Código: SIG-TI-CKE-PR015

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



### **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.

Código: SIG-TI-CKE-PR015

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



#### **TABLA DE CONTENIDO**

1.	OBJETIVO.	3
	ALCANCE.	
	DEFINICIONES	
	CONTENIDO.	
	FLUJO DEL PROCEDIMIENTO	
	DETALLE DEL PROCEDIMIENTO	
7.	CONTROL DE CAMBIOS.	16
8.	FLUJO DE APROBACIÓN	17

Código: SIG-TI-CKE-PR015

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



#### 1. OBJETIVO.

Gestionar y mantener el proceso de instalación, actualización y configuración de software en servidores, componentes, plataforma vmware de infraestructura del grupo Keralty.

#### 2. ALCANCE.

Mantener el proceso de instalación, actualización y configuración en sistemas operativos Linux y Windows Server, plataformas de Vmware; motores de Bases de Datos Oracle y SQLserver y los demás sistemas operativos y motores determinados por el estándar de Keralty.

#### 3. **DEFINICIONES**

- **Servidor:** Un **servidor** es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.
- Componentes infraestructura TI: Estos elementos incluyen el hardware, el software, los elementos de red, un sistema operativo (SO) y el almacenamiento de datos. Todos ellos se utilizan para ofrecer servicios y soluciones de TI.
- 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.
- Satellite: Desde una única consola Satellite puede gestionar: Aprovisionamiento, Auditoría, Gestión de Software, Gestión configuraciones y Gestión de suscripciones. El objetivo es proporcionar un repositorio local de contenido certificado para Red Hat Enterprise Linux. Este modelo amplia Red Hat Satellite para proporcionar actualizaciones, soluciones de errores y software.
- Motor base de datos: es el componente de software subyacente que un sistema de administración de la base de datos utiliza para ejecutar las diferentes operaciones en una base de datos.
- Vmware: Es un programa de virtualización a nivel de centro de datos producido por VMware, Inc. Es el componente de su producto VMware Infraestructure que se encuentra al nivel inferior de la capa de virtualización, el hipervisor, aunque posee herramientas y servicios de gestión autónomos e independientes.

Código: SIG-TI-CKE-PR015

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



• vCenter: vCenter Server es la utilidad de administración centralizada para VMware, y se usa para administrar máquinas virtuales, múltiples hosts ESXi y todos los componentes dependientes desde una única ubicación centralizada. VMware vMotion y svMotion requieren el uso de hosts vCenter y ESXi.

#### 4. CONTENIDO.

Este procedimiento determina el proceso para llevar el control de instalación y actualizaciones de los sistemas operativos y motores de bases de datos determinados en el estándar de la Organización.

#### 5. FLUJO DEL PROCEDIMIENTO

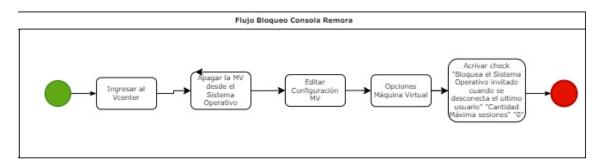


Ilustración 1 Flujo Bloqueo Consola Remota

#### Actualización Linux Satellite

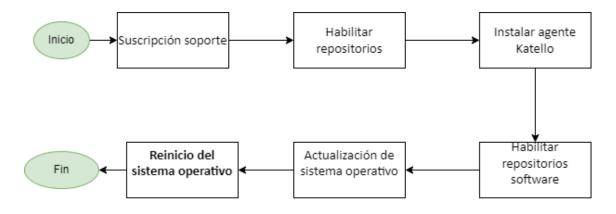


Ilustración 2 Actualización Linux Satellite

Código: SIG-TI-CKE-PR015

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



# Aseguramiento Nuevo servidor Windows Server

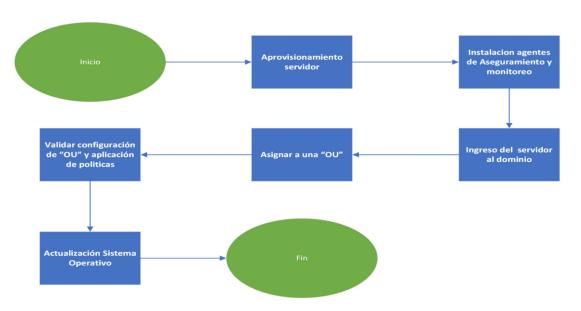


Ilustración 3 Aseguramiento Nuevo servidor Windows

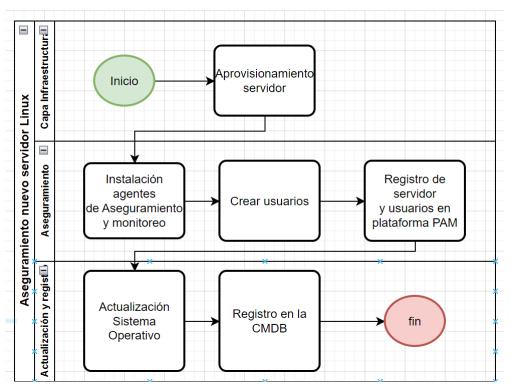


Ilustración 4 Aseguramiento nuevo servidor Linux

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



#### 6. DETALLE DEL PROCEDIMIENTO

**Aseguramiento nuevo servidor Windows Server:** El proceso de aseguramiento del sistema operativo Windows server consiste en lo siguiente:

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Aprovisionamie nto servidor	* Aplicar configuración servidor conforme a formato: "Creación equipo. *Aplicar la última versión de Windows server 2019 *Crear disco c: 100GB *Crear unidad de paginación: Asignar la misma capacidad de memoria RAM *Direccionar la paginación de memoria o swap (Linux) * Configurar tarjeta de red * Activar licencia de sistema operativo	Administrador	*clic derecho sobre mi pc - propiedades - avanzadas sistemas - preforman - avanzadas - cambia la memoria virtual asegura el rendimiento *opciones del adaptador de red, asignar IP, mascara, puerta de enlace y DNS Nota: Nube Azure se deja por defecto.
2	Instalaciones agentes de Aseguramiento y monitoreo	*Instalar los agentes de seguridad:  1.Antivirus – Trend Micro  2.Splunk  3.CrowdStrike  4.Zabbix - producción	Administrador	Revisar el estado funcionalidad de cada una de las herramientas – Aplicaciones predeterminadas

Código: SIG-TI-CKE-PR015

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
3	Ingresar al dominio el servidor	clic derecho mi pc - propiedades - donde aparece el nombre del computador - opción de cambiar - y agregar el nombre de dominio en el cambio de dominio "keralty.com" (productivo - el no productivo noprod.keralty.com. pide usuario y contraseña con permisos de administrador del dominio (si el usuario no tiene perfil de administrador, no le permite. administrador de dominio Nota: Hacer reinicio del servidor	Administrador	aparece mensaje confirmativo de adición de servidor al dominio.
4	Asignar a una "OU"	Se ingresa al controlador de dominio y se abre el service manager - directorio activo - usuarios y computadores (tools) En el Directorio activo buscamos "OU" buscamos el servidor que agregamos - seleccionamos el servidor - clic derecho mover - y se mueve a la "OU" infraestructura y se selecciona el proyecto al cual pertenece el servidor		Seleccionamos - usuarios y grupos locales y se agrega los usuarios locales que tiene permiso administrador de dominio (centro computo) - se asigna como miembro de grupo administradores Nota. se desactiva el usuario administrador que viene por default. clic derecho propiedades - se da check en cuanta desactivada.

Versión: 4.0

Fecha: 22-11-2024

Código: SIG-TI-CKE-PR015

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
		Ver Ejemplo    Add Ottom   State   Add Complete   STELAN   April Accions   Type   Operation   Add Complete   STELAN   April Accions   Add Complete   Add Com		
5	Validar configuración de "OU" y aplicación de politicas	Ingresamos con el comando cmd clic derecho ejecutar como administrador. gpresult /r ver ejemplo:  Objetos de directiva de grupo aplicados  Keralty - Admin RPA Keralty - AdminBackup Keralty - Forupo AAD Keralty - NTP Keralty - Scan Nessus Keralty - Enable WinRM Keralty - Enable WinRM Keralty - Security - 2019 Keralty - Security - 2019 Keralty - Security - 2019 Keralty - Grupo AAD Default Domain Policy Directiva de grupo local	Administrador	Ver el resultado de políticas de seguridad aplicadas. Nota. se analiza los objetivos de directivas aplicadas que correspondan a las políticas de la "OU", aplicación de Hardening por primera vez

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
6	Actualización Sistema Operativo	Ingresar al Windows update y realizar el proceso de búsqueda y actualización de parches o kb de seguridad Nota. se realiza el proceso de instalación de los paquetes requeridos se verifica el historial de las actualizaciones Nota. El historial informa si las actualizaciones se aplicaron de forma correo o fallaron * Se revisa la sincronización del nuevo servidor con el Wsus (repositorio de parches), la pantalla de Wsus muestra el estado de aplicación total de parches. e informa las actualizaciones que están faltando y cuáles.	Administrador	El servidor queda listo para entregar.
7	Registro de servidor y usuarios en plataforma PAM	<ol> <li>Diligenciar formato         "Crear Equipos.xlsx"</li> <li>Diligenciar formato         "Crear         usuarios.xlsx"</li> <li>Crear caso MAS         resolutor soporte         PAM</li> </ol>	Administrador	Verificación del cierre del caso y validad funcionalidad del usuario Registro en lista de administradores
8	Registro en la CMDB	Realizar el registro del nuevo servidor con toda la información relevante y de control.	Administrador	Lista de CMDB

Tabla 1 Aseguramiento nuevo servidor Windows Server

9 Uso Interno

9

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



**Aseguramiento nuevo servidor Linux:** El proceso de aseguramiento del sistema operativo Linux consiste en lo siguiente:

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCI A
1	Aprovisionamie nto servidor	* Aplicar configuración servidor conforme a formato: "Creación equipo. * Plantillas de Linux versiones 7x, 8x, 9x. *Sino cumple con la versión de las plantillas, se dewbe hacer la instalación inicial del sistema operativo Linux * Configurar tarjeta de red y nombre de máquina *Entrega para aseguramiento	Administrador	Se hace entrega al administrador responsable del aseguramiento
2	Instalaciones agentes de Aseguramiento y monitoreo	*Instalar los agentes de seguridad:  1.Antivirus – Trend Micro  2.Splunk  3.CrowdStrike  4.Zabbix - Producción  5. Dataprotector - producción	Administrador	Revisar el estado funcionalidad de cada una de las herramientas – Aplicaciones predeterminadas
3	Crear usuarios	*Validar lista de usuarios administradores *Crea usuarios administradores * Inhabilita usuarios admin *Cambio de contraseña usuario Root	Administrador	Realiza una prueba de los cambios de usuarios

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCI A
4	Registro de servidor y usuarios en plataforma PAM	<ol> <li>Diligenciar formato         "Crear Equipos.xlsx"</li> <li>Diligenciar formato         "Crear         usuarios.xlsx"</li> <li>Crear caso MAS         resolutor soporte         PAM</li> </ol>	Administrador	Verificación del cierre del caso y validad funcionalidad del usuario Registro en lista de administradores
4	Actualización Sistema Operativo	*Registrar y suscribir el servidor en RedHat para habilitar la suscripción de licenciamiento en el Red Hat Satellite.  *Ejecutar el comando (dnf update) o (yum update como suario root)  root()  root	Administrador	Muestra el proceso finalizado de aplicación de parches. Estos parches dependen de la liberación del fabricante Red Hat
8	Registro en la CMDB	Realizar el registro del nuevo servidor con toda la información relevante y de control.	Administrador	Lista de CMDB

Tabla 2 Aseguramiento nuevo servidor Linux

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



**Actualización sistemas operativos Red Hat Linux:** El repositorio de Satellite, permite descargar actualizaciones del sistema operativo desde las versiones 6x en adelante del repositorio del fabricante de Red Hat.

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDE NCIA
1	Suscripción soporte	Asignar licenciamiento de fabricante Red Hat	Administrador	visualización en la plataforma
2	Habilitar repositorios	Habilitar repositorios de software del fabricante en la plataforma satellite	Administrador	Visualización de repositorios de software
3	Instalar agente Katello	Instalar servicio goferd, que permite presentar actualizaciones, bug de seguridad, performance, mejoras de los software instalados.	Administrador	Visualización de paquetes en el servidor
4	Habilitar repositorios software	presentar repositorios disponibles en Satellite	Administrador	Visualización de repositorios
5	Actualización de sistema operativo	Aplicar parches y updates disponibles en la plataforma.	Administrador	Visualización en la plataforma.
6	Reinicio del sistema operativo	Si las actualizaciones aplican release de sistema operativo, se debe aplicar un reinicio.	Administrador	Visualización de la nueva versión del sistema operativo

Tabla 3 Actualización sistemas operativos Red Hat Linux

**Actualización sistemas Windows Server:** El repositorio de WSUS, permite descargar actualizaciones del sistema operativo desde las versiones 2012 en adelante del repositorio del fabricante Microsoft.

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDE
				NCIA
1	liberación Update	Se ingresa a la consola de WSUS en el servidor asignado y se aprueban las actualizaciones al grupo.	Administrador Sistema	en la consola de WSUS se verifica la aprobación del grupo a actualizar

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDE NCIA
2	Ejecutar comprobación de actualización Servidor	Ingresar al proceso de actualización de cada servidor y se realiza la comprobación de actualizaciones liberadas	Administrador Sistema	Proceso de Update del servidor se evidencia actualizaciones disponibles
3	Realizar la verificaciones de las actualizaciones que se van a liberar,	Se ingresa al listado de las actualizaciones disponibles del servidor y seleccionar las actualizaciones que se van a liberar	Administrador Sistema	Al momento de actualizarse verán las actualizaciones liberadas
4	Instalación de actualizaciones	Realizar la instalación de cada actualización liberada para el servidor	Administrador Sistema	Registro en software instalado en el sistema operativo
5	Reinicio servidor	Al terminar se reinicia el servidor para la activación de las actualizaciones instaladas	Administrador Sistema	Visor de evento de servidor por el reinicio controlado del Sistema operativo
6	Validación de servicios funcionando	Se verifica el correcto funcionamiento	Administrador Sistema y negocio	Se reporta por correo su correcto funcionamiento

Tabla 4 Actualización sistemas Windows Server

**Configuración consola remota máquinas virtuales Vmware**: Para dar cumplimiento al control 4.2 de la auditoría de Swift, se realiza a continuación la configuración para deshabilitar el acceso a los servidores de swift de forma directa desde la consola remota de vmware.

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDE NCIA
1	Apagado de la máquina virtual	Realizando el acceso a través del sistema operativo se ejecuta el comando de apagado del servidor	Administrador Sistemas	Log de eventos de la máquina virtual en el Vcenter

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDE NCIA
2	Editar Configuración	Desde Vmware, "Editar configuración" de la máquina virtual	Administrador de Sistemas	Log de eventos de la máquina virtual en el Vcenter
3	Opciones máquina virtual	Ingresar a las "Opciones de máquina virtual"	Administrador de Sistemas	Log de eventos de la máquina virtual en el Vcenter
4	Opciones Vmware Remote Console	Activar check "Bloquea el sistema operativo invitado cuando se desconecta el último usuario remoto" cambiar en "Cantidad máxima de Sesiones" "0"	Administrador de Sistemas	Log de eventos de la máquina virtual en el Vcenter

Tabla 5 Configuración consola remota máquinas virtuales Vmware

**Actualización motor base de datos:** Se descarga el software y actualizaciones del motor para las versiones vigentes desde el repositorio del fabricante Oracle o Microsoft.

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVID ENCIA
1	Definir el servidor	Solicitar aprovisionamiento del servidor o definir uno existente	DBA / Adm. Infraestructura	Formato
2	Validar prerrequisitos del SO	Asegurar que las condiciones a nivel de SO se cumplan	DBA / Adm. SO	Ticket con la solicitud
3	Descargar el software	Seleccionar y descargar la versión del software que se instalará	DBA	Portal oficial del Fabricante
4	Definir rutas en las que se instalarán los componentes del motor	Crear las rutas y permisos para la instalación	DBA	
5	Iniciar la instalación del software	Instalar el motor y/o parches que corresponda	DBA	

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVID ENCIA
6	Validar servicios	Asegurar que los servicios queden activos y funcionando	DBA	
7	Crear BD	Crear las BDs de los diferentes aplicativos según solicitud	DBA	Ticket con la solicitud
8	Tareas post instalación	Configurar los componentes para asegurar la operación del servicio (backup, monitoreo, temas de seguridad, etc)	DBA	
9	Entrega del servicio	Entregar los datos de conexión para el acceso al servicio	DBA	Correo

Tabla 6 Actualización motor base de datos

# PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



### 7. CONTROL DE CAMBIOS.

FECHA	САМВІО	VERSIÓN
12/09/2022	Creación documento	1.0
21/06/2023	21/06/2023 Adición aseguramiento Windows Server y Linux	
5/10/2023	Validación de contenido y formato	3.0
22/11/2024	Se actualizan las versiones de Sistema Operativo. El documento se revisa en el marco de la actualización del SGSI año	

Tabla 7 Control de Cambios

### PROCEDIMIENTO INSTALACIÓN, ACTUALIZACIÓN Y CONFIGURACIÓN DE SOFTWARE



### 8. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Equipo Operaciones TI Área/Proceso: Operaciones TI Fecha:14/11/2018		Nombre: Luisa Gineth Castaño Área/Proceso: Director Operaciones y comunicaciones TI Fecha: 22/11/2024

Tabla 8 Flujo de Aprobación

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