PLAN DE CONTINUIDAD DE NEGOCIO Y RECUPERACION DE DESASTRES

Elaborado por:
Oficina de Soporte y Desarrollo Tecnológico

Contenido

1. INTRODUCCIÓN

En un entorno donde los riesgos operativos y tecnológicos son cada vez más complejos, desde ciberataques hasta desastres naturales, la Institución Universitaria Mayor de Cartagena asume el reto de garantizar la continuidad de sus servicios educativos y la protección de su información crítica. Este informe establece el marco estratégico para implementar un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación de Desastres (DRP), alineados con estándares internacionales y la normativa colombiana. Su propósito es asegurar que, ante cualquier interrupción, la universidad mantenga su capacidad misional: formar profesionales, generar conocimiento y servir a la sociedad.

2. OBJETIVOS

2.1 Objetivo General

Implementar un sistema integrado de BCP y DRP para garantizar la resiliencia institucional.

2.2 Objetivo Específicos

- Identificar procesos críticos académicos y administrativos mediante un Análisis de Impacto al Negocio (BIA).
- Diseñar protocolos de continuidad y recuperación técnicamente viables.
- Establecer controles de seguridad (ISO 27001) para proteger datos sensibles.
- Capacitar a la comunidad universitaria en respuestas ante emergencias.

3. CONTEXTO INSTITUCIONAL

La Institución Universitaria Mayor de Cartagena es una entidad de educación superior comprometida con la formación académica, la investigación y la proyección social. Como organización clave en el desarrollo regional, gestiona procesos críticos que incluyen actividades académicas (clases presenciales y virtuales, laboratorios, investigación), servicios administrativos (matrículas, registros, pagos) y el manejo de información sensible (datos personales, historiales estudiantiles, producción científica).

La universidad opera en un entorno donde convergen riesgos tecnológicos (ciberataques, fallas en sistemas), operativos (interrupciones eléctricas, desastres naturales) y normativos (cumplimiento de protección de datos y regulaciones educativas). La ausencia de un plan estructurado de continuidad y recuperación ante desastres representa un riesgo institucional, ya que una interrupción prolongada podría afectar su capacidad misional, la experiencia estudiantil y su reputación.

4. MARCO NORMATIVO

Norma/Regulación	Aplicación en el BCP/DRP	Relevancia para la Universidad
NTC-ISO 22301:2019	Estándar para gestión de continuidad del negocio.	Define requisitos para proteger procesos misionales.
Guía MINTIC No. 5	Metodología para gestión de activos.	Define niveles de clasificación (Confidencialidad, Integridad, Disponibilidad).
ISO/IEC 27001:2022	Controles de seguridad de la información.	Protege datos académicos y personales (ej: historiales).
Ley 1581 de 2012 (Protección de Datos)	Tratamiento de información sensible.	Evita sanciones por pérdida o filtración de datos.
Decreto 1072 de 2015 (Sector Público)	Regulación de TI y gestión documental.	Cumplimiento como entidad pública.
Ley 1523 de 2012 (Gestión del Riesgo)	Enfoque preventivo ante desastres.	Alinea el BCP con políticas nacionales.

5. INVENTARIO DE ACTIVOS CRÍTICOS

Este inventario sistematiza los recursos tecnológicos y de información que requieren protección prioritaria, conforme a los estándares ISO 27001 (A.8.1) y Guía MINTIC No. 5. La clasificación por criticidad (C/I/D) y la asignación de responsables permitirá focalizar esfuerzos en activos con mayor impacto operacional, así también, garantizar cumplimiento legal (Ley 1581 de 2012 para datos personales) y desde luego, alimentar el BCP/DRP con métricas precisas (RTO/RPO).

5.1 Aplicaciones Críticas

ID	Nombre	Tipo	Clasificación (C/I/D)	RTO/RPO	Propietario	Ubicación
APP-01	Genesis	Académico	IPC / A / 1	4h / 24h	Dirección TIC	Sede Principal
APP-02	WAS	Administrativo	IPC / A / 1	4h / 24h	Dirección TIC	Sede Principal
APP-03	GitLab	Desarrollo	IPR / A / 1	2h / 1h	Dirección TIC	Sede Principal
APP-04	OJS	Investigación	IPC / M / 2	12h / 24h	Dirección de Investigación	Sede Principal
APP-05	Control de Acceso	Seguridad	IPR / A / 1	1h / 1h	Dirección TIC	Sede Principal

La Institución Universidad Mayor de Cartagena ha identificado un conjunto de aplicaciones críticas que respaldan los procesos académicos, administrativos, de desarrollo, investigación y seguridad institucional. Estas aplicaciones fueron clasificadas conforme a su nivel de confidencialidad, integridad y disponibilidad, así como por los tiempos de recuperación esperados ante incidentes (RTO/RPO).

Entre estas, Genesis y WAS representan plataformas fundamentales para la gestión académica y administrativa, respectivamente, ambas con una criticidad alta y una ventana de recuperación de 4 horas (RTO) y respaldo de 24 horas (RPO). Esto refleja la importancia de su disponibilidad continua para la operación diaria.

GitLab, herramienta de desarrollo institucional, y el sistema de Control de Acceso, presentan los niveles más altos de criticidad, con RTO de 2 horas y 1 hora, respectivamente, y RPO de 1 hora, lo que evidencia su necesidad de alta disponibilidad y respaldo frecuente para garantizar la integridad de los procesos de desarrollo y de seguridad física y lógica de la institución.

Finalmente, OJS, utilizado en los procesos de investigación, mantiene una clasificación de criticidad moderada, con un RTO de 12 horas y un RPO de 24 horas, acorde con la naturaleza no transaccional de sus funciones.

Este análisis permite enfocar las estrategias de continuidad operacional y gestión del riesgo, priorizando la protección y disponibilidad de las aplicaciones con mayor impacto institucional.

5.2 Infraestructura Tecnológica

ID	Equipo	Marca/Modelo	Criticidad	Ubicación	Propietario	Función
INF-01	Firewall	Fortigate 200E	Alta (1)	Sede Principal	Redes	Seguridad perimetral
INF-02	Switch Core	Mikrotik CRS354	Alta (1)	Data Center	Redes	Conectividad central
INF-03	Wireless AP	Ubiquiti UAPACPRO	Media (2)	Distribuidos en toda el área	Redes	Acceso WiFi
INF-04	Servidor Hypervisor	Windows Server 2019	Alta (1)	Data Center	TI	Virtualización (VMware)

La infraestructura tecnológica de la institución ha sido evaluada en términos de criticidad y funcionalidad. Se identificaron componentes clave como el Firewall Fortigate 200E, el Switch Core Mikrotik CRS354 y el Servidor Hypervisor con Windows Server 2019, todos clasificados con criticidad alta (nivel 1). Estos activos son esenciales para la seguridad perimetral, la conectividad de red y la virtualización de servicios, respectivamente, lo cual los posiciona como elementos fundamentales para la continuidad de los servicios TIC.

Asimismo, los puntos de acceso inalámbrico (AP) Ubiquiti UAP-AC-PRO se clasifican con una criticidad media (nivel 2), dado su rol de apoyo a la conectividad, pero sin comprometer directamente la operatividad crítica. Esta categorización

permite focalizar los esfuerzos de monitoreo, mantenimiento preventivo y respuesta ante incidentes en los activos de mayor impacto.

5.3 Datos Sensibles

ID	Tipo de Dato	Clasificación (C/I/D)	Almacenamiento	Custodio	Retención
DT-01	Historiales académicos	IPR / A / 1	BD Genesis	Registro Académico	10 años
DT-02	Investigaciones	IPC / M / 2	Repositorio OJS	Dirección Investigación	Permanente
DT-03	Credenciales de acceso	IPR / A / 1	Directorio Activo	Seguridad TI	2 años
DT-04	Historiales Administrativo	IPR / A / 1	WAS	Registro Administrativo	10 años

Se han identificado y clasificado los principales conjuntos de datos sensibles que administra Umayor, teniendo en cuenta su nivel de confidencialidad, integridad y disponibilidad. Entre los más críticos se encuentran los historiales académicos, historiales administrativos y las credenciales de acceso, todos con clasificación IPR / A / 1, lo que implica un alto nivel de protección requerido.

Estos datos están almacenados en sistemas como Genesis, WAS y el Directorio Activo, bajo custodia de unidades responsables como Registro Académico, Registro Administrativo y Seguridad TI. La gestión de estos datos incluye políticas

de retención adecuadas, que van desde 2 años (para credenciales) hasta 10 años (para historiales académicos y administrativos), y conservación permanente para los datos de investigación.

Este inventario refuerza la necesidad de aplicar controles técnicos y administrativos para prevenir accesos no autorizados, pérdidas de integridad o interrupciones en su disponibilidad.

5.4 Responsables (Propietarios/Custodios)

Rol	Nombre/Cargo	Activos Asociados (IDs)	Contacto
Propietario TIC	Director de TI	APP-01, APP02, APP-03, APP-04, APP-05, INF-04	d.sistemas@umayor.edu.co
Custodio Redes	Coordinador de Infraestructura	INF-01, INF-02, INF-03, INF-04	redesyseguridad@umayor.edu.co
Custodio Datos	Responsable de BD	DT-01, DT-02, DT-03, DT-04	d.sistemas@umayor.edu.co

Se ha definido una matriz clara de responsabilidades sobre los activos críticos identificados. El Director de TI figura como propietario principal de las aplicaciones críticas, mientras que el Coordinador de Infraestructura actúa como custodio de los activos de red y hardware, y el Responsable de Bases de Datos se encarga de los datos sensibles institucionales.

Esta asignación de roles garantiza la adecuada gestión, mantenimiento y protección de los activos, permitiendo responder de forma rápida y efectiva ante incidentes, auditorías o requerimientos de mejora continua. Además, se cuenta con canales de

contacto institucionales que aseguran la trazabilidad y comunicación eficiente en caso de eventos que comprometan la disponibilidad, seguridad o confidencialidad de los activos.

6. ANÁLISIS DE RIESGOS Y PLAN DE CONTINUIDAD (BCP)

6.1 Identificación de Riesgos

Los principales riesgos identificados en la Universidad Mayor incluyen:

Falla de infraestructura crítica, como el switch core, firewall o servidor hypervisor.

- **Interrupciones en aplicaciones críticas**, como Genesis, GitLab y Control de Acceso.
- **Pérdida de datos sensibles**, especialmente credenciales y bases de datos académicas.
- **Amenazas cibernéticas**, como ransomware o accesos no autorizados.
- **Eventos físicos**, como incendios, inundaciones o fallas eléctricas en el data center.

Cada riesgo se ha vinculado a los activos identificados, considerando su clasificación (C/I/D), ubicación y dependencia operativa.

6.2 Evaluación de Impacto al Negocio (BIA)

Se establecieron **niveles de impacto** basados en RTO y RPO.

- Sistemas como **Control de Acceso y GitLab** tienen impacto **crítico**, dado que su interrupción afecta la seguridad física y el desarrollo institucional.
- **Genesis y WAS** tienen impacto **alto**, al estar ligados a los procesos administrativos y académicos diarios.
- **OJS** presenta un impacto **moderado**, relevante para investigación, pero menos dependiente de operación inmediata.

Este análisis permite priorizar la atención y respuesta ante fallas, asignando recursos según el nivel de criticidad operativa.

6.3 Estrategias de Continuidad

Las estrategias definidas incluyen:

Redundancia de servicios en servidores virtualizados.

- **Respaldos diarios incrementales** y copias físicas fuera de línea.
- **Planes de recuperación documentados y pruebas de restauración periódicas**, como se indica en el procedimiento PR-ST-004.
- **Asignación clara de roles** para recuperación, operación y comunicación.
- **Monitoreo activo de infraestructura crítica** (Firewall, Switch, Hypervisor).

Estas acciones buscan minimizar el tiempo de inactividad y proteger los datos institucionales.

6.4 Comunicación de Crisis

Se ha previsto una estructura de comunicación para situaciones críticas:

- Activación inmediata del **Comité TIC**.
- Comunicación oficial a través de los canales institucionales.
- Informes periódicos al comité directivo y usuarios afectados.
- Coordinación entre el Director de TI, Coordinador de Redes y Responsables de Área para tomar decisiones informadas y mantener la operatividad esencial.

7. PLAN DE RECUPERACIÓN DE DESASTRES (DRP)

7.1 Procedimientos de Recuperación

Ante un evento crítico, se siguen pasos definidos:

- Evaluación del daño y notificación a responsables.
- Activación del protocolo de restauración desde backups.
- Reinstalación de servicios virtuales sobre el hypervisor.

  Verificación de integridad de los sistemas restaurados. Estos procedimientos se realizan conforme al plan documentado por el área TIC PR-ST-004..

7.2 Backup y Restauración de Datos

Según el procedimiento **PR-ST-004**, los respaldos se realizan de forma:

-
- **Automática e incremental diaria**, tanto para usuarios como para sistemas críticos.
- **Duplicados en nube (Google Drive)** y medios físicos desconectados de la red.
- **Pruebas periódicas de restauración** para garantizar efectividad.
- Custodia a cargo del **Director de Soporte** y **Coordinador de Redes**.

Esto garantiza que los datos puedan recuperarse eficazmente en caso de pérdida o corrupción.

7.3 Controles de Seguridad (ISO 27001)

Se aplican controles alineados con ISO 27001:

- **A.8.2.1 y A.12.3.1**: Copias de seguridad periódicas.
- **A.9.2.2**: Control de acceso a información crítica. • **A.11.2.4**: Protección física de equipos y medios.
- **A.17.1.2**: Planificación de continuidad de servicios.
  Esto fortalece la seguridad de la información institucional en todo su ciclo de vida.

7.4 Pruebas y Simulacros

Se programan **pruebas de restauración periódicas**, tanto en estaciones de trabajo como en servidores críticos, con registros documentados. Además, se planifican **simulacros anuales de recuperación de desastres**, involucrando a las áreas responsables y usuarios clave, para verificar la eficacia del plan DRP y ajustar procedimientos según los resultados.

8. CONCLUSIÓN

La gestión de riesgos tecnológicos, la planificación de la continuidad operativa (BCP) y el establecimiento de un plan de recuperación ante desastres (DRP) constituyen pilares fundamentales para garantizar la resiliencia institucional de la Universidad Mayor frente a incidentes que puedan comprometer la disponibilidad, integridad o confidencialidad de la información.

El análisis realizado permitió identificar los activos críticos —incluyendo aplicaciones, infraestructura tecnológica y datos sensibles — y asignar responsabilidades claras para su gestión, protección y recuperación. Asimismo, se establecieron estrategias e específicas de continuidad y recuperación, respaldadas por procedimientos documentados como el PR-ST-004, que refuerzan la capacidad de respuesta ante eventualidades tecnológicas o eventos disruptivos.

La implementación de respaldos automáticos, controles de seguridad alineados con ISO 27001, y pruebas periódicas de restauración, junto con una estructura de comunicación efectiva en situaciones de crisis, aseguran no solo la recuperación

técnica, sino también la coordinación institucional necesaria para mantener los servicios esenciales en funcionamiento.

Este esfuerzo integral fortalece la cultura de prevención, prepara a la institución para enfrentar posibles escenarios adversos y reafirma el compromiso con la protección de su infraestructura, servicios y comunidad universitaria.