CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como uso **“interno”**.
El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.
No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. **OBJETIVO.** 3
2. **ALCANCE.** 3
3. **DEFINICIONES** 3
4. **PAUTAS Y LINEAMIENTOS.** 3
- **4.1. Entorno configuración WSUS** 3
- **4.2. Esquema Propuesto** 4
- **4.3. Bases de datos y almacenamiento de actualizaciones** 4
- **4.4. Almacenamiento de actualizaciones:** 5
- **4.4. Descripción de Actualizaciones por Producto y Clasificaciones** 5
- **4.5. Grupos de Computadores de WSUS** 6
- **4.5. Configuración Actual** 7
5. **RECOMENDACIONES GENERALES DE WSUS** 9
6. **DESCRIPCIÓN** 9
7. **CONTROL DE CAMBIOS.** 12
8. **FLUJO DE APROBACIÓN.** 13

1. OBJETIVO.

Mantener el estándar de versión actualizado de los sistemas operativos Windows Server, con la herramienta WSUS para Windows Server.

2. ALCANCE.

El alcance del procedimiento es llevar el proceso de actualización a todos los servidores de Keralty Colombia, cumpliendo con los lineamientos y estándares de los fabricantes, haciendo uso de la herramienta WSUS.

3. DEFINICIONES

- **Windows Server Update Services (WSUS):** Provee actualizaciones de seguridad para los sistemas operativos Microsoft. Mediante Windows Server Update Services, los administradores pueden manejar centralmente la distribución de parches a través de actualizaciones automáticas a todas las computadoras de la red corporativa.

4. PAUTAS Y LINEAMIENTOS.

- Los parches o actualizaciones de seguridad en los servidores Windows Server se deberán realizar cada 3 meses, según actualizaciones emitidas por los fabricantes, por un evento de Seguridad u otras eventualidades y deberán ser presentados en comité de cambios mediante un cronograma para su aprobación.

- Cuando el fabricante lanza un parche de seguridad con severidad crítica, se deberá aplicar en un tiempo no mayor a un mes por medio del proceso de gestión de cambios de la compañía.

4.1. Entorno configuración WSUS

Windows Server Update Services (WSUS) permite implementar las actualizaciones de productos de Microsoft más recientes. En Windows Server recientes, WSUS es un rol de servidor que puede instalarse para administrar y distribuir actualizaciones. Un servidor WSUS puede ser el origen de actualización para otros servidores WSUS de la

organización. En una implementación de WSUS, al menos un servidor WSUS de la red debe conectarse a Microsoft Update para obtener información sobre actualizaciones disponibles.

WSUS tiene características de fácil uso, implementación y soporte. Provee muchas mejoras en los siguientes aspectos:

- Fácil uso
- Implementación mejorada
- Soporte mejorado en escenarios complejos corporativos
- Mejor rendimiento y administración de ancho de banda

Este documento contiene información de Diseño de la implementación de Windows Server Update Services para Keralty Colombia.

4.2. Esquema Propuesto

Esquema de varios servidores: Se propone un esquema de varios servidores. El cual debe tener un servidor de WSUS que descargue las actualizaciones directamente de internet de Microsoft Update y los demás servidores que sincronice todo el contenido dentro de la intranet de la organización. En Keralty Colombia existe un (1) servidor de WSUS que descarga las actualizaciones para los Sistemas Operativos Windows.

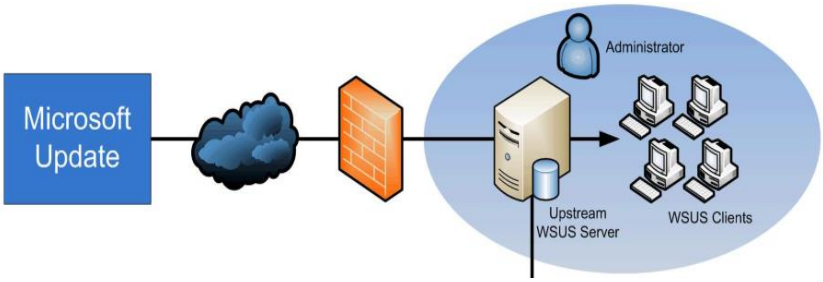

Ilustración 1. *Arquitectura actualización de servidores Windows Server*

4.3. Bases de datos y almacenamiento de actualizaciones

Base de Datos: El servidor de WSUS requiere una base de datos, puede ser ubicada localmente o de forma externa en servidores de SQL. La base de datos de WSUS almacena la siguiente información:

- Información de la configuración del servidor WSUS
- Metadata que describe cada actualización de Windows
- Información de clientes, actualizaciones y su interacción.

La base de datos para la implementación en Keralty Colombia se almacenará usando Windows Internal Database localmente en cada servidor.

4.4. Almacenamiento de actualizaciones:

Las actualizaciones en cada servidor WSUS se almacenarán de forma local, en una partición diferente a la del sistema operativo.

4.4. Descripción de Actualizaciones por Producto y Clasificaciones

Un producto es una edición específica de un sistema operativo o aplicación, como por ejemplo Windows Server 2019 u Office 2016. Una familia de producto es la base de un sistema operativo o aplicación desde el cual los productos individuales son derivados. Se puede especificar una familia de producto o individual a nivel de seleccionar las actualizaciones actuales o de versiones futuras.

Clasificaciones: Las clasificaciones de actualizaciones representan el tipo, para cada producto o familia de producto se presenta una clasificación de la siguiente forma (publicado por Microsoft):

Update Classification	Description
Critical updates	Broadly released fixes for specific problems addressing critical, non-security related bugs.
Definition updates	Updates to virus or other definition files.
Drivers	Software components designed to support new hardware.

Update Classification	Description
Feature packs	New feature releases, usually rolled into products at the next release.
Security updates	Broadly released fixes for specific products, addressing security issues.
Service packs	Cumulative sets of all hotfixes, security updates, critical updates, and updates created since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.
Tools	Utilities or features that aid in accomplishing a task or set of tasks.
Update rollups	Cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a specific component, such as Internet Information Services (IIS).
Updates	Broadly released fixes for specific problems addressing non-critical, non-security related bugs.

Tabla 1. Clasificación de actualizaciones

Lenguajes: Las actualizaciones disponibles en los servidores WSUS serían en español e Inglés.

4.5. Grupos de Computadores de WSUS

WSUS permite agrupar los computadores por Target tratando de reflejar la ubicación del computador o tipo de servidor reportado en la consola del servidor WSUS y visualizar los computadores de una forma organizada.

Los Grupos de Computadores pueden configurar con jerarquías, tratando de presentarlos como están ubicados en la Unidades Organizaciones de AD DS, y dicha jerarquía puede usarse para la aprobación de actualizaciones en la consola.

Para Keralty Colombia se sugiere crear Targets de computadores dependiendo del Sitio de AD al cual pertenece el computador y para servidores crear por ambientes en producción, preproducción y Directorio Activo.

Requerimientos Servidores WSUS: Se recomienda que los servidores WSUS tengan la siguiente configuración:

- **WSUS Server Root – Principal**
  - Sistema Operativo Windows Server
  - Procesador de 2.0 GHz 2 Cores o superior
  - Memoria RAM: 4 GB o superior
  - Discos: 60 GB para sistema operativo y 80 GB para almacenamiento de actualizaciones
  - Tarjeta de red de 1 GB

4.5. Configuración Actual

Descripción de Actualizaciones por Producto y Clasificaciones

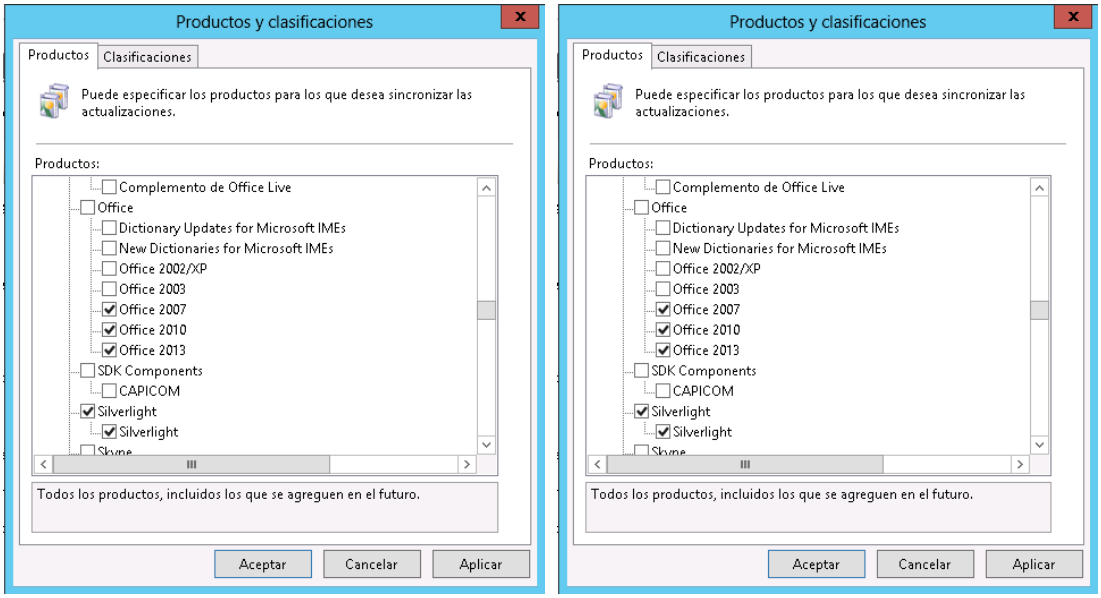

Ilustración 2. Paso a paso actualización producto y clasificaciones

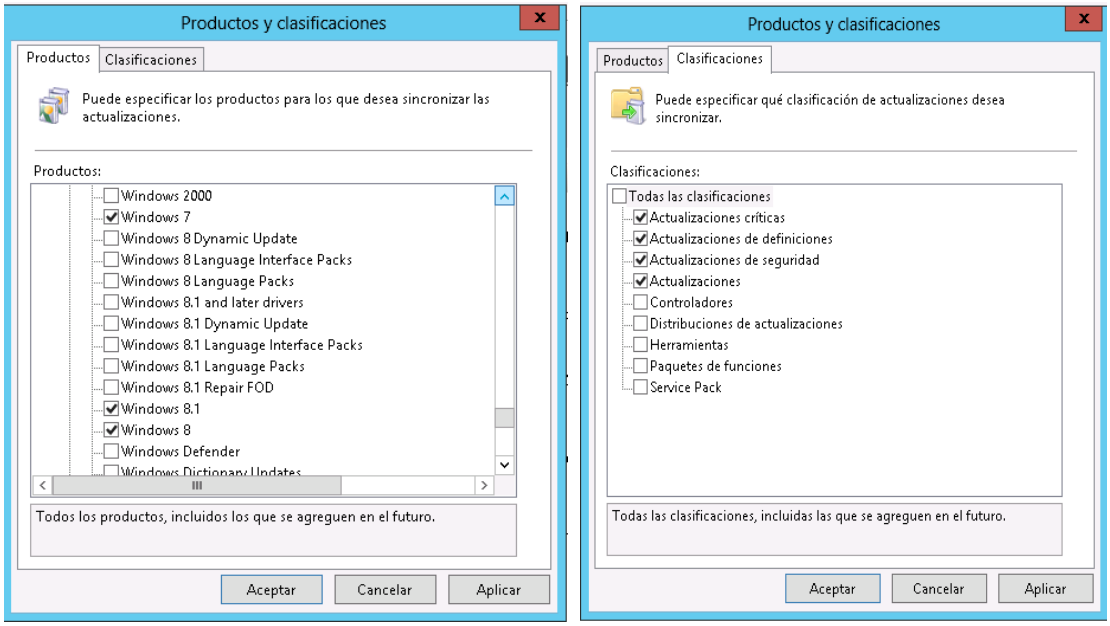

Ilustración 3. Paso a paso actualización producto y clasificaciones

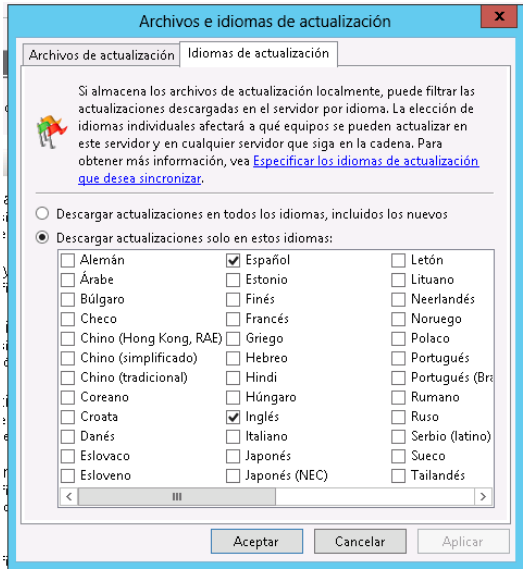

Ilustración 4. Paso a paso actualización producto y clasificaciones

Configuración de Políticas: Existe una política definida para cada uno de los ambientes y para el Directorio Activo.

Exclusiones de Antivirus: Es recomendado excluir las siguientes carpetas de WSUS del escaneo del antivirus con el fin de evitar problemas de rendimiento en el servidor:

- \WSUS\WSUSContent
- \WSUS\UpdateServicesDBFiles
- \SoftwareDistribution\Datastore
- \SoftwareDistribution\Download

5. RECOMENDACIONES GENERALES DE WSUS

- ✓ Se debe tener en cuenta que las actualizaciones de Microsoft se liberan el segundo martes de cada mes. Cada mes Microsoft envía un boletín el cual es público en el cual se da información específica de cada actualización. Esta información debe ser tenida en cuenta a la hora de aprobar las actualizaciones.
- ✓ Se recomienda realizar las actualizaciones en ambiente pre-productivo previa comunicación al Comité de Cambios para realizar las pruebas correspondientes antes de aprobar actualizaciones en el ambiente de producción.
- ✓ Se deben declinar las actualizaciones que ya expiraron y que no tienen clientes pendientes por instalar.
- ✓ Es buena práctica realizar por lo menos cada tres meses una limpieza de los objetos de WSUS en cada uno de los servidores.
- ✓ Las actualizaciones tienen prioridades, algunas son críticas otras de seguridad. Se debe dar prioridad de instalación a las críticas ya que son las que se supone que disminuyen riesgos mayores.
- ✓ Se recomienda que los servidores de WSUS estén separados del rol de actualización del Antivirus. Ya que en caso de ocurrir algún evento no es fácil identificar cual es la causa del problema
- ✓ Se recomienda llevar un control de la aprobación o declinación de las actualizaciones.

6. DESCRIPCIÓN

Actualización sistema operativo Windows Server:

ACTIVIDADES	RESPONSABLE	REGISTROS
1. **<u>Validación de las liberaciones de Windows por parte de Microsoft</u>** Se valida cuando se van a realizar actualizaciones críticas o de seguridad, las	Administrador de sistemas	Herramienta WSUS Formato RFC

ACTIVIDADES	RESPONSABLE	REGISTROS
cuales son almacenadas en un WSUS específicamente para este fin.		
2. <u>Notificación de nuevas actualizaciones disponibles al desarrollador de la aplicación</u> Se desarrolla un listado de cada uno de los equipos con las actualizaciones por aplicar, con su respectiva documentación para revisión y se notifica al dueño de la aplicación.	Administrador de sistemas	Informe Correo electrónico
3. <u>Feedback por parte del desarrollador de la aplicación</u> Se recibe una retroalimentación por parte del desarrollador de la aplicación, donde se evidencia y analiza el impacto de las actualizaciones requeridas.	Desarrollador de la aplicación	Informe Correo electrónico
4. <u>Despliegue en Pre-producción de las actualizaciones aprobadas</u> Se realiza una programación de una ventana de mantenimiento donde se hace la liberación de las actualizaciones y posteriormente el reinicio controlado de los equipos, el cual puede tener una duración hasta de aproximadamente dos horas.	Administrador de sistemas	Correo electrónico
5. <u>Solicitud a comité de cambios</u> Se solicita al comité de cambios por medio del **Formato RFC** la aplicación de las actualizaciones aprobadas en Pre-producción.	Administrador de sistemas	Formato RFC
6. <u>Verificación de medidas de seguridad</u> Se confirma que esté existente una copia de seguridad del equipo y coordinar con el área de copias de seguridad que no se ejecute dicha copia en el momento que se realicen las actualizaciones para evitar afectaciones a las mismas.	Administrador de sistemas	Correo electrónico

ACTIVIDADES	RESPONSABLE	REGISTROS
7. <u>Despliegue en Producción de las actualizaciones</u> Se realiza una programación de las ventanas de mantenimiento necesarias según la aprobación del Negocio, donde se hace la liberación de las actualizaciones y posteriormente el reinicio controlado de los equipos, el cual puede tener una duración hasta de aproximadamente dos horas.	Administrador de sistemas	Correo electrónico
8. <u>Rollback</u> Se realizará de acuerdo con el informe de resultados de Negocio y del estado de los servidores generado en la actividad anterior, en caso de ser necesario para realizar desinstalaciones.	Administrador de sistemas	Correo electrónico Llamada telefónica Solicitud requerimiento al MAS

Tabla 2. Actualización sistema operativo Windows Server

7. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
19/01/2016	Actualizaciones de información	1.0
10/08/2017	Actualizaciones de información	2.0
09/05/2022	Actualización lineamientos de Windows Server: Germán Heredia y Renné Barrera.	3.0
25/09/2023	Cambio de formato	4.0
10/10/2023	Modificación de pautas y lineamientos	5.0
11/11/2023	Pautas y lineamientos: Modificación de la periodicidad de los parches de seguridad con severidad crítica	6.0
18/10/2024	Se modifica el ítem: Requerimientos Servidores WSUS. El documento se revisa en el marco de la actualización del SGSI año 2024, se realiza inclusión de la sigla del país y la compañía en el código del documento.	7.0

Tabla 3 Control de Cambios

8. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: German Heredia Área/Proceso: Administrador de Sistemas Fecha: 11/10/2023	Nombre: Luisa Castaño Área/Proceso: Director de Operaciones TI Fecha: 18/10/2024	Nombre: Javier Alonso Galván Área/Proceso: Gerente Corporativo de Tecnología Fecha: 18/10/2024

Tabla 4 Flujo de Aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.