PLAN DE CONTINUIDIDAD DEL NEGOCIO – BCP
UNIDAD DE SALUD DE IBAGUE
AREA DE SSITEMAS

IBAGUÉ, CIUDAD QUE VIBRA
"NUESTROS SERVICIOS AL ALCANCE DE TODOS"
Carrera 8 No 24-01Barrio el Carmen
Teléfonos 2655534 - 2739595
Email: gerencia@usiese.gov.co

1. INTRODUCCIÓN

El presente Plan de Continuidad del Negocio (BCP) tiene como objetivo establecer las estrategias, herramientas, lineamientos y procedimientos que garantizan la operación continua de los servicios críticos de la Unidad de Salud de Ibagué, especialmente ante interrupciones no planificadas, fallas tecnológicas, eventos de seguridad de la información o desastres naturales.

La entidad dispone de infraestructura tecnológica, un sistema de información institucional robusto, mecanismos redundantes de comunicaciones, un esquema de replicación en tiempo real y elementos de seguridad que permiten minimizar el impacto de una interrupción y asegurar la prestación de los servicios asistenciales y administrativos a la comunidad.

2. Alcance

El BCP aplica a:

- Infraestructura tecnológica alojada en la **Sede San Francisco** (datacenter principal).
- Comunicaciones institucionales y radioenlaces entre sedes.
- Sistema de información **Dinámica Gerencial** y servicios asociados.
- Active Directory institucional, intranet y página web.
- Usuarios internos que acceden a servicios tecnológicos.
- Proveedores que soportan servicios críticos.

3. Marco Normativo

El BCP se fundamenta en:

Normatividad nacional

- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1377 de 2013 – Reglamentación de la Ley 1581.
- Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública.
- Ley 527 de 1999 – Validez jurídica de mensajes de datos.
- Ley 1266 de 2008 – Habeas Data Financiero.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC.
- Circular Externa 20211700000015-5 de la Supersalud – Lineamientos de TI, seguridad y continuidad.

Estándares internacionales

- ISO 22301 – Sistemas de Gestión de la Continuidad del Negocio.
- ISO 27001 – Gestión de Seguridad de la Información.
- ISO 27002 – Controles de Seguridad.
- ISO 31000 – Gestión del Riesgo.

Documentos internos

- Plan de Seguridad y Privacidad de la Información.
- Plan de Tratamiento de Riesgos.
- Inventario de Activos de TI (Drive institucional).
- Política de Backup y Replicación.
- Arquitectura de Red y Comunicaciones.

4. Infraestructura Tecnológica Institucional

4.1 Datacenter Principal – Sede San Francisco

- Hospeda los servidores del sistema **Dinámica Gerencial**.
- Administra bases de datos, servicios de autenticación y aplicativos internos.
- Cuenta con redundancia eléctrica y medidas de seguridad física.

4.2 Datacenter Alterno

- Actualmente opera un **site alterno externo** con backup y **replicación en tiempo real**, lo cual garantiza continuidad ante caída del datacenter principal.

- El sistema Dinámica Gerencial replica su información en modo near real-time, reduciendo la pérdida de datos a mínimos prácticamente nulos.

4.3 Datacenter Futuro – Unidad Intermedia Sur (PETI)

El PETI institucional contempla:

Construcción e implementación de un Datacenter en el sector sur de la ciudad, destinado a operar como sitio alterno geográficamente redundante de la Sede San Francisco.

Su propósito es garantizar:

- Muy alta disponibilidad
- Redundancia geográfica
- Conmutación automática entre sitios
- Mejora continua del modelo de continuidad

4.4 Comunicaciones y Red

- La Unidad de Salud opera una **red propia de radioenlaces**, los cuales convergen en el nodo central ubicado en **Cerro La Martinica**.

- Las sedes intermedias disponen de:

    - Enlace principal
    - Enlace secundario de contingencia

- Esto asegura comunicación operativa aun cuando el enlace principal falle.

4.5 Seguridad Perimetral

La entidad cuenta con:

- **Firewall institucional**, que provee:
    - Filtrado avanzado de tráfico
    - Prevención de accesos no autorizados
    - Segmentación de red
    - Inspección de paquetes
    - Políticas de seguridad centralizadas

4.6 Active Directory

- Gestión centralizada de identidades y accesos.
- Perfiles seguros según roles.

4.7 Intranet Institucional

- Medio de comunicación interna para procedimientos, circulares, manuales, documentos de control y gestión administrativa.
- El servicio es respaldado en la plataforma institucional y está cubierto por los planes de restauración.

4.8 Página Web Institucional

- Canal oficial de información al ciudadano, difusión de servicios, noticias y trámites.
- Su funcionamiento depende de infraestructura respaldada y protegida.

5. Análisis de Impacto al Negocio (BIA)

El BIA identifica procesos críticos, impactos y tiempos de recuperación.

5.1 Procesos Críticos

1. Gestión asistencial
2. Facturación – Cartera
3. Gestión administrativa
4. Recursos humanos
5. Comunicaciones entre sedes
6. Autenticación de usuarios (AD)

5.2 Objetivos de Recuperación

Servicio / Proceso	RTO	RPO
Dinámica Gerencial	2 horas	0–5 min (replicación)
Comunicaciones entre sedes	Continuidad inmediata (HA)	No aplica
Active Directory	2 horas	30 min
Intranet	4 horas	24 horas
Página web	4 horas	24 horas
Servidores generales	4 horas	4–12 horas

6. Proveedores Críticos

- Proveedor del Datacenter alterno
- Proveedor del Firewall
- Proveedor de Dinámica Gerencial
- Proveedor de radioenlaces y torres
- Proveedor del portal web, si aplica
- Proveedor de energía y telecomunicaciones

7. Riesgos Asociados a Continuidad

Riesgo	Impacto	Medidas de Mitigación
Caída del datacenter San Francisco	Alto	Replicación al datacenter alterno
Falla de radioenlaces	Medio/Alto	Enlace secundario en todas las sedes
Ataques cibernéticos	Alto	Firewall + controles de seguridad
Pérdida de energía	Alto	UPS/plantas + datacenter alterno
Corrupción de datos	Alto	Backups + replicación continua
Falla en Active Directory	Alto	Restauración desde backup
Fallo en servidor web	Medio	Backup + hosting alterno

8. Estrategias de Continuidad

- Redundancia de comunicaciones (enlace principal y secundario).
- Replicación continua del sistema Dinámica Gerencial.
- Backups automáticos diarios, semanales y mensuales.
- Recuperación en datacenter alterno.
- Firewall activo y monitoreo preventivo.
- Control de accesos centralizado con AD.
- Migración futura al datacenter sur para redundancia geográfica.

9. Plan de Respuesta y Activación

1. Identificación del incidente por el área TIC o Seguridad de la Información.
2. Clasificación del impacto (leve, moderado, crítico).
3. Notificación a la dirección administrativa.
4. Ejecutar el procedimiento correspondiente:
    - Restauración desde backups
    - Activación del datacenter alterno
    - Verificación de enlaces secundarios
5. Recuperación de servicios.
6. Validación con líderes operativos.
7. Documentación del incidente.

10. Pruebas y Validación

La Unidad realiza pruebas periódicas para asegurar eficacia del BCP:

- Pruebas de restauración de backups.
- Simulaciones de caída del enlace principal.
- Validación del enlace secundario (alta disponibilidad).
- Revisión del firewall ante incidentes simulados.
- Prueba de activación del datacenter alterno.

11. Mantenimiento y Mejora Continua

El BCP es revisado:

- Semestralmente.
- Cuando cambie la infraestructura o procesos críticos.
- Tras incidentes que generen lecciones aprendidas.

La implementación del datacenter sur fortalecerá la resiliencia institucional.

12. Conclusión

La Unidad de Salud de Ibagué cuenta con una infraestructura tecnológica robusta, un datacenter principal con respaldo en un site alterno, comunicaciones redundantes, políticas definidas de seguridad de la información y una arquitectura con visión de muy alta disponibilidad contemplada en el PETI.

Estas capacidades permiten asegurar la continuidad de los servicios esenciales y la protección de la información institucional, garantizando la prestación de servicios con el menor impacto posible ante eventos de interrupción.

SAUL BETANCOURT CARO
Profesional Universitario
USI-ESE