1. RESUMEN

El Plan de Continuidad de Negocio está conformado por un conjunto de medidas que la organización llevará a cabo para prevenir y reaccionar ante contingencias e incidentes de seguridad que puedan afectar su funcionamiento.

2. OBJETIVO

El objetivo de este plan es garantizar la recuperación rápida y efectiva de los servicios críticos ante incidentes graves, protegiendo los procesos esenciales de la empresa y minimizando el impacto en su continuidad operativa, independientemente de su causa ya sea natural, accidental o intencional.

3. ALCANCE

El ámbito de aplicación de las disposiciones contenidas en el presente plan comprende a toda la estructura la organización, es decir que todos los empleados, colaboradores, contratistas, consultores, temporales y demás trabajadores de la organización son responsables de hacer un uso adecuado de este documento, en cumplimiento con las políticas, leyes y regulaciones locales y las directrices establecidas por la organización.

4. PLAN

A continuación, se definen las fases de este plan de continuidad con el propósito de garantizar la recuperación y continuidad de procesos críticos, minimizando los impactos de interrupciones en los servicios, protegiendo sus activos de información, asegurando la confianza de sus clientes y cumpliendo con las normativas aplicables.

FASE 1: EVALUACIÓN Y ANÁLISIS

Objetivo: Identificar riesgos, procesos críticos y definir los parámetros de recuperación (RTO y RPO).

Roles:

- **Líder del PCN:** Responsable del análisis inicial y recopilación de datos.
- **Analista de Riesgos:** Evalúa amenazas y su impacto en los activos.
- **Gerente de TI:** Colabora en la identificación de sistemas y procesos críticos.

Actividades:

1. **Análisis de Impacto al Negocio (BIA)**
   - Identificar procesos y servicios críticos (ERP, CRM, servidores de TI).
   - Establecer el impacto de interrupciones en términos financieros y reputacionales.
   - RTO (Recovery Time Objective): 4 horas para servicios críticos, 12 horas para sistemas secundarios.
   - RPO (Recovery Point Objective): 30 minutos para información crítica, 2 horas para información secundaria.
2. **Evaluación de Riesgos**
   - Analizar amenazas potenciales: ciberataques, desastres naturales y fallas tecnológicas.
3. **Definición de Objetivos**
   - Garantizar la continuidad operativa en el menor tiempo posible.

FASE 2: PLANIFICACIÓN

Objetivo: Diseñar estrategias para mitigar riesgos y asegurar la recuperación.

Roles:

- **Gerente del PCN:** Lidera la planificación y asegura el alineamiento con los objetivos estratégicos.
- **Administrador de Infraestructura:** Diseña las soluciones tecnológicas de respaldo.
- **Coordinador de Comunicaciones:** Planifica la estrategia de comunicación durante incidentes.

Actividades:

1. **Definir Estrategias de Continuidad**
   - Migrar servicios críticos a una infraestructura híbrida (on-premise y nube).
   - Contratar servicios de recuperación ante desastres (DRaaS).
   - Implementar respaldo incremental y replicación en tiempo real.
2. **Diseñar Planes Específicos**
   - Plan de TI: Recuperación de sistemas y redes.
   - Plan de Comunicaciones: Estrategias para informar a clientes y empleados.
   - Plan Operativo: Procedimientos para la continuidad de las áreas críticas.
3. **Asignar Recursos**
   - Equipamiento tecnológico redundante.
   - Proveedores y socios estratégicos para servicios de recuperación.

FASE 3: IMPLEMENTACIÓN

Objetivo: Ejecutar las estrategias definidas en la fase de planificación.

Roles:

- **Director de TI:** Supervisa la implementación de las soluciones tecnológicas.
- **Encargado de Capacitación:** Diseña y ejecuta entrenamientos para el personal.

- **Analista de Soporte:** Asegura el funcionamiento correcto de las nuevas herramientas.

Actividades:

1. **Desplegar la Infraestructura**
   - Configuración de servidores redundantes y sistemas de respaldo.
   - Contratación y configuración del Data Center secundario.
2. **Capacitación del Personal**
   - Entrenamientos en procedimientos del PCN.
   - Simulacros iniciales para validar preparación.
3. **Establecer Monitoreo Continuo**
   - Implementar sistemas de alertas y monitoreo en tiempo real.

FASE 4: PRUEBAS Y VALIDACIÓN

Objetivo: Verificar que el plan sea efectivo y se cumplan los RTO y RPO.

Roles:

- **Auditor Interno:** Verifica la efectividad del PCN frente a las pruebas.
- **Equipo de TI:** Ejecuta simulaciones y reporta tiempos de recuperación.
- **Gerente de Riesgos:** Analiza los resultados y propone mejoras.

Actividades:

1. **Pruebas de Recuperación**
   - Simulaciones de fallas en sistemas críticos.
   - Evaluar tiempos de respuesta y ajustes necesarios.
2. **Documentación de Resultados**
   - Generar informes de desempeño y lecciones aprendidas.

3. **Validación de Estrategias**
    - Asegurar la alineación con ISO 27001 y normativas internas.

FASE 5: MONITOREO Y MEJORA CONTINUA

Objetivo: Asegurar la vigencia y efectividad del plan a lo largo del tiempo.

Roles:

- **Responsable del PCN:** Coordina auditorías y revisiones del plan.
- **Analista de Seguridad:** Evalúa nuevas amenazas y actualiza estrategias.
- **Equipo de Capacitación:** Realiza sesiones de actualización para el personal.

Actividades:

1. **Revisión Periódica**
    - Evaluar cambios en los riesgos o infraestructura.
    - Actualizar el PCN anualmente o tras incidentes significativos.
2. **Auditorías Internas**
    - Revisar el cumplimiento de las estrategias definidas.
3. **Capacitación Continua**
    - Mantener al personal actualizado en los procedimientos del PCN.

5. CUMPLIMIENTO

5.1 MEDICIÓN DEL CUMPLIMIENTO

La organización realizará un seguimiento y verificación del cumplimiento de este plan mediante una variedad de métodos, incluyendo:

- Visitas periódicas
- Monitoreo de video

- Informes generados por herramientas comerciales
- Auditorías internas y externas
- Inspecciones

Los resultados de estas actividades serán comunicados al propietario del plan y al gerente de la unidad de negocio correspondiente, con el fin de garantizar el cumplimiento y la mejora continua de la política.

5.2 EXCEPCIONES

Cualquier excepción a esta política deberá ser sometida a aprobación previa por parte del Gerente de área correspondiente y el Grupo Interdisciplinario de Seguridad de la Información (GISI), quienes evaluarán y autorizarán las excepciones de acuerdo con las necesidades y riesgos de la organización.

5.3 INCUMPLIMIENTO

Cualquier empleado que incumpla o viole esta política estará sujeto a medidas disciplinarias, que pueden incluir desde advertencias hasta el despido, dependiendo de la gravedad de la infracción y la discreción de la organización.

6. APROBACIÓN

Elaborado por	Verificado por	Aprobado por
Nombre **Oficial de Seguridad de la Información** Fecha:	Nombre **Gerente Administrativo** Fecha:	Nombre **Gerente General** Fecha: