

La capacidad para reestablecer las operaciones de TI y de negocio, ante eventos que pudieran interrumpir la habilidad de lograr sus objetivos estratégicos, es un elemento clave para las organizaciones de todo tipo. Los riesgos asociados son muy altos y la alta dependencia en las tecnologías de información y de telecomunicaciones ha motivado la necesidad de las organizaciones de contar con las medidas preventivas adecuadas y con la capacidad para recuperar la habilidad de entregar productos y servicios en el tiempo adecuado.

GCP Global apoya a las organizaciones a desarrollar, implantar y mejorar sus planes de continuidad en todo su ciclo de vida, esto es, identificar sus procesos y recursos críticos, entender los riesgos e impactos por interrupciones, definir estrategias y planes de recuperación, entrenar a las personas involucradas, realizar ejercicios de prueba y mantener actualizados los planes y procedimientos. Esto les permite proteger a su personal, sus recursos, su reputación y sus relaciones con clientes y proveedores, además de la ventaja competitiva que representa el contar con una habilidad demostrada de mantener la continuidad de sus operaciones y cumplir con sus compromisos.

La metodología para continuidad de negocio de GCP Global permite la alineación del proceso a las mejores prácticas de la industria, como son las publicaciones emitidas por BSI (British Standards Institution), BCI (The Business Continuity Institute), DRI International, NIST (National Institute of Standards and Technology) y NFPA (National Fire Protection Association).

Por otro lado, nuestra **Plataforma de Software Security Advisor** ha probado ser invaluable para quienes están en el proceso de implementar un plan de Continuidad de Negocios, así como para aquellos que desean tenerlo bajo control.

A continuación se describen las principales actividades comprendidas en una implementación típica de un programa de gestión de continuidad o BCP/DRP¹.

Plan de administración del proyecto

Elaboración del plan de administración del proyecto y definición de la organización del mismo.

Reuniones con el equipo de trabajo para revisar y definir:

- Objetivos y alcance del proyecto.
- Actividades, responsables, recursos, duración y dependencias.
- Requerimientos, entregables y criterios de aceptación.
- Dependencias de otras áreas.
- Supuestos, limitantes y riesgos.
- Estrategias de comunicación y seguimiento.

Principales entregables:

Plan de Administración del Proyecto para guiar la organización y planificación del proyecto, conteniendo al menos los siguientes elementos:

- Objetivo del proyecto.
- Alcance.
- Organización del proyecto.
- Comunicación y seguimiento.
- Supuestos, limitantes y riesgos.
- Plan de trabajo (diagrama de Gantt).
- Entregables.
- Hitos (milestones).
- Formatos y matrices de control.
- Definición de requerimientos y criterios de aceptación.

¹ De forma general, se entiende DRP (plan de recuperación de desastres) como las actividades para recuperar las operaciones de TI (tecnologías de información incluyendo telecomunicaciones), y el término BCP (plan de continuidad de negocio) como las actividades para recuperar todas las operaciones de negocio además de las operaciones de TI. En este documento se usa la nomenclatura BCP/DRP para indicar que podría tratarse indistintamente de cualquiera de los dos tipos de alcance.

Desarrollo del marco de trabajo

Desarrollo de la normatividad interna para el BCP/DRP.

Las principales tareas son:

- Identificación de los componentes de la política de BCP/DRP.
- Identificación de requerimientos regulatorios, normas y objetivos estratégicos a los que la política de BCP/DRP debe estar alineada.
- Desarrollar el documento de la política de BCP/DRP.
- Revisión y aprobación de la política por parte de la Dirección.
- Definir y documentar alcance, términos de referencia y estructura organizacional del BCP/DRP.

Principales entregables:

- Política de BCP/DRP.
- Organización (comité del BCP/DRP, coordinación del BCP/DRP, áreas de soporte).

Análisis de impacto al negocio (BIA)

El análisis de impacto al negocio tiene como objetivo identificar, cuantificar y calificar el impacto al negocio por pérdida o interrupción de las operaciones y provee la información con base en la cual se determinan las estrategias de recuperación más apropiadas.

Las principales tareas son:

- Definición, ponderación y aprobación de los niveles de impactos cualitativos y cuantitativos a utilizar.
- Desarrollo de procedimiento de análisis de impacto al negocio.
- Programación de entrevistas, talleres o aplicación de cuestionarios con los responsables de las operaciones de acuerdo al procedimiento definido.
- Ejecución del análisis de impacto identificando:
 - impactos al negocio;
 - tiempo máximo de tolerancia a no disponibilidad de los sistemas y recursos (Maximum Tolerable Outage o MTO);
 - objetivos de punto de recuperación (Recovery Point Objective o RPO);
 - periodos críticos de operación;
 - dependencias internas y externas;
 - recursos requeridos.
- Revisión y aprobación de los resultados del BIA por parte de la Dirección.

Principales entregables:

- Documento de Análisis de Impacto al Negocio (BIA).

Evaluación de riesgos e identificación de controles

Identificar y evaluar riesgos relacionados a la continuidad de las operaciones; esto es, la probabilidad y el impacto de una variedad de amenazas que pudieran ocasionar interrupciones a dichos servicios. Posteriormente se priorizan los riesgos y se determinan medidas a implementar para mitigarlos.

Las principales tareas son:

- Definición de un sistema de calificación de impactos y probabilidades para calcular el riesgo.
- Identificación de las amenazas a la continuidad de las operaciones.
- Determinación del nivel de impacto y la probabilidad de ocurrencia de las amenazas.
- Cálculo del riesgo con base en el impacto y probabilidad de las amenazas.
- Establecimiento de prioridades y determinación de las medidas adecuadas para el tratamiento de cada riesgo identificado, considerando las alternativas para reducirlo, transferirlo, evitarlo o aceptarlo.

Principales entregables:

- Evaluación de riesgos relacionados a la continuidad de las operaciones.
- Definición de controles para el tratamiento de los riesgos.

Desarrollo de estrategias de recuperación

Con base en el BIA, se establecen y seleccionan los métodos de operación alternativos a ser utilizados después de una interrupción para mantener los procesos y servicios críticos del negocio y sus dependencias, tanto internas como externas, con base en las prioridades y tiempos establecidos en el BIA.

Las principales tareas son:

- Revisión del alcance, las premisas y los hallazgos del BIA.
- Generación de diversas opciones de estrategias a seguir, para su discusión y análisis, considerando análisis costo-beneficio, análisis FODA (fortalezas, oportunidades, debilidades y amenazas) y tiempos objetivos de recuperación (Recovery Time Objective o RTO).
- Revisión, selección y aprobación de las estrategias por parte de la Dirección.
- Definición de proyectos y responsables para el desarrollo de planes de recuperación de las operaciones alineados a las estrategias.

Principales entregables:

- Análisis de alternativas de estrategias de BCP/DRP.
- Definición de las estrategias de BCP/DRP.

Desarrollo de respuestas

Desarrollo de planes con los procedimientos a seguir para la recuperación de las operaciones críticas posterior a un evento de desastre que interrumpa la continuidad del negocio. Los planes a desarrollar deben soportar las estrategias de recuperación seleccionadas.

También contempla el desarrollo de planes de restauración (regreso a la operación normal) una vez reestablecidos el sitio y los recursos de operación primarios.

Las principales tareas son:

- Nombrar a los responsables de elaborar y revisar las actividades específicas de recuperación.
- Definición de la estructura, formato, componentes y contenido de los planes.
- Determinar la logística para la documentación de planes.
- Obtener la información necesaria para contenido de los planes.
- Elaboración de planes documentados.
- Circular los planes para su revisión.
- Adecuación de los planes y obtener aprobaciones.
- Asesoría en el desarrollo de esquemas de operación alternativos por parte de los responsables.

Principales entregables:

- Planes documentados para recuperación y restauración de las operaciones del negocio.

Entrenamiento

Definición y ejecución de un programa de concientización y entrenamiento dirigido al personal involucrado en la recuperación y restauración de las operaciones.

Las principales tareas son:

- Definición de los conocimientos y mensajes específicos que deben ser asimilados por el personal involucrado.
- Definición de la audiencia y la logística para el entrenamiento.
- Ejecución del entrenamiento con fines de capacitación y concientización.

Entre los puntos a considerar en el temario de entrenamiento inicial están:

- Estrategias del BCP/DRP.
- Organización del BCP/DRP.
- Estructura y contenido de los planes.
- Responsabilidades.

- Apoyo para mantenimiento y pruebas de los planes.
Principales entregables:
- Programa de capacitación del BCP/DRP.
- Entrenamiento a los involucrados en la recuperación y restauración de las operaciones.

Pruebas y ejercicios

Desarrollo del plan de pruebas y ejercicios de los planes de recuperación considerando los diferentes tipos:

- Pruebas de escritorio
- Pruebas simuladas
- Pruebas en producción (parciales o completas)

Los principales puntos a considerar en la conducción de una prueba o ejercicio son:

- Definición y acuerdo del alcance y los objetivos.
- Estimación y aprobación de presupuesto.
- Definición y asignación del personal participante.
- Definición de los escenarios y supuestos.
- Evaluación de posibles impactos a las operaciones en producción.
- Conducción de la prueba o ejercicio.
- Registro y reporte de los resultados.
- Generación de planes de corrección de hallazgos.

Principales entregables:

- Plan de pruebas y ejercicios.
- Apoyo para la ejecución de pruebas según se acuerde previamente entre ambas partes.

Mantenimiento

Desarrollo del plan de mantenimiento del BCP/DRP para asegurar que las áreas permanezcan preparadas para el manejo de incidentes relacionados a la continuidad del negocio a pesar de los cambios a las personas, los procesos y la tecnología.

Los principales disparadores de mantenimientos al BCP/DRP son:

- Revisiones periódicas al BCP/DRP (mantenimiento programado).
- Adecuaciones identificadas por el control de cambios.
- Adecuaciones identificadas como resultado de pruebas o ejercicios.

Principales entregables:

- Procedimiento de revisión y mantenimiento al BCP/DRP.
- Calendario de revisiones al BCP/DRP.
- Procedimiento de control de cambios (para registro de cambios que sufran los elementos y procesos del BCP/DRP).
- Lista de verificación de puntos de auditoría.

Sobre GCP Global

Fundada en 1998, GCP Global es una corporación multinacional líder en el control de riesgos de seguridad de información. Nuestra mas reciente innovación, la plataforma de software **Security Advisor V3** se suma a T.R.U.S.T.® y SecuCare entre otros. Somos la única entidad certificadora en América para el Institute for Security And Open Methodologies, además de participar activamente en el proyecto OSSTMM del ISECOM. Organismos reguladores de varios países utilizan nuestra tecnología para monitorear el cumplimiento de normas y estándares. Nuestra tecnología ha sido implementada en más de una docena de países alrededor del mundo.