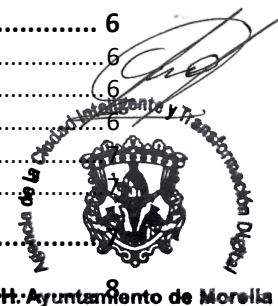
	<b>Sistema de Gestión de Seguridad de la Información</b>	Revisión: 0	Código:
		Página: 1 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	


## Tabla de contenido

<b>1. Propósito .....</b>	<b>1</b>
<b>2. Alcance.....</b>	<b>2</b>
2.1. Alcance de la Gestión de Capacidad .....	2
2.2. Alcance de la Gestión de Cambios .....	3
2.3. Tipología de Cambios Incluidos.....	3
2.4. Exclusiones.....	4
<b>3. Políticas de Gestión de la Capacidad y Gestión de Cambios .....</b>	<b>4</b>
3.1. Gestión Proactiva de la Capacidad (Control 8.6).....	4
3.2. Formalización de Proyectos Tecnológicos .....	4
3.3. Ciclo de Vida del Cambio (Control 8.32) .....	4
3.4. Pruebas y Entornos de Pre-Producción.....	5
3.5. Gestión de Cambios de Emergencia.....	5
3.6. Integridad de la Configuración (Control 8.29).....	5
3.7. Auditoría y Cierre de Cambios .....	5
<b>4. Procedimientos .....</b>	<b>6</b>
4.1. Procedimiento de Gestión de la Capacidad (Recurso Proactivo) .....	6
4.2. Inicio de Cambios y Proyectos.....	6
4.3. Evaluación y Aprobación del Cambio .....	6
4.4. Ejecución y Pruebas .....	6
4.5. Auditoría de Cierre y Lecciones Aprendidas .....	6
<b>5. Definiciones .....</b>	<b>6</b>
<b>6. Formatos.....</b>	<b>8</b>
<b>7. Relación Normativa (ISO 27001:2022) .....</b>	<b>9</b>



## 1. Propósito

El presente documento tiene como objetivo establecer el marco normativo y operativo para asegurar que los recursos tecnológicos del H. Ayuntamiento de Morelia sean suficientes para la demanda actual y futura (**Gestión de Capacidad**), y que cualquier modificación en la infraestructura o sistemas se realice de forma controlada, segura y documentada (**Gestión de Cambios**).

	Sistema de Gestión de Seguridad de la Información	Revisión: 0	Código:
		Página: 2 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

A través de esta política, se busca alcanzar los siguientes objetivos estratégicos:

- **Garantizar la Continuidad Operativa:** Evitar interrupciones en los servicios ciudadanos y administrativos causadas por cambios mal planificados, asegurando que cada modificación pase por un riguroso **Formato de Control de Cambios** antes de su implementación.
- **Planificación Proactiva del Crecimiento:** Establecer un monitoreo constante que permita, mediante el **Formato de Informe de Capacidad**, identificar cuellos de botella en servidores, almacenamiento y ancho de banda antes de que afecten el rendimiento institucional.
- **Mitigación de Riesgos Técnicos:** Minimizar el impacto de fallos mediante la evaluación previa de cada solicitud, obligando al uso del **Formato de Solicitud de Cambios** para analizar qué podría salir mal y cuál es el plan de retorno (rollback).
- **Estandarización de Proyectos Tecnológicos:** Asegurar que toda iniciativa de gran escala nazca bajo un orden administrativo mediante el **Acta de Proyecto**, vinculando los objetivos de seguridad de la información con las metas de desarrollo municipal desde el primer día.
- **Trazabilidad y Rendición de Cuentas:** Mantener un historial auditable que permita, a través del **Formato de Auditoría de Cambios**, verificar quién autorizó, ejecutó y validó cada movimiento en el ecosistema digital del Ayuntamiento, cumpliendo así con los estándares de la **ISO 27001:2022**.
- **Optimización de Recursos:** Maximizar la vida útil de los activos actuales y justificar las inversiones en nueva infraestructura basándose en datos reales de uso y proyecciones de demanda de la ciudadanía de Morelia.




## 2. Alcance

Esta política es de cumplimiento obligatorio para la Dirección de TI, jefaturas de área, desarrolladores y proveedores externos. Su aplicación se divide en dos grandes ejes:

### 2.1. Alcance de la Gestión de Capacidad

Aplica a todos los recursos críticos que soportan los servicios ciudadanos y administrativos del Ayuntamiento:

- **Recursos de Cómputo:** Procesamiento (CPU) y memoria RAM de servidores físicos y virtualizados.

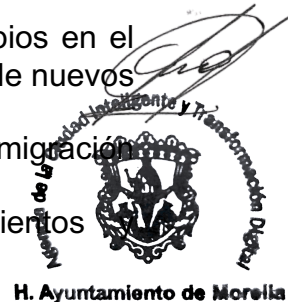
	<b>Sistema de Gestión de Seguridad de la Información</b>	Revisión: 0	Código:
		Página: 3 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

- **Almacenamiento de Datos:** Capacidad en discos duros, arreglos de almacenamiento (SAN/NAS) y cuotas de espacio en la nube para bases de datos y respaldos.
- **Comunicaciones y Redes:** Ancho de banda de los enlaces de internet (ISP), saturación de canales Wi-Fi y carga de los equipos de red (Switches/Firewalls).
- **Recursos de Infraestructura Física:** Capacidad de suministro eléctrico (UPS), plantas de emergencia y sistemas de enfriamiento (Aires acondicionados de precisión) en el SITE.
- **Recursos Humanos Técnicos:** Disponibilidad del personal calificado para atender la demanda de soporte y desarrollo en periodos de alta carga (ej. inicio de año fiscal).

## 2.2. Alcance de la Gestión de Cambios

Rige sobre cualquier modificación, actualización o eliminación que impacte la confidencialidad, integridad o disponibilidad de la información:


- **Hardware y Redes:** Sustitución de equipos, cambios en la topología de red, apertura de puertos en el Firewall o nuevas rutas de comunicación.
- **Software y Aplicaciones:** Actualizaciones de versiones (parches), cambios en el código fuente de aplicaciones internas (Portal de Trámites), y despliegue de nuevos módulos en producción.
- **Bases de Datos:** Cambios en esquemas, procedimientos almacenados, migración de tablas o modificaciones en permisos de acceso masivo.
- **Documentación del SGSI:** Modificaciones en políticas, procedimientos estándares que afecten la gobernanza de la seguridad de la información.



## 2.3. Tipología de Cambios Incluidos

Para efectos de este alcance, se gestionarán tres tipos de cambios:

1. **Cambios Estándar:** Modificaciones de bajo riesgo, rutinarias y pre-aprobadas (ej. creación de un usuario nuevo).
2. **Cambios Normales:** Aquellos que requieren evaluación, planeación y aprobación formal mediante el **Formato de Solicitud de Cambios**.
3. **Cambios de Emergencia:** Modificaciones urgentes para restaurar un servicio caído o mitigar un incidente de seguridad, los cuales se documentan retroactivamente.

	Sistema de Gestión de Seguridad de la Información	Revisión: 0	Código:
		Página: 4 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

## 2.4. Exclusiones

Quedan fuera de este alcance las actividades de mantenimiento preventivo menor que no alteren la configuración lógica de los sistemas, así como el reemplazo de consumibles de oficina (papelería, tintas) que no tengan componentes electrónicos de procesamiento.

## 3. Políticas de Gestión de la Capacidad y Gestión de Cambios

### 3.1. Gestión Proactiva de la Capacidad (Control 8.6)

La Dirección de TI debe asegurar que los recursos tecnológicos crezcan al ritmo de las necesidades del Ayuntamiento para evitar la degradación de los servicios ciudadanos.

- **Monitoreo Continuo:** Se deben establecer umbrales de alerta (ej. al alcanzar el 80% de ocupación en disco o CPU). El estado de estos recursos debe documentarse periódicamente en el **Formato de Informe de Capacidad**.
- **Alineación con el Presupuesto:** Los informes de capacidad servirán como sustento técnico para la planeación presupuestal anual, justificando la adquisición de infraestructura antes de que ocurra una saturación crítica.

### 3.2. Formalización de Proyectos Tecnológicos

Toda iniciativa que implique una transformación significativa en la infraestructura o desarrollo de nuevos sistemas para el Ayuntamiento (ej. un nuevo portal de Catastro) debe ser tratada como un proyecto formal.




- **Nacimiento del Proyecto:** Es obligatorio el llenado del **Acta de Proyecto**, donde se definan el alcance, los responsables, los recursos necesarios y los riesgos de seguridad asociados desde la fase de planeación.

### 3.3. Ciclo de Vida del Cambio (Control 8.32)

Ninguna modificación en los sistemas en producción (redes, servidores, bases de datos o software) debe realizarse de forma verbal o informal.

- **Solicitud Obligatoria:** Todo cambio debe ser iniciado mediante el **Formato de Solicitud de Cambios**, detallando la justificación técnica y el impacto esperado.

	Sistema de Gestión de Seguridad de la Información	Revisión: 0	Código:
		Página: 5 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

- **Evaluación de Riesgo y Rollback:** No se autorizará ningún cambio que no incluya un **Plan de Retorno (Rollback)** claro. Si el cambio falla, el sistema debe poder volver a su estado estable anterior en un tiempo predefinido.
- **Segregación de Funciones:** El personal que desarrolla o solicita el cambio no debe ser el mismo que lo aprueba en el entorno de producción, garantizando un control cruzado mediante el **Formato de Control de Cambios**.

### 3.4. Pruebas y Entornos de Pre-Producción

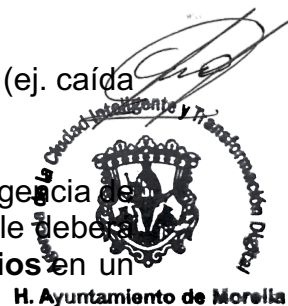
Queda estrictamente prohibido realizar pruebas directamente en los sistemas que dan servicio a la ciudadanía o a la administración.

- **Ambientes Espejo:** Todo cambio "Normal" debe ser probado primero en un entorno de desarrollo o calidad (QA) que replique las condiciones de producción sin comprometer datos reales (usando las políticas de enmascaramiento previamente definidas).

### 3.5. Gestión de Cambios de Emergencia

Se reconoce que existen situaciones críticas que requieren una acción inmediata (ej. caída total del sistema de pagos o un ataque activo).

- **Autorización Expedita:** El Director de TI podrá autorizar cambios de emergencia de forma verbal o por medios rápidos (WhatsApp/Correo), pero el responsable debe formalizar la documentación mediante el **Formato de Control de Cambios** en un plazo no mayor a 24 horas posteriores al evento.




### 3.6. Integridad de la Configuración (Control 8.29)

El Ayuntamiento debe mantener un registro exacto de "cómo se ve la red y los sistemas" hoy.

- **Línea Base:** Cualquier cambio aprobado debe derivar en la actualización inmediata de los inventarios y diagramas de red para evitar "configuraciones huérfanas" que representen un riesgo de seguridad.

### 3.7. Auditoría y Cierre de Cambios

El ciclo de cambio no termina con la implementación, sino con la verificación.

	Sistema de Gestión de Seguridad de la Información	Revisión: 0	Código:
		Página: 6 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

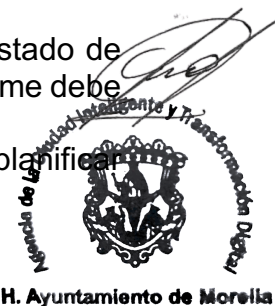
- **Verificación Post-Implementación:** Una vez ejecutado el cambio, se debe utilizar el **Formato de Auditoría de Cambios** para confirmar que el resultado fue el esperado, que no se abrieron vulnerabilidades nuevas y que la documentación fue actualizada. Los cambios que no pasen esta auditoría interna deberán ser revertidos o corregidos de inmediato.

## 4. Procedimientos

### 4.1. Procedimiento de Gestión de la Capacidad (Recurso Proactivo)

Este procedimiento asegura que los sistemas (como el portal de trámites o nómina) no se saturen en momentos críticos.

1. **Monitoreo y Recolección de Datos:** El administrador de infraestructura debe extraer métricas mensuales de los servidores y enlaces de red (CPU, RAM, Almacenamiento, Ancho de Banda).
2. **Análisis de Tendencias:** Se comparan las métricas con los periodos de alta demanda ciudadana (ej. pago de predial en enero).
3. **Generación del Formato de Informe de Capacidad:** Se documenta el estado de salud de los activos. Si un recurso supera el **75% de uso sostenido**, el informe debe incluir una recomendación de expansión.
4. **Toma de Decisiones:** El informe se entrega a la Dirección de TI para planificación de adquisiciones o ajustes técnicos antes de llegar a la saturación.




### 4.2. Inicio de Cambios y Proyectos

Dependiendo de la magnitud del movimiento, se eligen dos caminos:

- **Para Proyectos Mayores:** Si el cambio implica una nueva infraestructura o desarrollo desde cero, se debe formalizar el **Acta de Proyecto**, definiendo objetivos, presupuesto y responsables.
- **Para Cambios Operativos:** Si es una modificación a algo ya existente, el solicitante debe llenar el **Formato de Solicitud de Cambios**, justificando el porqué del movimiento y el impacto esperado.

### 4.3. Evaluación y Aprobación del Cambio

Ningún cambio "Normal" entra a producción sin pasar por este filtro:

	Sistema de Gestión de Seguridad de la Información	Revisión: 0	Código:
		Página: 7 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

1. **Análisis Técnico:** El equipo de seguridad y redes evalúa la solicitud. Se verifica que exista un **Plan de Rollback**(pasos para regresar al estado anterior si algo falla).
2. **Autorización Formal:** Se utiliza el **Formato de Control de Cambios** para recabar las firmas del responsable de área y el Director de TI.
3. **Programación de Ventana:** Se asigna un horario de baja actividad administrativa para ejecutar el cambio, minimizando la afectación a los servicios del Ayuntamiento.

#### 4.4. Ejecución y Pruebas

1. **Ambiente de Pruebas (Staging):** Antes de tocar el servidor real, se ejecuta el cambio en un entorno de pruebas.
2. **Restricción e accesos a producción:** todo acceso de producción debe estar limitado al personal autorizado o designado para despliegues.
3. **Implementación en Producción:** Se realiza la actividad siguiendo paso a paso lo descrito en el **Formato de Control de Cambios**.
4. **Plan de Retorno:** Si durante la implementación se detecta un error crítico que no se puede solucionar en la ventana de tiempo, se ejecuta el *Rollback* de inmediato para restablecer el servicio original.

#### 4.5. Auditoría de Cierre y Lecciones Aprendidas


El ciclo no termina hasta que se verifica el éxito:

1. **Validación Post-Cambio:** 24 horas después de la ejecución, se realiza una revisión de los sistemas afectados.
2. **Llenado del Formato de Auditoría de Cambios:** Un elemento de TI (distinto al que ejecutó el cambio) verifica que:
  - o La documentación esté completa.
  - o No existan vulnerabilidades nuevas.
  - o El sistema funcione según lo planeado.
3. **Actualización de Inventarios:** Si el cambio implicó nuevo hardware o cambio de IPs, se actualizan los diagramas de red y el inventario de activos.



### 5. Definiciones

- **Acta de Proyecto:** Documento formal que autoriza el inicio de una iniciativa tecnológica de gran escala, definiendo sus objetivos, alcances y riesgos de seguridad iniciales.

	Sistema de Gestión de Seguridad de la Información	Revisión: 0	Código:
		Página: 8 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	


- **Cambio de Emergencia:** Modificación que debe realizarse de inmediato para restaurar un servicio crítico caído o mitigar un incidente de seguridad activo; se documenta de forma retroactiva.
- **Control de Cambios:** Proceso de revisión y aprobación técnica que asegura que las modificaciones no introduzcan riesgos inaceptables en el entorno de producción.
- **Gestión de la Capacidad:** El proceso de asegurar que los recursos de TI (computo, red, almacenamiento) sean los adecuados para satisfacer las demandas actuales y futuras del Ayuntamiento.
- **Línea Base (Baseline):** El estado de configuración estable de un sistema antes de que se le aplique cualquier cambio.
- **Plan de Retorno (Rollback):** Procedimiento detallado para revertir un cambio fallido y regresar el sistema a su estado funcional anterior en el menor tiempo posible.
- **Staging / Pre-producción:** Entorno de pruebas que replica fielmente las condiciones del sistema real (producción), utilizado para validar cambios antes de su despliegue final.
- **Umbral de Capacidad:** Punto crítico (usualmente el 80% de uso) en el que se debe iniciar una acción correctiva o de expansión para evitar la degradación del servicio.

## 6. Formatos

Para que este proceso sea auditable, la Dirección de TI debe custodiar y mantener actualizados los siguientes cinco formatos:

1. **F-GC-01: Acta de Proyecto**
  - *Propósito:* Formalizar el nacimiento de nuevas infraestructuras o sistemas.
2. **F-GC-02: Formato de Solicitud de Cambios**
  - *Propósito:* Iniciar el trámite de modificación, justificando la necesidad y detallando el plan de *rollback*.
3. **F-GC-03: Formato de Control de Cambios**
  - *Propósito:* Registro maestro donde se firman las autorizaciones y se describe paso a paso la ejecución técnica.
4. **F-GC-04: Formato de Informe de Capacidad**
  - *Propósito:* Documento mensual/trimestral que reporta el estado de salud de los recursos (CPU, RAM, Disco) para planear compras.
5. **F-GC-05: Formato de Auditoría de Cambios**
  - *Propósito:* Validación final post-implementación para asegurar que el cambio fue exitoso y no dejó "cabos sueltos".



	<b>Sistema de Gestión de Seguridad de la Información</b>	Revisión: 0	Código:
		Página: 9 de 9	Fecha de Emisión:
		Procedimiento:	
<b>Políticas y Procedimientos para la Gestión de Capacidad y Gestión del Cambio</b>			
Elaborado por:		Autorizado por:	
Fecha de Actualización:		Fecha de Actualización:	

## 7. Relación Normativa (ISO 27001:2022)

Este documento es el pilar para el cumplimiento de los siguientes controles de la norma internacional:

Control	Título	Justificación del Cumplimiento
8.6	<b>Gestión de la capacidad</b>	Se cumple mediante el monitoreo de recursos y la generación del <b>Informe de Capacidad</b> .
8.32	<b>Gestión de cambios</b>	Se garantiza a través del flujo de <b>Solicitud, Control y Auditoría</b> de cada modificación técnica.
5.37	<b>Seguridad en la cadena de suministro</b>	El <b>Acta de Proyecto</b> asegura que los proveedores externos sigan los estándares del Ayuntamiento desde el inicio.
8.29	<b>Gestión de la configuración</b>	Asegura que tras cada cambio se actualicen los inventarios y diagramas de red institucionales.




H. Ayuntamiento de Morelia