# Política Continuidad de Negocio

RISK MANAGEMENT

UCI

## 1. Introducción

Dado el entorno cambiante y de riesgo en el que se encuentran inmersos los activos, así como los factores externos o internos que pueden ocasionar una potencial interrupción en la continuidad del negocio de UCI, resulta de vital importancia la definición de un marco global que establezca los principios básicos que permitan implementar, gestionar y mantener continuamente la capacidad operativa de las distintas áreas de los procesos de negocio, en especial los críticos y prioritarios, ante la potencial materialización de un incidente disruptivo.

Para prever las consecuencias de estas situaciones y definir las estrategias que aseguren la continuidad de la actividad en el menor tiempo, y con el menor impacto y pérdidas posibles, se hace preciso la elaboración de un Plan de Continuidad de Negocio (PCN) que proporcione continuidad a las distintas actividades de la empresa, con el fin de:

- Asegurar, que todos los recursos conocidos y disponibles, se utilizan para recuperar la función normalizada de la actividad tras una interrupción que haya afectado a alguno de los edificios claves de la compañía.

- Proporcionar un conjunto de procedimientos que serán ejecutados para restablecer las actividades críticas lo antes posible, y con el menor impacto sobre la actividad, empleados, proveedores y clientes de la empresa.

## 2. Objeto

El objetivo principal de la presente política es la definición de directrices que den soporte al Sistema de Gestión de Continuidad de Negocio (SGCN) de UCI, implantado para asegurar una respuesta efectiva y oportuna de la organización ante una posible interrupción de su actividad, estableciendo un marco apropiado en base a las características particulares de la organización (naturaleza, escala, complejidad, criticidad de las actividades...etc.).

Adicionalmente, se pretende alcanzar una adecuada metodología que permita identificar, desarrollar, implantar, mantener, revisar y probar las medidas de continuidad necesarias que garanticen el adecuado funcionamiento de los Planes de Continuidad de Negocio, en caso de materialización de un incidente.

## 3. Ámbito de aplicación

El alcance de la Política de Continuidad de Negocio y en general del SGCN de UCI a efectos de la certificación de la Norma UNE-EN ISO 22301-2019, está constituido por todas las actividades de negocio que se desempeñan desde UCI España en su actividad de concesión de créditos hipotecarios, así como los escenarios de indisponibilidad y su impacto en las partes interesadas.

Es aplicable, a su vez, a todos los niveles y equipos implicados en el Plan de Continuidad de Negocio de UCI con independencia de su nivel jerárquico y ubicación funcional.

## 4. Referencias

El desarrollo del Sistema de Gestión de Continuidad de Negocio y la Política de Continuidad de Negocio incluida en este documento se basan en la siguiente norma:

- ISO 22301:2019 - Sistemas de Gestión de la Continuidad de Negocio

## 5. Definiciones

| Término | Descripción | Fuente |
|---|---|---|
| 3.1 actividad (activity) | Conjunto de una o más tareas con un resultado definido. | ISO 22300:2018, 3.1 |
| 3.2 auditoría (audit) | Proceso (3.26) sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría. | ISO 22301:2019 |
| 3.3 continuidad del negocio (business continuity) | Capacidad de una organización (3.21) para continuar la entrega de productos y servicios (3.27) dentro de plazos aceptables a una capacidad predefinida durante una disrupción (3.10). | ISO 22300:2018, 3.24 |
| 3.4 plan de continuidad del negocio (business continuity plan) | Información documentada (3.11) que guía a una organización (3.21) a responder a una disrupción (3.10) y reanudar, recuperar y restaurar la entrega de productos y servicios (3.27) de acuerdo con sus objetivos de continuidad del negocio (3.3) (3.20). | ISO 22300:2018, 3.27 |
| 3.5 análisis de impacto sobre el negocio (business impact análisis, BIA) | Proceso (3.26) en el que se analiza el impacto (3.13) a lo largo del tiempo de una disrupción (3.10) en la organización (3.21). | ISO 22300:2018, 3.29 |
| 3.6 competencia (competence) | Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos. | ISO 22301:2019 |
| 3.7 conformidad (conformity) | Cumplimiento de un requisito (3.28). | ISO 22301:2019 |
| 3.8 mejora continua (continual improvement) | Actividad (3.1) recurrente para mejorar el desempeño (3.23). | ISO 22301:2019 |
| 3.9 acción correctiva (corrective action) | Acción para eliminar la causa o las causas de una no conformidad (3.19) y evitar que vuelva a ocurrir. | ISO 22301:2019 |
| 3.10 disrupción (disruption) | Incidente (3.14), bien sea esperado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios (3.27) de acuerdo con los objetivos (3.20) de una organización (3.21). | ISO 22300:2018, 3.70 |
| 3.11 información documentada (documented information) | Información que una organización (3.21) tiene que controlar y mantener, y el medio que la contiene. | ISO 22301:2019 |
| 3.12 eficacia (effectiveness) | Grado en el que se realizan las actividades (3.1) planificadas y se alcanzan los resultados planificados. | ISO 22301:2019 |
| 3.13 impacto (impact) | Resultado de una disrupción (3.10) que afecte a los objetivos (3.20). | ISO 22300:2018, 3.107 |
| 3.14 incidente (incident) | Evento que puede ser, o podría llevar a una disrupción (3.10), pérdida, emergencia o crisis. | ISO 22300:2018, 3.111 |
| 3.15 parte interesada (interested party) | Persona u organización (3.21) que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad (3.1). También denominado grupo de interés o stakeholder | ISO 22301:2019 |

| Término | Descripción | Fuente |
|---|---|---|
| 3.16 sistema de gestión (management system) | Conjunto de elementos de una organización (3.21) interrelacionados o que interactúan para establecer políticas (3.24), objetivos (3.20) y procesos (3.26) para alcanzar esos objetivos. | ISO 22301:2019 |
| 3.17 medición (measurement) | Proceso (3.26) para determinar un valor. | ISO 22301:2019 |
| 3.18 seguimiento (monitoring) | Determinación del estado de un sistema, un proceso (3.26) o una actividad (3.1). | ISO 22301:2019 |
| 3.19 no conformidad (non-conformity) | Incumplimiento de un requisito (3.28). | ISO 22301:2019 |
| 3.20 objetivo (objective) | Resultado a lograr. | ISO 22301:2019 |
| 3.21 organización (organization) | Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos (3.20). | ISO 22301:2019 |
| 3.22 contratar externamente (outsource) | Establecer un acuerdo mediante el cual una organización (3.21) externa realiza parte de una función o proceso (3.26) de una organización. | ISO 22301:2019 |
| 3.23 desempeño (performance) | Resultado medible. | ISO 22301:2019 |
| 3.24 política (policy) | Intenciones y dirección de una organización (3.21), como las expresa formalmente por su alta dirección (3.31). | ISO 22301:2019 |
| 3.25 actividad prioritaria (prioritized activity) | Actividad (3.1) a la que se da urgencia para evitar impactos (3.13) inaceptables al negocio durante una disrupción (3.10). | ISO 22300:2018, 3.176 |
| 3.26 proceso (process) | Conjunto de actividades (3.1) interrelacionadas o que interactúan, que transforman los elementos de entrada en resultados. | ISO 22301:2019 |
| 3.27 producto y servicio (product and service) | Salida o resultado proporcionado por una organización (3.21) a las partes interesadas (3.15). | ISO 22300:2018, 3.181 |
| 3.28 requisito (requirement) | Necesidad o expectativa establecida, generalmente implícita u obligatoria. | ISO 22301:2019 |
| 3.29 recurso (resource) | Todos los activos (incluyendo plantas y equipos), personas, habilidades, tecnología, locales, suministros e información (bien sea electrónica o no) que una organización (3.21) tiene que tener a su disposición para utilizar, cuando sea necesario, con el fin de operar y cumplir su objetivo (3.20). | ISO 22300:2018, 3.193 |
| 3.30 riesgo (risk) | Efecto de la incertidumbre en los objetivos (3.20). | ISO 22301:2019 |
| 3.31 alta dirección (top management) | Persona o grupo de personas que dirige y controla una organización (3.21) al más alto nivel. | ISO 22301:2019 |
| Amenaza | Causa potencial de un incidente no deseado, que podría provocar daños a las personas, los bienes, un sistema u organización, el medio ambiente o la comunidad | ISO 23000 |
| Nivel de Riesgo | Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad | ISO 27001 |
| Disponibilidad | Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada | ISO 27001 |
| Evento | Ocurrencia o cambio de un conjunto particular de circunstancias | ISO 31000 |
| Consecuencia | Resultado de un evento que afecta a los objetivos | ISO 31000 |
| Proveedor | Empresa involucrada en los procesos o actividades que producen valor en la forma de productos y servicios | ISO/TS 22318 |

## 6. Principios generales

La presente Política de Continuidad de Negocio viene a plantear y determinar las directrices a tener en cuenta y por las que actuar en el SGCN de UCI para asegurar una respuesta efectiva y oportuna de la organización ante una indisponibilidad que ocasione la interrupción de su actividad, salvaguardando la prestación de sus servicios a los grupos de interés de la organización, a un nivel aceptable previamente definido.

La Política se ha establecido bajo las siguientes premisas:

- Ser apropiada al propósito de la Organización y se encuentra alineada con los objetivos estratégicos.
- Servir como Marco para establecer los objetivos de Continuidad.
- Representar el compromiso para satisfacer los requisitos aplicables, contemplados en el análisis de impacto, así como la mejora continua del SGCN.
- Estar disponible y divulgarse a las partes interesadas para su puesta en conocimiento.
- Ha de ser aprobada por el Consejo de Administración.

La organización identifica un conjunto de principios que se exponen a continuación:

- Proteger y asegurar a las personas como primera premisa y objetivo prioritario de la organización, tanto en situación normal como en situación de crisis derivada de una interrupción.
- Asegurar un alcance formal, consistente, coordinado y costo-efectivo de la disciplina de Continuidad dentro de UCI, que contemple todas las áreas, proveedores, sistemas de información y servicios críticos bajo alcance, se encuentren externalizados o no.
- Asegurar el compromiso para la implantación y mantenimiento de un SGCN que establezca y norme las acciones necesarias para minimizar el tiempo de interrupción de los productos y servicios de la organización.
- Nombrar representantes y responsables, a todo nivel de la organización, que participen en las acciones relacionadas con Continuidad de Negocio para la elaboración, implantación, revisión, prueba y actualización de los planes de continuidad. Para ello, designa un Coordinador de Continuidad, el cual contará con la autoridad y competencias adecuadas para soportar metodológicamente a la organización y asesorar al Comité de Crisis.
- Crear conciencia dentro de la organización, tanto al personal con rol activo, como al personal que no cumple con un rol específico en el esquema de continuidad de UCI. Para ello, se realizarán labores anuales que aseguren de formación y sensibilización del personal.
- Garantizar que todo el personal involucrado se encuentre informado de las responsabilidades que le correspondan.

- Mantener un plan de formación y sensibilización que permita el desarrollo de una cultura de continuidad dentro de la organización, y brinde a los responsables las habilidades y conocimientos necesarios.
- Desarrollar e implantar planes de continuidad que salvaguarden la actividad de la organización, considerando las diferentes direcciones, proveedores, sistemas, recursos, entre otros.
- Gestionar, de manera efectiva y razonable, los riesgos de continuidad de negocio que se identifiquen, a través de la implantación de controles. Asegurar la revisión periódica de los resultados, con el objetivo de descubrir posibles vulnerabilidades nuevas.
- Asegurar, siempre que sea viable, que se tomen acciones preventivas para evitar la ocurrencia o recurrencia de situaciones adversas a través de la implantación de controles.
- Mantener una estrategia que permita a la organización reaccionar y recuperarse de situaciones adversas en línea con los niveles de riesgo aceptados.
- Mantener un programa de actividades que asegure a UCI tenga la habilidad de reaccionar y recuperarse apropiadamente de situaciones adversas, en línea con los objetivos de continuidad preestablecidos.
- Mantener planes de respuesta apropiados, con claros procedimientos de escalamiento, garantizando la documentación formal de los planes de respuesta y recuperación, y a disposición de todo el personal involucrado.
- Ejercitar y probar, al menos de manera anual, los planes de continuidad desarrollados. Estos ejercicios y pruebas deberán aumentar en complejidad en el tiempo, conforme el grado de madurez de la organización vaya creciendo.
- Considerar los cambios organizacionales y otros en el entorno de UCI, y garantizar que los planes de continuidad y las estrategias implementadas se revisen cada vez que sea necesario, con una periodicidad, al menos, anual y en el que se nutra de lecciones aprendidas durante los incidentes que se hayan podido materializar, así como de las pruebas y simulacros que se lleven a cabo.
- Fomentar la mejora continua del SGCN y el alineamiento de este con las buenas prácticas aplicables a nivel internacional y en la industria.
- Siempre que sea viable, proveer de los recursos requeridos para establecer, implantar, monitorizar, revisar, mantener y mejorar la gestión de continuidad en UCI.

## 7. Roles y responsabilidades

A continuación, se presentan los principales actores en esta materia:

**Comité de Dirección**

Máximo organismo dentro de la organización, responsable de aprobar los lineamientos y objetivos de continuidad de la organización, en línea con los objetivos estratégicos de UCI. Da seguimiento a las diferentes acciones relacionadas a la implantación, mantenimiento, actualización y prueba del SGCN, además de ser responsable final de la aprobación de la Política de Continuidad, y de los proyectos e iniciativas de continuidad que se propongan.

**Comité de Crisis**

Comité que cuenta con responsabilidades clave tanto en normalidad como ante la ocurrencia de una contingencia. La estructura completa del Comité, detallada en el Plan de Gestión de Crisis, se pone en marcha ante la activación del Plan de Continuidad de Negocio (PCN). Sin embargo, las responsabilidades en normalidad recaen únicamente en aquellos miembros de esta estructura que pertenecen al Comité de Dirección.

**Coordinador de Continuidad**

Rol que contribuye en la aplicación metodológica de la gestión de CN. Es el facilitador y responsable de procurar que las actividades relacionadas con la metodología sean realizadas de manera correcta por los responsables de recuperación de la actividad de UCI. Su función principal consiste en gestionar el SGCN de forma permanente, orientado a lograr niveles de respuesta efectivos en casos de interrupción.

**Responsables de Equipos de Recuperación (EE.RR.)**

Rol que dirige la ejecución de las actividades encomendadas para la recuperación de las actividades críticas. Su función principal consiste en implantar el PCN dentro de los departamentos en su ámbito de competencia.

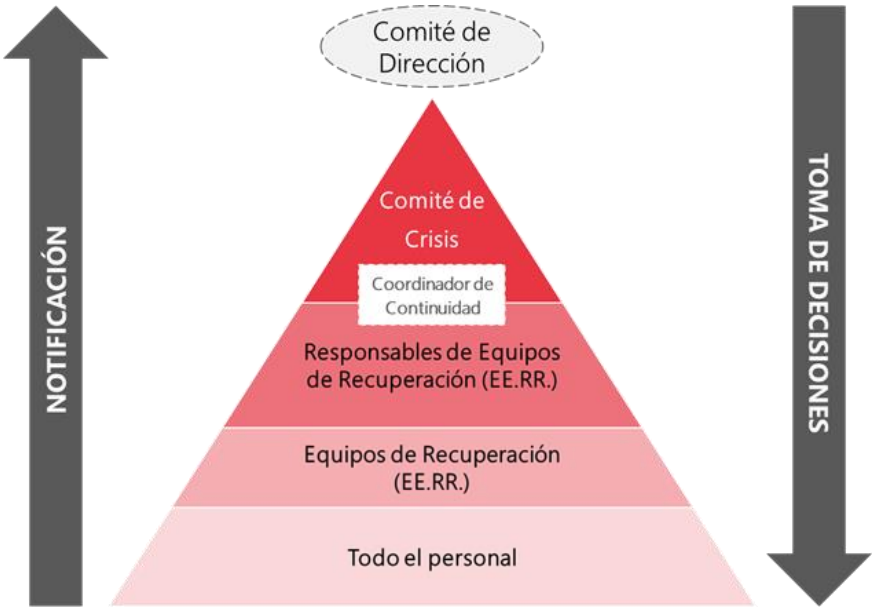
**Equipos de Recuperación (EE.RR.)**

Estos equipos son establecidos y conformados de acuerdo con las estrategias de recuperación de las actividades de la organización que están definidos en el PCN, para la recuperación de los procesos dentro de los tiempos objetivo y los niveles de operación preestablecidos.

**Todo el personal**

Todo el personal de UCI, inclusive aquellos que no tienen un rol activo en el Plan de Continuidad, deberán colaborar con las acciones y estrategias que la organización implemente para asegurar la continuidad de sus actividades críticas.

Adicionalmente, todos los empleados se encuentran en la obligación de comunicar con inmediatez y en base al procedimiento establecido, los incidentes o vulnerabilidades detectados en materia de continuidad.



Estructura organizativa de Continuidad de Negocio de UCI

## 8. Gobierno de la política de continuidad

La elaboración de esta política es responsabilidad de la función de continuidad de negocio perteneciente al Departamento de Risk Management, presentada ante la Dirección General para su aprobación y comunicada al Consejo de Administración de Unión de Créditos Inmobiliarios, S.A., EFC, órgano que en última instancia valida la política.

La política será revisada siempre que concurra cualquier circunstancia que así lo exija, como, por ejemplo, cambios normativos, directrices del regulador, cambios en la estructura de gobernanza o en el negocio.

Las modificaciones de esta política, tras la aprobación de la Dirección General, serán sometidas a la conformidad del Consejo de Administración. Los cambios no significativos serán validados por el Comité de Dirección y los significativos por el Consejo de Administración. En cualquier caso, el Consejo de Administración tendrá que validar de nuevo la política transcurridos 3 años, haya habido cambios o no y sean los mismos significativos o no.