CURADURÍA URBANA PRIMERA DE SINCELEJO

Sucre - Colombia

PLAN DE CONTINUIDAD DEL NEGOCIO

(BCP - Business Continuity Plan)

VIGENCIA 2025

Basado en ISO 22301:2019 - Sistema de Gestión de Continuidad del Negocio y el Modelo de Seguridad y Privacidad de la Información (MSPI)

www.curaduriaprimerasincelejo.com.co

Sincelejo, Enero 2025

CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN	ELABORADO POR
1.0	[DD/MM/2025]	Versión inicial del Plan de Continuidad del Negocio	[Responsable]

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Continuidad del Negocio (BCP) de la Curaduría Urbana Primera de Sincelejo establece las directrices, procedimientos y recursos necesarios para garantizar la continuidad de las operaciones críticas ante eventos disruptivos que puedan afectar la prestación del servicio público de expedición de licencias urbanísticas.

Este plan forma parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) y del Modelo de Seguridad y Privacidad de la Información (MSPI), cumpliendo con los lineamientos establecidos por el MinTIC y las mejores prácticas internacionales como la norma ISO 22301.

2. OBJETIVO

2.1 Objetivo General

Establecer un marco de actuación que permita a la Curaduría Urbana Primera de Sincelejo mantener la continuidad de sus procesos críticos y recuperar sus operaciones en el menor tiempo posible ante eventos que interrumpan el normal funcionamiento de la entidad.

2.2 Objetivos Específicos

1. Identificar los procesos críticos y sus tiempos máximos de interrupción tolerables.
2. Definir estrategias de continuidad para cada proceso crítico.
3. Establecer procedimientos de respuesta ante emergencias.
4. Minimizar el impacto de las interrupciones en los usuarios del servicio.
5. Proteger la información y los activos críticos de la entidad.

3. ALCANCE

El presente Plan de Continuidad del Negocio aplica a:

- Todos los procesos misionales relacionados con la expedición de licencias urbanísticas.
- Los sistemas de información: sitio web, sistema de gestión documental, correo electrónico.
- La infraestructura tecnológica: servidores, equipos, redes, telecomunicaciones.
- Las instalaciones físicas de la sede de la Curaduría.
- Todo el personal vinculado a la entidad.

4. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
ISO 22301:2019	Sistema de Gestión de Continuidad del Negocio - Requisitos
ISO/IEC 27001:2013	Sistema de Gestión de Seguridad de la Información - Control A.17 Continuidad
Decreto 1078/2015	Decreto Único Reglamentario del Sector TIC
Resolución 1519/2020	Lineamientos de estándares y publicación de información - MinTIC
CONPES 3854/2016	Política Nacional de Seguridad Digital
Ley 1523/2012	Política Nacional de Gestión del Riesgo de Desastres

5. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)

El Análisis de Impacto en el Negocio (Business Impact Analysis - BIA) identifica los procesos críticos de la Curaduría, evalúa el impacto de su interrupción y determina los tiempos de recuperación.

5.1 Procesos Críticos Identificados

PROCESO	RTO	RPO	MTPD	CRITICIDAD
Radicación de solicitudes de licencia	4 horas	0 horas	24 horas	**CRÍTICO**
Expedición de licencias urbanísticas	8 horas	24 horas	48 horas	**CRÍTICO**
Publicación de edictos y notificaciones	4 horas	0 horas	24 horas	**CRÍTICO**
Atención PQRSD	8 horas	4 horas	48 horas	**ALTO**
Gestión documental y archivo	24 horas	24 horas	72 horas	**ALTO**
Sitio web institucional	4 horas	1 hora	24 horas	**CRÍTICO**
Correo electrónico institucional	4 horas	0 horas	24 horas	**ALTO**
Gestión administrativa y contable	48 horas	24 horas	5 días	**MEDIO**

Definiciones:

- RTO (Recovery Time Objective): Tiempo máximo para restaurar el proceso.
- RPO (Recovery Point Objective): Máxima pérdida de datos tolerable.
- MTPD (Maximum Tolerable Period of Disruption): Tiempo máximo de interrupción tolerable.

6. ESCENARIOS DE INTERRUPCIÓN

Se han identificado los siguientes escenarios de interrupción que podrían afectar la continuidad de las operaciones:

ID	ESCENARIO	DESCRIPCIÓN	PROBABILIDAD	IMPACTO
E1	Falla del suministro eléctrico	Interrupción prolongada del servicio de energía eléctrica	Media	**ALTO**
E2	Falla de telecomunicaciones	Pérdida de conectividad a internet y telefonía	Media	**ALTO**
E3	Falla de servidores/equipos	Daño o falla en servidores, computadores o equipos críticos	Media	**CRÍTICO**
E4	Incidente de ciberseguridad	Ataque de ransomware, malware o intrusión	Media	**CRÍTICO**
E5	Desastre natural	Inundación, terremoto, incendio que afecte instalaciones	Baja	**CRÍTICO**
E6	Pandemia/emergencia sanitaria	Situación que impida la presencialidad del personal	Baja	**ALTO**
E7	Ausencia de personal clave	Falta simultánea de personal crítico por enfermedad u otra causa	Media	**MEDIO**
E8	Falla del proveedor de hosting	Caída del servicio de alojamiento del sitio web	Baja	**ALTO**

7. ESTRATEGIAS DE CONTINUIDAD

7.1 Estrategia de Respaldo de Información

COMPONENTE	ESTRATEGIA
Frecuencia de backup	Diario para información crítica (expedientes, licencias), semanal para información administrativa
Tipo de backup	Incremental diario, completo semanal
Ubicación primaria	Servidor NAS local con RAID
Ubicación secundaria	Servicio de nube (Google Drive, OneDrive o AWS S3)
Retención	30 días para backups diarios, 12 meses para mensuales
Pruebas de restauración	Trimestral

7.2 Estrategia de Sitio Alterno

Se establecen las siguientes opciones para operación en sitio alterno en caso de inaccesibilidad de las instalaciones principales:

6. Trabajo remoto: Personal con capacidad de conexión VPN a sistemas críticos desde sus hogares.
7. Espacio de coworking: Acuerdo con espacio de oficinas compartidas en Sincelejo para operación temporal.
8. Oficina alterna: Coordinación con otra curaduría o entidad pública para uso temporal de instalaciones.

7.3 Estrategia de Comunicaciones Alternas

SERVICIO	ALTERNATIVA
Internet principal	Enlace de datos móviles (4G/5G) como backup
Telefonía fija	Desvío a teléfonos móviles institucionales
Correo electrónico	Acceso vía webmail desde cualquier dispositivo
Sitio web	Hosting en la nube con alta disponibilidad y CDN

8. ESTRUCTURA DE RESPUESTA A EMERGENCIAS

8.1 Comité de Crisis

ROL	RESPONSABILIDADES	CARGO TITULAR
Director del Comité	Declarar emergencia, aprobar activación del BCP, tomar decisiones estratégicas	Curador Urbano
Coordinador de Continuidad	Coordinar actividades de recuperación, comunicar avances	Responsable de Seguridad
Líder Técnico	Recuperación de sistemas, infraestructura TI	Webmaster / Soporte TI
Líder Operativo	Continuidad de procesos misionales	Coordinador Área Técnica
Líder de Comunicaciones	Comunicación interna y externa, atención a medios	Área Jurídica

8.2 Niveles de Activación

NIVEL	DESCRIPCIÓN	CRITERIO DE ACTIVACIÓN	ACCIONES
NIVEL 1	Incidente Menor	Interrupción < 2 horas, afecta un proceso	Respuesta del área afectada
NIVEL 2	Incidente Moderado	Interrupción 2-8 horas, afecta varios procesos	Activación parcial del BCP
NIVEL 3	Incidente Mayor	Interrupción > 8 horas, afecta procesos críticos	Activación completa del BCP
NIVEL 4	Desastre	Pérdida de instalaciones o daño catastrófico	BCP + Plan de Recuperación de Desastres

9. PROCEDIMIENTOS DE RECUPERACIÓN

9.1 Procedimiento General de Activación

9. Detección: Identificar el incidente y evaluar su impacto inicial.
10. Notificación: Informar al Coordinador de Continuidad inmediatamente.
11. Evaluación: Determinar el nivel de activación requerido.
12. Activación: Convocar al Comité de Crisis si es Nivel 2 o superior.
13. Ejecución: Implementar los procedimientos de recuperación correspondientes.
14. Monitoreo: Seguimiento continuo hasta la normalización.
15. Cierre: Documentar lecciones aprendidas y actualizar el plan.

9.2 Procedimientos Específicos por Escenario

9.2.1 Falla del Suministro Eléctrico (E1)

16. Verificar funcionamiento de UPS y tiempo de autonomía disponible.
17. Guardar trabajo en curso y cerrar aplicaciones no críticas.
18. Contactar a la empresa de energía para conocer tiempo estimado de restablecimiento.
19. Si supera 1 hora: activar generador eléctrico (si está disponible) o suspender atención presencial.
20. Informar a usuarios sobre la situación.

9.2.2 Incidente de Ciberseguridad (E4)

21. Aislar inmediatamente los equipos afectados de la red.
22. No apagar los equipos (preservar evidencia).
23. Notificar al Coordinador de Continuidad y Líder Técnico.
24. Evaluar el alcance del incidente.
25. Activar procedimiento de gestión de incidentes de seguridad.
26. Reportar a COLCERT si es un incidente grave.
27. Restaurar desde backups limpios una vez contenida la amenaza.

9.2.3 Falla del Sitio Web (E8)

28. Verificar si la falla es del proveedor de hosting o del sitio.
29. Contactar soporte técnico del proveedor de hosting.
30. Si supera 2 horas: activar sitio de contingencia en hosting alterno.
31. Publicar aviso en redes sociales sobre la situación.
32. Habilitar canales alternativos de atención (teléfono, correo).

10. PLAN DE COMUNICACIÓN DE CRISIS

10.1 Principios de Comunicación

- Oportunidad: Comunicar a tiempo, evitando la especulación.
- Transparencia: Información veraz sobre lo ocurrido y las acciones tomadas.
- Consistencia: Mensaje unificado desde una sola fuente autorizada.
- Empatía: Reconocer el impacto en los usuarios y partes interesadas.

10.2 Matriz de Comunicación

AUDIENCIA	CANAL	RESPONSABLE	FRECUENCIA
Personal interno	WhatsApp, correo, reunión	Coordinador de Continuidad	Inmediata y cada 2 horas
Usuarios/ciudadanos	Sitio web, redes sociales	Líder de Comunicaciones	Inicio, actualizaciones, cierre
Alcaldía/Planeación	Oficio, llamada telefónica	Curador Urbano	Según gravedad
Organismos de control	Oficio formal	Curador Urbano	Si afecta servicio > 24h
Proveedores críticos	Teléfono, correo	Área Administrativa	Inmediata si son parte de la solución

11. PRUEBAS Y MANTENIMIENTO DEL PLAN

11.1 Programa de Pruebas

TIPO DE PRUEBA	DESCRIPCIÓN	FRECUENCIA	RESPONSABLE
Revisión documental	Verificar vigencia de contactos, procedimientos y recursos	Trimestral	Coord. Continuidad
Prueba de backup	Restauración de archivos desde backups	Trimestral	Líder Técnico
Ejercicio de escritorio	Simulación teórica de escenarios con el Comité	Semestral	Coord. Continuidad
Simulacro parcial	Prueba práctica de un procedimiento específico	Anual	Comité de Crisis
Simulacro completo	Prueba integral del BCP con todos los componentes	Cada 2 años	Comité de Crisis

11.2 Mantenimiento y Actualización

El Plan de Continuidad del Negocio debe actualizarse en los siguientes casos:

- Revisión anual programada.
- Cambios significativos en la estructura organizacional.
- Implementación de nuevos sistemas de información críticos.
- Después de la activación real del plan.
- Resultado de pruebas que identifiquen mejoras necesarias.
- Cambios en la normatividad aplicable.

12. ANEXOS - INFORMACIÓN DE CONTACTO DE EMERGENCIA

12.1 Contactos Internos del Comité de Crisis

NOMBRE / CARGO	TELÉFONO FIJO	CELULAR	EXT.
[Curador Urbano]	[XXX XXX XXXX]	[3XX XXX XXXX]	[XXX]
[Responsable Seguridad]	[XXX XXX XXXX]	[3XX XXX XXXX]	[XXX]
[Líder Técnico / Webmaster]	[XXX XXX XXXX]	[3XX XXX XXXX]	[XXX]
[Coordinador Área Técnica]	[XXX XXX XXXX]	[3XX XXX XXXX]	[XXX]

12.2 Contactos Externos de Emergencia

ENTIDAD / SERVICIO	TELÉFONO	HORARIO
Línea de emergencias	123	24/7
Bomberos Sincelejo	119 / (5) 282 XXXX	24/7
Policía Nacional	112	24/7
Defensa Civil	144	24/7
Empresa de Energía (Afinia)	01 8000 XXX XXX	24/7
Proveedor Internet	[Número del proveedor]	Lun-Sáb
Proveedor Hosting Web	[Número del proveedor]	24/7
COLCERT (Incidentes cibernéticos)	contacto@colcert.gov.co	Lun-Vie

---

URL de Publicación: https://curaduriaprimerasincelejo.com.co/transparencia/seguridad-digital/bcp