Plantilla de Plan de Continuidad Operacional

(PCO)

Prey Inc.

Introducción

Este documento constituye una plantilla base para la elaboración de un Plan de Continuidad Operacional (PCO) conforme a lo exigido por la Ley N° 21.663 sobre Ciberseguridad en Chile. Su objetivo es proporcionar una guía estructurada y estandarizada para ayudar a las organizaciones a planificar, documentar y ejecutar acciones que aseguren la continuidad de los servicios críticos en caso de incidentes disruptivos.

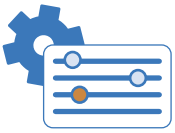
La presente plantilla ha sido diseñada para:

- Organizaciones públicas o privadas sujetas a las obligaciones de la Ley 21.663.
- Equipos de TI, ciberseguridad, operaciones o continuidad del negocio.
- Consultores o encargados de implementar planes de ciberresiliencia.

¿Cómo usar esta plantilla?

Revisión previa: Antes de completarla, asegúrate de tener acceso al inventario de servicios críticos, haber realizado un análisis BIA preliminar y contar con roles definidos dentro del equipo TI y de seguridad.

Completar los campos requeridos: Cada sección incluye campos editables, tablas estructuradas y ejemplos en gris que pueden ser reemplazados.



Adaptar a tu realidad: Agrega o elimina columnas según tu industria. Integra este plan con tus políticas de backup, incidentes o SGSI.

Validar y mantener: Este plan debe ser aprobado por dirección, revisado periódicamente y probado mediante simulacros.

Resultados esperados

Al completar esta plantilla, la organización contará con una visión clara de sus procesos críticos, procedimientos formales de respuesta y recuperación, historial documentado de pruebas y una base para cumplir con los requisitos legales.

1. Datos Generales

Organización	*Ejemplo: Hospital Regional del Maule*
Área responsable	*Ejemplo: Departamento de Tecnología y Comunicaciones*
Versión / Fecha	*Ejemplo: Versión 1.2 – 05/08/2025*
Responsable del PCO	*Ejemplo: Juan Pérez, CISO*
Aprobado por	*Ejemplo: María Soto, Directora General*

2. Alcance y Objetivos

Servicios y procesos críticos cubiertos	*Ejemplo: Sistema de fichas médicas electrónicas*
Objetivo del PCO	*Ejemplo: Asegurar continuidad del servicio médico*
Relación con el SGSI	*Ejemplo: Integrado con ISO 27001*

3. Análisis de Impacto al Negocio (BIA)

Identificar los procesos, sistemas o servicios críticos para la continuidad de la organización, evaluar el impacto ante su interrupción y definir los tiempos máximos de recuperación aceptables.

Instrucciones:

- **Proceso:** Nombre del servicio, sistema o función crítica (ej. Plataforma de fichas médicas).
- **Responsable:** Persona o área encargada de dicho proceso.
- **Impacto:** Nivel de afectación si el proceso se interrumpe (Bajo, Medio, Alto).
- **MTD (Maximum Tolerable Downtime):** Tiempo máximo que puede estar fuera de servicio sin consecuencias graves.
- **RTO (Recovery Time Objective):** Tiempo estimado para recuperar la operación.
- **RPO (Recovery Point Objective):** Punto en el tiempo al que se puede recuperar la información (ej. último backup de hace 12h).

Proceso	Responsable	Impacto	MTD	RTO	RPO
Core bancario	TI	Alto	4 horas	2 horas	15 min

Riesgos y escenarios:

Visualizar amenazas potenciales que puedan afectar los servicios críticos y priorizarlas según su probabilidad e impacto.

Instrucciones de llenado:

- **Riesgo:** Descripción breve del evento (ej. Ransomware, corte eléctrico).
- **Descripción:** Detalle del escenario posible.
- **Probabilidad:** Alta, media o baja, según historial o evaluación experta.
- **Impacto:** Consecuencias para la operación si ocurre.
- **Nivel de riesgo:** Resultado del cruce entre probabilidad e impacto (ej. Crítico, Alto, Medio, Bajo).
- **Controles existentes:** Medidas ya implementadas para mitigar ese riesgo.

Riesgo	Descripción	Probabilidad	Impacto	Nivel de Riesgo	Controles Existentes
Ransomware	Infección de red con cifrado de datos críticos	Alta	Alto	Crítico	Backup diario, EDR, política de correo

4. Estrategia de Continuidad

Documentar cómo se mantendrá o restaurará la operación ante una interrupción.

Instrucciones de llenado:

- **Componente crítico:** Sistemas o procesos clave (ej. Correo institucional, servidores clínicos).
- **Estrategia de continuidad:** Acciones para mantener la disponibilidad (ej. réplica activa, redundancia geográfica).
- **Infraestructura de respaldo:** Tipo y ubicación de infraescturura de respaldo.
- **RTO:** Tiempo estimado para restablecer ese componente.
- **Responsable:** Persona o equipo que ejecuta la recuperación.

Planes de contigencia por componente crítico:

Componente Crítico	Estrategia de Continuidad	Infraestructura de respaldo	RTO	Responsable
Sistema de fichas médicas	Replica activa en datacenter secundario	Nube (región segura)	2 horas	Jefe de Infraestructura

Roles y responsabilidades:

Rol	Responsable	Contacto	Función
Líder de crisis	Juan Pérez	+56 9 1234 5678	Coordina la respuesta

5. Procedimientos de Respuesta

Establecer pasos claros a seguir una vez detectado un incidente que pueda activar el PCO.

Instrucciones de llenado:

- **Fase:** Etapa del proceso de respuesta (Detección, Activación, Contención, Comunicación, Registro).
- **Acción:** Qué se debe hacer (ej. Aislar servidor afectado, notificar al líder de crisis).
- **Responsable:** Encargado de ejecutar la acción.
- **Tiempo estimado:** Cuánto debería tardar en ejecutarse.
- **Medio / Herramienta:** Canal, software o plataforma usada (ej. SIEM, teléfono, Jira, correo).

Fase	Acción	Responsable	Tiempo estimado	Medio / Herramienta
Detección	Confirmar el incidente mediante SIEM o EDR	Analista SOC	15 min	SentinelOne, Splunk, etc.
Activación	Notificar al líder de crisis y activar el PCO	Coordinador TI	10 min	Teléfono interno, correo
Contención	Aislar sistema comprometido	Especialista Redes	30 min	Consola Firewall/ EDR
Comunicación inicial	Notificar al equipo interno y ANCI	Líder de Comunicaciones	30 min	Plan de comunicación formal
Registro del incidente	Registrar hechos en bitácora y sistema de tickets	Jefe de Incidentes	60 min	Jira, Confluence, Excel

6. Plan de Recuperación

Definir cómo se restablecerán los sistemas críticos tras un incidente.

Instrucciones de llenado:

- **Componente / Sistema:** Activo afectado (ej. sistema de RR.HH., base de datos clínica).
- **Acciones de recuperación:** Pasos a seguir para restablecerlo.
- **Prioridad:** Alta, media o baja, según su impacto.
- **Tiempo estimado:** Tiempo aproximado para su restauración.
- **Responsable:** Persona o equipo a cargo.

Componente / Sistema	Acciones de recuperación	Prioridad	Tiempo estimado	Responsable
Red de comunicaciones	Restaurar switches y revisar logs	Alta	1 hora	Especialista de Redes
Aplicación clínica	Restaurar desde backup más reciente, verificar acceso	Crítica	2 horas	Admin Base de Datos
Correo electrónico	Verificar acceso, integridad de mensajes	Media	1.5 horas	Admin M365
Acceso remoto VPN	Restablecer túneles y políticas	Alta	45 min	Especialista Seguridad

7. Pruebas y Simulacros

Asegurar que el PCO funcione en la práctica, a través de ejercicios controlados y periódicos.

Instrucciones de llenado:

- **Tipo de prueba:** Ejercicio realizado (tabletop, restauración, simulacro en vivo).
- **Fecha realizada:** Día de ejecución.
- **Objetivo:** Qué se intentaba validar (ej. tiempos de reacción, integridad de backups).
- **Resultado:** Exitoso, parcial o fallido.
- **Observaciones / Mejora:** Lecciones aprendidas o ajustes requeridos.
- **Responsable:** Quien lideró o coordinó la actividad.

Tipo de prueba	Fecha realizada	Objetivo	Resultado	Observaciones / Mejora	Responsable
Simulacro Tabletop	10/04/2025	Validar coordinación entre equipos	Aprobado con observaciones	Falta claridad en escalamiento interno	Jefe de Seguridad TI
Prueba de failover	15/06/2025	Validar conmutación automática	Exitoso	Failover completado en 12 min	Infraestructura
Restauración backup	01/07/2025	Validar integridad de respaldo semanal	Parcial	Archivos corruptos en sistema de correos	Admin de Backups

8. Mantenimiento y Actualización

Asegurar que el plan se mantenga vigente y actualizado según cambios en la organización o la tecnología.

Instrucciones de llenado:

- **Componente crítico:** Periodicidad establecida (ej. anual, semestral).
- **Registro de cambios:**
  - Versión: Número correlativo (ej. 1.2).
  - Fecha: Día de la modificación.
  - Cambios: Qué se actualizó.
  - Responsable: Quien lo realizó o aprobó.

Versión	Fecha	Cambios	Responsable
1.2	05/08/2025	Actualización de responsables	Juan Pérez

9. Anexos

Incluir información complementaria clave para la ejecución del PCO.

- **Contactos de emergencia:** Nombres, roles y teléfonos internos y externos (ej. soporte TI, ANCI).
- **Diagramas de arquitectura:** Mapas de red, dependencias entre sistemas, puntos de falla críticos.
- **Políticas relacionadas:** Otros documentos aplicables (ej. gestión de incidentes, política de respaldo, SGSI).

Sobre Prey

Es una herramienta multi-plataforma para el **Rastreo y la Seguridad** de tus dispositivos remotos. Es un servicio que actualmente protege más de 8 millones de equipos y sus datos cada día, alrededor de todo el mundo.

Prey comenzó en 2009 como una pequeña compañía de tecnología que se propuso un solo objetivo: ayudar a las personas a mantener el control de sus dispositivos. 15 años más tarde, nuestro servicio ha evolucionado hasta convertirse en una confiable multi herramienta para personas y negocios. Somos expertos en localizar, proteger y administrar tus dispositivos tecnológicos para el ocio y el trabajo. Y un equipo de personas orgullosas de poder ofrecerte apoyo.

Prey para: Personas | Organizaciones | Escuelas y Universidades

Prey Inc. ©
548 Market St. #30152
San Francisco, CA 94104
USA