1. **OBJETIVO:** Establecer las directrices, actividades y controles necesarios para la definición y monitoreo y mantenimiento de configuraciones seguras en los activos tecnológicos del Instituto Colombiano de Bienestar Familiar ICBF, con el fin de garantizar su funcionamiento adecuado, prevenir cambios no autorizados, reducir vulnerabilidades, proteger la confidencialidad, integridad y disponibilidad de la información institucional.

2. **ALCANCE:**

Esta guía aplica en el ámbito nacional en la Dirección de Tecnología de la Información DTI, donde incluye todos los activos de tecnología de la información que soportan los sistemas de información y servicios digitales del ICBF, como, servidores (Windows y Linux), infraestructura de virtualización, plataformas de contenedores, infraestructura de red, dispositivos de seguridad perimetral (firewalls, IDS/IPS), sistemas operativos, bases de datos, aplicaciones institucionales, plataformas tecnológicas en la nube y cualquier otro componente que soporte servicios críticos de la Entidad.

3. **DEFINICIONES:**

Activo: elemento de hardware, software, red o infraestructura que soporta los servicios tecnológicos de la Entidad y que debe ser gestionado para garantizar su disponibilidad, integridad y seguridad.

CIS: CI (Elemento de Configuración) es cualquier componente o activo necesario para prestar un servicio de TI que debe gestionarse, controlarse y registrarse en la CMDB. Incluye hardware (servidores, redes), software (aplicaciones), esenciales para la gestión del ciclo de vida del servicio.

CMDB: Es una base de datos centralizada que almacena información detallada sobre los componentes de infraestructura de TI —denominados Elementos de Configuración o CIs— y sus interrelaciones. Su objetivo es proporcionar una vista unificada del entorno de TI para gestionar cambios, incidentes y activos con precisión.

Herramienta de Gestión ITSM: Es una herramienta que permite a las organizaciones diseñar, planificar, entregar y gestionar sus servicios tecnológicos.

Line Base Configuración: conjunto documentado de configuraciones base seguras establecidas para un activo tecnológico, que sirve como referencia para la implementación, control y verificación de su configuración.

Configuración: conjunto de parámetros, ajustes y características definidas en un sistema, dispositivo o aplicación que determinan su funcionamiento y comportamiento operativo.

Configuración Segura: configuración de un activo tecnológico establecida conforme a estándares de seguridad y buenas prácticas, orientada a reducir vulnerabilidades y minimizar riesgos de seguridad de la información.

Desviación de Configuración: diferencia identificada entre la configuración actual de un activo tecnológico y la configuración base establecida por la Entidad.

Gestión de Configuración: proceso mediante el cual se establecen, documentan, implementan, controlan y monitorean las configuraciones de los activos tecnológicos con el fin de mantener su funcionamiento seguro y controlado.

CMDB (Configuration Management Database – Base de Datos de Gestión de la Configuración): Repositorio centralizado que almacena y administra la información de los elementos de configuración (Configuration Ítems – CI), incluyendo sus atributos, estados, versiones y relaciones dentro de la infraestructura tecnológica de la Entidad.

En el marco de ITIL, la CMDB constituye un componente fundamental del Sistema de Gestión de la Configuración del Servicio (CMS), permitiendo la identificación, control, trazabilidad y verificación de los activos tecnológicos a lo largo de su ciclo de vida.

Su adecuada gestión es un punto clave para la práctica de Gestión de la Configuración, ya que soporta de manera transversal otros procesos como la gestión de cambios, incidentes, problemas y activos de TI, facilitando el análisis de impacto, la toma de decisiones informadas y la garantía de integridad de los servicios tecnológicos del ICBF.

Hardening: proceso de fortalecimiento de seguridad aplicado a sistemas operativos, aplicaciones, bases de datos y dispositivos tecnológicos mediante la eliminación de configuraciones inseguras y la implementación de controles de seguridad.

Línea Base: conjunto aprobado y documentado de configuraciones estándar que sirve como referencia para la implementación, control y verificación de los activos tecnológicos.

RFC (Request for Change): solicitud formal de cambio utilizada para registrar, evaluar y gestionar modificaciones en los activos tecnológicos, incluyendo su justificación, impacto, riesgos y plan de implementación.

Ambiente de Producción: entorno donde operan los sistemas de información en uso real por los usuarios finales y donde se procesan datos institucionales.

Ambiente de Pruebas (Testing): entorno controlado utilizado para validar configuraciones, cambios o desarrollos antes de su paso a producción.

Ambiente de Desarrollo: entorno donde se realizan actividades de construcción, configuración inicial o ajuste de sistemas sin afectar la operación productiva.

Principio de Mínimo Privilegio: práctica de seguridad que consiste en otorgar a los usuarios únicamente los permisos estrictamente necesarios para desempeñar sus funciones.

Trazabilidad: capacidad de rastrear y registrar todas las acciones, cambios o eventos realizados sobre un activo tecnológico a lo largo del tiempo.

Configuración por Defecto: parámetros iniciales establecidos por el fabricante o proveedor de un sistema, los cuales pueden representar riesgos si no son ajustados conforme a estándares de seguridad.

Superficie de Ataque: conjunto de puntos de un sistema o red que pueden ser explotados por amenazas para comprometer la seguridad.

Gestión de Incidentes de Seguridad de la Información: proceso para identificar, analizar, contener, erradicar y recuperar eventos que afecten la confidencialidad, integridad o disponibilidad de la información.

Control de Versiones: mecanismo que permite gestionar, identificar y mantener el historial de cambios realizados sobre configuraciones, sistemas o documentos.

Segregación de Ambientes: separación lógica o física de los entornos de desarrollo, pruebas y producción para reducir riesgos de seguridad y errores operativos.

4. DESARROLLO:

La guía asegura la identificación, control, mantenimiento y verificación de las configuraciones de los activos tecnológicos, garantizando su integridad, trazabilidad y alineación con los estándares de seguridad y operación definidos por la Entidad. En este sentido, todos los cambios y configuraciones realizados sobre los elementos de configuración (CI) deberán gestionarse conforme a los controles definidos, asegurando su registro, documentación y actualización en las fuentes autorizadas de información (CMDB o repositorio de configuración), en concordancia con las prácticas de ITIL y las políticas de seguridad de la información del ICBF.

4.1 Gobernanza y Responsabilidad: La configuración de los activos tecnológicos del Instituto Colombiano de Bienestar Familiar – ICBF requiere asignar roles claros y responsabilidades definidas, asegurando que las configuraciones base se implementen, monitoreen y mantengan de manera efectiva. Esto permite garantizar la confidencialidad, integridad y disponibilidad de la información institucional, y mantener trazabilidad de todos los cambios realizados.

Esta sección define los roles, responsabilidades y orientaciones de supervisión, asegurando que todos los procesos relacionados con la gestión de configuraciones, cambios y seguridad de la información se realicen de manera coordinada, trazable y conforme a las políticas institucionales:

ROL	RESPONSABILIDADES
Profesionales Líderes de Servicios DTIC	-Identificar activos tecnológicos sujetos a configuración. -Definir configuraciones base seguras. -Registrar la configuración aplicada. -Verificar cumplimiento de configuraciones y gestionar desviaciones.
Gestor de Control de Cambios	-Implementar configuraciones en los activos siguiendo el procedimiento de gestión de cambios. - Registrar evidencia de implementación de RFCs.
Gestor de Configuración	-Definir, implementar y mantener el proceso de gestión de configuraciones dentro de la organización. -Administrar y asegurar la correcta operación de la CMDB, garantizando la integridad, consistencia y actualización de la información registrada. -Identificar y controlar los elementos de configuración (CI), asegurando que estén debidamente documentados con sus atributos y relaciones. -Establecer, mantener y actualizar las líneas base de configuración (baseline) de los activos tecnológicos. -Verificar que todas las configuraciones y cambios en los activos tecnológicos se gestionen a través del proceso formal de gestión de cambios. -Garantizar la trazabilidad de los cambios realizados en los activos tecnológicos, asegurando su adecuado registro y documentación. -Gestionar y hacer seguimiento a las desviaciones de configuración, promoviendo la implementación de acciones correctivas.
Integrantes Comité de Control de Cambios	-Revisar y aprobar las configuraciones base definidas. - Asegurar que las configuraciones cumplan con los lineamientos de seguridad institucional y buenas prácticas.
CSIRT / Equipo de Seguridad	-Apoyar en la gestión de incidentes derivados de desviaciones de configuración. - Coordinar con CSIRT Gobierno o entidades externas en incidentes críticos.
Alta Dirección / Dirección de TI	-Aprobar políticas y lineamientos de configuración. - Garantizar recursos y soporte para la implementación, monitoreo y auditoría de configuraciones.

Gestor de garantía, Inventarios y CMDB	-Administrar y controlar los activos tecnológicos de la Entidad, asegurando el registro, actualización y trazabilidad de la información en inventarios y CMDB, así como la gestión de garantías.

4.2 Implementación de Configuraciones

4.2.1 El Instituto Colombiano de Bienestar Familiar – ICBF establecerá y mantendrá configuraciones base seguras para los activos tecnológicos que soportan los sistemas de información y servicios digitales de la Entidad, con el fin de garantizar su operación segura, reducir vulnerabilidades y prevenir cambios no autorizados que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional. Para ello, gestionará la configuración mediante la implementación de prácticas alineadas con ITIL, que incluyen la definición, documentación y control de líneas base de configuración, el registro y administración de los activos como ítems de configuración (CI) en la CMDB institucional, la ejecución de procesos formales de control de cambios, la validación periódica de configuraciones mediante herramientas que disponga la entidad y la trazabilidad de las relaciones entre los componentes tecnológicos. Asimismo, se garantizará que cualquier modificación a las configuraciones sea evaluada, autorizada, documentada y verificada conforme a los procedimientos establecidos, asegurando la integridad del entorno tecnológico y la mejora continua del servicio.

4.2.2 La gestión del cambio es un proceso fundamental para controlar el ciclo de vida de modificaciones en servicios componentes de los servicios tecnológicos del Instituto Colombiano de Bienestar Familiar – ICBF. A través de este proceso se asegura que cualquier modificación en las configuraciones de los activos tecnológicos sea evaluada, aprobada, implementada y documentada de manera controlada, reduciendo el riesgo de afectaciones operativas, incidentes de seguridad y pérdida de información.En este sentido, toda actividad relacionada con la configuración de activos tecnológicos deberá estar articulada con el proceso institucional de gestión de cambios, considerándose un control clave dentro del Sistema de Gestión de Seguridad de la Información.

4.2.3 Todas las configuraciones de hardware, software, redes, plataformas tecnológicas y sistemas de información deberán ser documentadas y gestionadas conforme a estándares de seguridad definidos por la Dirección de Tecnologías de la Información, los cuales deberán considerar buenas prácticas reconocidas en materia de seguridad de la información, tales como principios de mínimo privilegio, eliminación de configuraciones por defecto, des habilitación de servicios innecesarios y aplicación de controles de seguridad.

4.2.4 Cada líder de servicio será responsable de identificar, documentar y mantener actualizado el inventario de línea base de los activos de información bajo su gestión, incluyendo sus configuraciones iniciales y cambios realizados sobre dichos activos. Este inventario deberá ser entregado a la Dirección de Tecnologías de la Información conforme a los lineamientos definidos por la Entidad, garantizando su integridad, exactitud y oportunidad, con el fin de facilitar la gestión de configuraciones, la

trazabilidad de los cambios y el control de los activos tecnológicos. Este registro se podrá realizar de manera manual en la herramienta de Gestión ITSM y también , mediante el cargue masivo garantizando la estandarización de la información y su adecuada gestión documental, asegurando su integridad y oportunidad, con el fin de facilitar la gestión de configuraciones, la trazabilidad de los cambios y el control de los activos tecnológicos.

4.2.5 La implementación o modificación de configuraciones en los activos tecnológicos de la Entidad deberá realizarse obligatoriamente mediante la guía de gestión de cambios, el cual constituye un control esencial para garantizar que dichas modificaciones sean evaluadas previamente, cuenten con la autorización correspondiente, sean probadas cuando aplique y queden debidamente documentadas, asegurando la trazabilidad y reduciendo riesgos operativos y de seguridad de la información.

4.2.6 La Entidad deberá establecer mecanismos de validación y control sobre los cambios realizados a los elementos de configuración (CI), con el fin de garantizar la integridad, trazabilidad y consistencia de la información registrada en la CMDB.

4.2.7 Todos los cambios efectuados sobre los CI deberán estar asociados a una solicitud formal de cambio (RFC), la cual deberá ser gestionada mediante el formato institucional “F1.P4.GTI Formato Requerimiento de Cambios Informáticos – RFC”, debidamente evaluada, aprobada e implementada conforme al procedimiento institucional de gestión de cambios. Asimismo, cada modificación deberá ser registrada en la CMDB, incluyendo como mínimo: la fecha del cambio, descripción de la modificación, responsable, versión de la configuración y evidencia asociada. La Dirección de Tecnologías de la Información deberá asegurar que el historial de cambios de cada CI se mantenga actualizado y disponible para consulta, permitiendo el análisis de impacto, la gestión de incidentes y la toma de decisiones informadas. Se deberán realizar validaciones periódicas trimestrales para verificar la consistencia entre la configuración registrada en la CMDB y la configuración real de los activos tecnológicos, identificando desviaciones y gestionando las acciones correctivas correspondientes.

4.2.8 La Entidad deberá realizar revisiones periódicas mensuales de las configuraciones de los activos tecnológicos con el fin de verificar el cumplimiento de las configuraciones base establecidas, identificar desviaciones de seguridad y aplicar las acciones correctivas necesarias para mitigar riesgos asociados a configuraciones inadecuadas o no autorizadas.

4.2.9 Cuando se identifiquen desviaciones frente a las configuraciones base establecidas, estas deberán ser analizadas por las áreas responsables para determinar su impacto en la seguridad de la información y definir las acciones correctivas necesarias.

4.2.10 En aquellos casos en que la desviación no pueda ser corregida de manera inmediata o definitiva, se deberá documentar formalmente su justificación, análisis de riesgo, plan de tratamiento, responsable y tiempo estimado de resolución, así como contar con la aprobación correspondiente para su aceptación temporal, garantizando su registro y seguimiento hasta su cierre. Dichas acciones podrán gestionarse mediante el procedimiento de gestión de cambios o, cuando corresponda,

mediante “P25.GTI Procedimiento Gestión de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad”.

4.2.11 Las configuraciones base definidas para los activos tecnológicos deberán revisarse y actualizarse periódicamente con el fin de incorporar nuevas recomendaciones de seguridad, actualizaciones tecnológicas y lecciones aprendidas que permitan fortalecer la postura de seguridad de la Entidad.

4.2.12 La Dirección de Tecnologías de la Información podrá implementar herramientas automatizadas que permitan monitorear el cumplimiento de las configuraciones definidas, detectar desviaciones de seguridad y facilitar la gestión centralizada de configuraciones en los sistemas tecnológicos que soportan la operación institucional.

4.2.13 La Dirección de Tecnologías de la Información deberá garantizar que las configuraciones de los activos tecnológicos se gestionen de manera diferenciada según los ambientes tecnológicos de la Entidad, tales como desarrollo, pruebas, calidad y producción. En este sentido, las configuraciones aplicadas en ambientes productivos deberán ser previamente probadas y validadas en ambientes de prueba o desarrollo, con el fin de evitar afectaciones en la operación de los sistemas de información y garantizar la estabilidad y seguridad de los servicios tecnológicos institucionales.

4.2.14 La Entidad deberá implementar prácticas de fortalecimiento de seguridad o *hardening* en los sistemas operativos, aplicaciones, bases de datos, dispositivos de red y demás componentes tecnológicos que soportan la infraestructura tecnológica del ICBF. Estas prácticas deberán orientarse a reducir la superficie de ataque mediante la des habilitación de servicios innecesarios, eliminación de configuraciones inseguras, aplicación de controles de seguridad y cumplimiento de estándares técnicos definidos por la Dirección de Tecnologías de la Información. Asimismo, dichas prácticas deberán alinearse con marcos de referencia y buenas prácticas reconocidas, tales como ISO/IEC 27001:2022 en materia de controles de seguridad de la información, y con ITIL en lo relacionado con la gestión de la configuración y el control de cambios, asegurando su verificación periódica, trazabilidad y mejora continua.

4.2.15 La Dirección de Tecnologías de la Información deberá establecer lineamientos para la gestión de configuraciones en servicios tecnológicos desplegados en entornos de computación en la nube, garantizando que dichos servicios cumplan con los estándares de seguridad establecidos por la Entidad. Esto incluye la definición de configuraciones seguras para el acceso, almacenamiento de información, control de identidades, monitoreo de eventos de seguridad y protección de los datos institucionales alojados en dichas plataformas.

4.2.16 Las configuraciones críticas de los sistemas de información, dispositivos de seguridad, infraestructura de red y demás componentes tecnológicos que soportan los servicios institucionales deberán ser protegidas mediante controles de acceso adecuados y mecanismos de respaldo que permitan su recuperación en caso de fallas, incidentes de seguridad o errores de configuración. Asimismo, el acceso a dichas configuraciones deberá estar restringido únicamente al personal autorizado y debidamente documentado conforme a los procedimientos establecidos por la Entidad.

4.3 Etapas para la Gestión de Configuraciones Seguras

Con el fin de dar cumplimiento a los controles establecidos, el ICBF adoptará una metodología para la gestión de configuraciones seguras, mediante la cual se definen las actividades de identificación, control, mantenimiento y seguimiento de los activos tecnológicos. Está metodología se encuentra alineada con las buenas prácticas de ITIL, con los lineamientos de la norma ISO/IEC 27001:2022 y está estructurada en etapas que permiten su adecuada implementación, administración, verificación y mejora continua.

Etapa	Descripción	Registro/Evidencia	Responsable
5.1 Identificar los activos y CI	Identificación y clasificación de activos como CI y registro en CMDB	Inventario de activos CMDB	Líder de Servicio ICBF / Gestión de Configuración CMDB
5.2 Definir las configuraciones base	Definición y documentación de línea Base de seguridad	Documento Línea Base / hardening	Arquitectura TI/ Lideres de Servicios de ICBF / Profesional de Seguridad de la Información
5.3 Evaluar las configuraciones	Evaluación del estado de CI frente a línea Base	Checklists, reportes técnicos	Seguridad TI / Gestión de Configuración
5.4 Implementar las configuraciones seguras	Aplicación de hardening y controles	Actas, logs, bitácoras	Equipos de Infraestructura / Profesional Seguridad Perimetral y Profesional de Seguridad de la Información
5.5 Gestionar los cambios tecnológicos	Gestión de cambios mediante RFC	Reportes RFC aprobadas / CMDB	Gestor de Cambios / Líder de Servicio ICBF
5.6 Verificar y validar	Validaciones periódicas de cumplimiento	Informes y/o reportes	Lideres de Servicios de ICBF / Profesional de Seguridad de la Información
5.7 Gestionar las desviaciones	Registro, análisis y tratamiento de desviaciones	Registro de desviaciones	Profesional de Seguridad de la Información
5.8 Implementar las mejoras	Implementación de mejoras sobre configuraciones	Planes de mejora	Lideres de Servicios de ICBF / Profesional de Seguridad de la Información

5. DOCUMENTOS DE REFERENCIA:

- P4.GTI Procedimiento de Gestión de Cambios de Tecnologías de la Información
- P25.GTI Procedimiento Gestión de Eventos o Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad
- P8.GTI Procedimiento Gestión de Incidentes de Tecnología

6. RELACIÓN DE FORMATOS:

Código	Nombre del Formato
F1.P4.GTI	Formato Requerimiento de Cambios Informáticos-RFC
F1.P8.GTI	Formato Informe Incidente de Tecnología
F1.P25.GTI	Formato Informe de Eventos e Incidentes de Seguridad y Privacidad de la Información o Ciberseguridad

7. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
No Aplica	No Aplica	No Aplica

.