POLÍTICA DE GESTIÓN DE LA CONTINUIDAD DE LAS OPERACIONES DEL PNUD

(BCM)

**Resúmen ejecutivo**

La Política de Gestión de la Continuidad de las Operaciones (BCM) es la política del PNUD que establece el marco para que la organización responda a las amenazas internas y externas y garantice la preparación, la resiliencia y la capacidad de la organización para seguir cumpliendo su mandato cuando se producen dichas amenazas.

La Política de Gestión de la Continuidad de las Operaciones en el PNUD está en consonancia con el Sistema de Gestión de la Resiliencia Organizacional (ORMS) de la ONU y actúa como marco de gestión de emergencias para la organización. Incluye el Plan de Recuperación de Desastres Informáticos (ITDRP), los planes de seguridad (que incluyen la gestión de crisis, incidentes y emergencias) y la Planificación de la Continuidad de las Operaciones (BCP).

Un Plan de Continuidad de las Operaciones (BCP) se prepara sobre la base de una Evaluación de Riesgos operativos (RA) y un ágil Análisis de Impacto en el Negocio (BIA). La Evaluación de Riesgos y el Análisis de Impacto en el Negocio se basan en los procesos existente de Gestión de Riesgos Empresariales y en la Gestión de Riesgos de Seguridad (SRM) específica del país/área, al tiempo que tienen en cuenta el mandato general de la organización, la criticidad del programa[[1]](#footnote-1) y la continuidad de los servicios empresariales críticos, así como los Procedimientos Operativos Estándar para la respuesta a las crisis y la recuperación.

Índice

[A. Antecedentes 3](#_Toc179986712)

[B. Objetivos 3](#_Toc179986713)

[C. Valoración de riesgos 5](#_Toc179986714)

[D. Análisis de Impacto de las Operaciones (BIA) 5](#_Toc179986715)

[E. Plan de Continuidad de las Operaciones 5](#_Toc179986716)

[F. Funciones y responsabilidades para la BCM 8](#_Toc179986717)

[G. Factor desencadenante para la activación de Planes de Continuidad de Operaciones 9](#_Toc179986718)

[H. Formación, ejercicio y revisión 10](#_Toc179986719)

**Política de Gestión de Continuidad de las Operaciones del PNUD**

# Antecedentes

1. La protección y la seguridad de las poblaciones humanas se ve cada vez más comprometida por amenazas nuevas o potenciales, tanto naturales como provocadas por el hombre. Estas amenazas incluyen potenciales pandemias, ataques cibernéticos, eventos climáticos extremos o desastres naturales, y a menudo son amenazas interrelacionadas con conflictos armados, criminalidad, desorden civil y terrorismo transnacional. Estas amenazas ponen en peligro la vida humana, así como la estabilidad de los sistemas políticos, económicos y sociales. Como sucede con cualquier institución multilateral, estos eventos obligan al PNUD a gestionar y preparase para situaciones que pueden amenazar la capacidad y la continuidad de la organización.
2. Por lo tanto, el PNUD ha implementado corporativamente una política de **Gestión de Continuidad de las Operaciones (BCM)**, como parte de la política actual de valoración de riesgos y de **Gestión de los Riesgos Institucionales (ERM, *Enterprise Risk Management*, por sus siglas en inglés)**, con el fin de garantizar que la organización pueda seguir cumpliendo con sus misiones clave, manteniendo al mismo tiempo la seguridad y la protección del personal en caso de perturbaciones o amenazas. Estos riesgos pueden ser externos a la organización y por ende fuera del control del PNUD, como en el caso de una interrupción del suministro eléctrico, o internos, como un daño accidental a la propiedad.
3. Los elementos clave de la Gestión de la Continuidad de las Operaciones (**BCM)** en el PNUD son la gestión de incidentes que involucren crisis/emergencias/recuperación en casos de desastre (como se refleja en los Planes de Seguridad y Gestión de Crisis), la comunicación en casos de crisis, el Plan de recuperación de TI en casos de desastre (ITPRD) y las estrategias de continuidad de las operaciones y recuperación en casos de crisis para funciones operativas críticas, como se refleja en el **Plan de Continuidad de las Operaciones (BCP)** para la oficina/unidad (oficina en el país (CO), oficina/unidad en la sede, oficina de representación, oficina de enlace, oficina política, centros y nodos regionales) y los Bureau.

# Objetivos

1. El objetivo de la política de Gestión de la Continuidad de las Operaciones **(BCM)** es proteger los intereses del PNUD y sus partes interesadas internas y externas mediante el establecimiento de un marco estratégico y operativo inherente a las operaciones e impulsado por ellas, que garantice proactivamente la capacidad del PNUD para prepararse adecuadamente para los riesgos anticipados —y reaccionar ante estos— identificados en el contexto de una valoración de riesgos corporativos, los registros de riesgos a nivel de la oficina/unidad, o buró y cualquier perturbación inesperada y potencial, garantizando al mismo tiempo la seguridad y la protección del personal.
2. La metodología BCM del PNUD sigue la Organización Internacional de Normalización (ISO) 22301 Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio (Societal Security - Guidelines for Incident Preparedness and Operations Continuity Management).
3. La política de Gestión de la Continuidad de las Operaciones[[2]](#footnote-2) **(BCM)** en el PNUD está también alineada con el Sistema de Gestión de la Resiliencia Institucional de las Naciones Unidas (**ORMS**) y actúa como el marco de gestión de emergencias para la organización. Ayuda al PNUD a consolidar su resiliencia al alinear y armonizar los esfuerzos de preparación para mejorar la capacidad de la organización para cumplir con su mandato sin interrupciones.
4. La **BCM** complementa a la Gestión de los Riesgos Institucionales (**ERM**) y proporciona herramientas para gestionar los riesgos identificados a nivel de oficinas o unidades, que podrían afectar la continuidad de las operaciones. La BCM reconoce todas las actividades y los acuerdos existentes relacionados con la gestión de los riesgos, las respuestas a las crisis y la planificación para emergencias, lo que habilita a su vez al PNUD a:
5. Fortalecer la capacidad de cada oficina/unidad,o buró para continuar con sus operaciones luego de la respuesta inmediata a un incidente, basándose en una Valoración de Riesgos (**RA**) y un ágil Análisis del Impacto en las Operaciones (**BIA**) exhaustivos;
6. Interconectar estructuras y mecanismos establecidos para la Valoración de Riesgos y la respuesta inmediata a incidentes con las actividades necesarias para garantizar la continuidad de las operaciones;
7. Determinar hasta qué punto es necesario el **Plan de Continuidad de las Operaciones** (**BCP**) en cada oficina de país, en función de la probabilidad identificada de incidentes y el impacto en la seguridad y la protección del personal y la continuidad de las operaciones, que difieren significativamente entre las diversas oficinas/unidades, burós;
8. Se prepara un **BCP** después de que la oficina/unidad, o buró realiza y concluye la Valoración de Riesgos (**RA**) **y el Análisis de Impacto de las Operaciones** (BIA). Estas valoraciones se basan en la Gestión de los Riesgos Institucionales (ERM) y en las evaluaciones de riesgos para la salud, la sprotección y la gestión de los Riesgos para la Seguridad (**SRM**) específicas de cada país/área, tomando en cuenta al mismo tiempo el mandato general de la organización; la criticidad del programa (si procede) y la continuidad de las operaciones y servicios críticos, así como los procedimientos operativos normalizados para la respuesta a las crisis y la recuperación.
9. Cada oficina/unidad, o buró debe tener un Coordinador del **BCP**, que debe trabajar bajo las instrucciones directas del Jefe de Oficina/Unidad o Bureau.

# Valoración de riesgos

1. **La sede (HQ)-Nueva York**: Bajo la supervisión del **Grupo de Gestión de la Seguridad (SMG)**, se lleva a cabo anualmente **una Evaluación de los Riesgos de Seguridad en la sede**, en colaboración con los socios del sistema de las Naciones Unidas. En el caso de la sede del PNUD, **la Oficina de** **Servicios de Gestión (BMS)** inicia conversaciones con los socios de la Secretaría de las Naciones Unidas y otros organismos de la ONU durante el último trimestre de cada año para preparar una Evaluación de Riesgos común. Sobre esta base, la Oficina de Servicios de Gestión/Seguridad y los miembros asesores pertinentes del SMG colaboran (reuniendo la seguridad y otros riesgos operativos, por ejemplo, instalaciones, TI, salud y seguridad en el trabajo, etc.) para finalizar la Evaluación de Riesgos anual. El resultado de la Evaluación de Riesgos anual se comparte con el SMG y sirve de base para las decisiones y la planificación de la BCM para el año siguiente.
2. Oficinas/unidades fuera de la sede de Nueva York: Basándose en el proceso SRM para el país/zona, todas las oficinas/unidades llevan a cabo una evaluación de riesgos al menos una vez al año para identificar los riesgos de seguridad, salud y protección, y los riesgos operativos que puedan tener un impacto en las funciones empresariales de la oficina/unidad.

# Análisis de Impacto de las Operaciones (BIA)

1. El Análisis de Impacto de las Operaciones (**BIA**) es realizado por cada oficina/unidad, o buró, y es coordinado por el punto focal de BCP. Pueden solicitar asistencia técnica a la Dirección del Buró de Gestión de Servicios **(BMS**). El BIA incluye lo siguiente:
2. La identificación de las funciones operativas críticas;
3. La valoración de los impactos de los riesgos identificados que puedan perturbar las funciones operativas críticas;
4. La descripción detallada de los tiempos de recuperación en casos de perturbaciones y;
5. La definición de estrategias de recuperación para funciones operativas críticas, incluida la asignación de recursos apropiados.

# Plan de Continuidad de las Operaciones

1. Cada oficina/unidad y bureau debe preparar y mantener un Plan de Continuidad de las Operaciones (**BCP**), para garantizar que la organización pueda llevar a cabo sus funciones, en la medida en que sea razonablemente posible, en casos de emergencia. Las oficinas de país deben incluir sub-oficinas en el plan para asegurar la continuidad de las operaciones. El **BCP** debe ser revisado al menos anualmente.
2. A nivel de oficina/unidad, o buró, un Plan de Continuidad de las Operaciones (**BCP**) proporciona lo siguiente:
3. Un método probado para restaurar la capacidad del PNUD para mantener las funciones críticas de nivel corporativo y de servicio con los mejores estándares posibles, dentro de un período realista después de la perturbación;
4. Una capacidad verificable para mantener, probar, implementar, autorizar y auditar el **BCP** y;
5. Un protocolo de comunicación predefinido para garantizar que todas las unidades pertinentes conozcan el **BCP** cuando este se active.
6. A nivel organizativo, la Gestión de Continuidad de las Operaciones (**BCM**) proporciona lo siguiente:
7. Planes de Continuidad de las Operaciones completados, implementados y probados (incluidos los procedimientos de mantenimiento y seguimiento), que reflejan el alcance determinado de los preparativos necesarios correspondientes a la realidad de cada oficina/unidad, o buró con respecto a la exposición a incidentes críticos;
8. estructura y mecanismos de respuesta a las crisis, de gestión de riesgos y de continuidad de operaciones más interconectados y mejor fundamentados e integrados, en todas las oficinas de país del PNUD; y
9. La capacidad para:
   1. reaccionar ante un evento para mantener la seguridad y la protección del personal;
   2. continuar las funciones críticas operativas con las menores limitaciones o interrupciones posibles;
   3. recuperar la capacidad operativa plena lo antes posible luego de un desastre/crisis.
10. El BCP cubre a todo el personal administrado por el PNUD, las funciones operativas en todos los niveles, incluidos aquellos que han sido subcontratados a contratistas externos y proveedores, donde la responsabilidad legal general recae en el PNUD. El BCP no cubre la resiliencia de terceros; sin embargo, se debe solicitar a los subcontratistas que proporcionen pruebas de que han considerado posibles problemas de resiliencia. También se alienta las oficinas de proyecto a aplicar los principios de la **BCM**.
11. El **BCP** debe incluir todos los riesgos, incluidas las siguientes hipótesis principales que pueden afectar la continuidad de las operaciones:
12. Eventos que puedan generar la incapacitación o la pérdida de personal;
13. Eventos que interrumpan sistemas críticos de misión;
14. Eventos que puedan generar la pérdida del acceso a un edificio de oficinas o la pérdida de dicho edificio;
15. Eventos que puedan generar la pérdida de los servicios de proveedores.
16. Los Puntos focales de **BCP** coordinan la preparación de los BCP para sus oficinas/ unidades, o burós. El **BCP** incluye lo siguiente:
17. La lista de todas las funciones operativas críticas con los nombres de las personas que asisten o realizan dichas funciones, incluidas aquellas que están subcontratadas, con un tiempo predeterminado y procedimientos para la recuperación operativa;
18. La lista de equipos y materiales necesarios para llevar a cabo estas funciones;
19. El plan para comunicarse con asociados internos y externos; y
20. El plan para establecer un centro alternativo cuando se considere necesario.
21. Establece procedimientos claros de gestión, sucesión y delegación de autoridad, y esboza disposiciones para la formación, las pruebas y el mantenimiento.
22. El BCP debe ser aprobado y firmado por el Jefe de la oficina/unidad, o buró correspondiente. El BCP aprobado se cargará en el sitio web de la BCM junto con los anexos correspondientes. Las oficinas/unidades o burós pueden compartir el borrador del PBC con el Especialista en Gestión de Riesgos y Resiliencia de BMS/BPC para su revisión técnica y asesoramiento, si es necesario.
23. Además, para que se considere que cumplen esta política y directriz, los Jefes de oficinas/unidades o burós deben establecer calendarios claros de pruebas y revisión del **BCP** (al menos una vez al año o tras un cambio importante en los componentes del BCP). Las pruebas y las revisiones cubren los siguientes puntos:
    1. Propósito y alcance de las pruebas, eventos de simulación para pruebas;
    2. Duración de toda la prueba; procedimientos de evacuación del personal;
    3. Planes de comunicación de emergencia, copia de seguridad y recuperación de datos críticos;
    4. Preparación del edificio/las instalaciones y recursos necesarios para la prueba;
    5. Preparación de un sitio alternativo para continuar con las operaciones dentro de un período específico;
    6. Recuperación de funciones operativas críticas.
24. Los resultados de las pruebas y reportes de ejercicios BCP se evaluarán y utilizarán para mejorar el BCP cuando sea necesario asegurando que el BCP.
25. Además, el programa de Mantenimiento, Ejercicios y Revisión (ME&R)[[3]](#footnote-3) del ORMS también exige que todo el personal conozca los procedimientos de gestión de emergencias y participe en formaciones y ejercicios de concienciación.

# Funciones y responsabilidades para la BCM

Buró de Gestión de Servicios (BMS)

1. En el contexto de la política de gestión de riesgos institucionales (ERM), el BMS es responsable de la formulación y la revisión de la Política corporativa de la BCM y su puesta en funcionamiento.
2. **BMS/BCP** proporciona asistencia técnica y asesoramiento a los Coordinadores para la preparación de los BIA y los BCP, y mantiene registros de los BCP de todas las oficinas/unidades, burós, en la plataforma SharePoint de la BCM. El BMS supervisa la conformidad normativa de las oficinas/ unidades y bureaus de país e informa periódicamente al SMG respecto al estado de las actividades de la BCM y la conformidad de las oficinas. El BMS trabaja en estrecha colaboración con los Burós regionales **y los Burós centrales** y para garantizar que todas sus oficinas respectivas adhieran al cumplimiento de la política de Gestión de la Continuidad de las Operaciones (BCM).
3. **BMS/Oficina de Gestión y Tecnología de la Información (IMT, *Information Technology*, por sus siglas en inglés)** proporciona el apoyo necesario (si fuese necesario) al personal de Tecnología de la Información (TI) de la oficina/unidad, o buró para la preparación de los Planes de Recuperación de Tecnología de la Información en Casos de Desastre (ITDRPs).

Grupo de Gestión de la Seguridad del PNUD (SMG)

1. La supervisión de las actividades de **BCM** se delega al Grupo de Gestión de la Seguridad (SMG). Los Planes y la Gestión de la Continuidad de las Operaciones son puntos destacados en los órdenes del día del SMG de forma periódica.

Burós Regionales/Centrales:

1. Los Burós Regionales/Centrales, supervisan sus respectivas regiones y oficinas para garantizar que los Planes de Continuidad de las Operaciones (**BCP**) se revisen, actualicen y se prueben al menos anualmente.

Jefes de Oficinas/Unidades y Burós

1. Las actividades de la BCM deben incluirse en los planes de trabajo de la oficina/unidad, o buró. Se recomienda incluir una referencia a las responsabilidades de la Gestión de la Continuidad de las Operaciones (**BCM**) en las descripciones de los puestos para garantizar que el personal esté al tanto de su función y de las responsabilidades personales en caso de perturbaciones.
2. Los Puntos focales de BCP deben asignarse para coordinar el Análisis de Impacto de las Operaciones (**BIA**), así como la preparación y el mantenimiento de los BCP. Los Puntos focales BCP trabajan en estrecha colaboración con el personal que cubre las diversas funciones, incluido el personal directivo senior, así como el personal de TI que generalmente se asigna para mantener los **ITDRs**.
3. El Punto Focal del PBC presenta el borrador del PBC al Jefe de oficina/unidad, o buró para su revisión y aprobación final.

Gerentes de operaciones

1. Los gerentes de todos los niveles deben discutir la continuidad de las operaciones con regularidad en las reuniones de equipo y garantizar que la Gestión de la Continuidad de las Operaciones sea parte del proceso de presentación para todo miembro del personal que ingrese a sus equipos.

# Factor desencadenante para la activación de Planes de Continuidad de Operaciones

Sede (HQ - Nueva York):

1. En caso de incidentes que afecten a todas las operaciones del PNUD en Nueva York, el Grupo de Gestión de la Seguridad (**SMG**) aconsejará a las oficinas/unidades, burós activar sus Planes de Continuidad de las Operaciones (**BCP**). En el caso de incidentes que afecten solo a una unidad/buró (por ejemplo, un incendio limitado), el director de la unidad/buró afectado activará su **BCP** y aconsejará al personal sobre cómo proceder según el **BCP** de la oficina/unidad, o buró.

Todas las oficinas fuera de la Sede (Nueva York):

1. El Representante Residente, Jefe de Oficina / Unidad activará el Plan de Continuidad de las Operaciones (**BCP**) basándose en el asesoramiento del **Equipo de Gestión de la Seguridad (SMT**, ***Security Management Team*, por sus siglas en inglés**) del país/área, las decisiones del funcionario designado y/o de los comités de salud y seguridad en el trabajo (SST).
2. Para garantizar que el proceso de planificación de la continuidad de las operaciones cuente con una base sólida, oficina/unidad, o buró debe utilizar los recursos internos establecidos.

# Formación, ejercicio y revisión

1. Los BCP deben ser revisados por los Coordinadores de **BCP** para las oficinas/unidades o burós, correspondientes al menos una vez al año o con mayor periodicidad en los siguientes casos:
2. Actualización de la información de contacto;
3. Tras un cambio en la estructura de la organización y/o oficina/unidad, o buró;
4. Tras un cambio en la dotación de personal, incluido el personal crítico;
5. En respuesta a una nueva valoración de amenazas y riesgos;
6. Cambios en los requisitos reglamentarios nacionales.
7. El **BCP** debe ejercitarse al menos una vez al año. El formato del ejercicio puede variar y el Buró de Gestión de Servicios puede proporcionar asesoramiento en coordinación con oficinas/unidades o burós.
8. Los materiales de formación y la guía relacionados están a disposición de los puntos focales del PBC en el sitio del PBC.

*Disclaimer: This document was translated from English into Spanish. In the event of any discrepancy between this translation and the original English document, the original English document shall prevail.*

*Descargo de responsabilidad: esta es una traducción de un documento original en inglés. En caso de discrepancias entre esta traducción y el documento original en inglés, prevalecerá el documento original en inglés.*

1. El Marco de criticidad de los programas es una política común del sistema de las Naciones Unidas para la toma de decisiones sobre el riesgo aceptable. Establece principios rectores y un enfoque sistemático estructurado para garantizar que las actividades en las que participa el personal de las Naciones Unidas puedan equilibrarse con los riesgos de seguridad. Para más detalles, consulte: <https://programmecriticality.org/Static/index.html> [↑](#footnote-ref-1)
2. <https://unsceb.org/organizational-resilience-management-system-orms> [↑](#footnote-ref-2)
3. <https://unsceb.org/sites/default/files/2021-12/Approved%20revision%20of%20Add.2.Rev_.1_ORMS%20MER%20Regime.pdf> [↑](#footnote-ref-3)