Gestión de Continuidad de Negocio

Agosto de 2024 | Versión 2.0

Índice

Aviso General

Este documento pertenece al Sistema de Gestión de Continuidad de negocio (BCMS). Lo siguiente se aplica a este documento:

- Este documento está controlado como parte del control de gestión del Sistema de Gestión de Continuidad de negocio (BCMS).
- No se permiten cambios a este documento sin la aprobación formal del dueño del documento.
- Este documento es clasificado, controlado por versión y revisado periódicamente.
- Cualquier pregunta relacionada con este documento debe ser efectuada al dueño del mismo.
- La distribución, las modificaciones y el acceso deben abordarse según la clasificación de información de TMF Group.
- La versión de este documento se puede encontrar en la portada.
- La información referente a la revisión se describe a continuación.
- Este documento puede estar disponible en varios idiomas; no obstante, prevalecerá la versión en inglés.

CLASIFICACIÓN
Interna

PARTES INTERESADAS	
Propietario	Director de seguridad de la información y resiliencia
Aprobador	Comité de Riesgo de TMF Group
Patrocinador	**Director de tecnología y operaciones**

REVISIÓN	
Período	Anual
Última revisión	27 de mayo de 2024
Estado	Final
Aprobado el	8 de agosto de 2024
Vigencia	8 de agosto de 2024

PUNTO DE CONTACTO	
Contacto	TMF Group ISMS
Detalles	**Contacte al equipo a través de ISMS@tmf-group.com**

1. Introduccion, propósito y alcance

El propósito de la Política de Gestión de Continuidad de negocio (BCM por sus siglas en inglés) (la "**Política**") es proteger los intereses de TMF Group y de sus partes interesadas internas y externas, al tener acuerdos de contingencia para responder, recuperar y reanudar las servicios de negocios, en la medida de lo comercialmente razonable.

Esta Política proporciona las intenciones y la dirección de TMF Group expresadas formalmente por nuestro Consejo de Administración. Como una organización de servicios profesionales, TMF Group comprende la importancia de sus servicios comerciales para las partes interesadas externas e internas y por lo tanto, la importancia de contar con un programa integral de Gestión de la Continuidad del Negocio.

El propósito de esta Política es, por lo tanto, proteger los intereses de TMF Group y sus partes interesadas internas y externas, mediante la implementación de acuerdos de contingencia para responder, recuperar, reanudar y restaurar a un nivel operativo previamente definido las funciones críticas de negocio identificadas, en la medida en que sea razonablemente posible.

Esta política es aplicable a TMF Group y sus subsidiarias.

2. Declaración de Política

2.1 Principios fundamentales

> Continuidad de Negocio (BCM) es una parte integral de los procesos de gestión principales y de negocio de TMF Group;

> La seguridad de las personas es la prioridad de la organización. La salud y la seguridad del personal deben considerarse parte de todos los procesos y actividades comerciales. Durante un incidente, la organización debe priorizar la seguridad y el bienestar del personal;

> La organización garantizará que los procesos de la continuidad de negocio (BC por sus siglas en inglés) deben establecerse para habilitar la continuidad de los principales servicios críticos de negocio de TMF Group, en caso de interrupción;

> Se deben identificar y priorizar todos los procesos y recursos comerciales críticos, incluidos los de terceros, necesarios para prestar los servicios;

> El plan de recuperación de desastres para los activos y servicios tecnológicos que se requieren para respaldar los procesos comerciales críticos debe crearse en función de las evaluaciones de riesgo / modos de falla apropiados, mantenerse y probarse periódicamente;

> El Equipo de Gestión de Crisis (CMT) es responsable de la declaración de crisis / ejecución del Plan BC y el responsable general de la gestión de cualquier situación de crisis;

> Las funciones de TMF Group se esforzarán por respaldar los procesos de respuesta, continuidad y recuperación. Se llevarán a cabo revisiones posteriores a la crisis para determinar las lecciones aprendidas y permitir que TMF Group mejore sus procesos de continuidad del negocio y su respuesta.

> La organización debe asegurarse de que todas las comunicaciones relacionadas con la continuidad del negocio con las partes interesadas internas y externas se coordinen a través de TMF Group Communications, de manera oportuna y adecuada;

2.2 Requerimientos generales

> Cada oficina / país se asegurará de que se identifiquen y cumplan los requisitos legales, reglamentarios y contractuales relacionados con la continuidad del negocio;

> Cada oficina / país debe implementar y mantener un proceso de evaluación formal conocido como Análisis de Impacto Comercial (BIA) para determinar las prioridades, objetivos y metas de continuidad y recuperación;

> Cada oficina / país y función global debe realizar evaluaciones de riesgos formales y periódicas para identificar y tratar los riesgos de interrupción;

> Cada oficina / país y función global debe mantener un plan de tratamiento de riesgos para reducir la exposición al riesgo a un nivel del apetito por el riesgo de la Organización;

> Cada oficina / país debe determinar y seleccionar estrategias para cumplir con los períodos de tiempo priorizados establecidos para reanudar los procesos críticos de negocio y las actividades

priorizadas en un nivel mínimo aceptable especificado, después de un evento de continuidad del negocio;

- Cada oficina / país es responsable de crear, implementar, monitorear, revisar, mantener y mejorar continuamente los planes de Continuidad del Negocio para garantizar que los servicios críticos se entreguen según los niveles previamente identificados, en caso de una interrupción;
- Cada país, a menos que estén explícitamente exentos por el Líder Regional y de Mercado, deben contar con un Coordinador de Continuidad del Negocio (BCC por sus siglas en inglés), que trabaje bajo la dirección de su Líder de País o equivalente, quien es responsable de la creación, mantenimiento, prueba y ejercicio de Plan de Continuidad del Negocio;
- Cada oficina / país debe revisar y mantener la documentación BCM de manera continua o al menos una vez al año.
- Se identificarán recursos de respaldo para las funciones/servicios críticos. Se mantendrán los Procedimientos Operativos Estándar (SOP, por sus siglas en inglés) / manuales / guías para los procesos críticos y se pondrán a disposición para ayudar a la transición del proceso a un nuevo recurso en ausencia de recursos críticos identificados
- Cada oficina / país es responsable de identificar los activos y servicios tecnológicos que son críticos para sus procesos comerciales y acordar formalmente los objetivos de recuperación con la función de Operaciones y Tecnología;
- Mientras se opere en modo de Continuidad del Negocio, la oficina afectada de TMF Group debe continuar operando de conformidad con todas las políticas de TMF Group y los requisitos legislativos locales de salud, seguridad y protección
- Los roles y responsabilidades del personal asignado a las funciones de continuidad de negocio l deben estar claramente definidos en el Plan de Continuidad de Negocio (BCP, por sus siglas en inglés) de la oficina

2.3 Gerencia y Compromiso

El Consejo de Administración demostrará liderazgo y compromiso con respecto al BCMS, garantizando

La Gerencia Local garantizará:

- Se asignan y comunican las funciones y responsabilidades de BCM dentro de la organización.
- desarrollo, implementación y mantenimiento de Planes de Continuidad de Negocio y medidas eficaces
- la ejecución del programa BCM, es coherente con la estrategia global de la empresa;
- la provisión de los recursos adecuados necesarios para BCM;
- promoción de la integración de BCMS en los procesos empresariales
- la organización cuenta con un programa de sensibilización
- Se informa sobre los riesgos y problemas de BCMS
- mejora continua de BCMS

2.4 Responsabilidades y Actividades

Las responsabilidades y actividades requeridas para ejecutar los Planes de BC se detallan a continuación.

El Coordinador de Continuidad de negocio (BCC) actuará como el principal punto de contacto (POC) para asuntos relacionados con BCP en el país. El BCC trabajará con la Gerencia local y las partes interesadas para establecer y mantener un Plan de BC rentable relevante a las necesidades de la unidad de negocios de conformidad con la política, en particular:

- Herramientas para registrar, interpretar e informar a TMF Group:
  - Riesgos operativos y estrategias de mitigación;
  - Actividades comerciales claves; e
  - Impactos potenciales de la pérdida financiera.
- Requisitos de recuperación
- Asistencia localizada.
- Gestión de terceros.
- Capacitación y conocimiento del personal según corresponda a sus responsabilidades de BC.

Los miembros delegados de la gestión proporcionarán:

- Información soporte para:
  - Evaluación de riesgo;
  - Análisis de impacto de negocio; y
  - Consideraciones locales específicas, legales o de otro tipo en el desarrollo, revisiones y ensayos del ERP y BCP local.
- Participación en la instrucción local al personal, capacitación y concienciación.

2.5 Pruebas, ejercicios, capacitación y conocimiento

Las acciones tomadas en las primeras horas de una interrupción significativa y / o un evento físicamente peligroso son fundamentales para determinar el resultado general. El personal deberá responder con flexibilidad a una variedad de escenarios. Por lo tanto, se proporcionará lo siguiente:

- Pruebas dirigidas para:
  - Validar planes de continuidad; y
  - Datos de contacto con miembros del personal (es decir, disposición en cascada, mensajes de emergencia, proveedores críticos, etc.).
- Miembros claves identificados del personal que forman una parte esencial del BCP del TMF Group. Este ejercicio permitirá a TMF Group:
  - Informar al personal sobre sus respectivos roles y responsabilidades;
  - Mejorar las capacidades de respuesta a incidentes, recuperación y restauración;
  - Identificar brechas en la planificación y problemas potenciales y evaluar alternativas; y

- Ejercitar al personal y obtener la aceptación de los empleados en todos los niveles de la organización.

> Identificar a las personas que reciben capacitación relacionada para:

- Proporcionar una mayor comprensión de su rol y responsabilidades específicas; y
- Garantizar la competencia en el tema del que son responsables.

> Iniciativas de concienciación para obtener una mejor visibilidad de BCM y las lecciones aprendidas.

2.6 Documentación y Mantenimiento

Para garantizar que la documentación relevante esté disponible para las partes interesadas, el BCC debe:

> Asegurarse de que las copias de ERP y BCP actualizadas sean fácilmente accesibles para:

- todos los miembros de Equipo de Dirección
- Los miembros del Equipo de soporte de Dirección
- Contactos regionales o del Grupo que apoyan el BCP

> Asegurarse de que la documentación se revise y mantenga, sobre la siguiente base:

- Revisar y actualizar anualmente la Evaluación de Riesgos e Incidentes (RIA) por parte de los propietarios del plan o cuando se produzcan cambios internos o externos importantes que podrían introducir nuevos riesgos o cambiar el nivel de los riesgos existentes;
- Revisar y actualizar el Plan de Tratamiento de Riesgos para los riesgos que no están dentro del interés de riesgo de la organización. Monitorear y garantizar que las acciones identificadas en el Plan de Tratamiento de Riesgos sean completadas por propietarios identificados según el plan;
- Revisión y actualización del Análisis del Impacto de negocio (BIA) por parte de los propietarios del plan y TI anualmente;
- Revisar y actualizar los Planes de Respuesta ante Emergencias (ERP) por parte de los propietarios del plan **por lo menos una vez al año**, o cuando haya habido un cambio significativo;
- Revisar y actualizar los BCP de los propietarios del plan **por lo menos una vez al año**, o cuando haya habido un cambio significativo;
- Prueba del sistema / proceso de mensaje de emergencia/ llamada en cascada regularmente;
- Prueba y ejercicio de los ERP de la oficina (sujeto a las regulaciones locales);
- Prueba y ejercicio del BCP de la oficina al menos una vez al año;
- Capacitación y conocimiento a nivel de oficina, país, región y grupo al menos anualmente; y
- Informe de las reuniones departamentales / de equipo / oficina sobre las disposiciones del BC, de manera continua.

> Auditoría

- Los documentos se someterán a auditoría por parte de auditores calificados para evaluar la eficacia y adecuación del programa BCMS al menos una vez cada tres años. Los resultados de la auditoría se documentarán, controlarán y abordarán mediante un plan de medidas correctivas.

- Mejora continua
  - La organización debe determinar si existen necesidades u oportunidades relacionadas con el negocio o el BCMS que deban abordarse como parte de la mejora continua, teniendo en cuenta las conclusiones del análisis y la evaluación, las no conformidades, así como los resultados de la revisión por la gerencia.

2.7 Seguridad de los empleados

> En caso de emergencia y/o evento en el extranjero que pueda requerir la evacuación de los empleados, tratamiento médico u otra forma de asistencia, TMF Group ha designado a personas autorizadas que están autorizadas para aprobar la ayuda financiera y actuar como primer punto de contacto para SOS International en caso de que se deban tomar decisiones críticas.

> Para obtener más información, consulte el portal de bienestar del TMF Group y la política de viajes y gastos..

Definiciones y Abreviaturas

TPERMINO Y DEFINICIÓN
Consejo de Administración: Gerencia del Grupo
Gerencia local: Líderes de cada país
Auditoría: Proceso sistemático, independiente y documentado para obtener pruebas de auditoría y evaluarlas objetivamente con el fin de determinar en qué medida se cumplen los criterios de auditoría.
Continuidad de Negocio (BC): Capacidad de la organización para seguir suministrando productos o servicios a niveles aceptables predefinidos tras un incidente perturbador. **(*Fuente: ISO 22301:20192; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)**
Coordinador de Continuidad de Negocio (BCC): Coordina la planificación y la implementación para la recuperación general de una organización o unidades. *(Fuente: Diario de Recuperación de Desastres (DRJ) / Instituto de Continuidad de Negocio (BCI)*
Análisis de Impacto de Negocio (BIA): Proceso de análisis del impacto a lo largo del tiempo de una perturbación en la organización. *(Fuente: ISO 22301:2019; Seguridad y Resiliencia,, Sistema de Gestión de Continuidad de Negocio)*
Competencia: Capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos. **(*Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)**
Mejora continua: Actividad recurrente para mejorar el rendimiento **(*Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)**
Conformidad: Cumplimiento de un requisito *(Fuente: ISO 22301:2019; Seguridad y Resiliencia Sistema de Gestión de Continuidad de Negocio)*
Acción correctiva: Acción para eliminar la(s) causa(s) de una no conformidad para evitar que se repita. **(*Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)**
Interrupción: Incidente, previsto o imprevisto, que provoca una desviación negativa y no planificada de la entrega prevista de productos y servicios de acuerdo con los objetivos de una organización. **(*Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)**
Eficacia: Grado de realización de las actividades previstas y de consecución de los resultados previstos **(*Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)**
Salud y Seguridad (HandS): El proceso mediante el cual se salvaguarda el bienestar de todos los empleados, contratistas, visitantes y público en general. **(*Fuente: Diario de Recuperación de Catástrofes* (DRJ))**
Impacto: Resultado de una interrupción que afecta a los objetivos

TPERMINO Y DEFINICIÓN
(*Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)
Incidente: Evento que puede ser o podría dar lugar a una interrupción, pérdida, emergencia o crisis. **Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)**
Plan de Respuesta de Emergencia (ERP): La reacción y respuesta inmediatas a una situación de emergencia centrada normalmente en garantizar la seguridad de la vida y reducir la gravedad del incidente. (*Fuente: Guía de Prácticas Profesionales del Instituto Internacional de Recuperación de Catástrofes* **(DRII))**
Plan de Continuidad de Negocio (BCP): Información documentada que guía a una organización para responder a una interrupción y reanudar, recuperar y restablecer la entrega de productos y servicios coherentes con su objetivo de Continuidad de Negocio (*Fuente: ISO 22301:20122019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio*)
Plan de Gestión de Incidentes (PGI): Plan de acción claramente definido y documentado para su uso en el momento de un incidente, que suele abarcar el personal clave, los servicios y las acciones necesarias para aplicar el proceso de gestión de incidentes. ***(Fuente: Diario de Recuperación de Catástrofes (DRJ) / Continuidad de Negocio de Incidentes (BCI))***
Plan de recuperación de la tecnología de la información en caso de catástrofe (ITDRP): documento aprobado por la dirección que define los recursos, acciones, tareas y datos necesarios para gestionar el esfuerzo de recuperación tecnológica. ***(Fuente: Diario de Recuperación de Catástrofes (DRJ))***
Crisis: Acontecimiento o situación anómala o extraordinaria que amenaza a una organización o comunidad y requiere una respuesta estratégica, adaptativa y oportuna para preservar su viabilidad e integridad. ***(Fuente: ISO 22361:2022 Seguridad y Resiliencia - Gestión de Crisis – Directrices)***
Gestión de Crisis (CM): Actividades coordinadas para liderar, dirigir y controlar una organización en relación con las crisis. ***(Fuente: ISO 22361:2022 Seguridad y Resiliencia - Gestión de Crisis - Directrices)***
Plan de Gestión de Crisis (CMP): Documento que especifica qué procedimientos y recursos asociados deben ser aplicados por quién y dónde en caso de crisis ***(Fuente: ISO 22361:2022 Seguridad y Resiliencia - Gestión de Crisis - Directrices)***
Equipo de Gestión de Crisis (CMT): Grupo de personas funcionalmente responsables de dirigir la respuesta de gestión de crisis de la organización. ***(Fuente: ISO 22361:2022 Seguridad y Resiliencia - Gestión de Crisis - Directrices)***
Alta Dirección/Gerencia: Persona o grupo de personas que dirige y controla una organización al más alto nivel ***(Fuente: ISO 22361:2022 Seguridad y Resiliencia - Gestión de Crisis - Directrices)***
Parte interesada: Persona u organización que puede afectar, verse afectada o que se percibe afectada por una decisión o actividad ***(Fuente: ISO 22361:2022 Seguridad y Resiliencia - Gestión de Crisis - Directrices)***
Monitoreo: Determinar el estado de un sistema, proceso o actividad.

TPERMINO Y DEFINICIÓN
(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)
No conformidad: Incumplimiento de un requisito *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)* **Objetivo: Resultado a alcanzar.** *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)* **Organización: Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.** *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)* **Política: Intenciones y dirección de una organización, expresadas formalmente por su alta dirección.** *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)*
Proceso: Conjunto de actividades interrelacionadas o que interactúan y que transforman insumos en productos. *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)* **Requisito: Necesidad o expectativa declarada, generalmente implícita u obligatoria.** *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)* **Recurso: Todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, locales y suministros e información (ya sea electrónica o no) que una organización tiene que tener disponible para usar, cuando sea necesario, con el fin de operar y cumplir con su objetivo** *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)* **Riesgo: Efecto de la incertidumbre sobre los objetivos** *(Fuente: ISO 22301:2019; Seguridad y Resiliencia, Sistema de Gestión de Continuidad de Negocio)*

Referencia a los documentos asociados

GUÍAS Y MANUALES RELACIONADOS
Biblioteca de Políticas de TMF Group
Política de seguridad de la información
Documentación ISMS
Guía de viajes y gastos de TMF Group

Historial de Revisiones y Registros

VERSIÓN	FECHA	AUTOR	DETALLES
1.0	09-Mar-2017	Deepak Iyer	> Primera versión Cambios realizados después de la revisión y en línea con los comentarios recibidos de BCSC
1.1	17-Ene-2019	Deepak Iyer	Revisado. Ningún cambio realizado. Adecuado para el propósito.
1.2	10-Mar-2020	Devender Kumar	Revisión anual; secciones actualizadas sobre roles y responsabilidades; cambio de Aprobador al Comité de Riesgo y Cumplimiento; actualizaciones para reflejar cambios estructurales; cambio del Responsable de la Política
1.3	22-Mar-2021	Anuj Tewari	Revisión anual; Cláusulas específicas sobre los requisitos de BIA, RA, Estrategia y BCP incluidas en la sección de Primeros Principios. Se ha eliminado el apartado 2.2 de la versión anterior
1.4	22-Jun-2022	Anuj Tewari	Revisión anual; cambios menores en Primeros Principios y Documentación y Mantenimiento
1.5	19-Jul-2023	Anuj Tewari, Ze Mei Chiang, Rohit Rajput,	Revisión anual; pequeñas actualizaciones y reformulaciones
2.0	**27-May-2024**	**Subhodh Subramanian, Darshilla Rive, Alvaro Guerrero, Rohit Rajput**	**Revisión anual; inclusión de una sección "Gerencia y Compromiso", modificaciones menores en la sección "Documentación y mantenimiento", actualización de la sección "Definición y abreviaturas".**