CUMPLIMIENTO INTEGRAL

Plan de Continuidad del Negocio (BCP) - COLBITS S.A.S.

Marzo de 2026

TABLA DE CONTENIDO

1. Generalidades y Alcance del Plan 3

2. Análisis de Impacto al Negocio (BIA) 3

3. Identificación y Evaluación de Riesgos de Interrupción 4

4. Estrategias de Continuidad y Recuperación Tecnológica (DRP) 4

5. Especificaciones Técnicas de Recuperación 5

6. Plan de Respuesta ante Incidentes 6

7. Mantenimiento, Pruebas y Mejora Continua 6

8. Declaración Institucional de Compromiso 6

1. Generalidades y Alcance del Plan

El presente Plan de Continuidad del Negocio (BCP) de COLBITS S.A.S. constituye el marco estratégico y operativo diseñado para garantizar la resiliencia de la organización ante eventos disruptivos. Su propósito es salvaguardar los procesos críticos, asegurar la disponibilidad de los servicios de telemetría e IoT, y proteger la integridad de la información técnica y operativa.

El alcance de este plan es integral y abarca la totalidad del ciclo de valor definido en nuestra política institucional, cubriendo las siguientes fases y procesos:

- **Diseño Electrónico y Hardware:** Desarrollo de circuitos impresos (PCB) y arquitectura de dispositivos.
- **Abastecimiento y Fabricación Tercerizada:** Gestión de la cadena de suministro internacional para la manufactura de PCB.
- **Ensamble Local:** Integración de componentes y control de calidad en instalaciones propias.
- **Desarrollo de Firmware:** Creación, versionamiento y mantenimiento del código embebido.
- **Desarrollo de Software y Analítica:** Operación de plataformas de telemetría y procesamiento de datos en la nube.
- **Gestión de Fin de Vida (RAEE):** Protocolos de recolección, reutilización y disposición final de residuos electrónicos.
- **Infraestructura Crítica:** Servidores, servicios cloud, repositorios de código y conectividad.

2. Análisis de Impacto al Negocio (BIA)

COLBITS S.A.S. ha evaluado el impacto de interrupciones prolongadas considerando variables operativas, financieras, reputacionales y contractuales. A continuación, se detallan los tiempos objetivos para la recuperación de la operación normal:

Proceso Crítico	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)
Plataforma de telemetría	4–8 horas	< 1 hora
Firmware (repositorios)	24 horas	< 4 horas
Ensamble de dispositivos	48–72 horas	No aplica*
Soporte técnico a clientes	8–24 horas	< 2 horas

***Nota técnica**: Aunque no existe un riesgo de pérdida de datos digitales en el ensamble físico, el RPO "No aplica" está respaldado por una estrategia de mitigación de pérdida de stock mediante un **Inventario Mínimo de Seguridad**.*

3. Identificación y Evaluación de Riesgos de Interrupción

Riesgos Tecnológicos

Fallas críticas en la infraestructura de servicios cloud (Google Cloud), pérdida de integridad en bases de datos de telemetría y vulnerabilidades ante ciberataques que comprometan la disponibilidad del servicio.

Riesgos Operativos

Indisponibilidad de personal técnico especializado en desarrollo de firmware o fallas en los equipos de diagnóstico y ensamble local que detengan la cadena de producción.

Riesgos de Cadena de Suministro

Dependencia de fabricantes internacionales de PCB, posibles retrasos en logística de importación o escasez global de componentes críticos que afecten la modularidad funcional de los dispositivos.

Riesgos Externos

Desastres naturales, fallas eléctricas prolongadas y factores de **Orden Público**. Este último es crítico para operaciones de campo, donde la continuidad del servicio depende de las condiciones de seguridad que permitan el acceso físico para mantenimiento y reinstalación de sensores.

4. Estrategias de Continuidad y Recuperación Tecnológica (DRP)

Infraestructura y Software

Se garantiza la alta disponibilidad mediante el uso de arquitecturas escalables en la nube con redundancia geográfica. Se ejecutan backups automáticos y periódicos de las bases de datos de telemetría para cumplir con el RPO menor a 1 hora.

Firmware

La resiliencia del desarrollo se fundamenta en repositorios distribuidos (Git) con espejos externos. Se prioriza el uso de **Actualizaciones Remotas (OTA - Over-the-Air)** como herramienta de recuperación rápida, permitiendo corregir fallos críticos de software embebido o realizar ajustes funcionales sin necesidad de intervención física en campo, extendiendo así la vida útil del hardware.

Cadena de Suministro y Seguridad (LA/FT)

Para mitigar fallas de proveedores, se mantiene un stock crítico de componentes. En caso de requerir **proveedores alternos de emergencia**, la selección debe superar estrictos protocolos de **Debida Diligencia (KYC/KYS)** según nuestro Programa Integral de Cumplimiento. Esto asegura que la urgencia de la crisis no comprometa la integridad de la empresa al contratar con entidades sancionadas o vinculadas a actividades ilícitas.

Talento Humano

Se implementa la capacitación cruzada y la documentación técnica rigurosa para evitar que la operación dependa de un único individuo, facilitando la transferencia de conocimiento en situaciones de emergencia.

5. Especificaciones Técnicas de Recuperación

Para asegurar la continuidad del servicio en el dominio institucional, es posible la migración de los servicios actualmente alojados en la nube de COLBITS hacia una infraestructura propia del cliente. Los requerimientos técnicos mínimos para la **Máquina Virtual** son:

- **Almacenamiento:** 100 GB.
- **RAM:** 8 GB.
- **Cores:** 4 núcleos.
- **Sistema Operativo:** Distribución Linux server 64 bits, Ubuntu última versión LTS.

Nota de Soporte: Si la migración no se completa por indisponibilidad del servidor, COLBITS garantiza la continuidad y el soporte bajo la figura de garantía técnica durante el periodo estipulado.

6. Plan de Respuesta ante Incidentes

La ruta crítica de actuación ante una interrupción se divide en seis fases:

1. **Detección:** Identificación de la falla mediante monitoreo continuo.
2. **Evaluación:** Clasificación del impacto (BIA).
3. **Activación:** Inicio formal del BCP y notificación a interesados.
4. **Ejecución:** Aplicación de las estrategias de recuperación (DRP).
5. **Restablecimiento:** Retorno a la operación en condiciones normales.
6. **Lecciones Aprendidas:** Análisis post-mortem y actualización del plan.

Responsabilidades:

- **Coordinador de Continuidad:** Toma de decisiones estratégicas y liderazgo de la respuesta.
- **Equipo Técnico:** Ejecución de la **restauración de repositorios Git**, **migración de bases de datos de telemetría** y reconfiguración de servicios cloud.
- **Equipo Operativo:** Gestión de logística de emergencia, soporte técnico en sitio y restablecimiento de procesos de ensamble.

7. Mantenimiento, Pruebas y Mejora Continua

COLBITS S.A.S. aplica el ciclo **PHVA (Planear-Hacer-Verificar-Actuar)** para mantener la vigencia del plan. Se realizarán simulacros anuales de recuperación de backups y pruebas de redundancia de servicios cloud para validar la efectividad de las estrategias frente a los tiempos establecidos.

El desempeño del BCP se medirá mediante los siguientes indicadores clave (KPIs):

- **Tiempo real de recuperación vs. RTO.**
- **Disponibilidad del sistema (% Uptime).**
- **Número de incidentes críticos registrados.**

Este plan se articula con la Política de Economía Circular, fomentando la reparación y el mantenimiento preventivo para evitar la generación prematura de RAEE, y con el Programa de Prevención de LA/FT para asegurar la transparencia en las contrataciones de emergencia.

8. Declaración Institucional de Compromiso

COLBITS S.A.S. garantiza la continuidad de sus operaciones mediante la implementación de estrategias tecnológicas, operativas y organizacionales que permiten mantener la disponibilidad de sus servicios, proteger la información y responder de manera oportuna ante eventos disruptivos, asegurando el cumplimiento de sus compromisos contractuales ante sus clientes y entidades contratantes.