Plan de Continuidad del Negocio (PCN) TI

TECNOLOGÍA INFORMACIÓN

Fecha de elaboración: Cali, enero, 2025

1. Introducción

INTENALCO es una Institución Educativa de carácter oficial nacional enfocada en la excelencia académica y la gestión de riesgos. El Departamento de Tecnología de la Información (TI) desempeña un papel fundamental en la continuidad operativa de la institución.

El presente Plan de Continuidad del Negocio (PCN) establece las estrategias y procedimientos necesarios para garantizar la disponibilidad de los servicios críticos de TI y mitigar el impacto de interrupciones en las operaciones institucionales.

2. Objetivo

Garantizar la continuidad de los servicios críticos de Tecnología de la Información en INTENALCO, minimizando el impacto de posibles interrupciones mediante estrategias proactivas y reactivas. Esto incluye:

- Implementar medidas preventivas para la protección y continuidad de los sistemas críticos.
- Establecer tiempos de recuperación adecuados para minimizar las interrupciones.
- Proteger la integridad, confidencialidad y disponibilidad de la información crítica.
- Asegurar la capacitación del personal clave para la gestión de incidentes y la implementación del PCN.

3. Alcance

El presente plan abarca todas las áreas relacionadas con la gestión de Tecnología de la Información en INTENALCO, asegurando la continuidad de los procesos académicos, administrativos y de seguridad. Su aplicación se extiende a:

- **Sistemas Académicos:** Incluye plataformas de registro académico (SIGA, Q10), sistemas de permanencia estudiantil (ADVISER), KOHA (biblioteca) y plataformas de aprendizaje en línea (Moodle), garantizando la operatividad de los servicios educativos.
- **Sistemas Administrativos y Financieros:** Abarca el sistema financiero CG-UNO, SIGA (para gestión de registros administrativos), Sevenet, ControlRoll y plataformas

externas reguladas por MEN, MH, etc. asegurando la correcta gestión de recursos y procesos administrativos.

- **Infraestructura Tecnológica:** Se enfoca en la operatividad de servidores, respaldos de datos, el directorio activo e internet, fundamentales para la continuidad de las operaciones institucionales.

- **Sistemas de Comunicación:** Incluye correo electrónico, telefonía IP y plataformas de mensajería interna, garantizando la conectividad y coordinación de los equipos de trabajo.

- **Sistemas de Seguridad:** Comprende los sistemas de videovigilancia, firewalls y medidas de seguridad perimetral, asegurando la protección de la infraestructura y la información institucional.

- **Sistemas de Almacenamiento y Respaldo de Datos:** Para garantizar la integridad y disponibilidad de los datos críticos en todo momento

- **Usuarios Clave y Procedimientos de Recuperación:** Asegura la participación de todos los actores responsables de la ejecución del PCN y su correcta Implementación en caso de incidentes o fallos.

Este plan se aplicará a todas las dependencias y usuarios que interactúan con los servicios de TI, garantizando que cada área esté preparada para actuar en caso de contingencia.

4. Análisis de Impacto al Negocio (BIA)

4.1 Identificación de funciones y procesos críticos

Se han identificado los sistemas y servicios esenciales cuya interrupción podría afectar significativamente las operaciones de INTENALCO:

Función/Proceso	Importancia
Registro Académico (SIGA)	Crítico
Gestión Financiera (CG-UNO)	Crítico
Plataformas de Aprendizaje (Moodle)	Importante
Biblioteca Digital (KOHA)	Moderado
Directorio Activo y Servidores	Crítico
Comunicaciones Institucionales (Correo, IP)	Crítico
Seguridad Informática (Firewalls, Backups)	Crítico

4.2 Evaluación de impactos operacionales

Se han determinado los impactos en tres niveles: alto, medio y bajo, considerando la pérdida de productividad, afectación en la reputación y costos de recuperación.

Sistema	Impacto Operacional
SIGA, Q10	Alto (afecta inscripciones, calificaciones)
ADVISER	Medio (afecta seguimientos e informes)
CG-UNO	Alto (afecta pagos y contabilidad)
MOODLE	Bajo (uso reducido, alternativas clases presenciales)
KOHA	Bajo (uso reducido, alternativas físicas)
FIRMAS DIGITALES	Bajo (uso reducido, alternativas físicas)
COPIAS DE SEGURIDAD	Medio (afecta copias automáticas a sistemas de información e copias a funcionarios)
SEVENET	Medio (afecta correspondencia, seguimientos, pqrs e informes)
Comunicaciones	Alto (interrupción total en correo, página web y telefonía)

4.3 Definición de tiempos de recuperación

Para cada sistema crítico, se han definido los siguientes parámetros:

Sistema	RTO (Tiempo Máximo de Recuperación)	RPO (Punto de Recuperación)
SIGA, Q10	1-4 horas	15 min - 1 hora
ADVISER	24 horas	6-12 horas
CG-UNO	4-12 horas	2-4 horas
Moodle	24 horas	6-12 horas
KOHA	24 horas	6-12 horas
FIRMAS DIGITALES	24 horas	6-12 horas
COPIAS DE RESPALDO	24 horas	6-12 horas
SEVENET	24 horas	6-12 horas
Comunicaciones	1-4 horas	15 min - 1 hora

5. Gestión del Riego

5.1. Identificación de Riesgos

Los principales riesgos identificados incluyen:

- Desastres naturales: Inundaciones, incendios y terremotos.
- Ataques cibernéticos: Malware, ransomware, phishing y accesos no autorizados.
- Fallos de infraestructura: Pérdidas de energía, fallos de hardware y software desactualizado.
- Errores humanos: Configuraciones incorrectas, uso inadecuado de sistemas y falta de capacitación.
- Riesgos de proveedores: Dependencia de servicios externos sin redundancia**.**

5.2. Identificación de amenazas

- Brechas de seguridad: Esto incluye ataques de hackers, malware, ransomware y otras amenazas cibernéticas que podrían comprometer la seguridad de los sistemas y datos de TIC.
- Interrupción del Suministro Eléctrico: Cortes de energía inesperados que pueden dejar los sistemas de TIC inoperables.
- Fallas de Hardware: El mal funcionamiento de servidores, equipos de red o software crítico podría causar interrupciones.
- Fallas de Software: Posibilidad de fallas Software renovación de licenciamientos y renovación de contratos con los softwares críticos (mantenimientos y soportes).
- Deterioro de Rendimiento: La disminución del desempeño o funcionamiento de sistemas, procesos o actividades relacionadas con la tecnología, como consecuencia de diversos riesgos. Estos riesgos pueden surgir en el contexto de la implementación, operación y mantenimiento de tecnologías de la información y comunicación, infraestructuras tecnológicas, software, hardware, y otros componentes tecnológicos.
- Incumplimiento normativo: Riesgo de no cumplir con las leyes y regulaciones relacionadas con la privacidad y seguridad de la información o por cambios en las regulaciones gubernamentales que podrían afectar los requisitos de seguridad de la información y la operación de TIC.
- Perdida de datos: Posibilidad de pérdida de información crítica debido a fallos en los sistemas o acciones no autorizadas.
- Amenazas Físicas: Intrusión, robo o vandalismo en las instalaciones de TIC.

- Riesgos de Terceros: Problemas con proveedores de servicios de TIC o subcontratistas que puedan afectar la entrega de servicios.

5.3. Evaluación de vulnerabilidades

.

- Infraestructura de TI

  Vulnerabilidades asociadas con el hardware, los sistemas operativos y los recursos tecnológicos físicos:

  - Obsolescencia del hardware: Equipos antiguos (servidores, estaciones de trabajo, UPS) con alto riesgo de fallos.
  - Falta de redundancia: Ausencia de sistemas de respaldo para servidores o componentes esenciales.
  - Interrupciones eléctricas: Dependencia de una infraestructura eléctrica no estabilizada o sin respaldo suficiente (UPS, generadores).
  - Mantenimiento insuficiente: Falta de mantenimiento preventivo, que aumenta el riesgo de fallos en servidores, switches, o routers.
  - Ubicación insegura del hardware: Equipos críticos ubicados en zonas sin control de temperatura, humedad o acceso restringido.

- Redes

  - Fallas en la configuración de red: Errores en las VLAN, falta de segmentación, o políticas de firewall mal configuradas.
  - Dependencia de un solo proveedor de internet: Ausencia de enlaces redundantes para garantizar alta disponibilidad.
  - Ciberataques: Amenazas como ataques DDoS, intrusiones no autorizadas, y explotación de vulnerabilidades en protocolos (como SMB o FTP).
  - Puntos de acceso Wi-Fi inseguros: Uso de contraseñas débiles o falta de autenticación robusta, lo que facilita accesos no autorizados.
  - Equipos obsoletos: Uso de switches, routers o firewalls que no soportan las actualizaciones necesarias para protegerse contra amenazas modernas.

- Software

  - Sistemas desactualizados: Uso de software sin soporte técnico o sin actualizaciones de seguridad regulares.
  - Dependencia de aplicaciones críticas sin alternativas: Por ejemplo, sistemas de gestión académica o bibliotecas digitales sin respaldo funcional.
  - Fallas de integración: Problemas en la interoperabilidad entre sistemas, como bases de datos, plataformas de aprendizaje y herramientas administrativas.
  - Falta de controles de acceso: Cuentas compartidas o contraseñas débiles que facilitan accesos no autorizados.
  - Vulnerabilidades en aplicaciones web: Riesgo de inyección SQL, ataques XSS o CSRF en sistemas como portales académicos o plataformas de

inscripción.

- Datos Sensibles

  - Falta de cifrado: Datos en tránsito o en reposo no cifrados, exponiendo información confidencial.
  - Falta de respaldos frecuentes: Riesgo de pérdida de información crítica (calificaciones, matrículas, registros financieros) ante desastres o ataques.
  - Acceso no autorizado: Personal o estudiantes accediendo a información sensible sin permisos adecuados.
  - Cumplimiento regulatorio insuficiente: No adherirse a normativas de protección de datos personales como la Ley 1581 en Colombia o equivalentes internacionales (GDPR, FERPA).
  - Amenazas internas: Empleados, docentes o estudiantes que comprometen los datos de forma accidental o malintencionada.

5.4. Evaluación y Mitigación de Riesgos

Cada riesgo es evaluado según su probabilidad de ocurrencia e impacto, estableciendo estrategias de mitigación.

Riesgo	Probabilidad	Impacto	Estrategia de Mitigación
Ataque cibernético	Alta	Alto	Implementación de firewalls, antivirus y autenticación multifactor
Fallo de hardware	Media	Alto	Redundancia en servidores y mantenimiento preventivo
Pérdida de energía	Media	Alto	Uso de UPS y generadores eléctricos
Errores humanos	Alta	Medio	Capacitación continua del personal
Fallo en la red	Media	Alto	Redes redundantes y monitoreo proactivo

5.5. Plan de Respuesta ante Incidentes

- Identificación del incidente: Monitoreo constante y alertas tempranas.
- Notificación y activación del equipo de respuesta: Comunicación inmediata con los responsables.
- Análisis y contención: Diagnóstico del problema y aplicación de medidas temporales.
- Recuperación: Restauración del sistema afectado utilizando respaldos y procedimientos definidos.

- Evaluación post-incidente: Análisis de causa raíz y aplicación de mejoras preventivas.

6. Planificación y estrategias de Recuperación

6.1 Fases de Plan de Continuidad

1. **Prevención:** Implementación de medidas de seguridad, monitoreo proactivo y mantenimiento preventivo de infraestructura crítica.
2. **Preparación:** Desarrollo de procedimientos y políticas documentados, pruebas de simulación y capacitación del personal.
3. **Respuesta:** Acciones inmediatas tras un incidente para mitigar el impacto y restablecer servicios esenciales.
4. **Recuperación:** Restauración completa de sistemas y evaluación de daños.
5. **Mejora Continua:** Revisión de incidentes, implementación de mejoras y optimización del plan.

6.2 Roles y Responsabilidades

Funcionario	Responsabilidad
Vicerrector Admón. Y Financiera	Supervisión general del PCN, toma de decisiones estratégicas.
Profesional Universitario TI	Implementación y monitoreo del plan.
Ingenieros de Soporte	Ejecución de protocolos de contingencia y recuperación.
Personal Clave	Reporte de incidentes y cumplimiento de procedimientos de respuesta.

6.3 Estrategias de Recuperación

- **Espera en caliente:** Infraestructura redundante lista para operar en caso de falla.
- **Espera tibia:** Sistemas preparados con respaldo de datos reciente, pero no activos.
- **Espera fría:** Recuperación desde copias de seguridad externas con tiempos de restauración más largos.

6.4 Procedimientos de Recuperación

1. **Activación del Plan:**
    - Notificación a los equipos de respuesta.
    - Evaluación del impacto del incidente.
    - Definición de acciones prioritarias.

2. **Recuperación de Sistemas Críticos:**
    - Restauración de servidores y bases de datos.
    - Verificación de integridad de la información.
    - Pruebas de funcionamiento.
3. **Normalización de Operaciones:**
    - Reinicio de servicios en producción.
    - Validación con usuarios finales.
    - Documentación del incidente y lecciones aprendidas.

6.5 Requerimiento de Recursos

TIPO	SERVICIO QUE SOPORTA	CPU/MODEL	PROCESADOR	RAM	DISCO	PROVEEDOR	SISTEMA OPERATIVO
SERVIDOR	Domain Controler	12 CPUs x Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz	Intel(R) Xeon(R	64GB	12 TB	DELL	Proxmox
SERVIDOR	Firmas DIgitales	12 CPUs x Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz	Intel(R) Xeon(R	64GB	12 TB	Lenovo	WINDOWS 10
SERVIDOR	GLPI	12 CPUs x Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz	Intel(R) Xeon(R	32GB	6 TB	Lenovo	Linux
SERVIDOR	Sevenet	CPU E3-1220 V2 @ 3.1 Ghz 3100 Mhz 4 Procesadores	Intel(R) Xeon(R	4GB	1TB	HP	Server 2012 R
SERVIDOR	OCS INVENTORY	12 CPUs x Intel(R) Xeon(R) CPU E5-2603 v3 @ 1.60GHz	Intel(R) Xeon(R	32GB	6 TB	Lenovo	Linux
SERVIDOR	COPIAS DE RESPALDO	Intel Celeron 2.8 Ghz	SR 550	12	9 TB	Dell	Linux
SERVIDOR	CGUNO	CPU E3-1220 V2 @ 3.1 Ghz 3100 Mhz 4 Procesadores	Intel(R) Xeon(R	4GB	1TB	HP	Server 2022
SERVIDOR	KOHA	CPU E3-1220 V2 @ 3.1 Ghz 3100 Mhz 4 Procesadores	Intel(R) Xeon(R	4GB	1TB	HP	Linux

TIPO	SERVICIO QUE SOPORTA	CPU/MODEL	PROCESADOR	RAM	DISCO	PROVEEDOR	SISTEMA OPERATIVO
SERVIDOR	TELEFONIA IP		ProDesk	4	500 TB	HP	Linux

7. Implementación

7.1. Estrategias de Implementación

7.1.1. Diagnóstico y Evaluación Inicial:

- Identificación de necesidades y vulnerabilidades.
- Priorización de áreas críticas.

7.1.2. Desarrollo de Infraestructura y Recursos:

- Adquisición y configuración de servidores de respaldo.
- Implementación de políticas de seguridad y redundancia.

7.1.3. Capacitación y Simulacros:

- Entrenamiento del personal en procedimientos de contingencia.
- Realización de pruebas periódicas de recuperación.

7.1.4. Monitoreo y Mantenimiento:

- Evaluación continua del estado del PCN.
- Aplicación de mejoras y actualización de estrategias según nuevas amenazas.

7.2. Plan de acción

Actividad	Descripción	Responsable	Registros
Evaluar el daño del servidor y la cantidad de Información perdida. (en caso de daño en bases de datos)	Luego de reconocer el daño y evaluar si se ha perdido información se procede a activar el plan de contingencia, restaurando la última copia disponible en un Servidor temporal.	Profesional Universitario TI	Acta
Requisitos de Software y Hardware	Elementos que se deben custodiar en la caja fuerte ubicada en el edificio operativo de la compañía: 1. Disco Duro externo o servidor de copias – contiene la copia diaria. 2. Restaurar Copia 3. Comprar o Alquilar Servidor de contingencia. (Características mínimas: Memoria 64Gb, Disco 6	Profesional Universitario TI	Check list de Requisitos para el Plan de Contingencia.

Actividad	Descripción	Responsable	Registros
	teras, procesador Intel Xeon de 3.0 GHz) 4. Comprar o Alquilar equipos de comunicación (router, switch, AP, etc.) 5. Buscar apoyo en proveedores si es el caso.		
Servidor de Contingencia	Si se requiere alquilar o comprar servidor, se tiene el proveedor Pymes Online, teléfono 3045770507 que nos alquila un servidor de contingencia en 2 horas. O si no es necesario alquilar en Informática hay un equipo disponible para montar la copia y que funcione de manera temporal.	Vicerrector Admon. Fianancierо Profesional Universitario TI	N/A
Firewall	Pasos de Restauración: Paso 1: Implementación de Contingencia Objetivo: Garantizar la continuidad del servicio de Internet mientras se realiza la restauración del firewall. Acciones: Redirigir la conexión WAN al router MikroTik, asegurándose de que la configuración previa esté cargada y operativa. Verificar que los dispositivos internos puedan acceder a la red y tengan salida a Internet. Monitorear la estabilidad de la conexión y realizar ajustes en caso de ser necesario. Paso 2: Solicitud de Soporte y Reemplazo del Firewall Objetivo: Gestionar la garantía y reposición del equipo con el proveedor. Acciones: Contactar al soporte técnico de Sophos a través del número 601 5087605. Proporcionar los detalles del incidente, incluyendo logs y diagnóstico del fallo. Iniciar el proceso de RMA (Return Merchandise Authorization) para la reposición del equipo. Coordinar la recepción del nuevo dispositivo y confirmar tiempos de entrega. Paso 3: Reemplazo y Restauración del Firewall Objetivo: Instalar el nuevo equipo y restablecer la configuración de seguridad. Acciones: Desconectar el firewall defectuoso y conectar el nuevo dispositivo. Restaurar la configuración utilizando la copia de seguridad almacenada en el servidor de backup o en un disco externo.	Profesional Universitario TI	

Actividad	Descripción	Responsable	Registros
	Validar que todas las reglas de firewall, VPNs, accesos y políticas de seguridad estén correctamente aplicadas. Realizar pruebas de conectividad, tráfico y seguridad para verificar el correcto funcionamiento. Documentar la restauración y actualizar el registro de incidentes y procedimientos.		
Server Dominio 172.16.3.253:8006 Servidor Físico DELL	La imagen de este servidor está creada con el software que provee en promox Se encuentra ubicada en el servidor de copia \\IN1SRVBACKUP y en disco duro externo. Para la restauración se debe alquilar un servidor, tener el disco duro externo donde se encuentra los archivos de backup. Para las imágenes de las máquinas virtuales se encuentran en un disco duro externo Pasos para la restauración: 1. Tener los requisitos de software y hardware. 2. Arrancar el sistema en el nuevo servidor 3. Seleccionar idioma. 4. Servidor de Red – 172.16.3.253:8006 5. Instalar virtualizador de máquinas PROMOX. 6. Restaurar backup. 7. Reiniciar. Instalar Drivers si es necesario.	Profesional Universitario TI. Equipo de Apoyo	N/A
Servidor Backup	La imagen de este servidor esta creada manualmente Se encuentra ubicada en el servidor de copia \\IN1SRVBACKUP y en un disco externo Para la restauración se debe alquilar un servidor para virtualizar, tener el disco duro externo donde se encuentra la imagen Pasos para la restauración: 1. Tener los requisitos de software y hardware. 2. Arrancar el sistema en el nuevo servidor 3. Instalar virtualizador de máquinas PROMOX.	Profesional Universitario TI. Equipo de Apoyo	N/A

Actividad	Descripción	Responsable	Registros
	4. Restaurar imagen de la copia de seguridad 5. Validar funcionalidad del servidor, archivos copiardos 6. Verificar errores y restaurar 7. Reiniciar. Instalar Drivers si es necesario.		
Revisiones	Cada 6 meses se debe realizar revisiones de los servidores, con el fin de verificar la eficacia de las copias de seguridad.	Profesional Universitario TI. Equipo de Apoyo	N/A
Después de la Contingencia.	1. Recuperar la información perdida, con los documentos físicos, ejemplo: pedidos, facturas, recibos de caja, comprobantes, etc. 2. Reparar o adquirir un servidor para colocar en funcionamiento, el que se monta en un plan de contingencia es temporal. 3. Documentar el paso a paso de la contingencia. 4. Documentar lecciones aprendidas. 5. Documentar planes de acción con las causas del daño del servidor.	Profesional Universitario TI. Equipo de Apoyo	Planes de acción
OBSERVACIONES: - Cada 6 meses se realizarán revisiones del Servidor principal de la compañía. - Cada 6 meses se realizarán mantenimientos de UPS y Servidores. - En caso de necesitar proveedor externo que nos apoye en la labor: John Arango - Alquiler de equipos de cómputo necesarios con respuesta inmediata empresa AP			

8. Evaluación de Desempeño

8.1 Auditorías internas

- Revisiones periódicas para asegurar la efectividad del plan

8.2 Indicadores Clave de Desempeño (KPI)

- Métricas para medir tiempos de respuesta, impacto reducido, etc

8.3 Análisis Post

- Evaluación de la eficacia de la respuesta y mejora de procesos

9. Mejora Continua

9.1 Revisión del plan

- Actualización de acuerdo con nuevas amenazas o cambios operativos.

9.2 Resultados de auditorías

- Implementación de acciones correctivas basadas en hallazgos

9.3 Comunicación y reporte

- Informes regulares a la alta dirección y a las partes interesadas.

10. Anexos

.

- **Inventario de recursos TIC**: Equipos, software, bases de datos.

11. Control de Cambios

Control de Cambios		
Versión	**Fecha**	**Observaciones**
1	15 enero 2024	Creación del Documento de conformidad con lineamientos institucionales establecidos y normativa vigente
2	31 enero 2025	Actualización de documento se incluye análisis de impacto