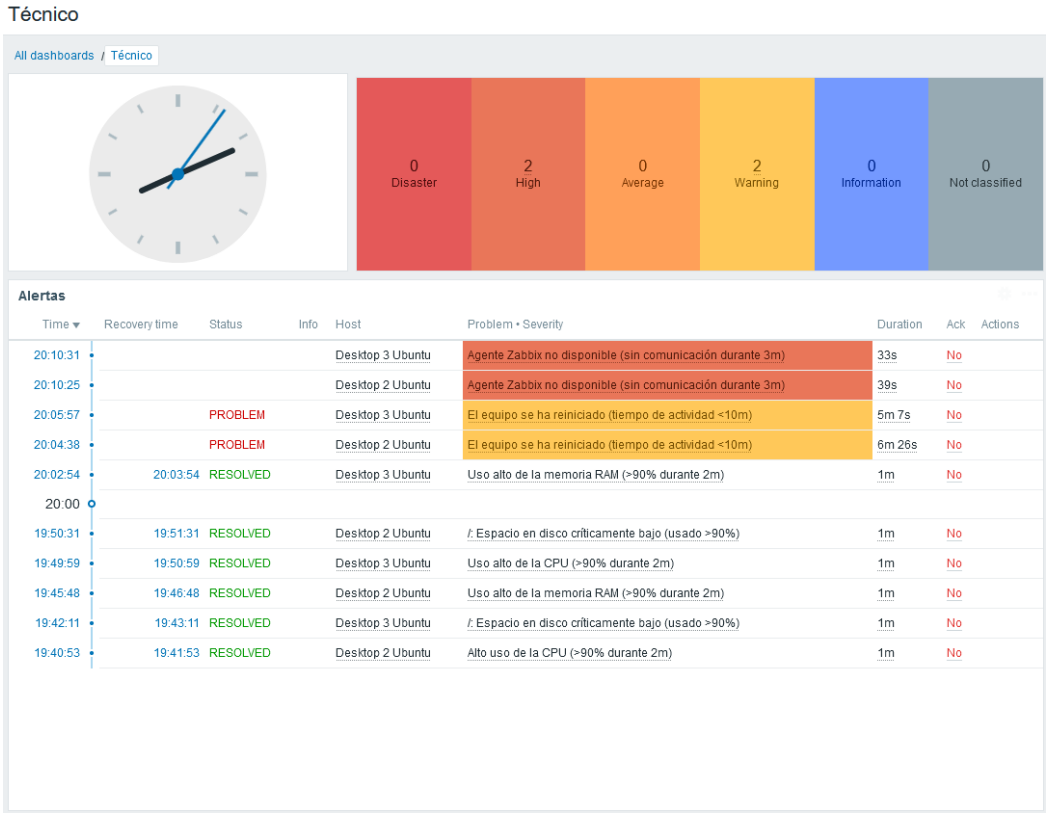


Figura 111: Monitorización. Ejemplo - Alertas reinicio y apagado equipo Linux

- **Alertas generadas desde otros sistemas**

  La monitorización es aplicable a cualquier sistema, por lo que realizaremos pruebas reiniciando y apagando servidores para observar que también se generan alertas en estos equipos.

  Para realizar estas pruebas, reiniciaremos y apagaremos el servidor Windows “SV-WINSRV-WSUS” y el servidor Ubuntu “SV-UBUSRV-GLPI”.

  Tras realizar el reinicio y posterior apagado, se han generado cuatro alertas producidas por el host “Server WSUS” y “Server GLPI” que se corresponden con los servidores “SV-WINSRV-WSUS” y “SV-UBUSRV-GLPI” respectivamente.

  El orden de las alertas por orden cronológico de más antiguas a más actuales es: reinicio en “Server WSUS” y posteriormente en “Server GLPI”, pérdida de conexión con el agente “Server WSUS” y posteriormente en “Server GLPI”. El motivo de este orden es alternar un poco la generación de las alertas entre varios servidores, las cuales podemos observar en la siguiente imagen.

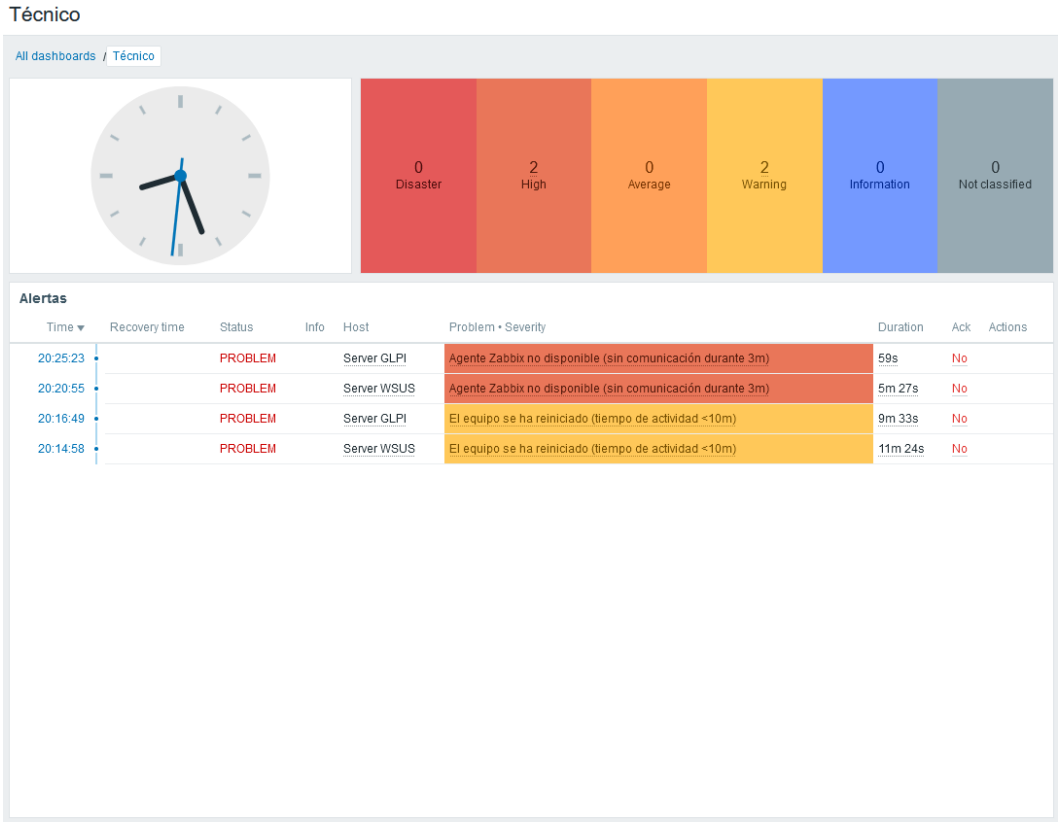


Figura 112: Monitorización. Ejemplo - Alertas reinicio y apagado serv. Windows y Linux

Inconvenientes que pueden surgir al monitorizar los sistemas

En el ejemplo comentado podemos observar que las alertas se generan correctamente, pero no siempre es así, ya que puede ocurrir que por alguna razón el agente de monitorización instalado en el sistema que está siendo monitorizado, comience a fallar y no envíe datos de forma correcta a la herramienta de monitorización, produciendo falsas alertas o simplemente no produciéndolas, viendo comprometida su fiabilidad.

En este caso, lo mejor es revisar el sistema con el agente de monitorización y mediante scripts para la generación de alertas, realizar pruebas para determinar la causa del problema y poder solventarlo.

Anexo XV: Resolución de incidencias (ejemplos e inconvenientes)

Ejemplo 1: Caso práctico de resolución de una incidencia comunicada

A continuación, se describen los pasos que un técnico de primer nivel deberá realizar para resolver una incidencia comunicada a través de teléfono o en este caso correo electrónico:

1. En el buzón de incidencias del NOC se recibe un correo entrante donde se expone el motivo de la incidencia.

Problemas con la pantalla del equipo PC-WIN10-000024

De: i.mora@tfg.com

Para: incidencias@tfg.com

Fecha: 27/03/2023 16:35

La pantalla de mi equipo (PC-WIN10-000024) parpadea y a veces se apaga cuando estoy trabajando.

Este problema está presente desde hace varios días, pero últimamente es mucho más frecuente, impidiéndome realizar mis tareas.

Figura 113: Resolución de incidencias. Ejemplo 1 - Correo informando de una incidencia

2. El técnico de turno encargado de la revisión del buzón de incidencias crea un ticket con los datos de la incidencia.

   Para crear un nuevo ticket es necesario acceder al tablero de la herramienta GLPI y pulsar en el menú de la izquierda “Soporte – Abrir petición”, una vez cargado el formulario, es necesario completar los datos de la incidencia añadiéndolos al ticket.

   En la parte izquierda del formulario se rellenan los datos relativos a la incidencia, asignándole un t*ítulo* representativo y una *descripción* detallada del problema extraída del correo electrónico anterior.

   En la parte de la derecha del formulario se especifican los siguientes datos:

   - *Fecha de apertura de la incidencia*: Normalmente la fecha en la que se crea el ticket, aunque también puede ser otra.
   - *Tipo*: En este caso “Incidencia”, aunque también puede ser una “Solicitud” para el caso de los procedimientos.

- *Estado*: “Nuevo”, dado que es una nueva petición.
- *Origen de la petición*: “E-mail”, dado que la incidencia se ha comunicado por esta vía, aunque también puede ser “Teléfono” (si la incidencia se comunica por teléfono) o “Directa” (si la petición la realiza algún superior o departamento autorizado).
- *Urgencia*: En este caso “Media”, aunque dependiendo de la urgencia de la incidencia también puede ser “Muy baja, Baja, Alta o Muy Alta”.
- *Impacto*: En este caso “Medio”, aunque dependiendo del impacto de la incidencia también puede ser “Muy bajo, Bajo, Alto o Muy Alto”.
- *Prioridad*: En este caso “Media”, aunque dependiendo de la prioridad que se le quiera asignar a la incidencia también puede ser “Muy baja, Baja, Alta, Muy Alta o Primordial”.
- *Solicitante*: Es el técnico que abre el ticket.
- *Asignada a*: Es el técnico que procesa el ticket. Normalmente se la asigna el mismo técnico que lo solicita, aunque puede ser adjudicado a cualquier otro técnico por un compañero o un nivel superior.

Una vez cumplimentado todos los datos, creamos el ticket pulsando el botón **Añadir** para que este pase a estar disponible para su asignación.

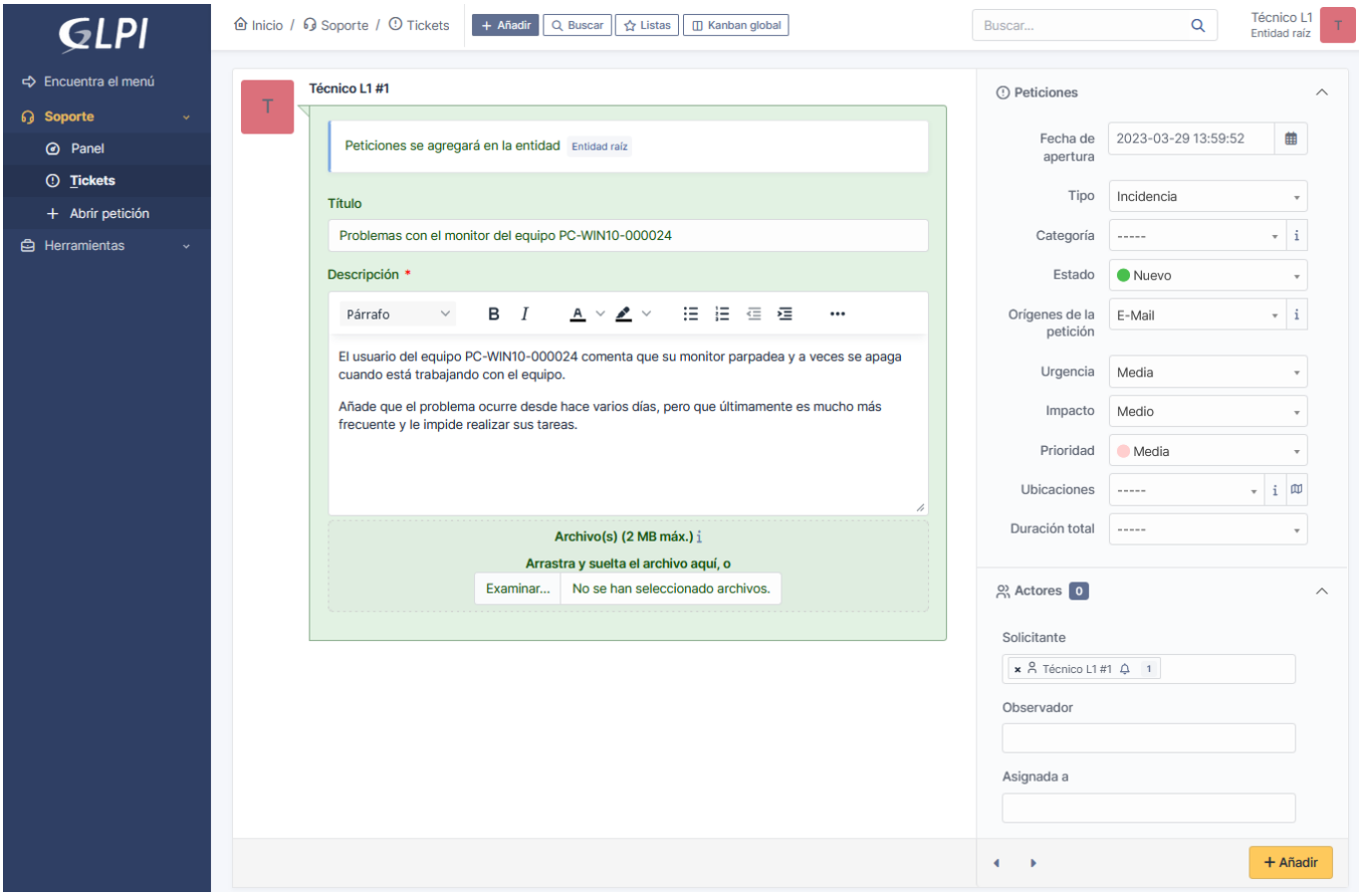


Figura 114: Resolución de incidencias. Ejemplo 1 - Crear ticket para procesar la incidencia

Pulsando en el menú de la izquierda “Soporte – Tickets”, podemos ver el nuevo ticket creado con “ID 14”, estado “Nuevo”, tipo “Incidencia” y sin asignar a ningún técnico.

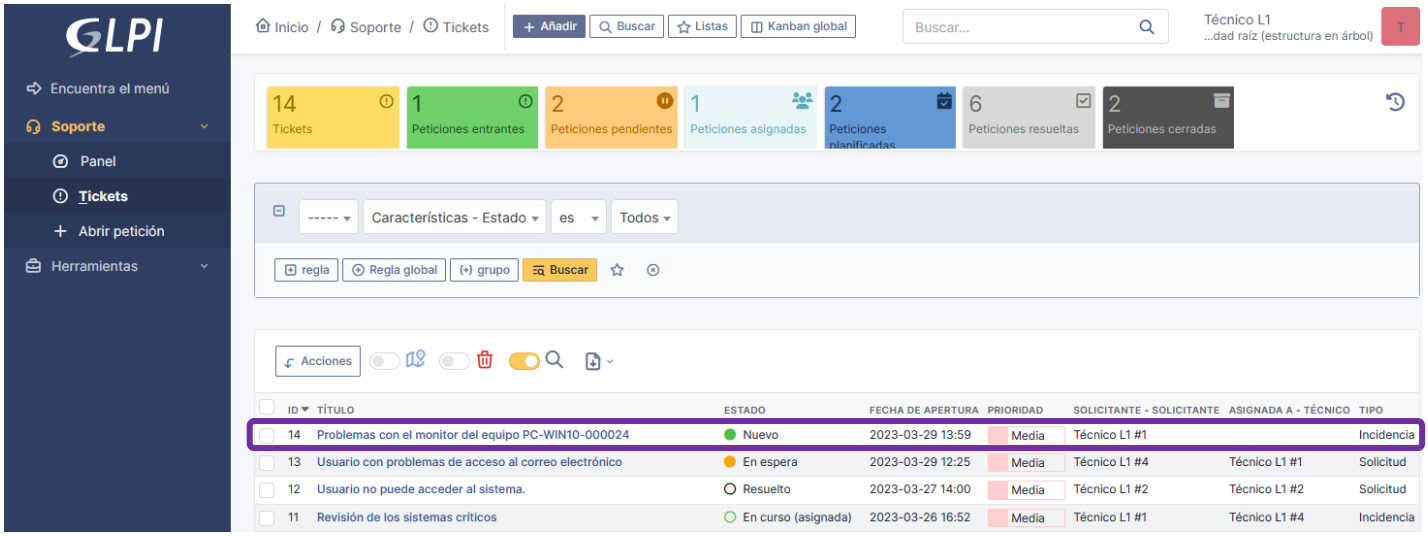


Figura 115: Resolución de incidencias. Ejemplo 1 - Estado del ticket creado

3. La asignación del ticket por norma general la realiza el propio técnico que va a procesarlo, aunque también puede serle asignado.

   La auto asignación del ticket por parte del técnico garantiza que dedique la mayor parte del tiempo a resolver el problema y que este no se asigne más tickets de los que pueda tratar.

   En el caso de que el ticket no esté asignado a ningún técnico, significa que está pendiente para ser asignado y el técnico que le corresponda o esté libre se lo asigne.

   Los tickets con carácter urgente se derivan a un técnico que siempre tendrá menos carga de trabajo o se dedicará a resolver en ese momento otros tickets de menor urgencia para poder gestionarlo sin problemas. En caso de que se produzcan varias incidencias de carácter urgente con sus correspondientes tickets, se pausaran las actividades que lo permitan para atender dichas incidencias, llegando incluso a utilizar personal técnico de segundo nivel para atender el pico de trabajo.

   Continuando con el ejemplo, el técnico número 4 de primer nivel será el encargado de resolver la incidencia, por lo que deberá tener asignado el ticket para poder comenzar con su resolución.

A continuación, se detallará el proceso de asignación y resolución del ticket correspondiente a la incidencia:

- Pulsamos sobre el ticket creado anteriormente y realizamos la asignación seleccionando en el desplegable del campo *Asignada a*, el técnico que va a procesar la incidencia, en este caso "Técnico L1 #4". Una vez seleccionado el técnico pulsamos sobre el botón **Guardar**.

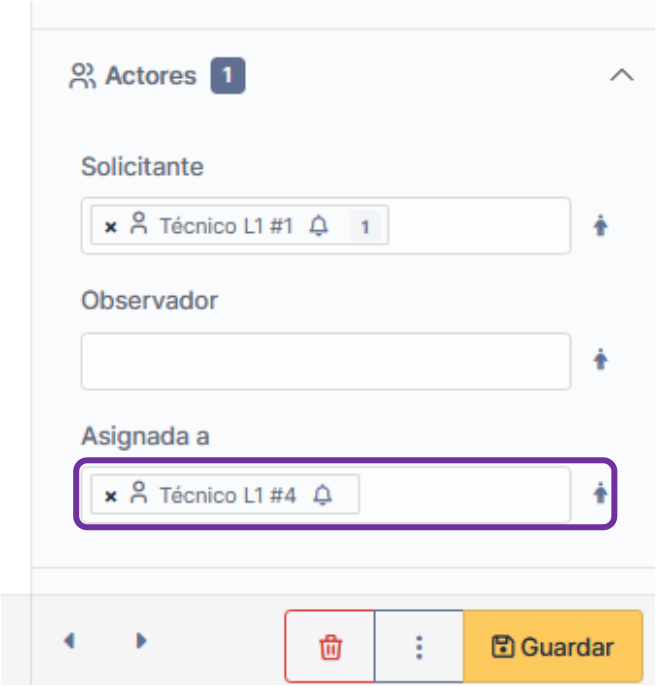


Figura 116: Resolución de incidencias. Ejemplo 1 - Asignación de ticket a un técnico

- Ahora el ticket aparecerá con estado "En curso (asignada)" a un técnico.

  También es posible filtrar todos los ticket que ese técnico tiene en asignados o en curso para que sea más fácil su gestión y visualización.

Figura 117: Resolución de incidencias. Ejemplo 1 - Asignación de ticket realizada

- Una vez asignado el ticket, se comienza con su resolución. Para ello se vuelve a pulsar sobre el ticket, donde se irá comentando las acciones realizadas para resolver el problema.

  Como primera tarea para poder resolver la incidencia, el técnico debe informarse y documentarse sobre problema, buscando en la base de conocimientos algún documento relacionado si lo hubiera. En caso de que se utilice una instrucción técnica debe quedar reflejada en los comentarios del ticket como información para la resolución de la incidencia y en caso de que el técnico sepa resolver el problema y no necesite consultar nada, solamente mencionarlo.

  Una vez el técnico ha estudiado las posibilidades, este encuentra una instrucción técnica llamada "IT0003-SW10-Problemas con los drivers de la pantalla v20230327_1.0" que quizás resuelva este problema y la pone en práctica, añadiendo el siguiente comentario al ticket:

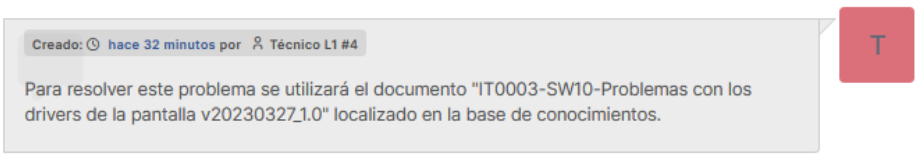


Figura 118: Resolución de incidencias. Ejemplo 1 - Añadido comentario al ticket

  Tras ejecutar dicha instrucción técnica, la incidencia se resuelve y el problema desaparece, por lo que hay que añadir un comentario de solución o de cierre al ticket, que automáticamente modificará su estado a "Resuelto" y guardará la fecha de resolución.

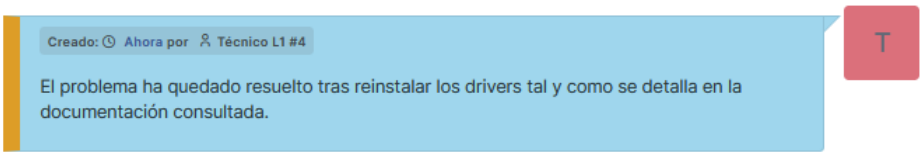


Figura 119: Resolución de incidencias. Ejemplo 1 - Comentario de cierre del ticket

  En la siguiente imagen se puede observar el ticket completo incluyendo sus comentarios antes de guardar los cambios y el estado final del ticket tras guardar los cambios.

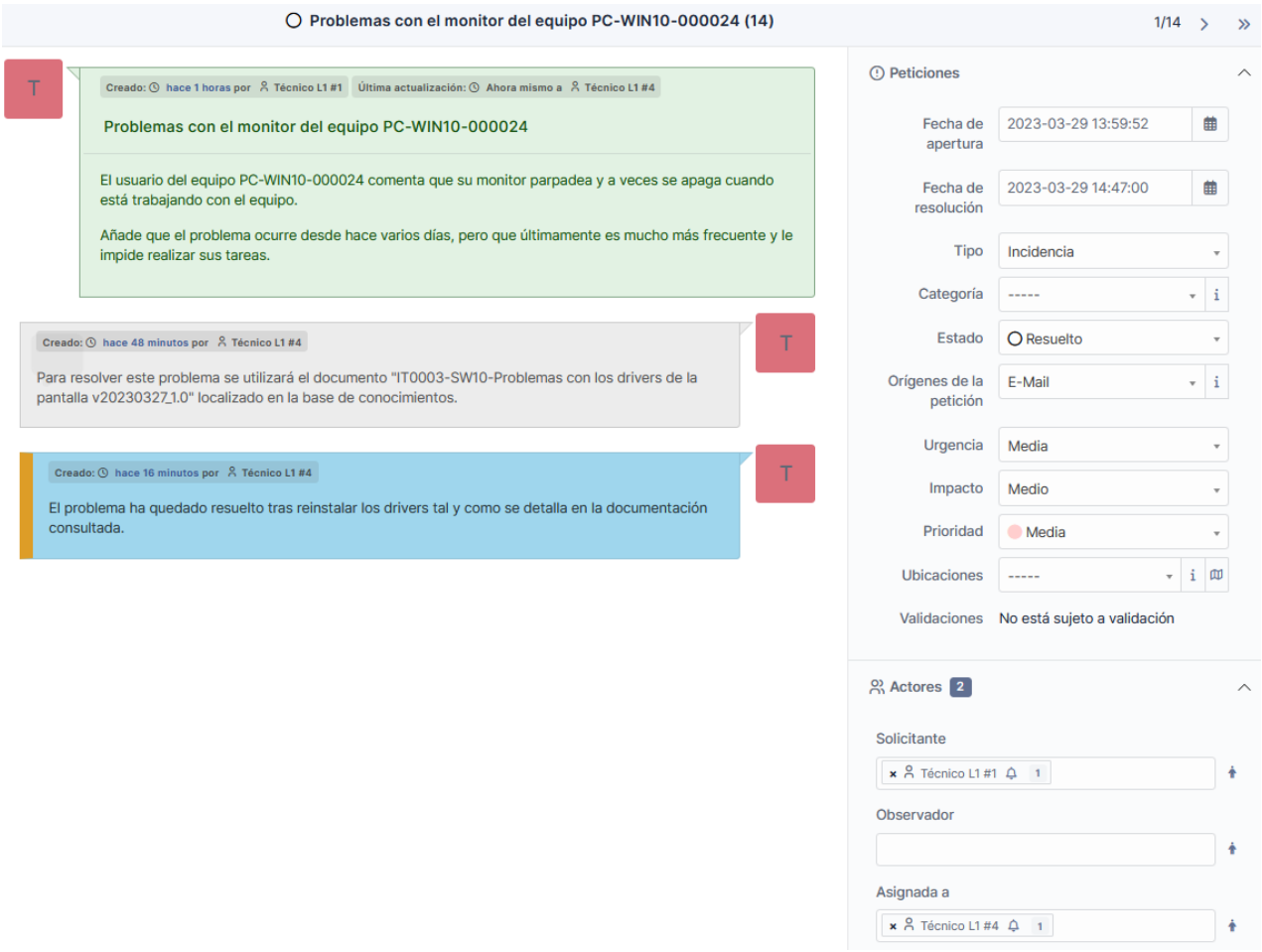


Figura 120: Resolución de incidencias. Ejemplo 1 - Ticket resuelto y completo

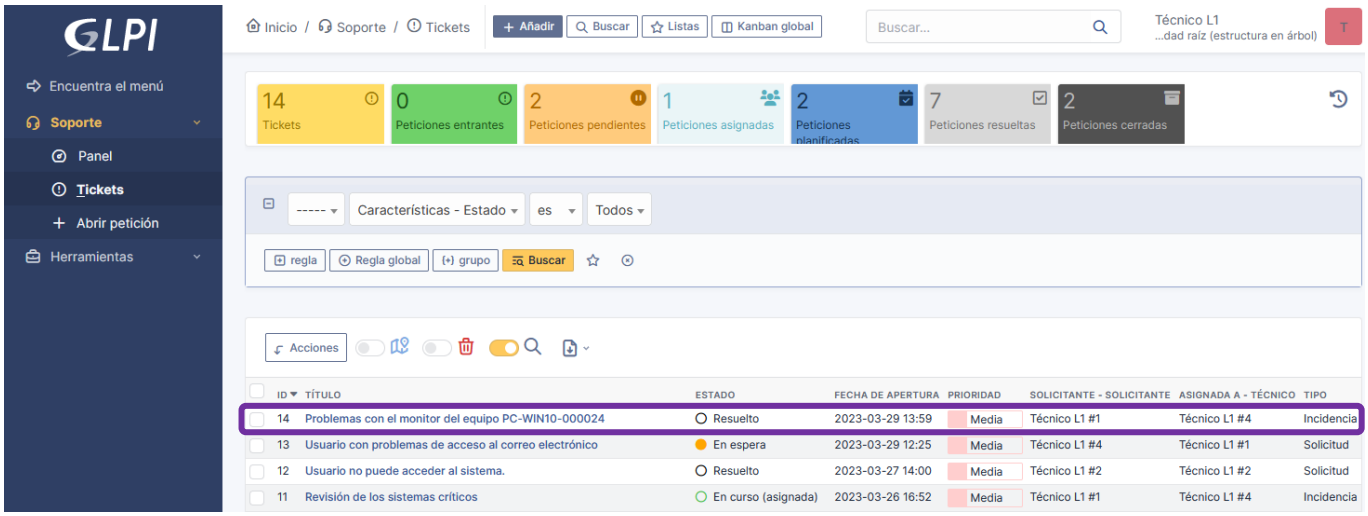


Figura 121: Resolución de incidencias. Ejemplo 1 - Estado del ticket "Resuelto"

4. Para finalizar la gestión de la incidencia, se informa al usuario, normalmente de la misma forma que realizo la comunicación inicial que en este caso sería correo electrónico.

Ejemplo 2: Caso práctico de resolución de una incidencia generada por una alerta

A continuación, se describen los pasos que un técnico de primer nivel deberá realizar al detectar una alerta en el sistema de monitorización y crear un ticket para para resolver la incidencia generada:

1. En el sistema de monitorización se muestra una alerta, que informa de una posible falta de espacio en disco en el sistema, por lo que esta alerta es interpretada como una incidencia.

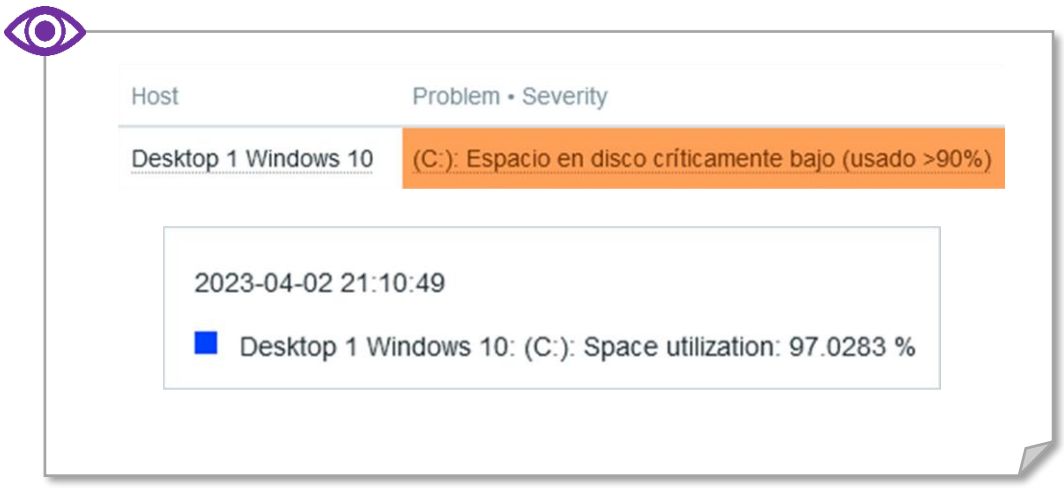


Figura 122: Resolución de incidencias. Ejemplo 2 - Alerta sistema de monitorización

2. El técnico de turno encargado de la revisión del programa de monitorización crea un ticket con los datos de la incidencia generada por la alerta.

   Para crear un nuevo ticket es necesario acceder al tablero de la herramienta GLPI y pulsar en el menú de la izquierda “Soporte – Abrir petición”, una vez cargado el formulario, es necesario completar los datos de la incidencia añadiéndolos al ticket.

   En la parte izquierda del formulario se rellenan los datos relativos a la incidencia, asignándole un *título* representativo y una *descripción* detallada del problema extraída de los datos ofrecidos por el sistema de monitorización.

   En la parte de la derecha del formulario se especifican los siguientes datos:

   - *Fecha de apertura de la incidencia*: Normalmente la fecha en la que se crea el ticket, aunque también puede ser otra.
   - *Tipo*: En este caso “Incidencia”.
   - *Estado*: “Nuevo”, dado que es una nueva petición.

- *Origen de la petición*: "Monitorización", dado que la incidencia se ha detectado en el sistema de monitorización, aunque también puede ser "Otro" (si la incidencia la detecta un técnico sin ayuda de una herramienta).
- *Urgencia*: En este caso "Alta", aunque dependiendo de la urgencia de la incidencia también puede ser "Muy baja, Baja, Media o Muy Alta".
- *Impacto*: En este caso "Alto", aunque dependiendo del impacto de la incidencia también puede ser "Muy bajo, Bajo, Medio o Muy Alto".
- *Prioridad*: En este caso "Alta", aunque dependiendo de la prioridad que se le quiera asignar a la incidencia también puede ser "Muy baja, Baja, Media, Muy Alta o Primordial".
- *Solicitante*: Es el técnico que abre el ticket.
- *Asignada a*: Es el técnico que procesa el ticket. Normalmente se la asigna el mismo técnico que lo solicita, aunque puede ser adjudicado a cualquier otro técnico por un compañero o un nivel superior.

Una vez cumplimentado todos los datos, creamos el ticket pulsando el botón **Añadir** para que este pase a estar disponible para su asignación.

3. Este apartado se resuelve de la misma forma que el apartado 3 del ejemplo anterior Anexo XV. Ejemplo 1.

4. Para finalizar la gestión de la incidencia, se informa al responsable del servicio o sistema afectado por correo electrónico para que tenga constancia de lo ocurrido.

   Dicho responsable podemos encontrarlo en el documento *Matriz de contactos* que se encuentra en la carpeta "/SOS" de la base de conocimientos.

Inconvenientes que pueden surgir al resolver los tickets relativos a incidencias

En los ejemplos comentados, podemos observar que las incidencias se resuelven de una forma más o menos sencilla, ya que existe una instrucción técnica que ofrece la información necesaria para su resolución, pero también puede pasar que se complique y que no se pueda avanzar por diversos motivos, bien porque no se conozca un proceso que ayude con su resolución, o bien porque haya que elevarlo al no tener suficientes permisos o conocimientos que permitan su resolución.

A continuación, se describen las causas que pueden generar nuevos estados en los tickets, debido a que no se puede avanzar con su resolución por algunos de los motivos comentados:

- El ticket necesita alguna acción que incumba a otro departamento, permiso o autorización, persona, etc.

  En este caso se pone en pausa, cambiando su estado a “En espera”, pudiendo ser retomado en cualquier momento.

- El técnico no conoce procedimiento que pueda solucionar el problema.

  En este caso el técnico debe asignarle el ticket a un técnico de segundo nivel, el cual podrá verlo en su listado de pendientes, además de llegarle un aviso por correo electrónico.

  De esta misma forma, si un técnico de segundo nivel no puede avanzar, podrá asignarlo a un técnico especialista de tercer nivel.

- El ticket que está siendo procesado no se finaliza porque el técnico de turno acaba su jornada.

  En este caso se realiza una reasignación del ticket al técnico que lo releva en su puesto sin cambiar el estado, que seguirá siendo “En curso (asignada)” y de esta forma se podrá garantizar que se continue con la tarea.

Anexo XVI: Procedimiento programado (ejemplo e inconvenientes)

Ejemplo: Caso práctico de ejecución de un procedimiento programado

A continuación, se describen los pasos que un técnico de primer nivel deberá realizar para ejecutar un procedimiento programado comunicado a través de correo electrónico por el responsable de un departamento, aunque también pueden ser procedimientos que deban realizarse de forma periódica:

1. En el buzón de solicitudes del NOC se recibe un correo entrante donde se solicita la ejecución de un procedimiento programado.

Instalación de agente de monitorización en dos nuevos equipos Ubuntu

De: a.paz@tfg.com

Para: solicitudes@tfg.com

Fecha: 24/03/2023 16:22

Se solicita la instalación del agente de Zabbix para su posterior monitorización a los equipos que actualmente se encuentran en proceso de instalación y configuración (PC-UBUDSK-000001 y PC-UBUDSK-000002).

Los equipos anteriores estarán finalizados el 29/03/2023 a las 10:00.

Figura 123: Procedimiento prog. Ejemplo - Correo solicitando un procedimiento

2. El técnico de turno encargado de la revisión del buzón de solicitudes crea un ticket con los datos de la solicitud.

   Para crear un nuevo ticket es necesario acceder al tablero de la herramienta GLPI y pulsar en el menú de la izquierda “Soporte – Abrir petición”, una vez cargado el formulario, es necesario completar los datos de la solicitud añadiéndolos al ticket.

   En la parte izquierda del formulario se rellenan los datos relativos a la solicitud, asignándole un *título* representativo y una *descripción* detallada del procedimiento a realizar extraída del correo electrónico anterior. También se añade información adicional, como el documento necesario para poder ejecutar el procedimiento que se encuentra en la base de conocimientos.

   En la parte de la derecha del formulario se especifican los siguientes datos:

   - *Fecha de apertura de la solicitud*: Fecha en la que se planifica que dé comienzo el procesamiento del ticket.

- *Tipo*: En este caso “Solicitud”.
- *Estado*: “En curso (planificada)”, dado que es una solicitud programada.
- *Origen de la petición*: “E-mail”, dado que la solicitud se ha realizado por esta vía. Se descartan otras vías de comunicación, dado que es de vital importancia que quede constancia de dicha solicitud por escrito.
- *Urgencia*: “Alta” en este caso, aunque dependiendo de la urgencia de la incidencia también puede ser “Muy baja, Baja, Media o Muy Alta”.
- *Impacto*: “Alto” en este caso, aunque dependiendo del impacto de la incidencia también puede ser “Muy bajo, Bajo, Medio o Muy Alto”.
- *Prioridad*: “Alta” en este caso, aunque dependiendo de la prioridad que se le quiera asignar a la incidencia también puede ser “Muy baja, Baja, Media, Muy Alta o Primordial”.
- *Solicitante*: Es el técnico que abre el ticket.
- *Asignada a*: Es el técnico que procesa el ticket.

Una vez cumplimentado todos los datos, creamos el ticket pulsando el botón **Añadir** para que este pase a estar disponible para su asignación.

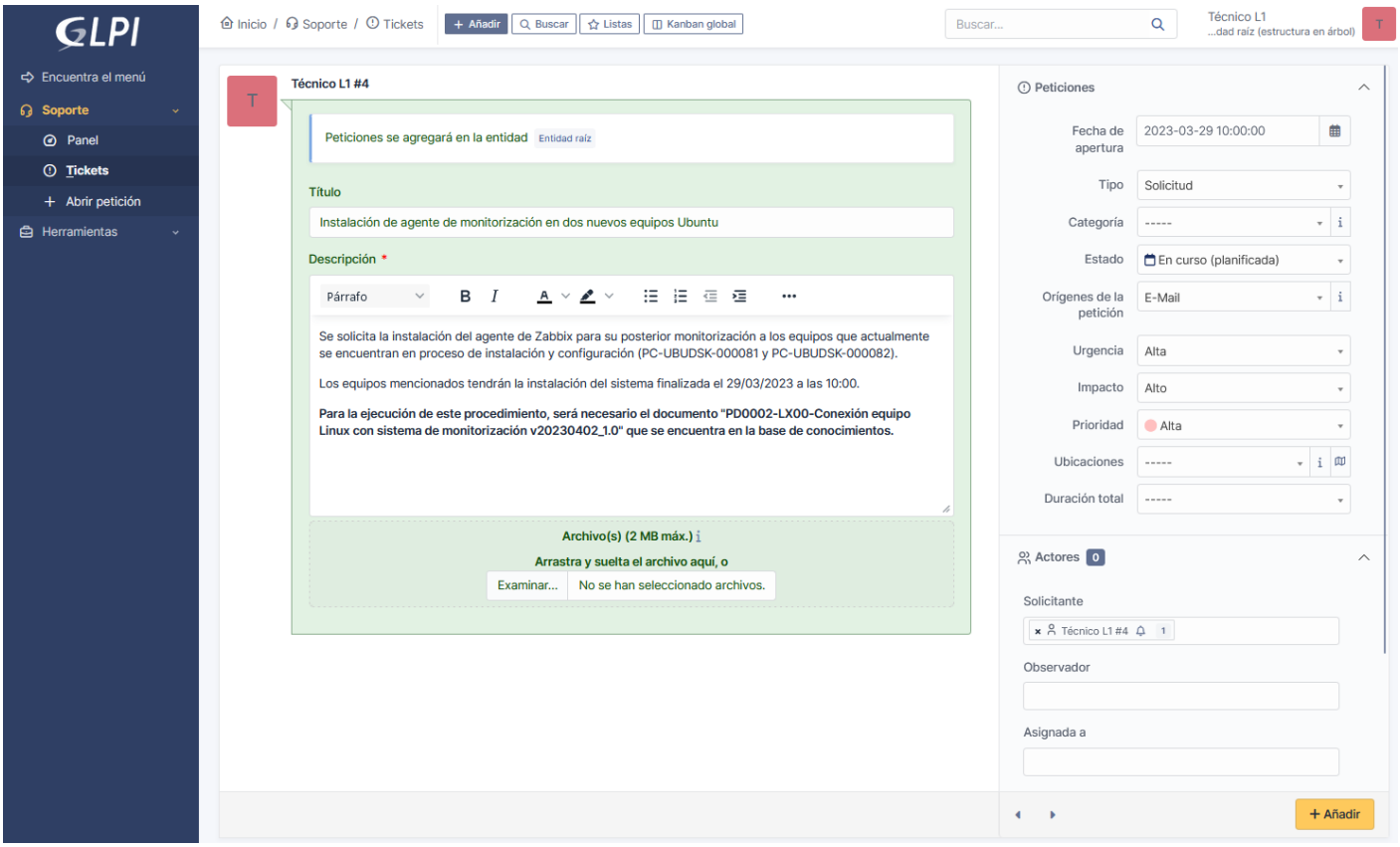


Figura 124: Procedimiento prog. Ejemplo - Crear ticket para procesar el procedimiento

Pulsando en el menú de la izquierda “Soporte – Tickets”, podemos ver el nuevo ticket con “ID 7”, estado “En curso (planificada)”, tipo “Solicitud” y sin asignar a ningún técnico.

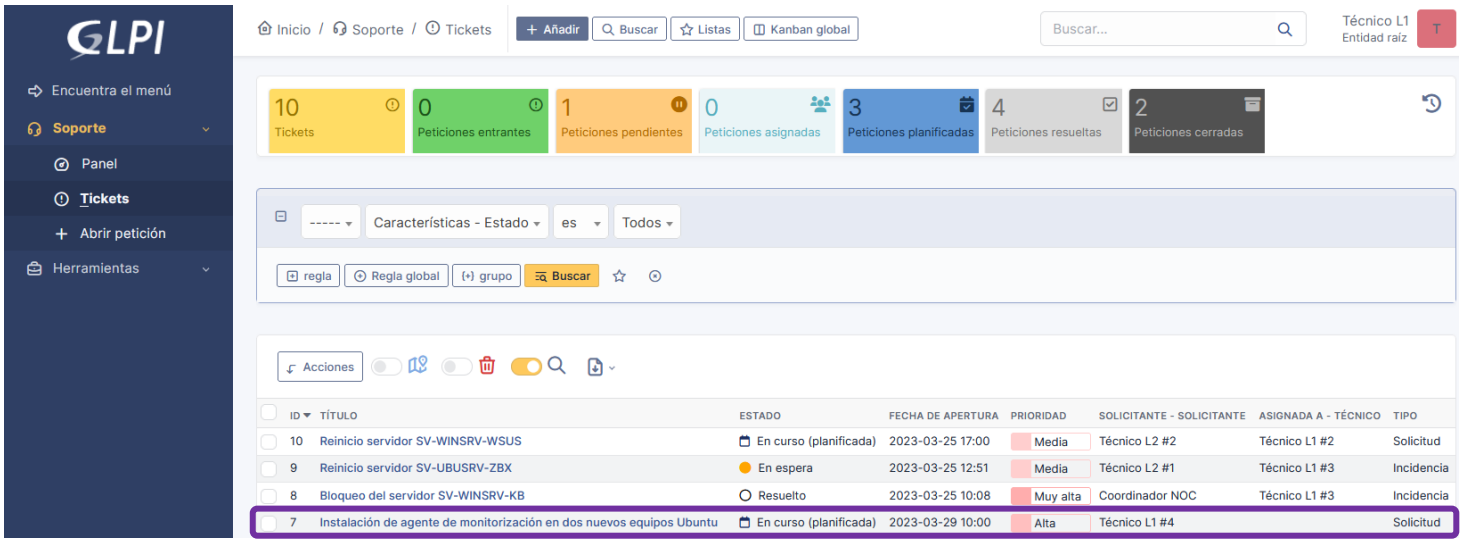


Figura 125: Procedimiento prog. Ejemplo - Estado del ticket “En curso (planificado)”

3. Una vez llegada la fecha planificada, el técnico encargado se asigna el ticket si aún no lo está, aunque también puede ser asignado por cualquier técnico del departamento a cualquier compañero con bastante antelación, para permitir una mejor planificación.

   Continuando con el ejemplo, el técnico número 2 de primer nivel será el encargado de realizar el procedimiento, por lo que deberá tener asignado el ticket para poder comenzar con su ejecución.

   A continuación, se detallará el proceso de asignación y ejecución del procedimiento:

   - Pulsamos sobre el ticket creado anteriormente y realizamos la asignación seleccionando en el desplegable del campo *Asignada a*, el técnico que va a procesar la incidencia, en este caso “Técnico L1 #2”. Una vez seleccionado el técnico pulsamos sobre el botón **Guardar**.

Figura 126: Procedimiento prog. Ejemplo - Asignación de ticket a un técnico

- Una vez asignado el ticket, se comienza con su ejecución. Para ello se vuelve a pulsar sobre el ticket, donde se irá comentando las acciones realizadas en la ejecución del procedimiento.

  Como primera tarea para poder ejecutar el procedimiento, el técnico debe consultar la documentación necesaria, localizándola en la base de conocimientos. El documento utilizado debe quedar reflejado en los comentarios del ticket y en caso de que no exista ningún documento, solamente mencionarlo.

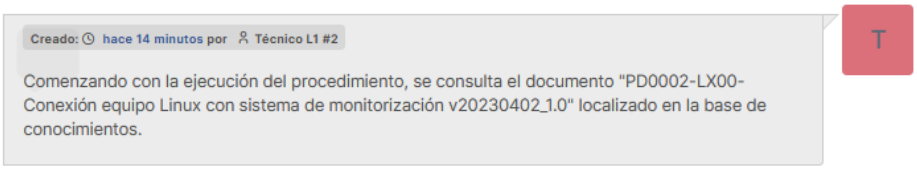


Figura 127: Procedimiento prog. Ejemplo - Añadido comentario al ticket

Una vez el técnico tiene claro las tareas a realizar, procede a ejecutarlas, añadiendo la información más relevante y pasos realizados al ticket:

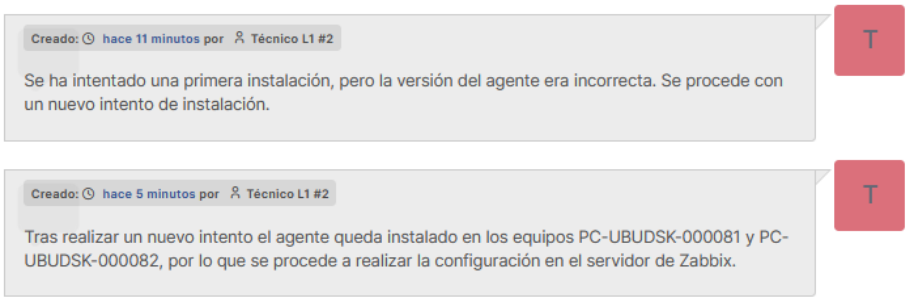


Figura 128: Procedimiento prog. Ejemplo - Añadidos más comentarios al ticket

Tras ejecutar dicho procedimiento, hay que añadir un comentario de solución o de cierre al ticket, que automáticamente modificará su estado a “Resuelto” y guardará la fecha de resolución.

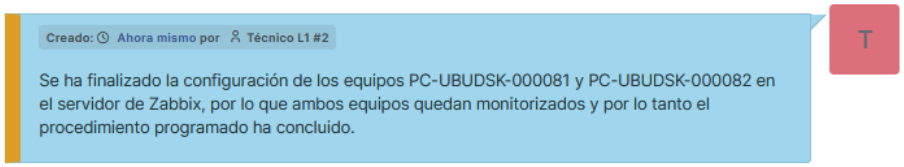


Figura 129: Procedimiento prog. Ejemplo - Comentario de cierre del ticket

En las siguientes imágenes se puede observar el ticket completo incluyendo sus comentarios antes de guardar los cambios y el estado final del ticket tras guardar los cambios.

Figura 130: Procedimiento prog. Ejemplo - Ticket resuelto y completo

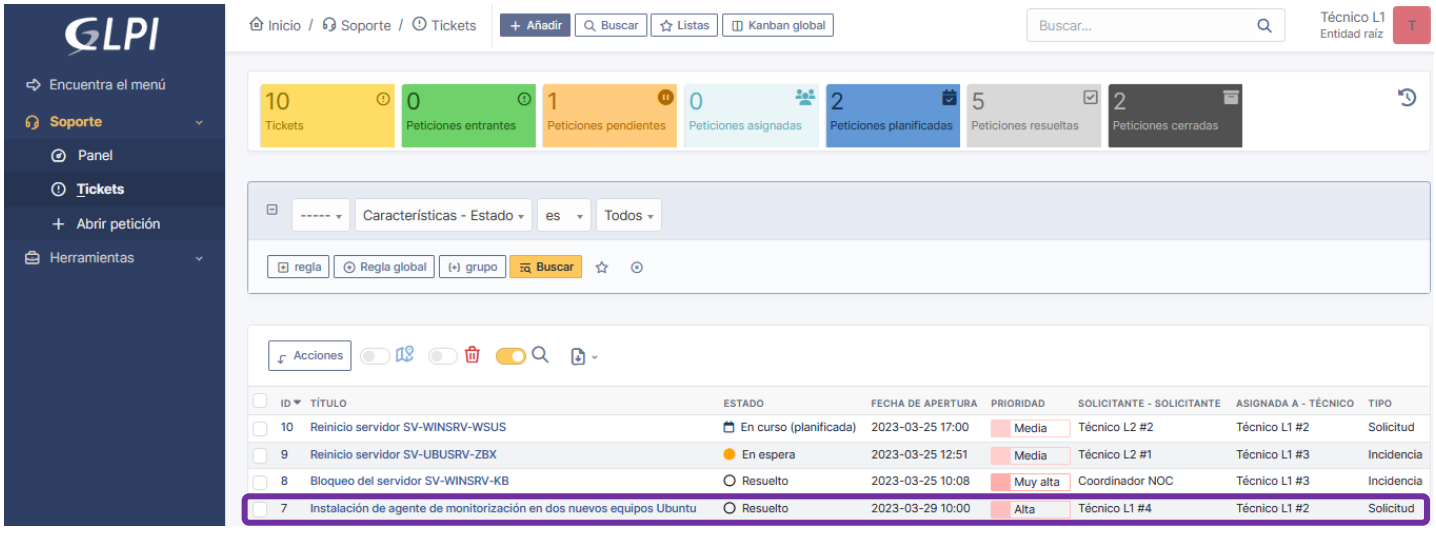


Figura 131: Procedimiento prog. Ejemplo - Estado del ticket "Resuelto"

4. Para finalizar la ejecución del procedimiento programado, se informa al usuario que solicitó dicho procedimiento mediante correo electrónico, respondiendo al mensaje de la solicitud y explicando de forma breve si ha surgido algún altercado durante la realización del procedimiento.

Inconvenientes que pueden surgir al resolver los tickets relativos a procedimientos

En el ejemplo comentado, podemos observar que la ejecución del procedimiento transcurre sin grandes altercados, ya que existe un documento que ofrece la información necesaria para su ejecución, pero también puede pasar que se complique y que no se pueda avanzar por diversos motivos, bien porque desde que se realizó el documento hayan surgido cambios importantes, o bien porque haya que elevarlo al no tener suficientes permisos o conocimientos que permitan su resolución.

En el caso de que no se pueda avanzar por cualquier motivo en un procedimiento programado, la situación cobra especial importancia y urgencia, ya el procedimiento estaba planificado y esto puede requerir hacerlo en momentos en que los sistemas se encuentran en mantenimiento o en una parada planificada, por lo que, en este caso el ticket se convierte en crítico y hay que solucionarlo en el menor tiempo posible.

A continuación, se describen las causas que pueden generar nuevos estados en los tickets, debido a que no se puede avanzar con ejecución del procedimiento programado por algunos de los motivos comentados:

- El ticket necesita alguna acción no detectada o que no se ha tenido en cuenta, que incumba a otro departamento, permiso o autorización, persona, etc.

  En este caso se pone en pausa, cambiando su estado a “En espera”, se modifica la urgencia a “Muy Alta”, el impacto dependerá de la importancia del sistema afectado y la prioridad “Primordial”, pudiendo ser retomado en cualquier momento.

- El técnico conoce procedimiento, pero pese a ello se producen errores que no se reconocen de forma fácil.

  En este caso el técnico debe asignarle el ticket a un técnico de segundo nivel, cambiando la urgencia a “Muy Alta”, el impacto dependerá de la importancia del sistema afectado y la prioridad “Primordial”. Una vez asignado el ticket a una técnico de segundo nivel, este podrá verlo en su listado de pendientes, además de llegarle un aviso por correo electrónico.

  De esta misma forma si un técnico de segundo nivel no puede avanzar, podrá asignarlo a un técnico especialista de tercer nivel.

- El ticket que está siendo procesado no se acaba porque el técnico de turno acaba su jornada.

  En este caso se realiza una reasignación del ticket al técnico que lo releva en su puesto, sin cambiar el estado, que seguirá siendo “En curso (asignada)”, pero si la urgencia a “Muy Alta”, y de esta forma se podrá garantizar que se continue con la tarea de forma prioritaria.

Anexo XVII: Aplicación de actualizaciones (ejemplo e inconvenientes)

Ejemplo: Caso práctico de aplicación de actualizaciones mediante WSUS

A continuación, se describen los pasos que un técnico de primer nivel deberá realizar para aplicación periódica de actualizaciones en equipos Windows mediante la herramienta WSUS como un nuevo servicio, solicitado por el responsable del departamento de ciberseguridad y aprobado por el coordinador del NOC:

1. En el buzón de servicios del NOC se recibió hace varios años, un correo entrante donde se realiza una petición para realizar una tarea periódica de actualización de sistemas Windows.

Petición para actualizar de forma periódica sistemas Windows

De: d.cueto@tfg.com

Para: servicios@tfg.com

Fecha: 18/08/2019 12:30

Se solicita al NOC la aplicación de actualizaciones de forma periódica mensual de los sistemas Windows como uno más de sus servicios.

También la regularización de las actualizaciones y puesta al día de sistemas Windows de reciente instalación.

Estos sistemas deben quedar completamente actualizados en un plazo máximo de cinco días tras su instalación, convirtiéndose en una prioridad a partir del tercer día.

Se comunicará al NOC la disponibilidad para poder acceder al sistema con una antelación de al menos siete días, para que puedan planificar correctamente la intervención.

Se pide la puesta en marcha de esta solicitud a la mayor brevedad posible y será válida indefinidamente mientras no se reciba una notificación de modificación.

Departamento de Ciberseguridad

Figura 132: Actualizaciones. Ejemplo - Correo solicitando aplicación actualizaciones

2. Tras la revisión del buzón de petición de servicios por parte del coordinador del NOC y tras una primera valoración, se acepta la petición del departamento de ciberseguridad y se procede con la planificación mensual para la aplicación de actualizaciones en sistemas Windows de forma periódica.

También se realizará la aplicación de actualizaciones para regularizar y poner al día los sistemas de nueva instalación. Los correos que informan de la disponibilidad del sistema para su acceso y aplicación de actualizaciones se recibirán en el buzón de solicitudes (solicitudes@tfg.com) y se gestionarán de la misma forma que un procedimiento programado, cuya fecha de ejecución nunca podrá ser posterior a cinco días (aumentando la prioridad a partir del tercer día) desde que el sistema este accesible.

Una vez aceptado y definido el nuevo servicio que ofrecerá el NOC, nos centraremos en la planificación mensual de actualizaciones Windows, ya que las peticiones para realizar actualizaciones en los sistemas de nueva instalación se tratarán como un procedimiento programado, del cual podemos consultar un ejemplo de ejecución en el Anexo XVI. Ejemplo.

3. Procediendo con la tarea de actualización mensual de equipos Windows, el técnico de turno encargado crea un ticket con los datos de la solicitud periódica.

   Para crear un nuevo ticket es necesario acceder al tablero de la herramienta GLPI y pulsar en el menú de la izquierda “Soporte – Abrir petición”, una vez cargado el formulario, es necesario completar los datos de la solicitud periódica añadiéndolos al ticket.

   En la parte izquierda del formulario se rellenan los datos relativos a la solicitud periódica, asignándole un *título* representativo y una *descripción* detallada de la actuación a realizar. También se añade información adicional, como la guía que hay que seguir para poder actualizar los sistemas y que se encuentra en la base de conocimientos.

   En la parte de la derecha del formulario se especifican los siguientes datos:

   - *Fecha de apertura de la solicitud*: Fecha en la que se planifica que dé comienzo el procesamiento del ticket.
   - *Tipo*: En este caso “Solicitud”.
   - *Estado*: “En curso (planificada)”, dado que es una solicitud programada de forma periódica.
   - *Origen de la petición*: “Servicio”, dado que es parte del servicio que ofrece el NOC. Se descartan otras vías de comunicación.
   - *Urgencia*: “Media” en este caso, aunque dependiendo de la urgencia de la incidencia también puede ser “Muy baja, Baja, Alta o Muy Alta”.
   - *Impacto*: “Alto” en este caso, aunque dependiendo del impacto de la incidencia también puede ser “Muy bajo, Bajo, Medio o Muy Alto”.

- Prioridad: “Media” en este caso, aunque dependiendo de la prioridad que se le quiera asignar a la incidencia también puede ser “Muy baja, Baja, Alta, Muy Alta o Primordial”.
- Solicitante: Es el técnico que abre el ticket.
- Asignada a: Es el técnico que procesa el ticket.

Una vez cumplimentado todos los datos, creamos el ticket pulsando el botón **Añadir** para que este pase a estar disponible para su asignación.

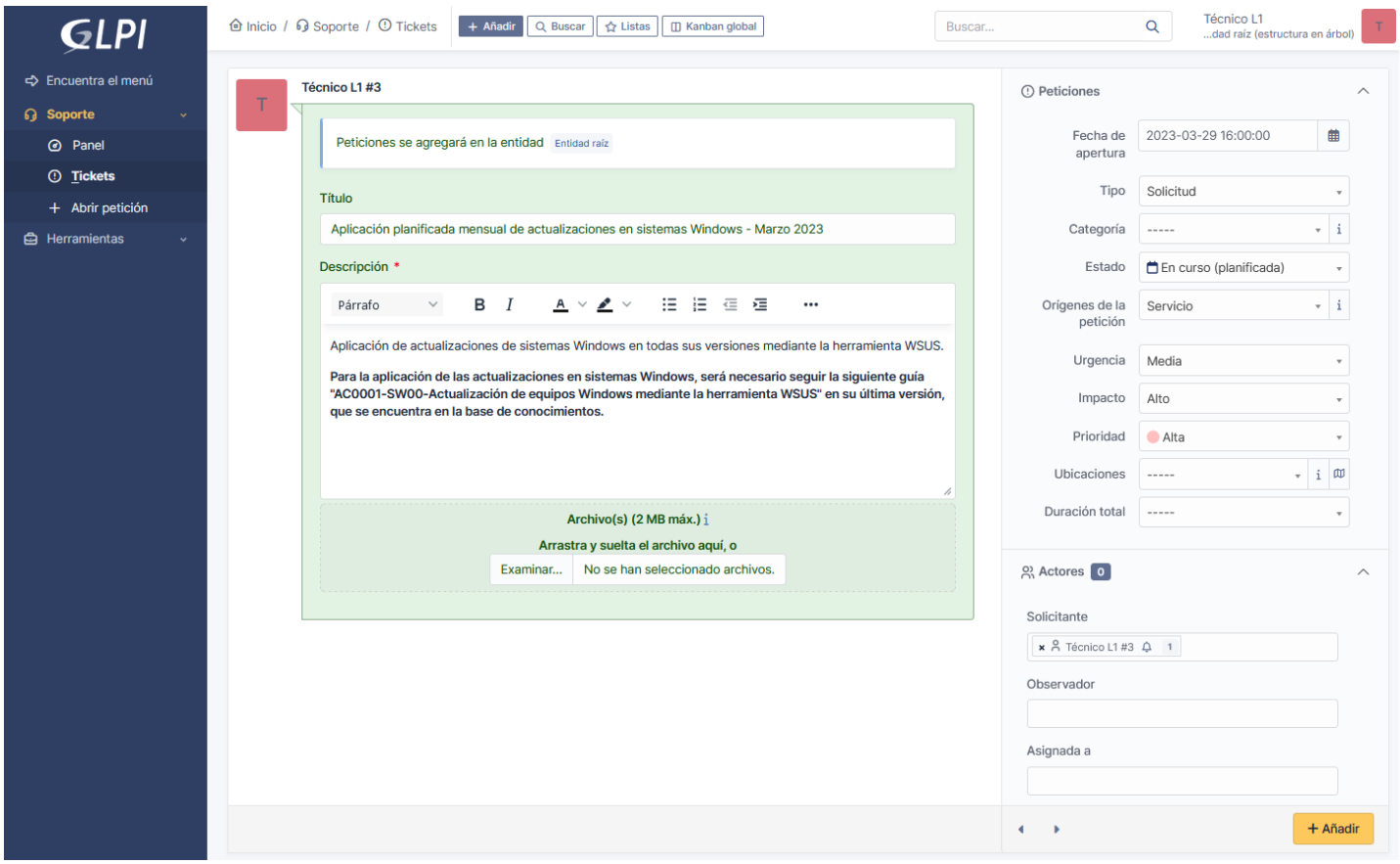


Figura 133: Actualizaciones. Ejemplo - Crear ticket para procesar la tarea de actualización

Pulsando en el menú de la izquierda “Soporte – Tickets”, podemos ver el nuevo ticket con “ID 16”, estado “En curso (planificada)”, tipo “Solicitud” y sin asignar a ningún técnico.

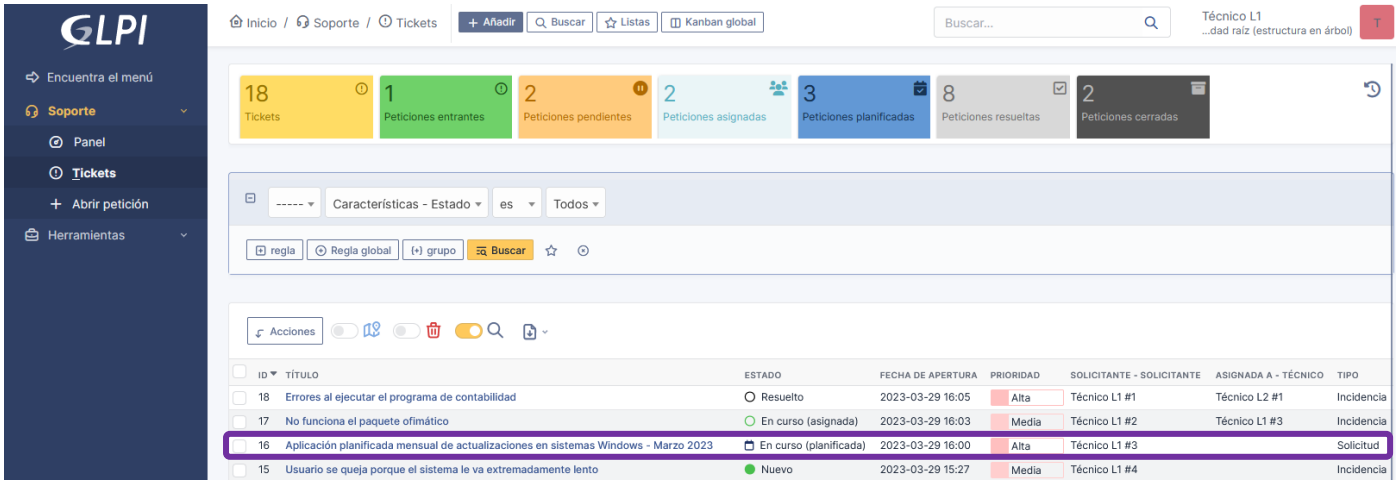


Figura 134: Actualizaciones. Ejemplo - Estado del ticket “En curso (planificado)”

4. Una vez llegada la fecha planificada, el técnico encargado se asigna el ticket si aún no lo está, aunque también puede ser asignado por cualquier técnico del departamento a cualquier compañero con bastante antelación, para permitir una mejor planificación.

   Continuando con el ejemplo, el técnico número 1 de primer nivel será el encargado de realizar la tarea de actualización, por lo que deberá tener asignado el ticket para poder comenzar con su ejecución.

   A continuación, se detallará el proceso de asignación y ejecución de la tarea de actualización:

   - Pulsamos sobre el ticket creado anteriormente y realizamos la asignación seleccionando en el desplegable del campo *Asignada a*, el técnico que va a procesar la incidencia, en este caso “Técnico L1 #1”. Una vez seleccionado el técnico pulsamos sobre el botón **Guardar**.

Figura 135: Actualizaciones. Ejemplo - Asignación de ticket a un técnico

- Una vez asignado el ticket, se comienza con su ejecución. Para ello se vuelve a pulsar sobre el ticket, donde se irá comentando las acciones realizadas en la ejecución del proceso de actualización.

  Como primera tarea para poder ejecutar el procedimiento, el técnico debe consultar la documentación necesaria, localizándola en la base de conocimientos. El documento utilizado debe quedar reflejado en los comentarios del ticket y en caso de que no exista ningún documento, solamente mencionarlo.

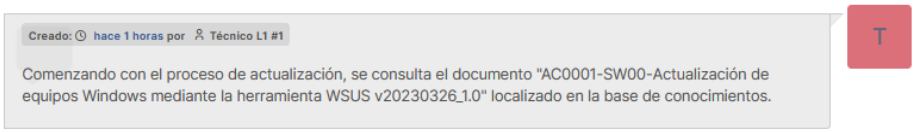


Figura 136: Actualizaciones. Ejemplo - Añadido comentario al ticket

- Después de haber leído la documentación, el técnico procede a realizar una revisión en la herramienta WSUS para ver el estado de los sistemas y las actualizaciones que demandan cada uno de los equipos y servidores.

  En la siguiente imagen podemos observar que hay un equipo “PC-WIN10” y un servidor “SV-WINSRV-WSUS”, siendo este último el que demanda la aplicación de solamente una actualización.

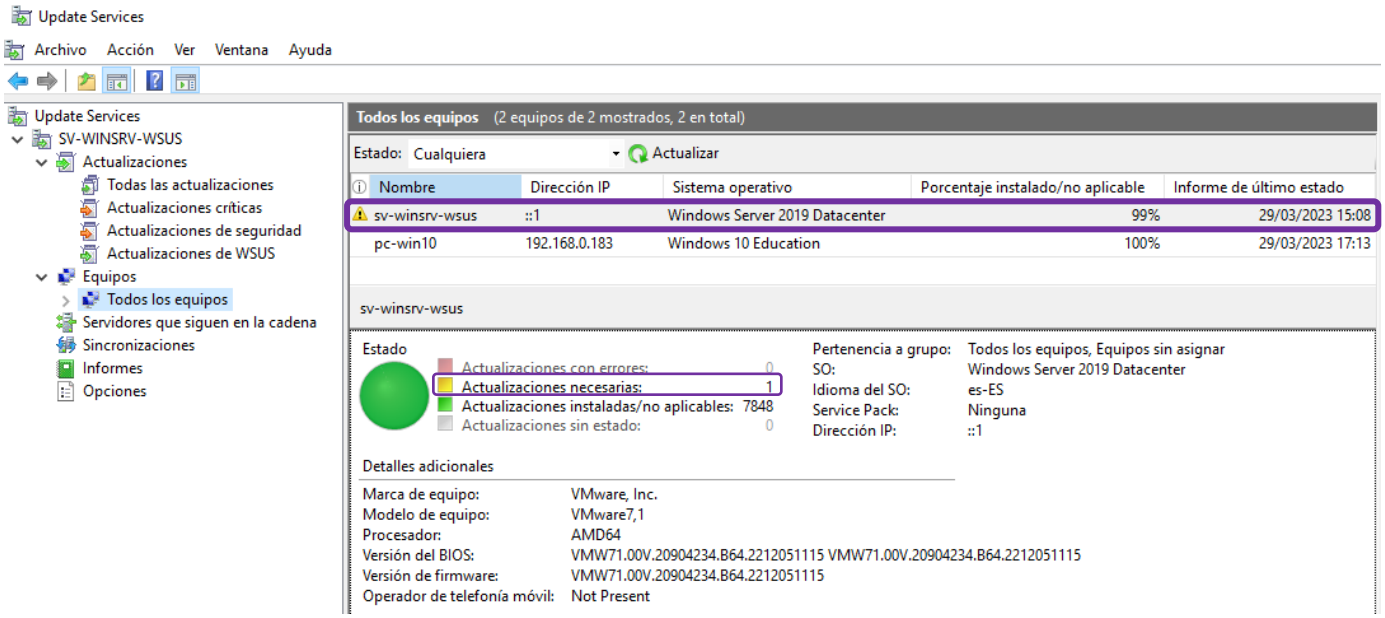


Figura 137: Actualizaciones. Ejemplo - Consola WSUS. Estado de actualización inicial

En la siguientes imágenes podemos observar los detalles de la actualización que hay que aplicar en el servidor “SV-WINSRV-WSUS”.

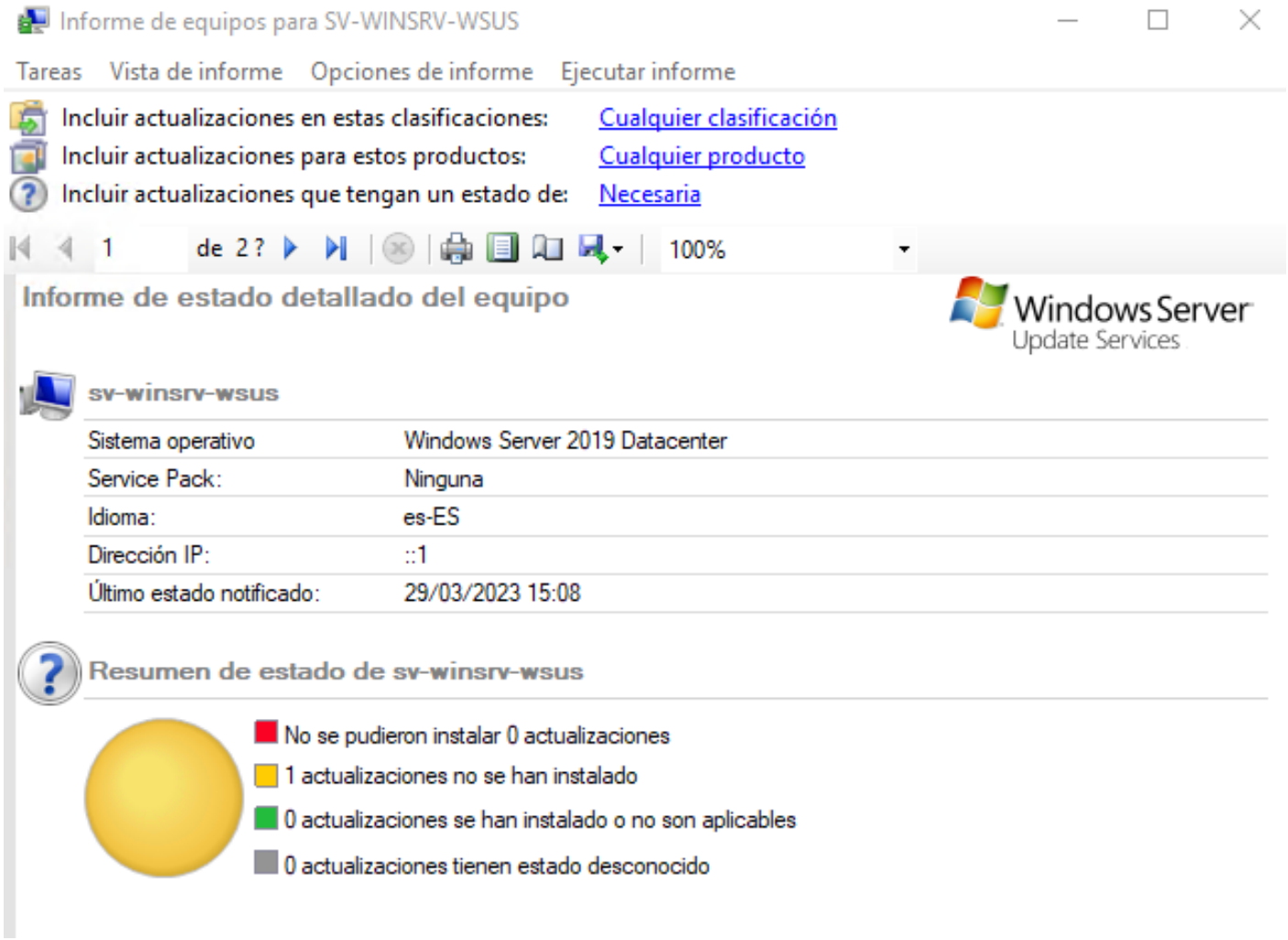


Figura 138: Actualizaciones. Ejemplo - Consola WSUS. Detalle actualización faltante 1

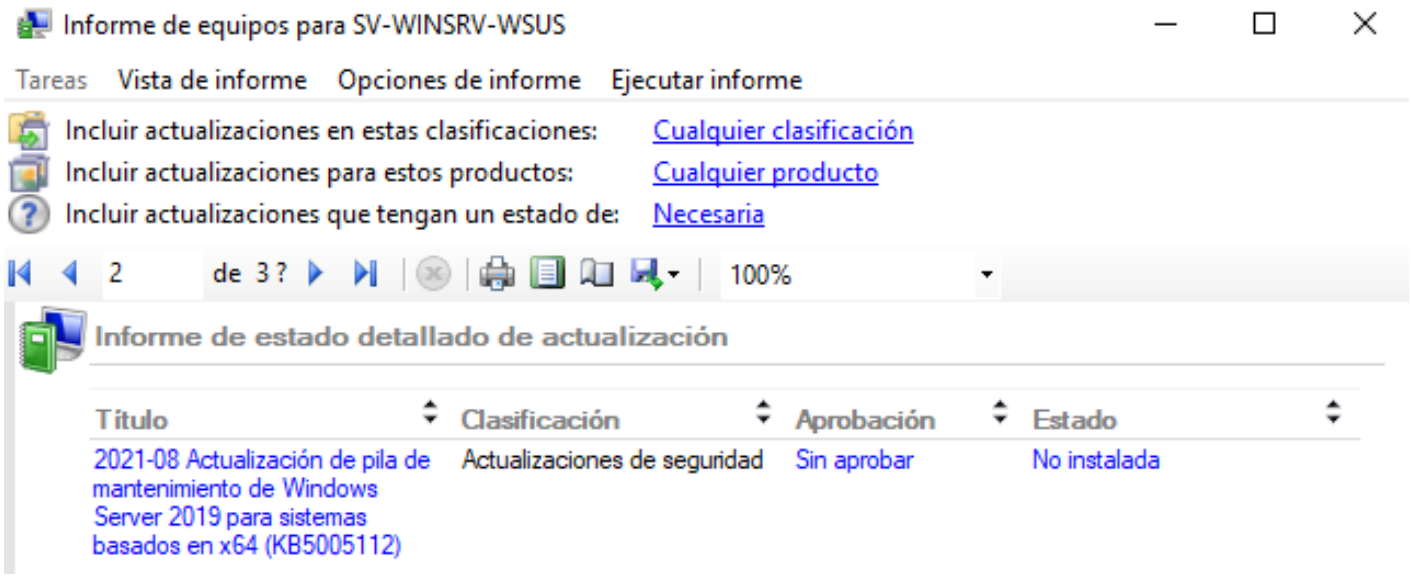


Figura 139: Actualizaciones. Ejemplo - Consola WSUS. Detalle actualización faltante 2

En la siguientes imágenes podemos observar el procedimiento de aprobación de la actualización, para que los equipos que la demanden puedan comenzar con su instalación. El tiempo de actualización tras la aprobación puede variar dependiendo del sistema y cuando le toque a este comunicarse con WSUS.

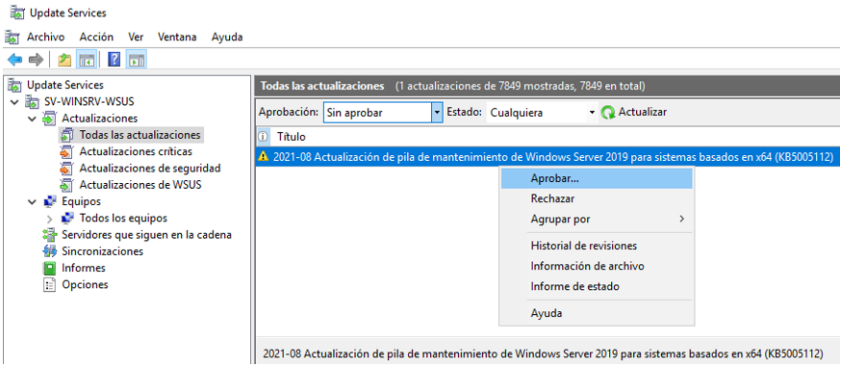


Figura 140: Actualizaciones. Ejemplo - Consola WSUS. Aprobación de actualizaciones 1

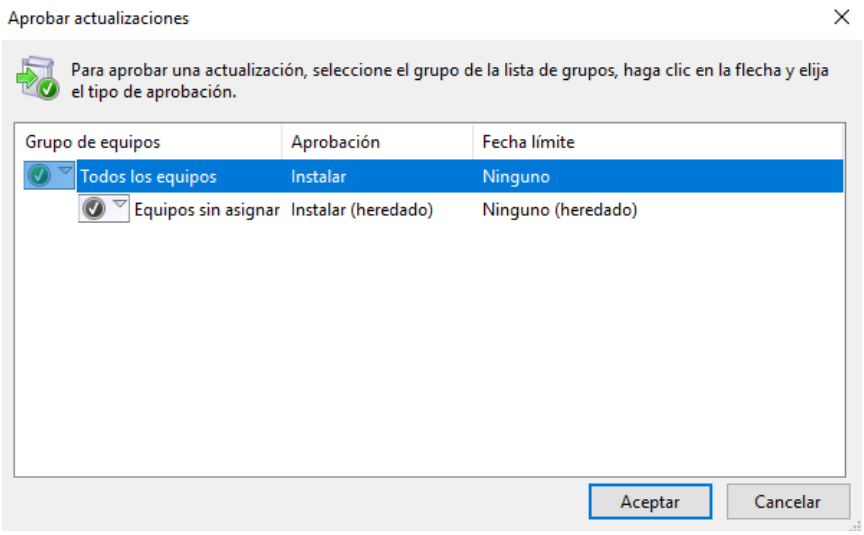


Figura 141: Actualizaciones. Ejemplo - Consola WSUS. Aprobación de actualizaciones 2

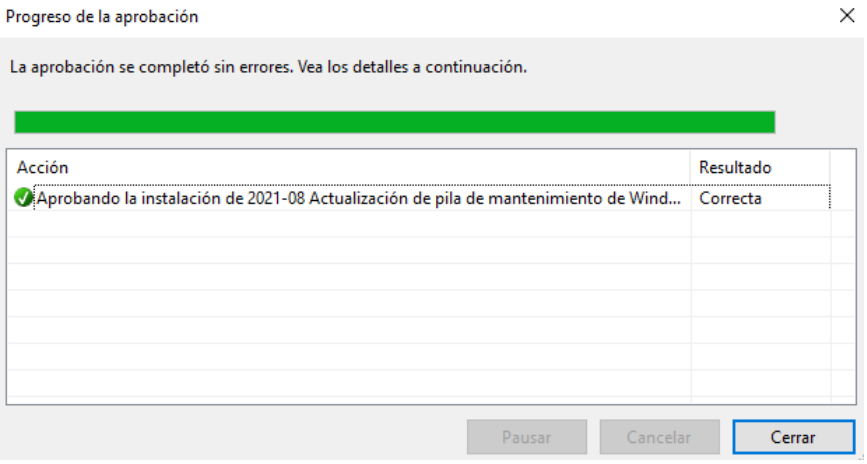


Figura 142: Actualizaciones. Ejemplo - Consola WSUS. Aprobación de actualizaciones 3

Realizada la revisión y aprobadas las actualizaciones, se agrega al ticket un segundo comentario, que describirá el estado de los sistemas y a cuáles se le han aplicado actualizaciones.

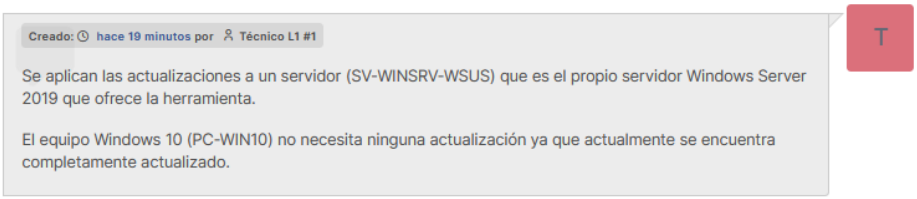


Figura 143: Actualizaciones. Ejemplo - Añadido comentario equipos actualizados

El comentario anterior es muy útil en el caso que ocurra algún problema derivado de la actualización del sistema, ya que nos proporcionará información que servirá para relacionar si el problema es derivado del proceso de actualización, además de poder remediarlo dando marcha atrás como plan de contingencia, mientras se busca una alternativa.

- Una vez desplegadas las actualizaciones a instalar, el técnico debe comprobar que estas se apliquen de forma adecuada, revisando para ello la información de reporte en la consola de WSUS y el estado de actualización del sistema.

  Para ver que el proceso se lleva a cabo, accedemos al servidor "SV-WINSRV-WSUS" y revisaremos que se aplican las actualizaciones de forma adecuada.

  En la siguientes imágenes podemos observar el proceso de actualización del servidor y el mensaje que informa de que el sistema está actualizado correctamente.

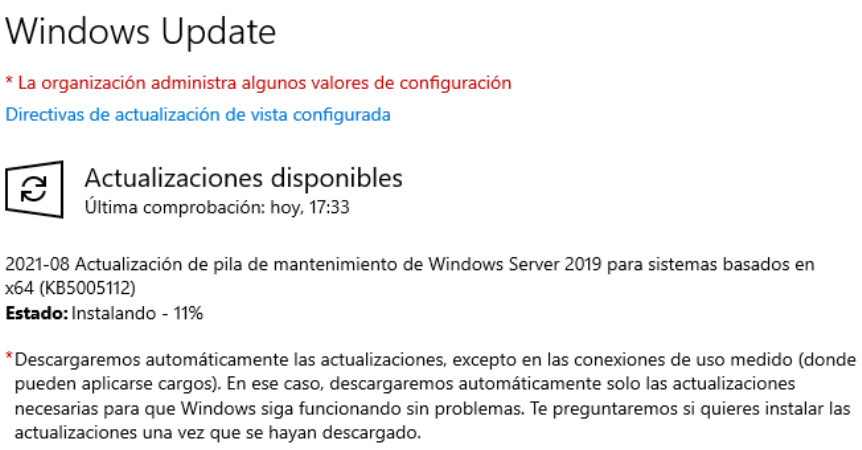


Figura 144: Actualizaciones. Ejemplo - Sistema Windows. Aplicación de actualizaciones

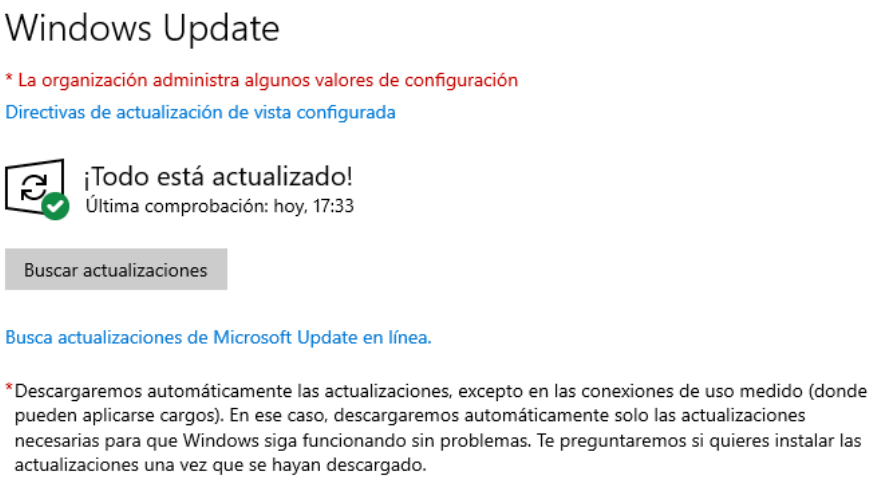


Figura 145: Actualizaciones. Ejemplo - Sistema Windows. Finalización de actualizaciones

En la siguiente imagen podemos observar desde la consola de WSUS, que el servidor "SV-WINSRV-WSUS" ha quedado completamente actualizado, al igual que el equipo "PC-WIN10".

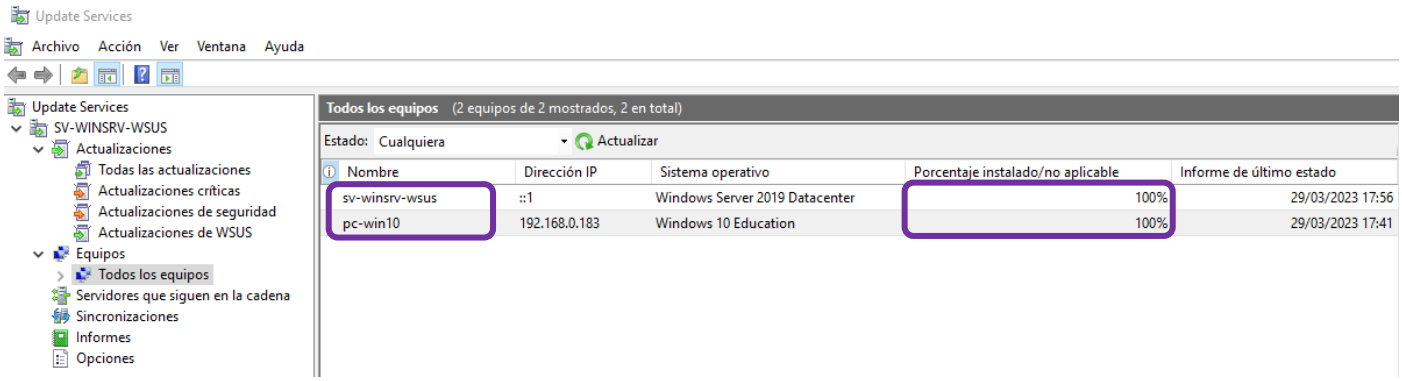


Figura 146: Actualizaciones. Ejemplo - Consola WSUS. Estado de actualización final

Una vez finalizado el procedimiento de actualización, hay que añadir un comentario de solución o de cierre al ticket, que automáticamente modificará su estado a "Resuelto" y guardará la fecha de resolución.

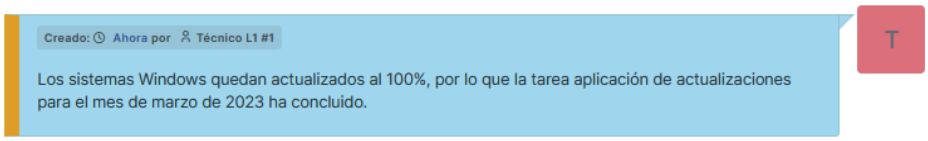


Figura 147: Actualizaciones. Ejemplo - Comentario de cierre del ticket

En la siguientes imágenes se puede observar el ticket completo incluyendo sus comentarios antes de guardar los cambios y el estado final del ticket tras guardar los cambios.

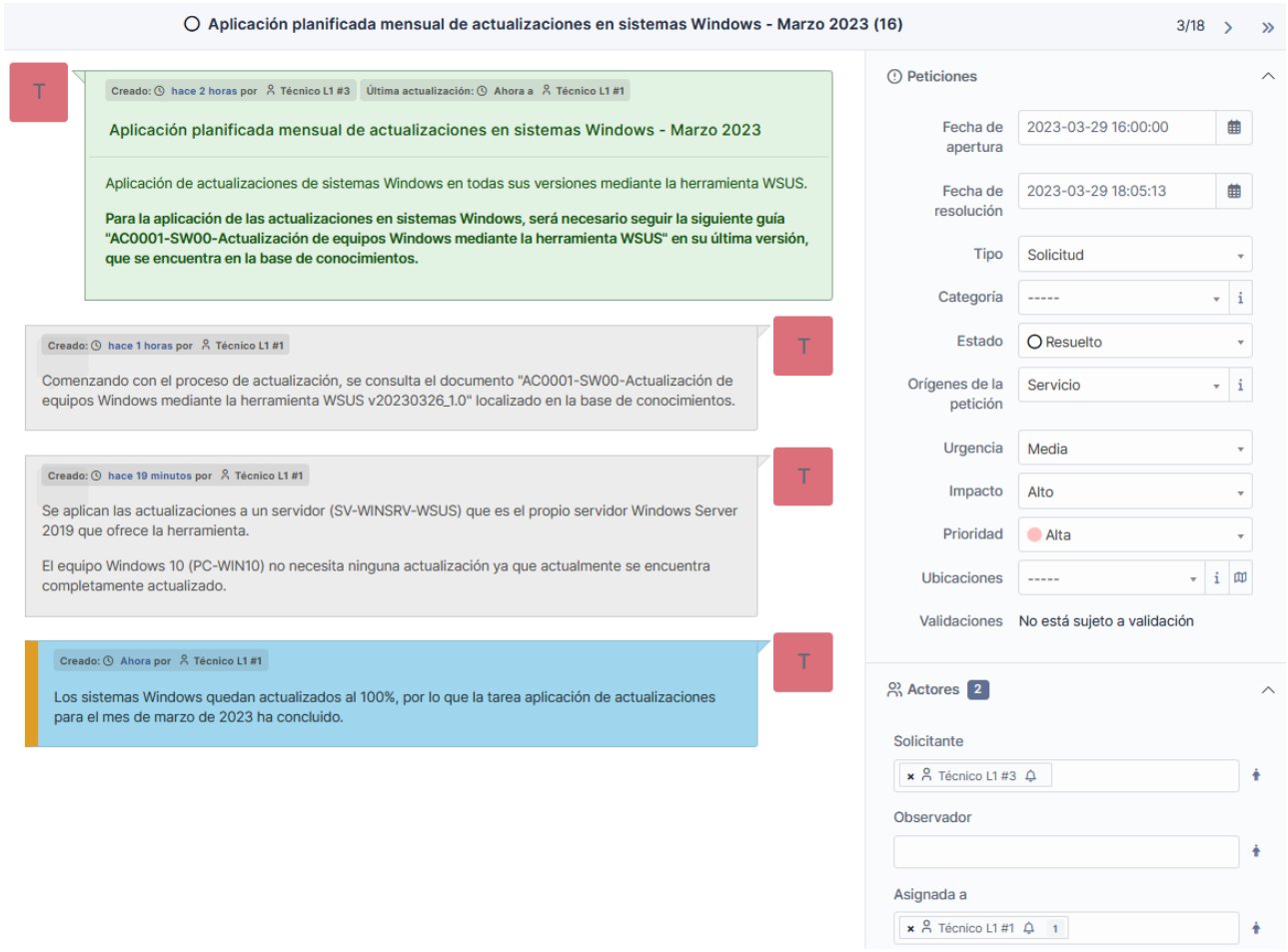


Figura 148: Actualizaciones. Ejemplo - Ticket resuelto y completo

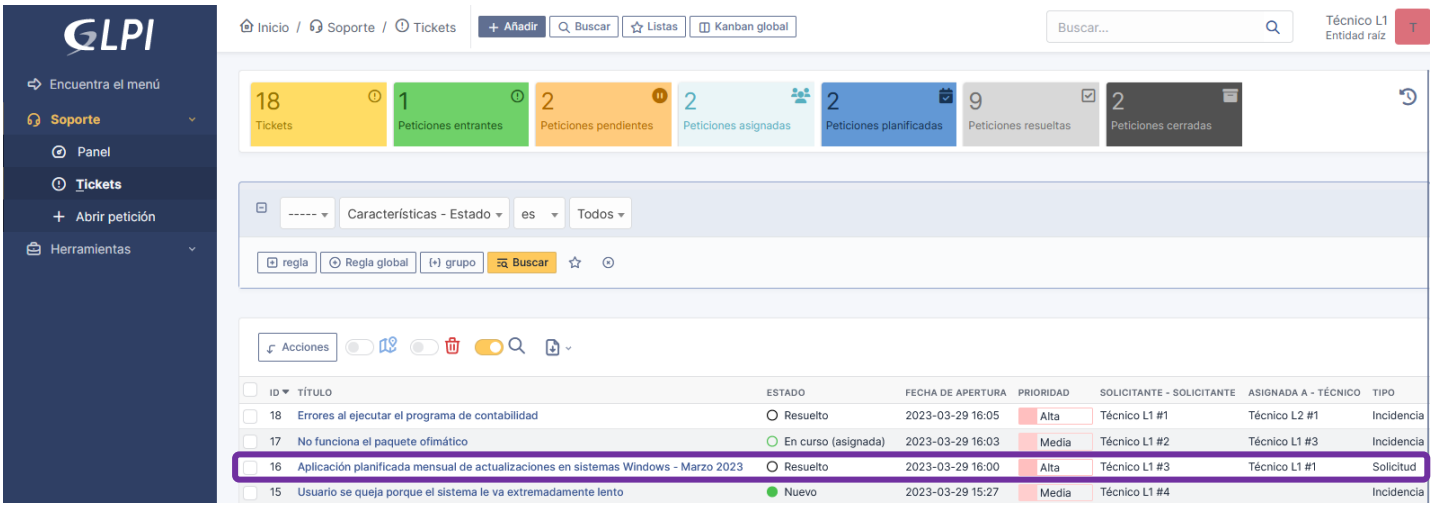


Figura 149: Actualizaciones. Ejemplo - Estado del ticket "Resuelto"

5. Para finalizar la tarea de actualización, se informa al responsable del departamento mediante correo electrónico, explicando de forma breve si ha surgido algún altercado durante la realización del procedimiento de actualización.

Inconvenientes que pueden surgir al aplicar actualizaciones a un sistema

En el ejemplo comentado, podemos observar que la ejecución de la tarea de actualización transcurre sin grandes altercados, ya que existe un documento que ofrece la información necesaria para su ejecución, pero también puede pasar que se complique y que no se pueda avanzar por diversos motivos, bien porque desde que se hizo el documento hayan surgido cambios importantes, o bien porque se produzcan multitud de inconvenientes que impidan la correcta aplicación de actualizaciones.

En el caso de que no se pueda avanzar por cualquier motivo en una tarea de actualización, la situación puede volverse crítica, dependiendo de la gravedad de la interrupción en el sistema que se está actualizando y si existe pérdida de servicio o de datos. También hay que tener en cuenta que el tiempo estimado de la aplicación de actualizaciones no supere la ventana de tiempo planificada, sobre todo si se aprovecha un proceso de mantenimiento para realizar la actualización de los sistemas.

Si durante el proceso de actualización ocurre algún inconveniente, hay que comunicarse con el responsable de la tecnología de forma inmediata, que normalmente se localiza en el tercer nivel, para que proponga la solución más adecuada y modificar la urgencia del ticket convenientemente.

A continuación, se describen las causas que pueden generar nuevos estados en los tickets, debido a que no se puede avanzar con ejecución de las tareas de actualización:

- El equipo que se está actualizando se queda bloqueado y no avanza.

  En este caso debemos comprobar en la herramienta de monitorización, los recursos totales y consumidos del equipo que se está actualizando, aumentándolos si es necesario.

  En este escenario casi siempre se soluciona aumentando recursos, por lo que no es necesario modificar la urgencia ni la prioridad del ticket y simplemente añadir un comentario, pero si no se recupera el proceso de actualización, hay que comunicarse con el tercer nivel exponiéndole los hechos, aumentando la urgencia del ticket a “Muy Alta” y su prioridad a “Primordial”.

- El equipo que se quiere actualizar no ofrece información desde hace unos días.

  En este caso la política o el servicio encargados de la comunicación con WSUS no funcionan correctamente, por lo que hay que acceder a la máquina tiene el problema y realizar una serie de acciones correctoras.

  En este escenario casi siempre se soluciona ejecutando las medidas correctoras, por lo que no es necesario modificar la urgencia ni la prioridad del ticket y simplemente añadir un comentario, pero si no se consigue comunicar con el servidor WSUS a tiempo, puede ser necesario posponer la tarea y volver a solicitar una nueva ventana de tiempo para la intervención a su responsable.