1. Propósito

Garantizar que **todos los cambios** que puedan afectar la confidencialidad, integridad y disponibilidad de la información de **la organización** se planifiquen, autoricen, implementen y verifiquen de forma controlada, reduciendo riesgos y evitando interrupciones no deseadas del servicio.

2. Alcance

Aplica a:

- **Procesos, activos y servicios** incluidos en el **MAN 001 Manual del SGSI** y dentro del **DOC 001 Alcance del SGSI**.
- Cambios en infraestructura física, lógica y de personal que tengan impacto en la seguridad de la información.
  No cubre actividades de mantenimiento de rutina que estén claramente documentadas como “cambios estándar” y pre-aprobados en esta misma política.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Controles 8.9, 8.32, 5.37, 7.13.
- **MAN 002 Manual de Procedimientos** – Sección Gestión de Cambios.
- **DOC 005 Control de Documentación**.
- **FOR 017 Registro de Cambios**.
- **PSC 002 Gestión de Incidentes** y **PSC 003 Plan de Continuidad del Negocio** (para cambios emergentes).

4. Definiciones

Término	Descripción
Cambio	Cualquier adición, modificación o eliminación de un activo, proceso o configuración que pueda afectar la seguridad de la información.
Solicitud de Cambio (RFC)	Registro formal que detalla el propósito, alcance, riesgos y recursos requeridos para un cambio.
Cambio estándar	Cambio recurrente, de bajo riesgo, documentado y pre-aprobado.
Cambio urgente	Cambio necesario para restaurar un servicio crítico o mitigar un riesgo inminente.

5. Principios de la Gestión de Cambios

1. **Aprobación formal previa**: Ningún cambio se ejecuta sin la autorización correspondiente.
2. **Evaluación integral de riesgos**: Se analiza impacto sobre la seguridad, continuidad y cumplimiento (ver **PRO 001** y **PRO 002**).
3. **Trazabilidad y registro**: Todos los cambios se documentan en **FOR 017** desde la solicitud hasta el cierre.
4. **Segregación de funciones**: Quien aprueba no implementa; quien implementa no verifica.
5. **Capacidad de reversión**: Cada plan de cambio incluye un procedimiento de rollback probado.

6. **Revisión posterior**: Se valida que los objetivos se cumplieron y se detectan lecciones aprendidas (ver **PSC 008 Mejora Continua**).

6. Roles y Responsabilidades

Rol	Responsabilidades clave
Comité de Seguridad de la Información	Definir la estrategia de cambios, aprobar cambios mayores y urgentes.
Propietario del Activo/Proceso	Iniciar la RFC, evaluar riesgos, validar resultados.
Responsable de TI	Planificar, coordinar y ejecutar el cambio o delegar su ejecución.
Usuarios afectados	Probar y confirmar la operatividad post-cambio.
Auditor Interno (PSC 004)	Verificar cumplimiento de esta política y registrar hallazgos.

7. Proceso de Gestión de Cambios

1. **Registro de RFC**
   - El solicitante completa **FOR 017** describiendo: motivo, alcance, riesgo, recursos, plan de reversión y ventana de mantenimiento.
2. **Clasificación**
   - **Estándar**, **Mayor** o **Urgente**, según matriz de impacto-criticidad (**DOC 018 Matriz de Riesgo**).
3. **Evaluación y Aprobación**
   - Cambios estándar → Responsable de TI.
   - Cambios mayores → Comité de Seguridad.
   - Cambios urgentes → aprobación ad-hoc por la Dirección y documentación retroactiva en 24 h.
4. **Planificación**
   - Definir tareas, responsables, pruebas, comunicación (ver **PRO 007 Comunicación**).
5. **Implementación**
   - Ejecución según plan; registro de evidencias y bitácoras.
6. **Verificación y Cierre**
   - Pruebas post-implementación, actualización de documentación (**DOC 013**, **DOC 021**, **PRO 014**).
   - Revisión post-cambio y firma de conformidad del propietario del proceso.

8. Documentación y Registros

- **FOR 017 Registro de Cambios** (obligatorio).
- Bitácoras de sistemas y controles (**FOR 024**, **FOR 032**).
- Actas de aprobación (**DOC 009**) y de socialización (**DOC 010**).
- Actualizaciones en la **Declaración de Aplicabilidad (SOA 001)** si los nuevos controles afectan la matriz.

9. Indicadores de Desempeño (KPI)

Indicador	Fórmula	Meta
% de cambios implementados sin incidentes	(Cambios exitosos / Cambios totales) × 100	≥ 95 %
Tiempo medio de evaluación de RFC	∑ horas evaluación / Nº RFC	≤ 48 h
Nº cambios urgentes	Conteo mensual	Tendencia descendente

10. Cumplimiento y Sanciones

El incumplimiento de esta política se considera falta grave y puede derivar en medidas disciplinarias según el **PRO 004 Planificación y Control Operacional** y el **Código de Conducta** interno. Además, la Dirección evaluará acciones correctivas y preventivas bajo **PSC 006**.

11. Revisión y Mejora

Esta política se revisa **anualmente** o tras incidentes significativos, mediante:

- **Auditoría interna (PSC 004)**.
- **Revisión por la Dirección (PSC 005)**.
- Actualización de requisitos legales aplicables (**DOC 006** y **DOC 007**).

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO