Plan de Trabajo para Mantenimiento Preventivo y Actualización de Cortex XSOAR de la Versión 6.12 a 6.13

# 1. Antes del Mantenimiento

## 1.1 Planificación y Preparación

- Revisión de Notas de la Versión: Lee las notas de la versión 6.13 para identificar los cambios y las mejoras que podrían afectar tu entorno actual.

- Validación del Script: Asegúrate de que el script de actualización ha sido probado en un entorno de pruebas para evitar problemas durante la implementación.

- Respaldo Completo:  
 - Realiza un respaldo completo de la configuración actual de Cortex XSOAR, incluidas bases de datos, configuraciones de playbooks, integraciones, y cualquier archivo personalizado.  
 - Asegura que los respaldos sean accesibles y estén correctamente etiquetados.

- Notificación a los Usuarios: Comunica a los usuarios finales sobre el mantenimiento programado, incluyendo la ventana de tiempo en la que el sistema no estará disponible.

- Verificación de Dependencias:  
 - Asegúrate de que todas las dependencias necesarias para la versión 6.13 estén instaladas.  
 - Revisa los requisitos de hardware y software para confirmar que el sistema cumple con las especificaciones necesarias para la nueva versión.

## 1.2 Revisión de Entorno

- Estado del Sistema: Verifica que el sistema actual esté funcionando sin problemas y documenta el estado del sistema antes de la actualización.

- Plan de Contingencia: Prepara un plan de reversión en caso de que la actualización falle. Esto incluye cómo restaurar los respaldos y volver a la versión anterior de Cortex XSOAR.

# 2. Durante el Mantenimiento

## 2.1 Ejecución del Script de Actualización

- Apagado Controlado: Detén todos los servicios de Cortex XSOAR para asegurar que no haya procesos en curso que puedan interferir con la actualización.

- Ejecución del Script:  
 - Ejecuta el script de actualización conforme a las instrucciones. Monitorea la ejecución para identificar posibles errores o advertencias.  
 - Documenta cada paso y cualquier salida que genere el script para referencias futuras.

## 2.2 Verificación Inicial

- Reinicio de Servicios: Una vez completada la actualización, reinicia los servicios de Cortex XSOAR.

- Verificación de la Integridad: Realiza pruebas básicas para asegurarte de que el sistema se inicia correctamente y que las funcionalidades principales están operativas.

- Resolución de Problemas: Si se detectan problemas durante la actualización, utiliza los logs generados para identificar y corregir los errores.

# 3. Después del Mantenimiento

## 3.1 Verificación Post-Actualización

- Validación Completa: Realiza pruebas exhaustivas de todas las funciones críticas (playbooks, integraciones, informes, etc.) para asegurar que todo funciona como esperado.

- Monitoreo Intensivo: Durante las primeras horas y días posteriores a la actualización, monitorea el sistema de manera intensiva para detectar cualquier comportamiento anómalo.

## 3.2 Documentación y Reporte

- Documentación de la Actualización: Actualiza la documentación interna para reflejar los cambios realizados durante la actualización.

- Reporte Final: Genera un informe detallado que incluya el estado previo al mantenimiento, los pasos realizados, cualquier problema encontrado y cómo se resolvió, y el estado final del sistema.

## 3.3 Comunicación Final

- Notificación a Usuarios: Informa a los usuarios finales sobre la finalización del mantenimiento y la disponibilidad del sistema.

- Revisión con el Equipo: Realiza una reunión con el equipo para discutir la actualización, revisar cualquier incidente y planificar mejoras para futuros mantenimientos.

# Consideraciones para el Backup Antes de la Actualización

## Tipos de Datos a Respaldar

- Configuraciones del Sistema: Respaldar todas las configuraciones del sistema, incluyendo configuraciones de red, autenticación, y cualquier ajuste personalizado.

- Playbooks y Scripts: Realiza un backup de todos los playbooks, scripts y cualquier código personalizado que esté en uso.

- Integraciones y Configuraciones de Conectores: Asegúrate de respaldar todas las integraciones activas, junto con sus configuraciones específicas.

- Base de Datos: Respaldar la base de datos completa, que incluye incidentes, tareas, y registros históricos.

- Archivos Personalizados: Cualquier archivo de configuración personalizado o script debe ser respaldado manualmente.

## Herramientas y Métodos de Backup

- Herramientas Integradas de XSOAR: Utiliza las funcionalidades de respaldo integradas en Cortex XSOAR si están disponibles.

- Snapshots de Máquina Virtual: Considera tomar un snapshot completo del sistema si XSOAR está corriendo en una máquina virtual.

- Copias Externas: Almacena los backups en una ubicación externa segura.

## Validación del Backup

- Verificación de Integridad: Verifica que los archivos estén completos y sin corrupción.

- Documentación del Proceso: Documenta todo el proceso de respaldo, incluyendo las ubicaciones de almacenamiento de los backups.

## Planificación de la Restauración

- Simulacro de Restauración: Realiza una restauración de prueba en un entorno aislado para asegurarte de que el proceso de restauración funcione correctamente.