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.

Garantizar la gestión y aplicación de los lineamientos de la política de operación TI SIG-TICC05.

2. ALCANCE.

Asegurar los procesos de operación TI, gestionando actividades sobre la infraestructura para mantener la disponibilidad, rendimiento, y demás funciones que soportan los servicios tecnológicos de la Organización.

3. DEFINICIONES

NTP(Network Time Protocol): Protocolo de internet utilizado para tener sincronizados los servicios de hora en los sistemas informáticos.

4. CONTENIDO

4.1. Gestión del NTP (Network Time Protocol)

Configurar el servicio NTP (Network Time Protocol), este protocolo permite sincronizar todos los relojes de los servidores de la Organización, mediante los controladores de dominio ubicados en las sedes principales del grupo Keralty.

4.2. Terminación contrato servicios en nube o servicios con terceros.

Con 90 días o mayor tiempo de anticipación se conoce la terminación del servicio de nube o contrato de servicios con terceros. Todo proceso de RFP debe llevar este criterio de evaluación.

En caso de dar por terminado el contrato, se debe programar el proceso de descarga de bases de datos, aplicaciones y archivos correspondientes al negocio.

4.3. Aplicación de guías de endurecimiento “Hardening Cis” a servidores

La organización cuenta con un plan de aseguramiento de acuerdo con las publicaciones o documentos entregados por el área de ciberseguridad, esta actividad se realiza para todos los sistemas operativos estandarizados en la organización, una vez entregada es

analizada e implementada en el primer semestre de cada año, para el aprovisionamiento de nuevos sistemas se toma como base las plantillas que se almacenan en el repositorio Drive asignado, las plantillas deben ser actualizadas mensualmente para garantizar que se mantengan en las últimas versiones liberadas por el fabricante.

4.4. Inventario de servicios y puertos de red permitidos y no permitidos

Los servidores implementados en la infraestructura de la organización se entregan con una línea base de puertos permitidos para la gestión del sistema operativo y servicios predefinidos:

Windows:

Windows	
3389/tcp – udp	RDP – Windows
5555/tcp	DataProtector
10050/tcp	Zabbix
123/UDP	NTP

FileServe	
135/tcp	epmap
139/tcp	Netbios-ssn
445/tcp	Microsoft-ds
3389/tcp	RDP – Windows
5555/tcp	DataProtector
10050/tcp	Zabbix
123/UDP	NTP

Linux:

Linux	
22/tcp	SSH
5555/tcp	DataProtector
10050/tcp	Zabbix
123/UDP	NTP

Linux Oracle	
22/tcp	SSH
111/tcp	sunrpc
1521/tcp	Oracle
5555/tcp	DataProtector
10050/tcp	Zabbix
123/UDP	NTP

4.5. Mantener redundancia en dispositivos de alta criticidad de la infraestructura

La organización en sus componentes de infraestructura transversales cuenta con soluciones redundantes activo - pasivo en Balanceadores de carga, switch de red, Cluster Oracle y servicios de máquinas virtuales “Vmware”.

Debe mantenerse un seguimiento continuo de la disponibilidad y riesgos sobre los puntos de falla que lleven a un tiempo considerable en la recuperación del servicio. Este análisis se debe hacer de forma mensual.

4.6. Gestión de centros de datos de sedes y datacenter

Gestión sobre el cumplimiento de los estándares técnicos, ambientales y de seguridad de los centros de datos tales como: Humedad, temperatura, energía redundante, Ups, control de acceso de personal autorizado, luces de emergencia, mantenimiento equipos. Por otra parte, el control de visitantes al centro de datos sede calle 100 # 11B67 Bogotá así:

- Todo el personal de la Organización debe solicitar la necesidad de ingreso mediante correo las personas con nombre completo, cédula, EPS y ARL de afiliación, fecha y hora de ingreso, además de la justificación de ingreso al centro de datos de calle 100.
- El personal se debe anunciar en la portería y allí verifican la autorización de ingreso al centro de datos, además de contactar a la persona que hará el acompañamiento.
- Estar con un acompañante de la Organización que está autorizado para el ingreso al centro de datos por el dispositivo facial.
- El personal autorizado debe portar el carnet que acredite la identificación dentro de las instalaciones del edificio Colsanitas sede calle 100 # 11B67 Bogotá.
- El personal autorizado debe registrar todos los elementos que ingresa o retira del centro de datos. El área de seguridad locativa de la sede de calle 100 no se hace responsable de elementos como: Portátiles, discos duros, equipos de medición, partes de equipos de cómputo, entre otros, que no hayan sido registrados en el momento del ingreso.
- Está prohibido el ingreso a las instalaciones de los siguientes elementos:
    - Armas de fuego
    - productos explosivos
    - Botellas de vidrio
    - Bebidas embriagantes o cualquier tipo de sustancias alucinógenas o psicoactivas
- Sólo el área de seguridad física puede autorizar el ingreso de los siguientes elementos:
    - Filmadores
    - Cámaras fotográficas especializadas
    - Encendedores
    - Elementos cortopunzantes
    - Sustancias químicas e inflamables
- Toda persona que ingrese a la sede está registrada y grabada por la cámara desde el inicio y permanencia en el centro de datos.
- En caso de necesidad de retiro de elementos o equipos del centro de datos debe solicitar el retiro mediante formato autorizado.
- De incumplir este lineamiento la persona autorizada se hace acreedora a sanciones y el área de seguridad locativa levanta un incidente del caso.

4.7. Gestión y manejo de log de software

Los servidores, como plataformas de software e infraestructura generan registros de las transacciones del software en una ruta estándar la cual cuenta con capacidad suficiente para su almacenamiento, así como la integración con SIEM para su análisis, y un respaldo periódico alineado a las políticas de log de la organización, de los ambientes productivos y de alta criticidad o sistemas CORE.

4.8. Creación y Gestión de redes datacenter

Las redes de la organización están divididas en vlan quien a su vez tiene una segmentación de red independiente garantizando que de acuerdo a su asignación no se comuniquen entre sí, para mantener esta política se cuenta con un firewall que se encarga por medio de políticas y reglas permitir o denegar el tráfico entre redes.

Las redes que pertenecen al mismo segmento o vlan pueden generar tráfico entre ellas.

La política 0 (cero) por defecto del firewall restringe todo el tráfico entre redes de diferente segmento o vlans.

5. FLUJO DEL PROCEDIMIENTO

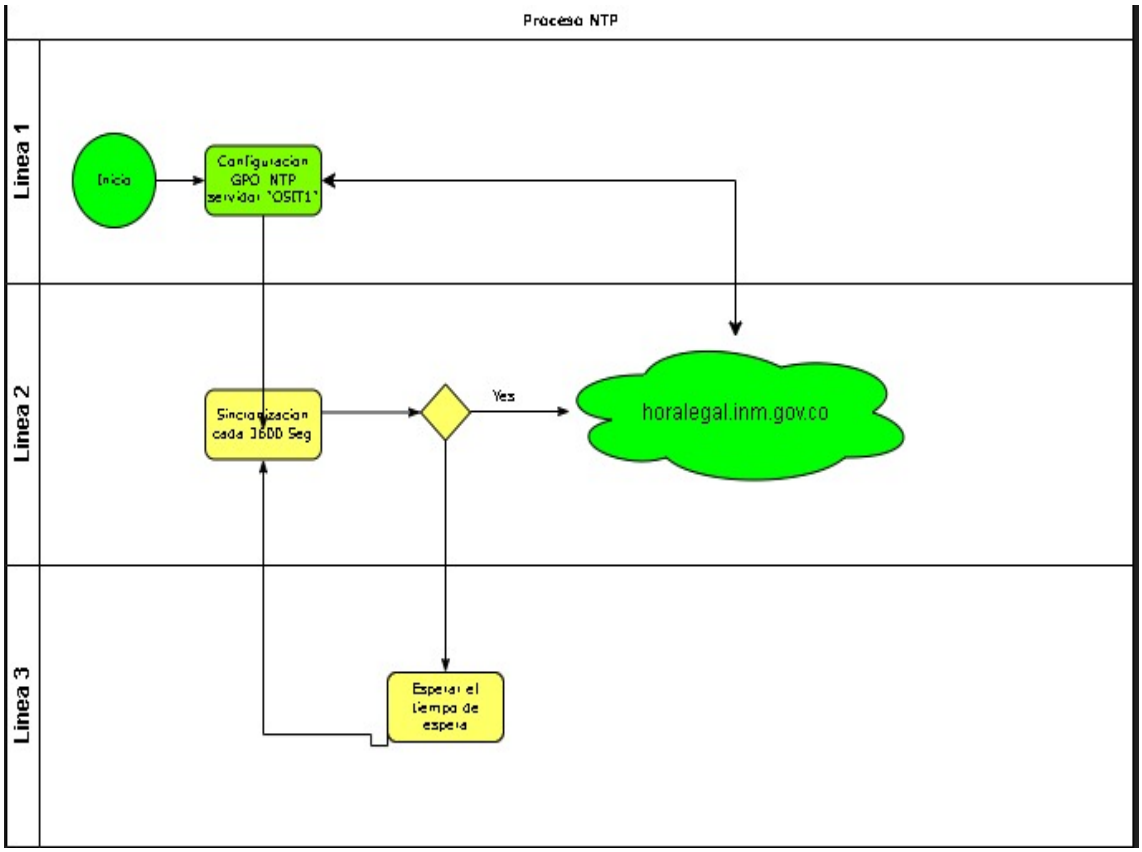

Ilustración 1 Flujo de procedimiento

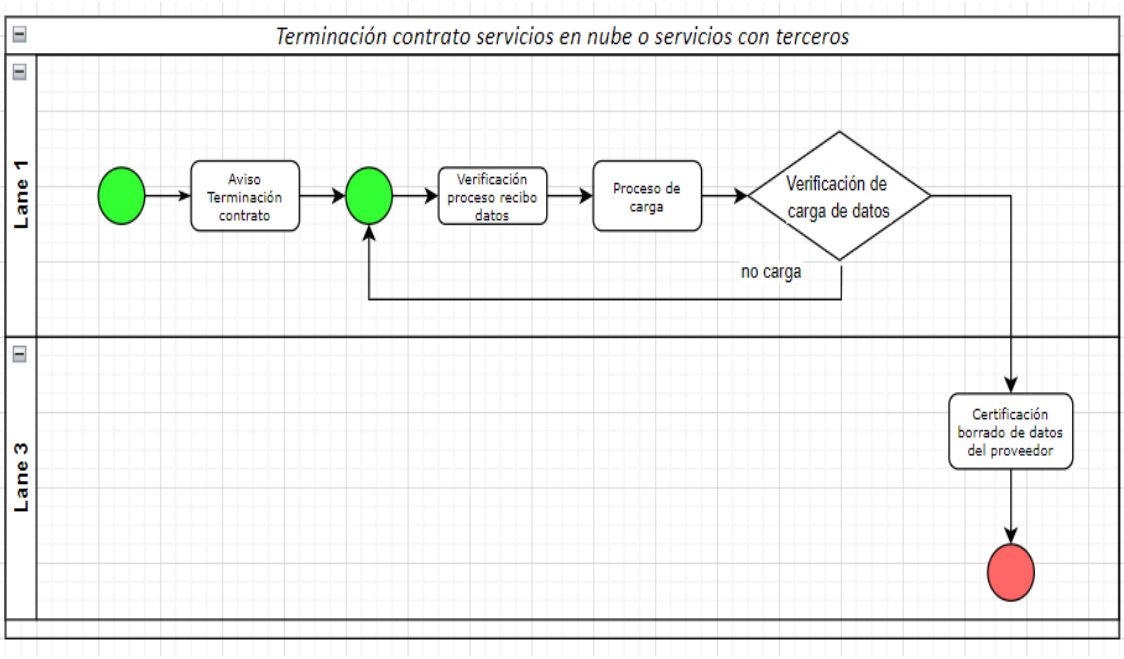

Ilustración 2 Terminación Contrato

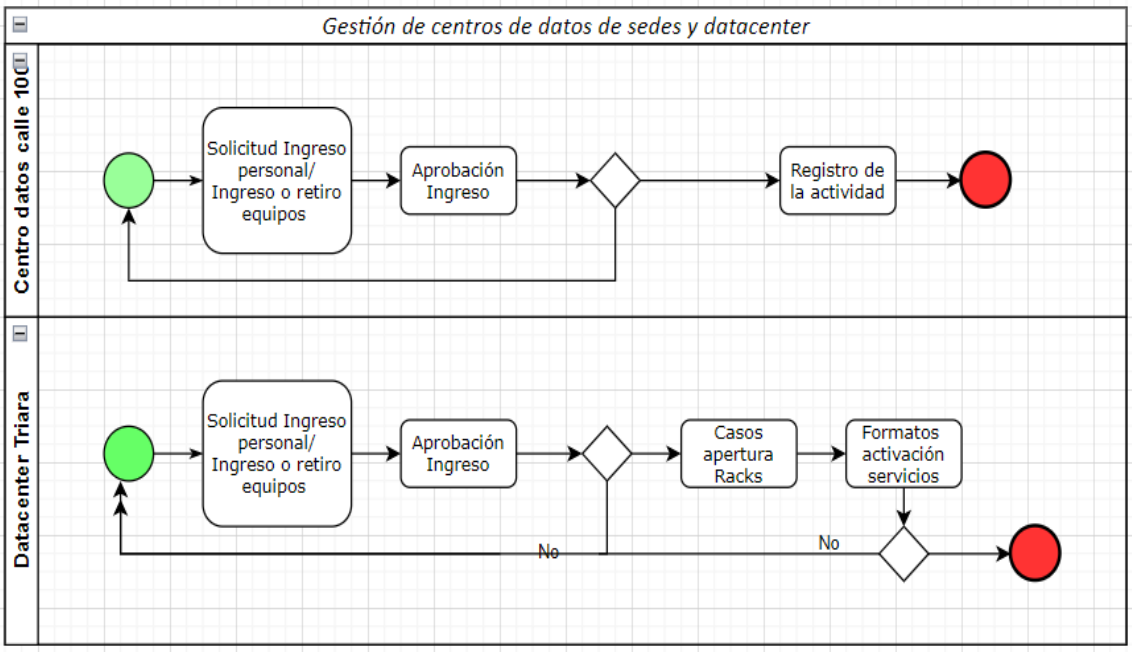

Ilustración 3 Gestión de centros de datos

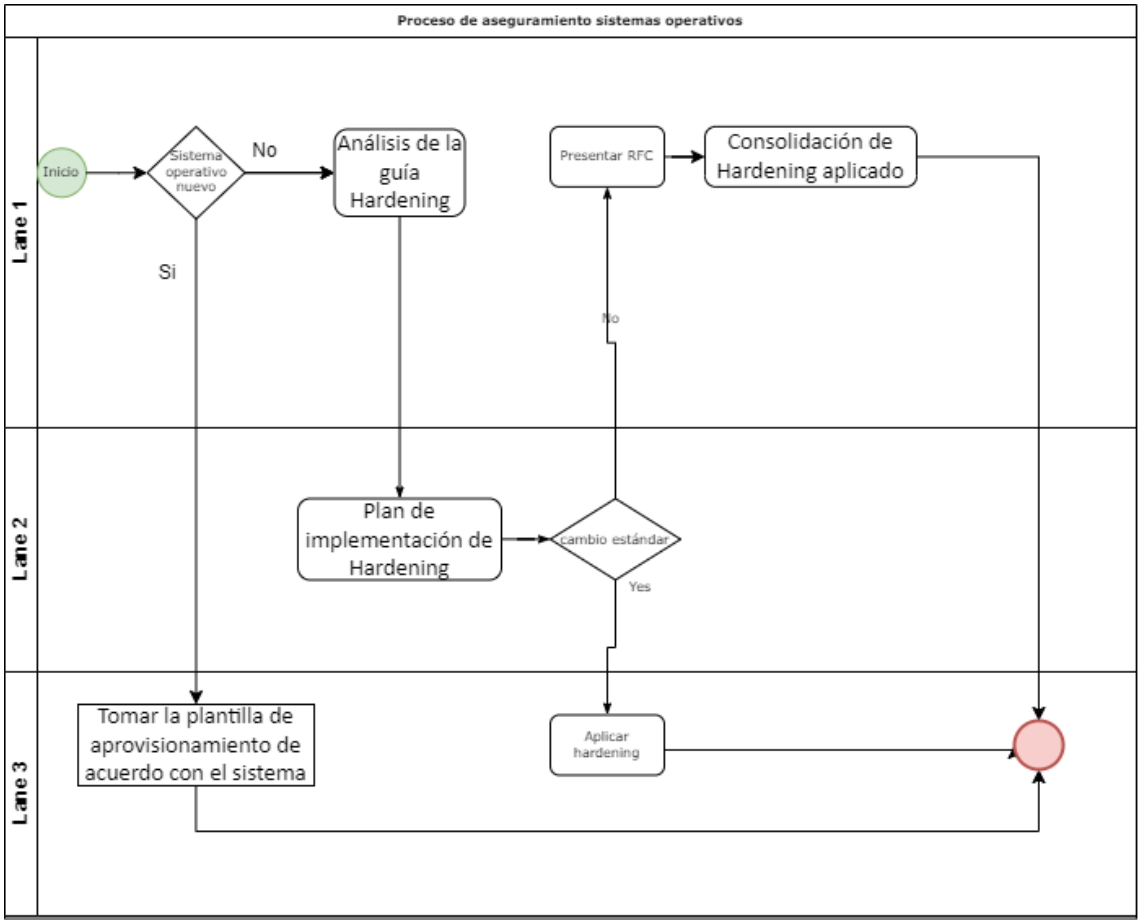

Ilustración 4 Proceso de aseguramiento sistemas operativos

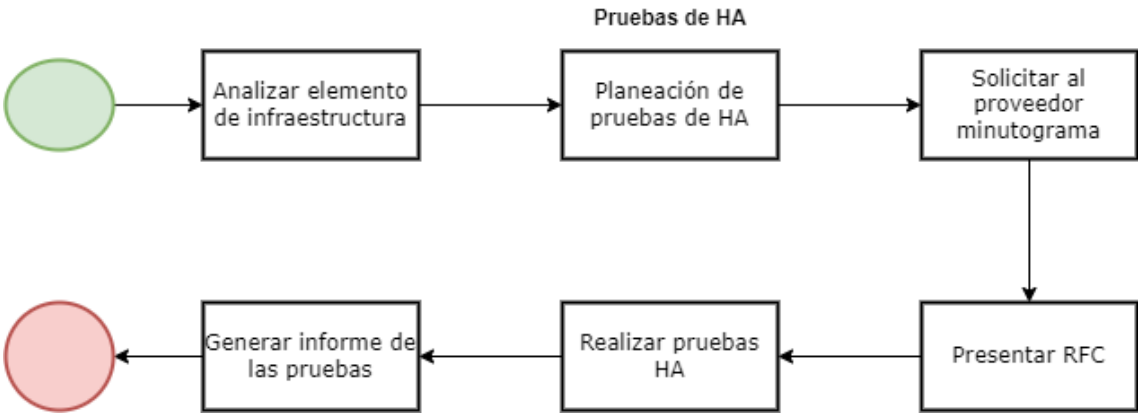

Ilustración 5 Pruebas de HA

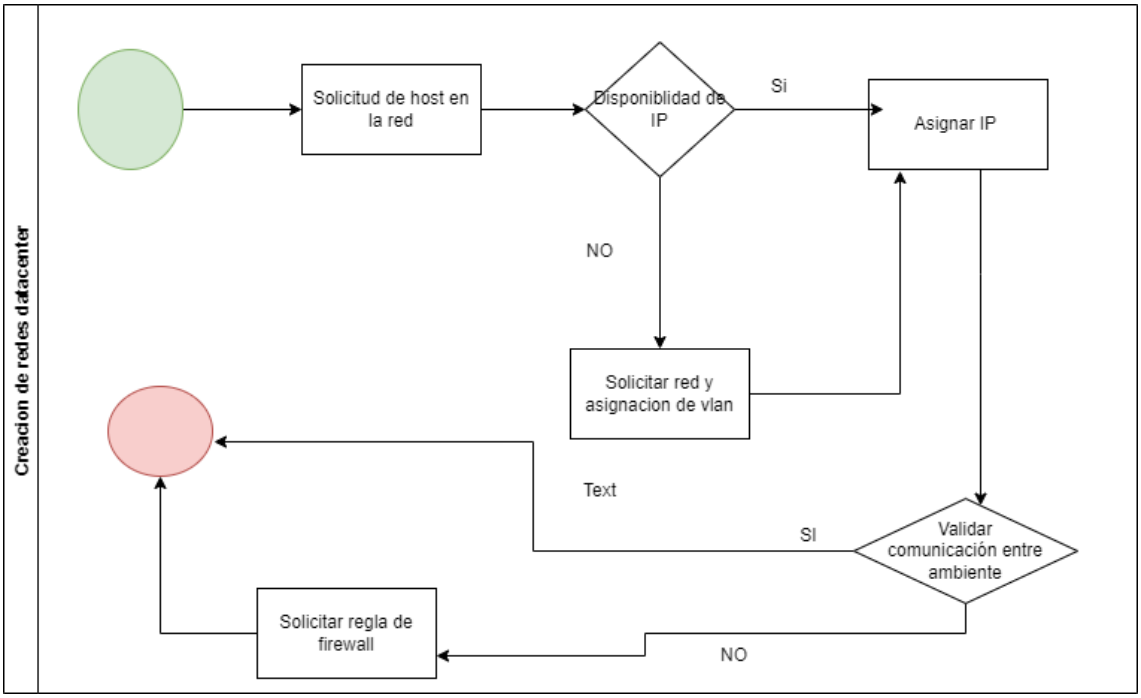

Ilustración 6 Creación de redes Datacenter

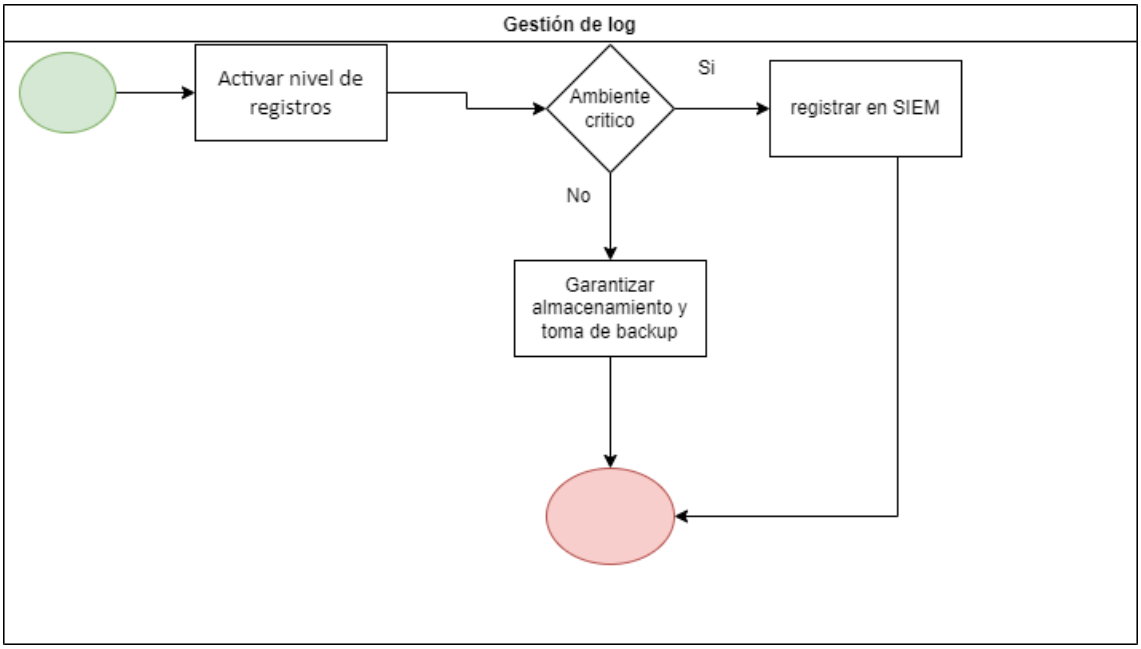

Ilustración 7 Gestión de Log

6. DETALLE DEL PROCEDIMIENTO

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Configuración GPO	Se valida política NTP para sincronización de hora en servidores	Administrador de sistema	Servicio automático controlador de dominio
2	Tiempo de sincronización	La GPO consulta cada 3600 seg el proveedor externo de hora	Administrador de sistema	Servicio automático controlador de dominio
3	Proveedor de hora	El proveedor externo de hora es la página horalegal.imn.gov.co	Administrador de sistema	Servicio automático controlador de dominio
4	Replica hora	GPO realiza réplica de la hora en los servidores de la red Keralty	Administrador de sistema	Servicio automático controlador de dominio

Tabla 1 NTP

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Informar el proceso de terminación contrato	Anuncio por escrito de terminación contrato y acordar las condiciones de entrega de información y el tiempo	Supervisor del contrato	Correo y carta firmada por el representante legal
2	Proceso recibo información	Proceso mediante el cual se acuerda las condiciones técnicas y medios magnéticos o comunicaciones, para el proceso de recuperación de datos y aplicaciones	Equipo técnico de Operaciones y el dueño de los datos del Negocio.	Reunión meet y acta de reunión
3	Proceso de carga información recibida	Proceso de carga de datos, aplicaciones a la plataforma de la Organización	Equipo de centro cómputo	Registro de carga
4	Verificación Datos por el negocio	Proceso de verificación de la información recibida	Líderes del negocio	Registro de pruebas
5	Termina el proceso de migración y	Proceso de validación y aseguramiento de la eliminación de datos y accesos a la	Líder del negocio y Operaciones	Acta de borrado seguro de la información por el proveedor

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
	borrado de sitio proveedor	plataforma del tercero		

Tabla 2 Terminación contrato servicios en nube o servicios con terceros

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Análisis de la guía Hardening	Revisar cada uno los ítems recomendados para determinar la viabilidad de aplicación sobre el SO	Administrador del Sistema	Ajuste plantilla Hardening
2	Plan de implementación de Hardening	Presentar inventario de servidores y generar actividades a realizar durante el proceso de implementación, presentar RFC estándar y/o normales.	Administrador del Sistema	
3	Aplicación de Hardening	Aplicar checklist de ítems de hardening de los diferentes servidores de acuerdo con la viabilidad.	Administrador de sistemas	Checklist de actividades.
4	Consolidación de Hardening aplicado	Entregar la documentación de las actividades realizadas	Administrador de sistemas	Documentación.
5	Implementación de nuevos sistemas	Tomar la plantilla de aprovisionamiento de acuerdo con el sistema	Administrador de sistemas	Entrega de sistema

Tabla 3 Guía de endurecimiento servidores

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Activación puertos	Se verifican los puertos por defecto por sistema operativo para la administración remota	Administrador del Sistema	
2	Definición de puertos Servicio	Según el servicio implementado con puertos estándar como 389, 445 o 25	Administrador del Sistema	Documentación
3	Definición de puertos Personalizados	Si el servicio es publicación de desarrollos de aplicaciones se utilizan puertos personalizados que se	Administrador del Sistema	Documentación de aplicación

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
		habilitan según documentación Ej: 8180-8989		

Tabla 4 Gestión inventario de servicios y puertos permitidos y no permitidos

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Validación de configuración de Balanceo de cargas	Garantizar que las configuraciones de los nodos de balanceo se encuentren homologadas e Activo - Pasivo	Administrador de sistemas	Configuración de balanceo
2	Validación configuración de switch de redes datacenter	Garantizar que las configuraciones de los dispositivos de redes se encuentran homologadas Activo - Pasivo	Administrador de sistemas	Configuración de Switches LAN
3	Pruebas de HA de cluster de Oracle	Realizar pruebas de HA de los nodos de base de datos que soportan los diferentes sistemas de la organización	DBA - Bases de datos	Checklist de pruebas de HA

Tabla 5 Mantener redundancia en los dispositivos de alta criticidad de la infraestructura

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
0		**Centro datos sede calle 100**		
1	Revisión diaria	Temperatura, luces, funcionamiento de cámara de acceso	Operador de Soporte	Registro en archivo
2	Cámaras de grabación Centro de datos y control acceso	Revisión funcionalidad cámara video y control facial de acceso	Centro seguridad locativo	Software control seguridad locativo “Myintelli”
3	Aires Acondicionados	Dos visitas al año de verificación de	Mantenimiento Locativo	Un mantenimiento al año de Aires

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
		funcionamiento de equipos		
4	Ups	Carga y funcionalidad de UPS	Mantenimiento Locativo	Un mantenimiento preventivo al año de las Ups
5	Control Ingreso o Retiro equipos	Formato de control de acceso o retiro	Operador de soporte	Archivo de formatos digitales
6	Autorización acceso a personal externo	Solicitud a través de correo justificando el ingreso al CDP, Nombre, cédula, ARL y EPS	Autorización del Director de Operación TI	Correo autorizado, centro se seguridad
		Datacenter Triara		
7	Funcionarios con acceso permanente	Registro de acceso permanente con tarjeta de Ingreso al Datacenter Triara	Director de Operación TI	Formulario con las personas autorizadas
8	Funcionarios o terceros que ingresan a gestionar la infraestructura	Diligenciar el formato de ingreso y crear un caso en la plataforma de Service Manager, ser autorizado	Director de Operación TI	Formato de Ingreso al Datacenter

Tabla 6 Gestión de centros de datos de sedes y datacenter

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Activar nivel de registros	Validar los registros que genera el software	Desarrollo y Administrador de sistemas	almacenamiento de trazas
2	Incluir en plataforma de SIEM	Validar el grado de criticidad del sistema de información e integrar de ser posible en el SIEM	Seguridad Administrador de sistemas	Analisis de log
3	Toma de Backup	Configurar en la plataforma de backup el respaldo	Administrador de sistemas	Registros de backup

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
		de las rutas donde se están almacenando los registros del software.		

Tabla 7 Gestión de centros de datos de sedes y datacenter

NO.	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO/EVIDENCIA
1	Solicitud de host en la red	Identificar para qué ambiente se requiere el nuevo dispositivo	Administrador de sistemas	N/A
2	Asignación de IP	Asignar identificador al host o equipo que va a hacer parte de la red de la organización dependiendo el ambiente	Administrador de sistemas	N/A
3	Crear política	Realizar solicitud de política o regla que permita la comunicación entre redes de otros segmentos o vlan.	Administrador de sistemas/ Administrador de Firewall	N/A

Tabla 8 Gestión de redes datacenter

7. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
04/10/2022	Creación documento	1.0
5/10/2023	Validación de Contenido y formato	2.0
22/11/2024	Se actualiza el inventario de puertos de Sistema Operativos. 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.	3.0

Tabla 9 Control de Cambios

8. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Iván Andres Pedraza G Área/Proceso: Operaciones TI Fecha: 26/09/2022	Nombre: Luisa Gineth Castaño Área/Proceso: Director de Operaciones TI Fecha: 22/11/2024	Nombre: Luisa Gineth Castaño Área/Proceso: Director de Operaciones TI Fecha: 22/11/2024

Tabla 10 Flujo de Aprobación

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