GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
AGENCIA ESTATAL DE ADMINISTRACIÓN DIGITAL

Propuesta de mejora en las medidas de seguridad: Red Hat Satellite

Operativa del proyecto

Tipo de documento	Operativa del proyecto
Asunto	Propuesta de mejora en las medidas de seguridad: Red Hat Satellite
ID Redmine	300093
Versión	1.0
Fecha versión	04/04/2025


Financiado por la Unión Europea


Plan de Recuperación, Transformación y Resiliencia

HOJA DE CONTROL

Información del documento

Nombre del Documento:	Propuesta de mejora en las medidas de seguridad: Red Hat Satellite		
Responsable del Documento:	GRUPO-SISTEMAS-IAL1B	**Fecha de creación:**	04/04/2025
Ubicación			
Código:	300093	**Fecha último cambio:**	04/04/2025
Preparado por:		**Última versión:**	1.0
Revisado por:			
Ámbito de distribución:			
Descripción del documento:			

Lista de distribución

De	Fecha

Para	Acción*	Fecha de la acción

** Tipos de acción: Aprobar, Revisar, Informar, Archivar, Acción requerida, Asistir a reunión*

Histórico de versiones

Versión	Fecha	Revisado por	Descripción	Nombre del archivo
1.0	04/04/2025		Propuesta inicial	
1.1	14/08/2025		Se añade detalle al proceso de parcheo	

Aceptación

Fecha ver.	Responsable	Firma

Información de la versión

Versión	Comentarios

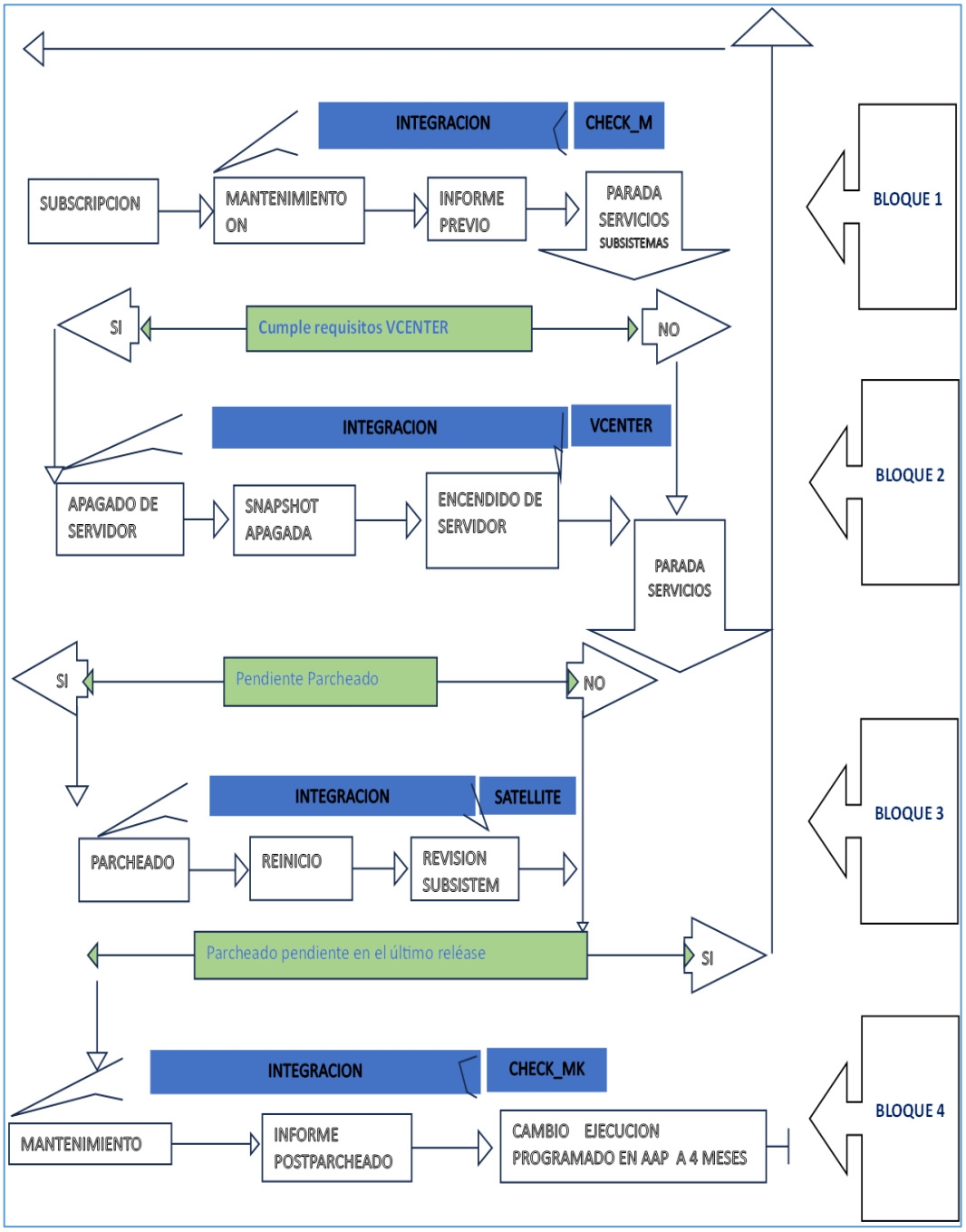
ÍNDICE DE CONTENIDO

1 Introducción

El objetivo de este documento es describir los pasos que forman el procedimiento para las intervenciones de actualización y parcheado mediante la plataforma Red Hat Satellite. Estas intervenciones persiguen mejorar la seguridad de la plataforma de la SGAD.

2 Visión global del proceso de parcheado

Los pasos que componen el proceso de parcheado semiautomático con *Ansible Automation Platform* se reflejan en el siguiente esquema:



El objetivo de este proceso es conseguir programar la actualización automática del mayor número de máquinas para el parcheado de su sistema operativo, actuando de forma manual en el menor número posible de máquinas durante el parcheado.

El proceso de parcheo se resume en los siguientes pasos:

- Preparación: creación del fichero de inventario de máquinas a parchear, programación de templates y ejecución de los chequeos previos al parcheo.
- Ejecución: Instalación de parches y reinicio de la máquina.
- Postparcheo: Resolución de posibles incidencias.

La ejecución del procedimiento se realiza desde AAP.

2.1 Orden de ejecución

La ejecución de los Templates debe realizarse en el siguiente orden:

Antes de la intervención se deberán ejecutar en este orden los siguientes templates:

- *SubscribeSO:* se ejecuta bajo demanda en las máquinas disponibles para actualizar, que se encuentran en el inventario de parcheo.
- *previoInforme:* se ejecuta bajo demanda en las máquinas incluidas en el inventario de parcheo, una vez ejecutado *SubscribeSO*. Se ejecutará con antelación suficiente para su revisión y la corrección de incidencias antes de la fecha de la intervención.
- *inicioActivaBlackout*: encargado activar el blackout, se ejecuta al iniciar la ventana de intervención.
- *Snapshot:* se realiza según la operativa de VMware, en el entorno de integración y en la primera intervención. En las siguientes intervenciones, en caso necesario se restaura el backup.

Intervención

- *actualiza*.

Tras la intervención y la ejecución de *actualiza*, se ejecutarán:

- *postInforme*, para evidenciar el estado de la máquina después del parcheado.
- Para cerrar la intervención se ejecuta *finalDesactivaBlackout* que desactiva el blackout finalizando la intervención.

2.2 Envío de correos asociados

Previo a la ejecución del proyecto, se envía un correo con el calendario de actuación sobre cada una de las máquinas.

La ejecución de los Templates conlleva el envío de los siguientes correos asociados:

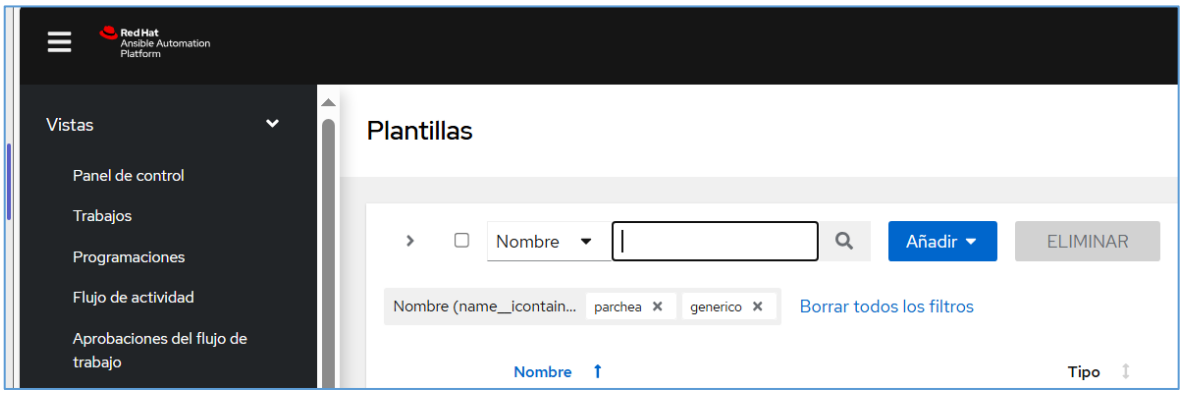
CORREO	OBJETIVO	DESTINATARIOS	ENVIO
inicioActivaBlackout	Indica el inicio de la intervención	sistemas.24x7@correo.gob.es; centrodeservicios.sgad@correo.gob.es; sistemas.balanceadores@correo.gob.es (balanceadores solo si se solicita sacarlos)	

previoInforme	Informe que recoge el estado de la plataforma antes de la intervención	Equipo Lote 1B y Administradores del servicio	Opcional a petición del responsable
postInforme	Informe que recoge el estado de la plataforma después de la intervención	Equipo Lote 1B y Administradores del servicio	Opcional a petición del responsable
finalDesactivaBlackout	Indica el fin de la intervención	sistemas.24x7@correo.gob.es; centrodeservicios.sgad@correo.gob.es; sistemas.balanceadores@correo.gob.es (balanceadores solo si se solicitó sacarlos en el paso de inicio)	
actualiza	Resultado de la ejecución	Técnico 1B	

2.3 Operativa en Ansible Automation Platform (AAP)

Dentro de AAP, los Templates se localizan y ejecutan de la siguiente forma:

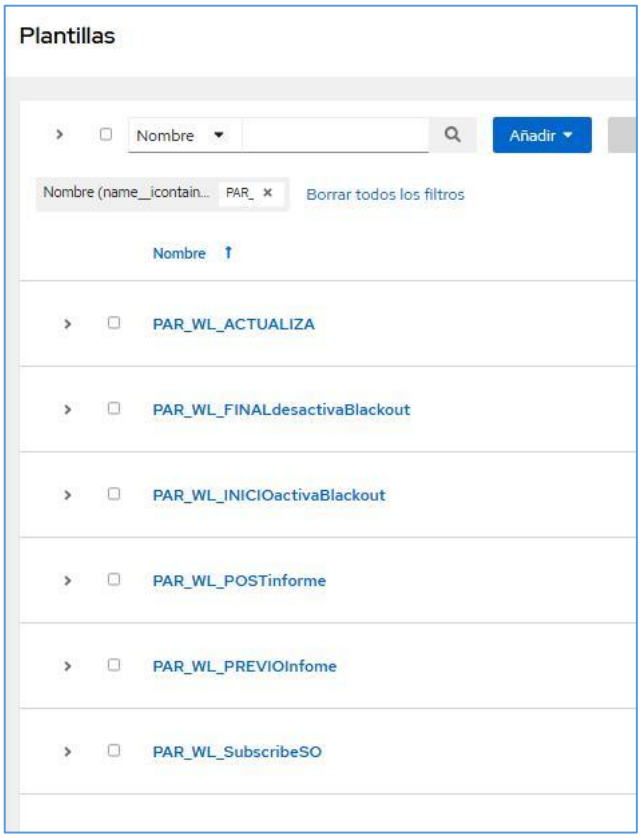
1. Buscar los Templates a ejecutar filtrando por PAR_" y nombre del trabajo:



Se han definido los siguientes Templates hasta el momento para proyectos Red Hat:

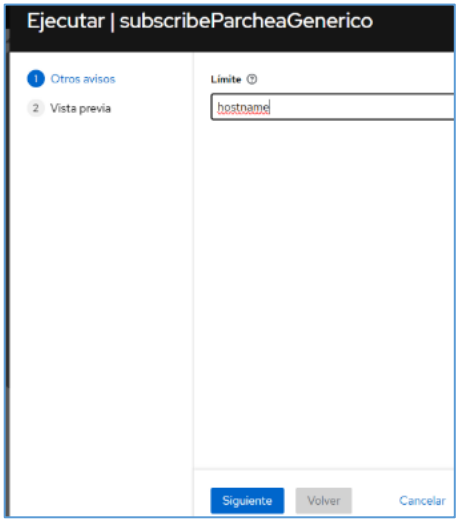
- PAR_WL: proyectos Weblogic.
- PAR_CL: proyectos Cloudera.
- PAR_Nvidia: proyectos Nvidia.

La búsqueda devuelve los siguientes resultados:



2. Pulsar sobre el icono de ejecución del Template correspondiente dependiendo del momento de la intervención en que nos encontremos:

3. Indicar en AAP la máquina sobre la que se va a intervenir.



2.4 Operativa en WMWare

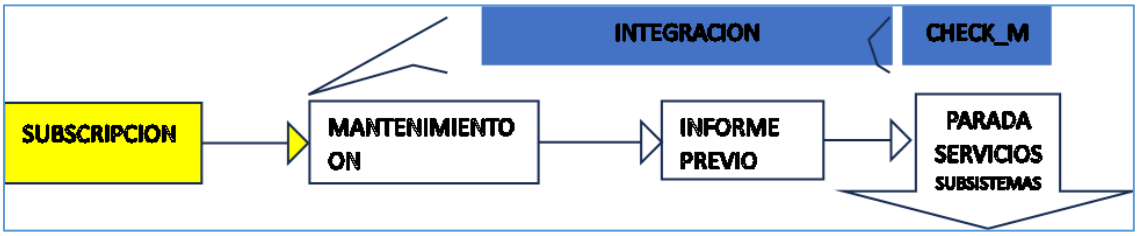
Se ejecuta la operativa de snapshot en WMWare según la operativa definida.

3 Anexo: Detalle del proceso

En este apartado se detallan los pasos enumerados en el apartado anterior y el contexto de funcionamiento de las plantillas y generación del snapshot.

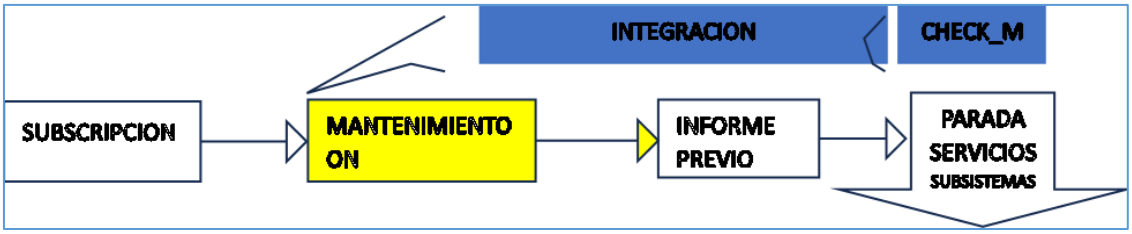
3.1 Preintervención

3.1.1 Subscribir la máquina a Satellite (SuscribeSO)



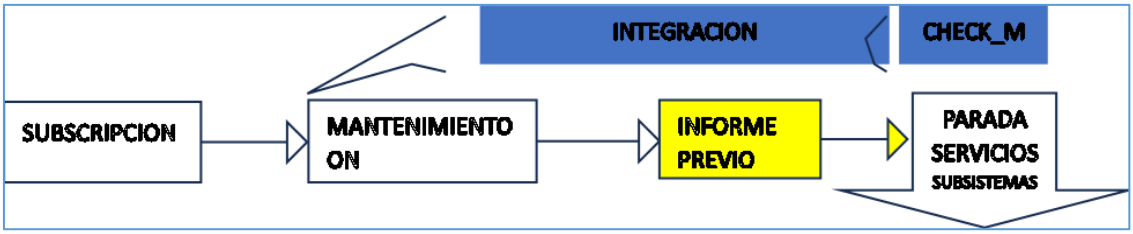
Objetivo	El objetivo de la ejecución de este Template es asegurar que la suscripción es la correcta para la actualización. Se realizará la suscripción de la máquina en el entorno, versión de SO, Ministerio o Release que corresponda. Este Template se ejecuta para que fuerce el registro de todas las máquinas bajo demanda, y se pueda usar de manera automática en toda la plataforma en un inventario vivo, colocando la máquina en estado “lista para parchear”. El Template revisará si existe cliente *katello* en la máquina, lo eliminará y lo volverá a instalar para volver a registrar la máquina en Satellite. Se ha incluido también la eliminación de la máquina en Satellite, ya que, la configuración de los clientes *insights-clients* y *rhsm* de Red Hat, daba errores al forzar la suscripción.
Ejecución	Para evitar la creación de demasiadas plantillas, se preguntará en la ejecución de la plantilla genérica desde AAP el Hostname de destino de la máquina.
Programación	Ejecución bajo demanda en AAP.

3.1.2 Inicio de la intervención y mantenimiento de la máquina en monitorización (inicioActivaBlackout)



Objetivo	El objetivo de este Template es lanzar los emails configurados (según lo indicado en la tabla anterior) para informar del inicio de la intervención y solicitar la puesta de la máquina en monitorización.
Ejecución	Durante la intervención, se pondrán las máquinas en mantenimiento para que cesen los eventos de monitorización, mientras se trabaja en ellas en la ventana acordada con el fin de no influir en los SLA acordados con el cliente en los periodos de intervención, y evitar llamadas a grupos de actuación ajenos a la intervención. Actualmente, esta acción se establece avisando a Operación de la intervención en la máquina para que eviten llamadas a los grupos, pero no se están poniendo las máquinas en mantenimiento para forzar el corte de incidencias en los sistemas de monitorización durante las intervenciones. Está creado el automatismo para el envío de correos de “inicio de intervención”, usando una plantilla acordada con operación. Para evitar demasiados correos, el correo genérico llegará al equipo de intervención y este enviará un correo con todas las máquinas incluidas. Este Template enviará correo a los emails configurados.
Programación	Ejecución bajo demanda en AAP.

3.1.3 Informe previo de parcheado (previoInforme)



Objetivo	El objetivo es asegurar que los datos desde el servidor a parchear son correctos y nos permiten hacer un esquema del estado de la máquina antes del parcheado, permitiendo una primera revisión antes de la intervención. Este template genera el informe previo al parcheado.

Ejecución	Para evitar la creación de demasiadas plantillas, se preguntará en la ejecución desde AAP el Hostname de destino de la máquina. El informe previo, se puede lanzar en cualquier momento antes del inicio de la intervención mediante un correo con ficheros adjuntos con las evidencias de parcheado recopiladas.
Programación	Ejecución bajo demanda en AAP.

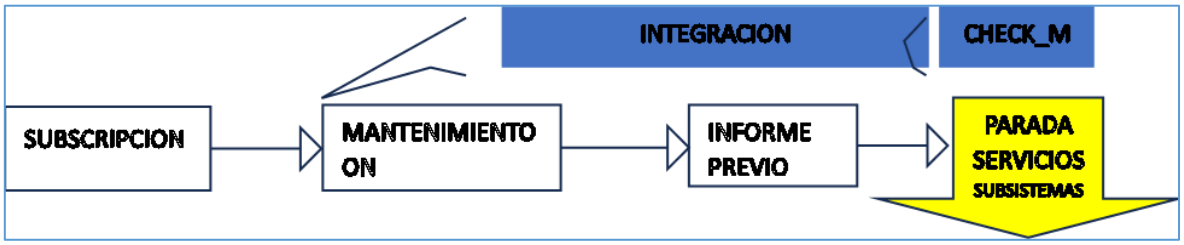
El informe tendrá las siguientes secciones recopiladas:

1. Versión de sistema operativo antes de la actualización.
2. Versión de kernel actual antes de la actualización.
3. Versión recomendada por RedHat
4. Repositorios activos.
5. Paquetes disponibles pendientes de actualizar.
6. Últimos paquetes instalados y la fecha de instalación.
7. Histórico de actualizaciones.
8. Parches de seguridad instalados (RHBA, RHSA o RHEA con el número de bugfix y el paquete afectado).
9. Paquetes de seguridad que pueden instalarse.
10. Paquetes de seguridad que pueden ser instalados en la actualización (RHBA, RHSA o RHEA con el número de bugfix, el paquete afectado y los CVE que comprenden).
11. Rutas, servicios activos y fallidos
12. Fechas de parcheado previstas
13. Contenido de ficheros hosts, fstab
14. Ocupación identificación y montaje de los discos
15. Usuarios de sistema, usuarios sudo
16. Datos de contacto de los responsables del sistema y aplicación asociada. Destinatarios de los correos
17. Estado del servicio sincronización horaria

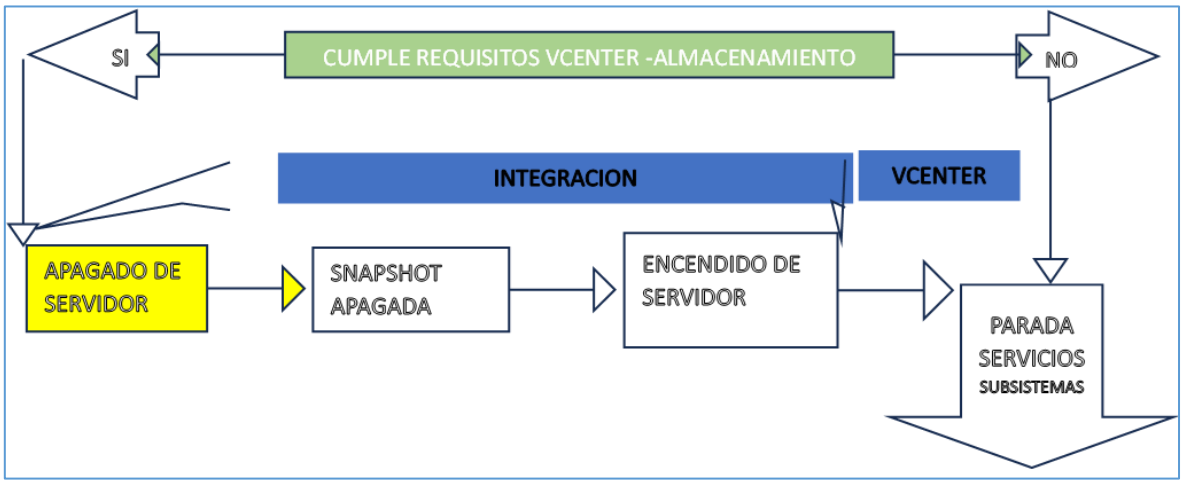
3.1.4 Generar snapshot

Según operativa definida.

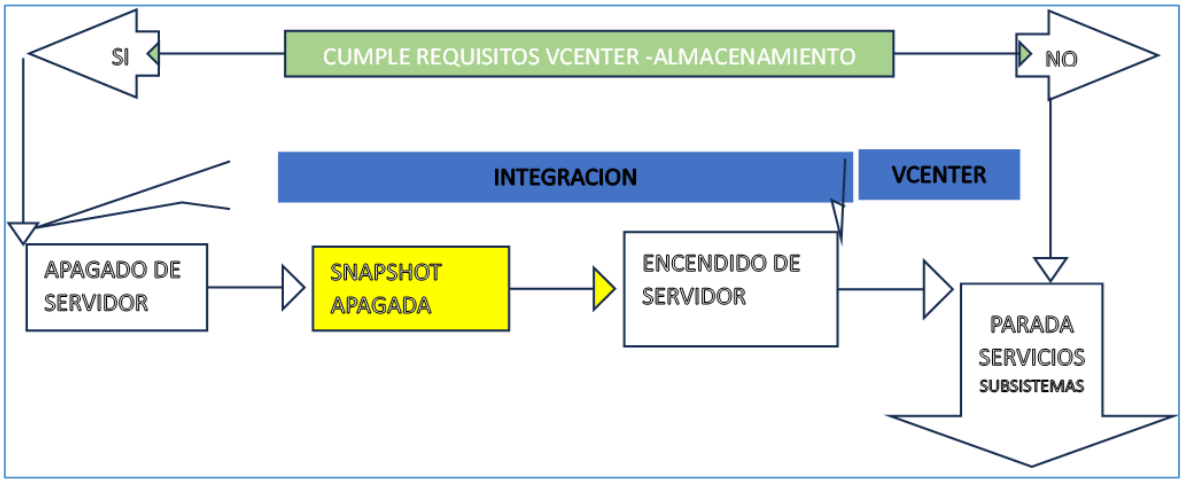
3.1.4.1 Parada de aplicación



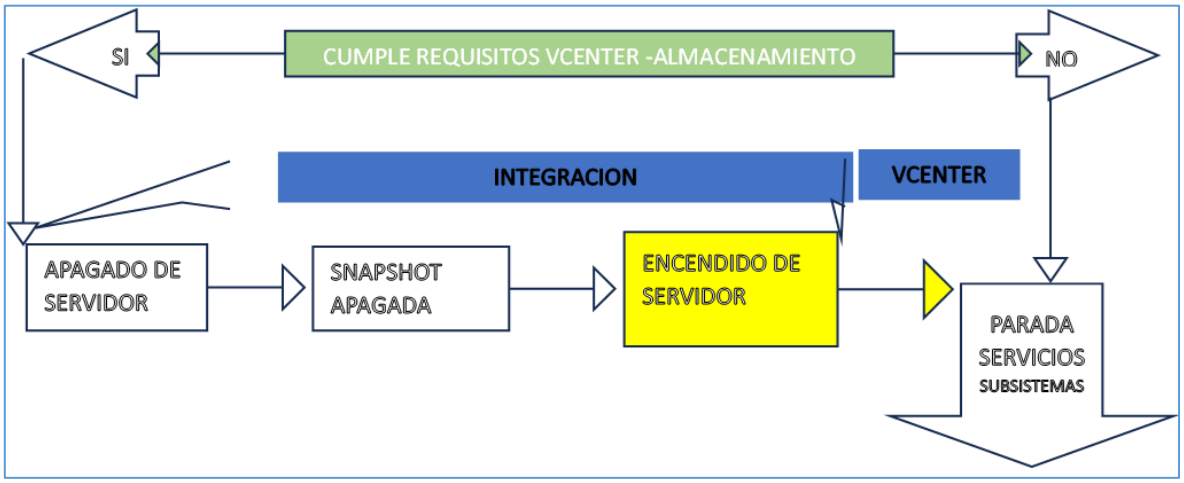
3.1.4.2 Apagado de la máquina



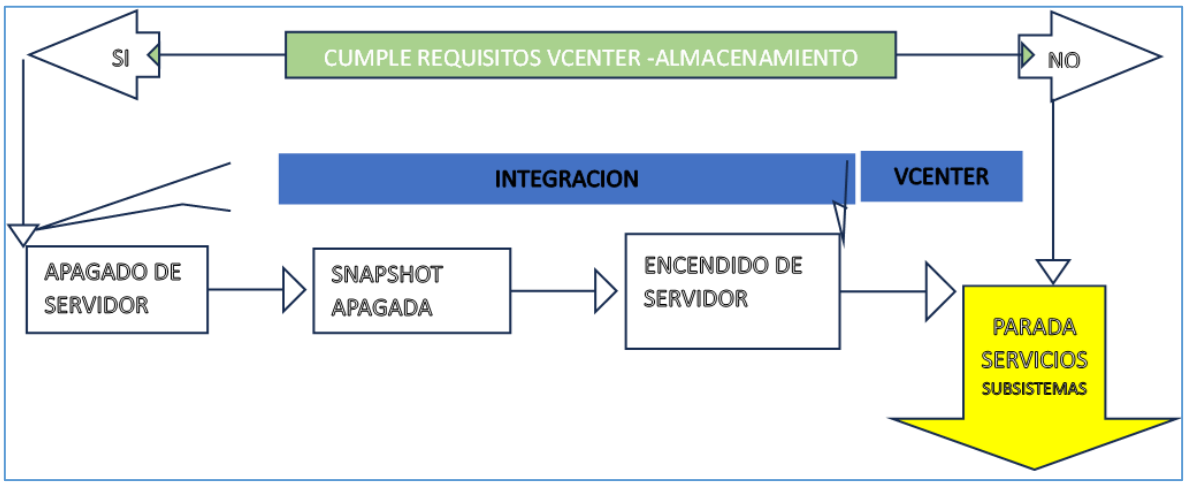
3.1.4.3 Generar snapshot



3.1.4.4 Arrancar la máquina



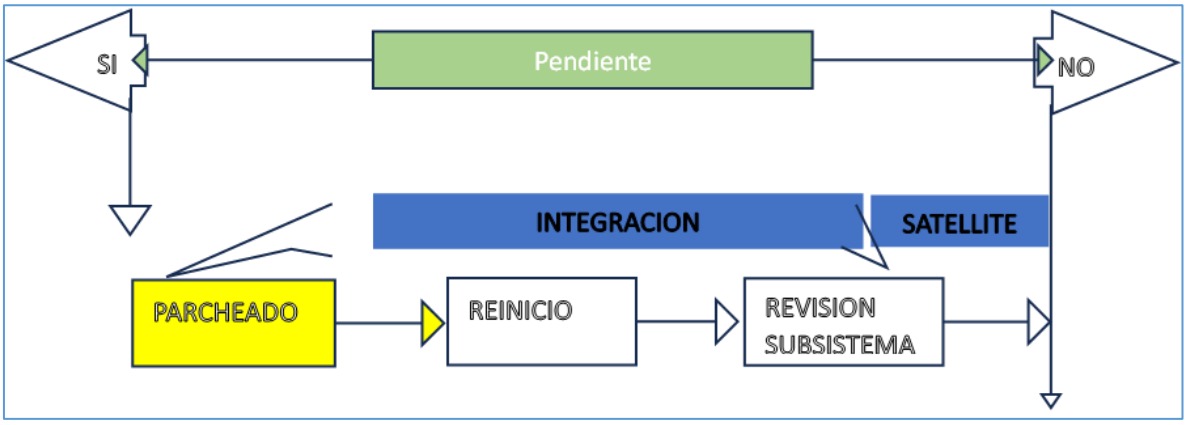
3.1.4.5 Parar aplicación



3.2 Intervención

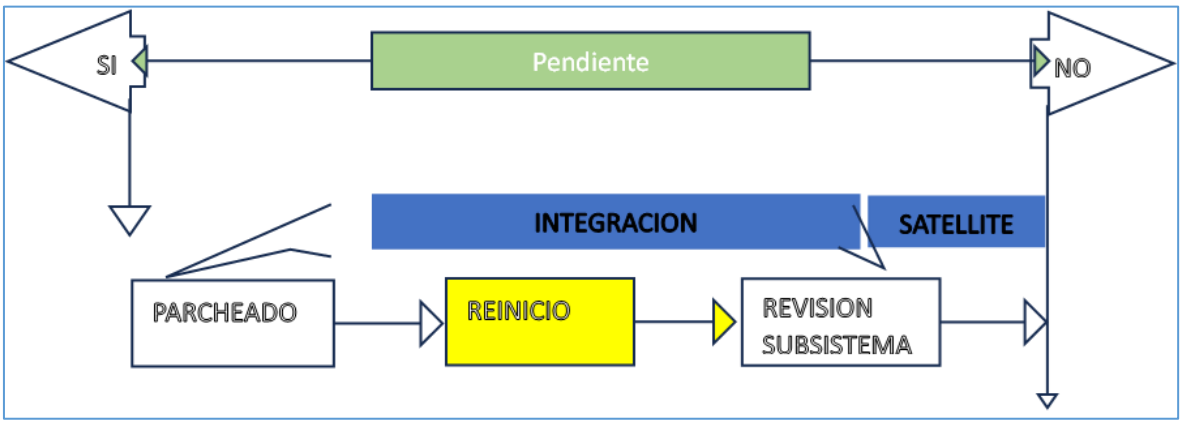
3.2.1 Ejecución del parcheado y reinicio (actualiza)

Parcheado



Objetivo:	El objetivo, es agregar al Template de parcheado las versiones y las soluciones que generen incidencias en las intervenciones, y que deban ser consideradas en el parcheado de otras máquinas. Incluir en la ejecución de parcheado las soluciones a incidencias encontradas durante la ejecución de parcheados para que en las siguientes ejecuciones no se produzcan reduciendo la intervención manual en las máquinas en los parcheados.
Ejecución	El resultado de la ejecución de actualización se envía por correo al técnico responsable de la ejecución con las evidencias para su revisión.
Programación	Ejecución bajo demanda en AAP.

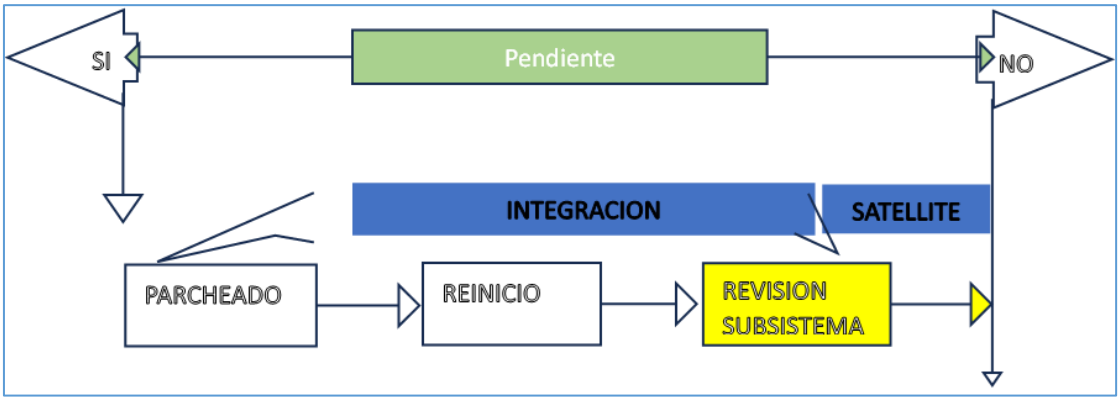
Reinicio



Objetivo	Este template se encarga de reiniciar las máquinas tras la ejecución de la actualización.

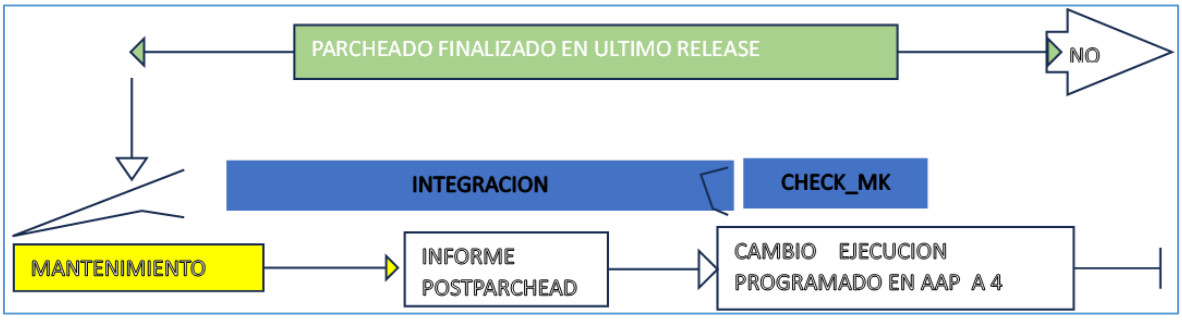
3.3 Post intervención: Detalle del proceso después del parcheado

3.3.1 Revisión de la aplicación



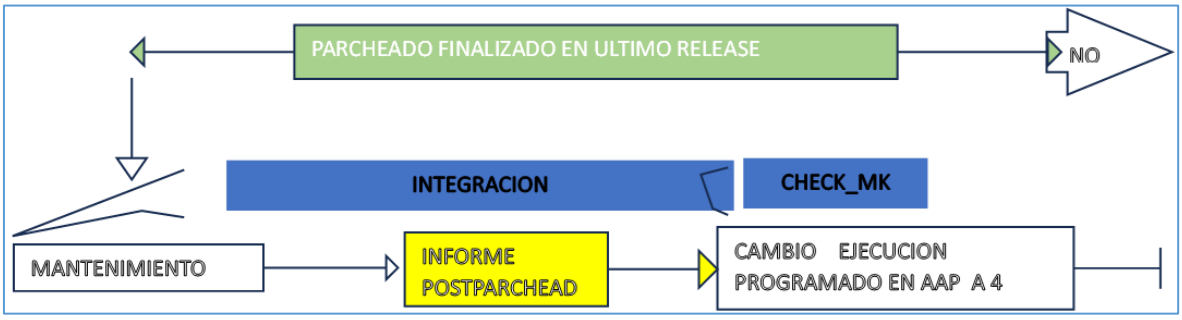
Objetivo	El objetivo de este paso es que el grupo propietario de la aplicación revise si la actualización ha tenido alguna afectación en la aplicación que aloja la máquina, es decir, si la aplicación funciona correctamente tras la intervención. Se revisará e incluirá en los informes, si la aplicación levanta junto a la máquina o es necesario intervención manual para habilitar el servicio.
Ejecución	Según la operativa definida para cada aplicación.
Programación	

3.3.2 Final de la intervención y sacar de mantenimiento en monitorización (finalDesactivaBlackout)



Objetivo	Actualmente no hay un proceso de mantenimiento en monitorización y estamos revisando el tratamiento mediante API.
Ejecución	Con la ejecución, se enviará un correo para indicar la finalización de la intervención.
Programación	Ejecución bajo demanda en AAP.

3.3.3 Informe posterior al parcheado (postInforme)



Objetivo	La finalidad es tener las evidencias del estado después de parcheado. Las actualizaciones de seguridad pendientes pasarán a la lista de actualizaciones instaladas. El informe es igual que el informe previo, únicamente cambian las cabeceras.
Ejecución	El informe post parcheado y el envío del informe por mail, marcará el final de la intervención de parcheado y le llegará a todos los involucrados por correo.
Programación	Ejecución bajo demanda en AAP.

3.4 Gestión del ciclo de parcheado

3.4.1 Programación y siguiente ciclo

Una vez finalizada la primera intervención se podrán establecer las fechas de, al menos, las dos siguientes intervenciones de parcheado de la máquina, incrementando el número de máquinas por día en cada ciclo.

3.4.2 Ficheros de gestión

Los ficheros de gestión son ficheros planos construidos a partir de las máquinas que se van a parchear, permitiendo el uso de un solo fichero para enriquecimiento e inventario, o ficheros distintos de inventario y de enriquecimiento, facilitando así la gestión de los trabajos programados.

Esta plantilla (**paraenriquecerParchea.lst**) enviará los correos a **los emails configurados** en el fichero de inventario en el servidor de Satellite. El dato usado es el que aparece en la última columna de la fila correspondiente al Hostname a parchear.

/home/reexus/enriquece/paraenriquecerParchea.lst

IP(10.254.199.142)	ansible_hostname=<hostname de la máquina#>	Red Hat	LC_SGAD/CV_RHEL	Fecha parcheado(25/11/2024)	Aplicación	Correos destino

La máquina para parchear, la fecha de parcheado inicial y los destinatarios de los correos están inventariados para filtrar en los ficheros de gestión de parcheados y su objetivo es realizar un enriquecimiento de los datos “fecha inicial de parcheado” e insertar en los correos los destinatarios.

Actualmente, los automatismos están usando los tres últimos campos del fichero de enriquecimiento, dejando colocados el primer campo y el segundo (IP alcanzable desde Satellite y nombre de la máquina) para su uso como fichero de inventario:

Fecha parcheado(25/11/2024)	Aplicación	Correos destino

Ejemplo de **contenido del fichero de enriquecimiento**:

```
10.254.199.142  ansible_hostname=adposacarprom5# 10.254.193.142 RedHat
LC_SGAD/CV_RHEL 2024-11-25 CARPETACIUDADANA
david.bdominguez@externos.correo.gob.es;carlostomas.pinedo@digital.gob.es;lucia.a
lvarez@digital.gob.es;jorge.garciadelarosa@digital.gob.es;jorge.garciadelarosa@di
gital.gob.es;carmen.delvillar@digital.gob.es;carpeta.desarrollo@correo.gob.es;ale
jandro.ares@externos.correo.gob.es;aida.suarez@externos.correo.gob.es;cristina.cu
enca@externos.correo.gob.es

10.254.199.143  ansible_hostname=adposacarprom6# 10.254.193.143 RedHat
LC_SGAD/CV_RHEL 2024-11-14 CARPETACIUDADANA
david.bdominguez@externos.correo.gob.es;carlostomas.pinedo@digital.gob.es;lucia.a
lvarez@digital.gob.es;jorge.garciadelarosa@digital.gob.es;jorge.garciadelarosa@di
gital.gob.es;carmen.delvillar@digital.gob.es;carpeta.desarrollo@correo.gob.es;ale
jandro.ares@externos.correo.gob.es;aida.suarez@externos.correo.gob.es;cristina.cu
enca@externos.correo.gob.es

 Fichero inventarioParcheado
```

El uso de este fichero permite filtrar las máquinas a parchear evitando la ejecución en máquinas no previstas y traducir también la IP desde la que se llega desde la máquina para poder hacer las ejecuciones por el Hostname.

Se creará dependiendo de las máquinas a parchear con esta estructura:

Ejemplo raw del archivo:

```
dpewlpfprec3 ansible_host=10.254.225.86
adpewlfirprec1 ansible_host=10.254.225.87
adpewlfirprec2 ansible_host=10.254.225.88
adpewlfirprec3 ansible_host=10.254.225.89
adpewlcitaprec1 ansible_host=10.254.225.90
```

donde "*ansible_host*" es la IP desde la que se llega desde Satellite (no tiene por qué ser la misma que se accede desde AAP), y ansible_host el Hostname con el que se registra en Satellite.

3.4.3 Histórico de informes

Todos ficheros .csv de los informes (previos y post) se guardan en la carpeta almacén de la máquina de Satellite para su gestión.