

Norma de Continuidad de Negocio y Tecnológica

*Plan de Continuidad de Negocio y Tecnológico*

CONTROL DE DOCUMENTACIÓN

LISTA DE DISTRIBUCIÓN

|  |  |
| --- | --- |
| Nombre del destinatario | Ámbito del destinatario |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

CONTROL DE CAMBIOS DEL DOCUMENTO

|  |  |  |  |
| --- | --- | --- | --- |
| Ver. | Fecha | Descripción cambios | Páginas afectadas |
| 1.0 | Jul’2016 | Incorporación de PCT |  |
| 1.01 | 4-10-17 | Actualización Responsable PCN |  |
| 1.02 | 7-11-17 | Revisión 2017 del documento |  |
| 1.10 | 11-07-18 | Revisión 2018 del documento |  |
| 1.20 | 27-03-19 | Revisión 2019 del documento |  |
| 1.30 | 18-11-19 | Revisión 2019 S2 tras cambios orgranizativos |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Elaborado por | | Revisado por | | Aprobado por | |
| FS/SJ - SolCN | | Sr. Javier Sánchez  Sr. Santiago Uriel | | Sr. Javier Sánchez | |
| Firma | | Firma | | Firma | |
| Fecha | Noviembre 2019 | Fecha | Noviembre 2019 | Fecha | Noviembre 2019 |

ACCIONES PENDIENTES

|  |  |  |
| --- | --- | --- |
| Descripción | Responsable | Fecha objetivo |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

ÍNDICE

[1 OBJETO Y ALCANCE 4](#_Toc6214469)

[1.1 OBJETO 4](#_Toc6214470)

[1.2 ALCANCE PCN 4](#_Toc6214471)

[1.3 ALCANCE PCT 5](#_Toc6214472)

[1.4 SUPUESTOS DE LOS PLANES 6](#_Toc6214473)

[1.4.1 SUPUESTOS DEL PLAN DE CONTINUIDAD DE NEGOCIO (PCN/PCT) 6](#_Toc6214474)

[1.4.2 SUPUESTOS DEL PLAN DE CONTINUIDAD TECNOLÓGICO (PCT) 7](#_Toc6214475)

[2 DESARROLLO 8](#_Toc6214476)

[2.1 ANTECEDENTES 8](#_Toc6214477)

[2.2 RESPONSABLES DEL CUMPLIMIENTO 8](#_Toc6214478)

[2.3 NORMATIVA DE APLICACIÓN 9](#_Toc6214479)

[2.3.1 CICLO DE VIDA DEL PLAN DE CONTINUIDAD 10](#_Toc6214480)

[2.3.2 Gestión y revisión de la documentación DEL PLAN DE CONTINUIDAD DE NEGOCIO 13](#_Toc6214481)

[2.3.3 Gestión y revisión de la documentación DEL PLAN DE CONTINUIDAD TECNOLÓGICO 16](#_Toc6214482)

[2.3.4 ROLES Y RESPONSABILIDADES 18](#_Toc6214483)

[2.3.5 PlanES DE FORMACIÓN, pruebas y mantenimiento 20](#_Toc6214484)

[2.4 GLOSARIO DE TÉRMINOS 23](#_Toc6214485)

# OBJETO Y ALCANCE

## OBJETO

El objeto de la Normativa de Continuidad de Negocio y Tecnológica es desarrollar los principios de la Política de Continuidad de Negocio, así como marcar las pautas a seguir para mantener actualizado el Plan de Continuidad de Negocio (PCN) y Tecnológico (PCT) de HRE.

El presente documento es de aplicación a todos los niveles y equipos implicados en el Plan de Continuidad de Negocio y Tecnológico de HRE.

Se trata de un documento en el que se:

* Define el ciclo de vida de los Planes de Continuidad, marcando las distintas fases y las tareas a realizar en cada una de ellas.
* Definen los roles y las responsabilidades a alto nivel de los distintos actores que forman parte de los Planes de Continuidad.
* Establece un flujo de aprobación de la nueva documentación, así como los plazos para las aprobaciones y validaciones.
* Fijan los plazos máximos para la revisión de la documentación que forma parte de los Planes de Continuidad.

## ALCANCE PCN

Como desarrollo de los principios que marca la Política de Continuidad de Negocio aprobada por la Dirección de HRE, se desarrolla la presente Norma.

Los escenarios que se cubren inicialmente dentro del Plan de Continuidad de Negocio son los afectados por la "Indisponibilidad de la ubicación por inaccesibilidad o destrucción", "Indisponibilidad de información crítica por fallos en tecnología", "Indisponibilidad de recursos Humanos críticos" e "Interrupción de proveedores críticos".

A continuación, se muestran los escenarios mencionados y el período de implantación en la Compañía:

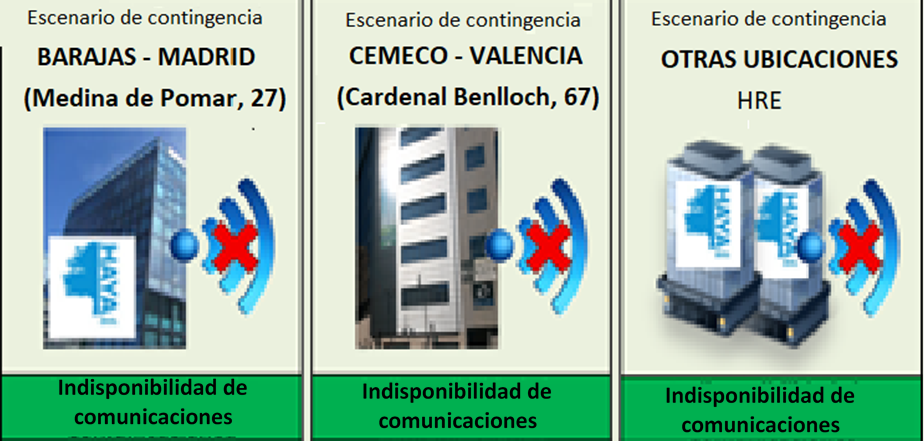


## ALCANCE PCT

Los escenarios que se cubren inicialmente dentro del Plan de Continuidad Tecnológicos quedan abarcados dentro de dos planes identificados en el mismo:

* **DRP** – Disaster Recovery Plan
* **SCP** – Site Contingency Plan

Dichos escenarios se muestran a continuación:





## SUPUESTOS DE LOS PLANES

### SUPUESTOS DEL PLAN DE CONTINUIDAD DE NEGOCIO (PCN/PCT)

El Plan de Continuidad de Negocio de HRE se ha desarrollado, partiendo como base de los siguientes supuestos:

* El Plan de Continuidad de Negocio tendrá en cuenta el peor escenario posible (en inglés “worst-case scenario”) para cada una de las contingencias contempladas, para poner en marcha las actividades críticas identificadas en caso de que la contingencia se materialice.
* No se contempla la posibilidad de que ocurran 2 contingencias simultáneas que necesiten activar el Plan de Continuidad de Negocio a la vez.
* El personal clave (directores, jefes de área, etc.) podrían no estar disponibles como consecuencia de la contingencia (para este supuesto se definirán alternativas válidas en cada caso).
* Habrá suficiente personal (propio y/o externo, fijo y/o temporal) y con los conocimientos adecuados como para poder desarrollar todas las actividades de recuperación requeridas.
* Los tiempos críticos de recuperación objetivo para cada actividad crítica de negocio se corresponden con los que se identificarán en el Análisis de Impacto de Negocio (BIA) y constituyen el intervalo temporal máximo durante el cual pueden dejar de realizarse las actividades críticas de negocio, sin que ello suponga un impacto (cuantitativo y cualitativo).
* La recuperación o re-establecimiento de las actividades críticas, se comenzará con unos requerimientos mínimos de personal y equipamientos, desde el Centro Alternativo (en el caso de contingencia de ubicación) o de la manera alternativa definida (para el resto de contingencias).
* De todos los documentos, archivos y registros vitales para implementar las actividades críticas se efectúan copias regularmente que se almacenan en un lugar alternativo.
* Las comunicaciones, ya sea telefonía móvil y fija (particular o de la empresa), funcionan una vez declarada la contingencia.
* Existe, a disposición del Comité Estratégico, del Comité Táctico y del resto de Equipos de recuperación, suficiente espacio disponible para el establecimiento de las Salas de Crisis dentro de la ubicación alternativa.

### SUPUESTOS DEL PLAN DE CONTINUIDAD TECNOLÓGICO (PCT)

El desarrollo del presente PCT se basa en una serie de premisas que han de tenerse en cuenta para entender la documentación disponible y el alcance del mismo. Los supuestos son los siguientes:

* No se contempla una contingencia total que afecte a dos CPDs de Madrid simultáneamente.
* En el Plan de Continuidad de Negocio (PCN/PCT), en caso de contingencia de la ubicación del Edificio Barajas-Madrid o del edificio CEMECO-Valencia, donde están ubicados los equipos tecnológicos, está contemplada la estrategia de recuperación de ubicaciones y sala de contingencia para cubrir al personal crítico, de manera que las actividades no se vean interrumpidas.
* HRE tiene alojados los sistemas de información que le dan soporte en diferentes CPDs: un CPD contratado en Telefónica (sistemas de información y servidor de archivos), otro en RSI (subcontratado por PFS) y un tercero en Interoute (subcontratado por Shebel).
* Existen contratos de soporte y mantenimiento con los fabricantes de los sistemas en producción, y allí donde estos no prestan el servicio directamente al cliente final, a través de partners con acreditación suficiente para poder prestar este tipo de servicios. Dichos contratos cubren los servicios 24x7 para los entornos de producción.
* Se realizan pruebas periódicas para contrastar el nivel de redundancia y respuesta ante contingencias parciales.

# DESARROLLO

## ANTECEDENTES

Para la elaboración del presente documento, se ha utilizado como material documental las siguientes referencias:

* Norma UNE 71599\_2:2010
* Norma BS 25999\_2
* Norma ISO 22301
* Norma ISO 27031
* Norma ISO 24762
* Norma ISO 27002
* Norma ISO 22317

## RESPONSABLES DEL CUMPLIMIENTO

Para la gestión de la continuidad de negocio se definirán los siguientes responsables, que serán los encargados de establecer y velar por el cumplimiento de la presente normativa:

**I. Responsable de Continuidad de Negocio y Tecnológico**

* Responsable de proporcionar la metodología de la gestión de la documentación.
* Responsable de cumplir los plazos de generación y revisión de la documentación.
* Certificar el cumplimiento de los requerimientos definidos.
* Coordinar las acciones correctoras de las pruebas.
* Actualizar la Norma de Continuidad de Negocio y Tecnológica.
* Planificar las pruebas y el mantenimiento periódico.

**II. Equipos de las Áreas Críticas de Negocio y Tecnológicas**

* Generar con la periodicidad definida toda la documentación (así como desarrollar los procedimientos operativos alternativos).
* Responsables del Contenido de la documentación.
* Poner en marcha las actividades Críticas identificadas en caso de contingencia.

**III. Coordinador/es y sustitutos de los Equipos de las Áreas Críticas de Negocio y Tecnológicas**

* Responsable de la continuidad de Negocio/Tecnológica del Área.
* Definición y realización de las pruebas y el mantenimiento.
* Puesta en marcha de las acciones de mejora tras las pruebas periódicas.
* Actualización y pruebas del Árbol de Llamadas.
* Actualización y pruebas de la Estrategia de Registros Vitales.

**IV. Comité Estratégico de Crisis**

* Declarar la situación como crítica y activar el Plan de Continuidad de Negocio/Tecnológico.
* Dirigir todas las acciones iniciales durante las primeras 72 horas siguientes al momento en que se activó el plan.
* Asegurar, tanto al principio como en el transcurso de la contingencia, que los responsables de los distintos Equipos de Negocio y/o Tecnológicos están en contacto.
* Marcar la comunicación y acciones de HRE a los proveedores, socios, accionistas, clientes y medios de comunicación.

**V. Comité Táctico de Crisis**

* Determinar si algunos impactos negativos como resultado de la contingencia advierten que se ha de activar el Plan de Continuidad de Negocio/Tecnológico.
* Informar al Comité Estratégico sobre la contingencia y/o desastre.
* Autorizar la activación de las ubicaciones alternativas para las Áreas Críticas de Negocio/Tecnológicas afectadas por la contingencia o desastre.
* Coordinar y dirigir la reacción inicial y todos los esfuerzos posteriores de HRE para restablecer la vuelta a la normalidad.
* Coordinar los medios de comunicación externos con los internos de HRE.
* Seguimiento y supervisión de actividades críticas a llevar a cabo por los Equipos de Negocio/Tecnológicos.

**VI. Comité de Continuidad de Negocio y Tecnológico**

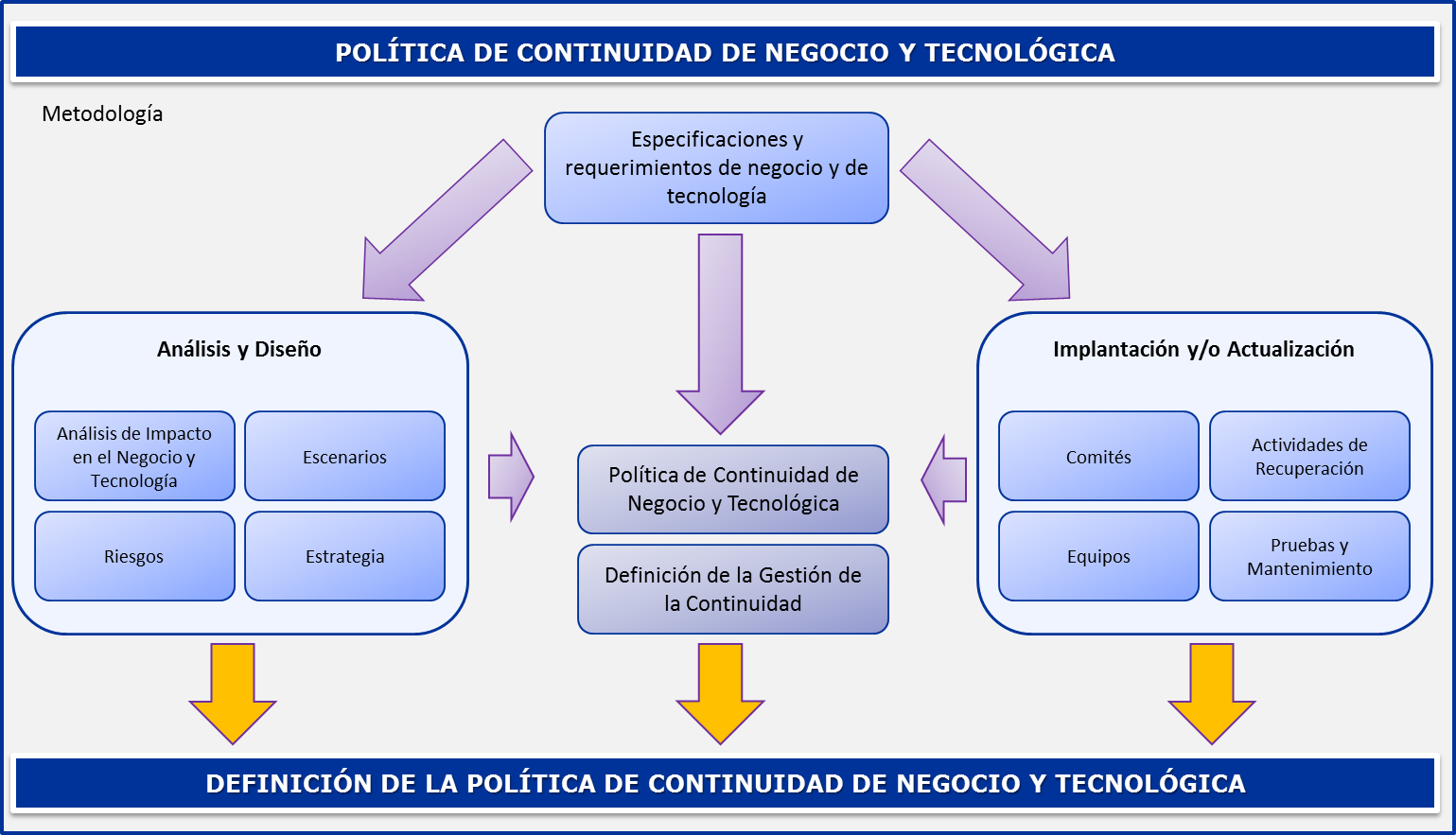
* Responsable de aprobar y actualizar la Norma de Continuidad de Negocio y Tecnológica, así como el resto de documentación general del plan.

## NORMATIVA DE APLICACIÓN

La presente Norma de Continuidad del Negocio y Tecnológica, marca las pautas a seguir para mantener actualizado el Plan de Continuidad de Negocio y Tecnológico. Éste se desarrolla en base a las Actividades Críticas (servicio o función prioritaria del día a día), esenciales para el funcionamiento normal del negocio y de la tecnología. Para más información véase el Glosario al final de este documento

Las especificaciones y requerimientos establecidos por el negocio y tecnología para la recuperación de estas actividades críticas pueden cambiar en el transcurso del tiempo, como consecuencia de cambios en la propia Organización, etc. de manera que es necesario establecer mecanismos para la revisión y actualización periódicas de los planes. El diseño de la Norma de Continuidad de Negocio y Tecnológica debe contemplar los requisitos de negocio y la tecnología asociada, sus riesgos asociados, la estrategia a desarrollar para minimizar dichos riesgos, las actividades de recuperación a llevar a cabo en caso de materializarse una crisis, etc.

En el siguiente gráfico se detalla la metodología aplicada para la implantación de la Normativa de Continuidad de Negocio:



La presente Norma define los siguientes aspectos en relación al proceso global de gestión de la continuidad de negocio:

* **Ciclo de vida del Plan de Continuidad de Negocio y Tecnológico**
* **Gestión y revisión de la documentación**
* **Roles y responsabilidades (alto nivel)**
* **Planes de formación, pruebas y mantenimiento (alto nivel)**

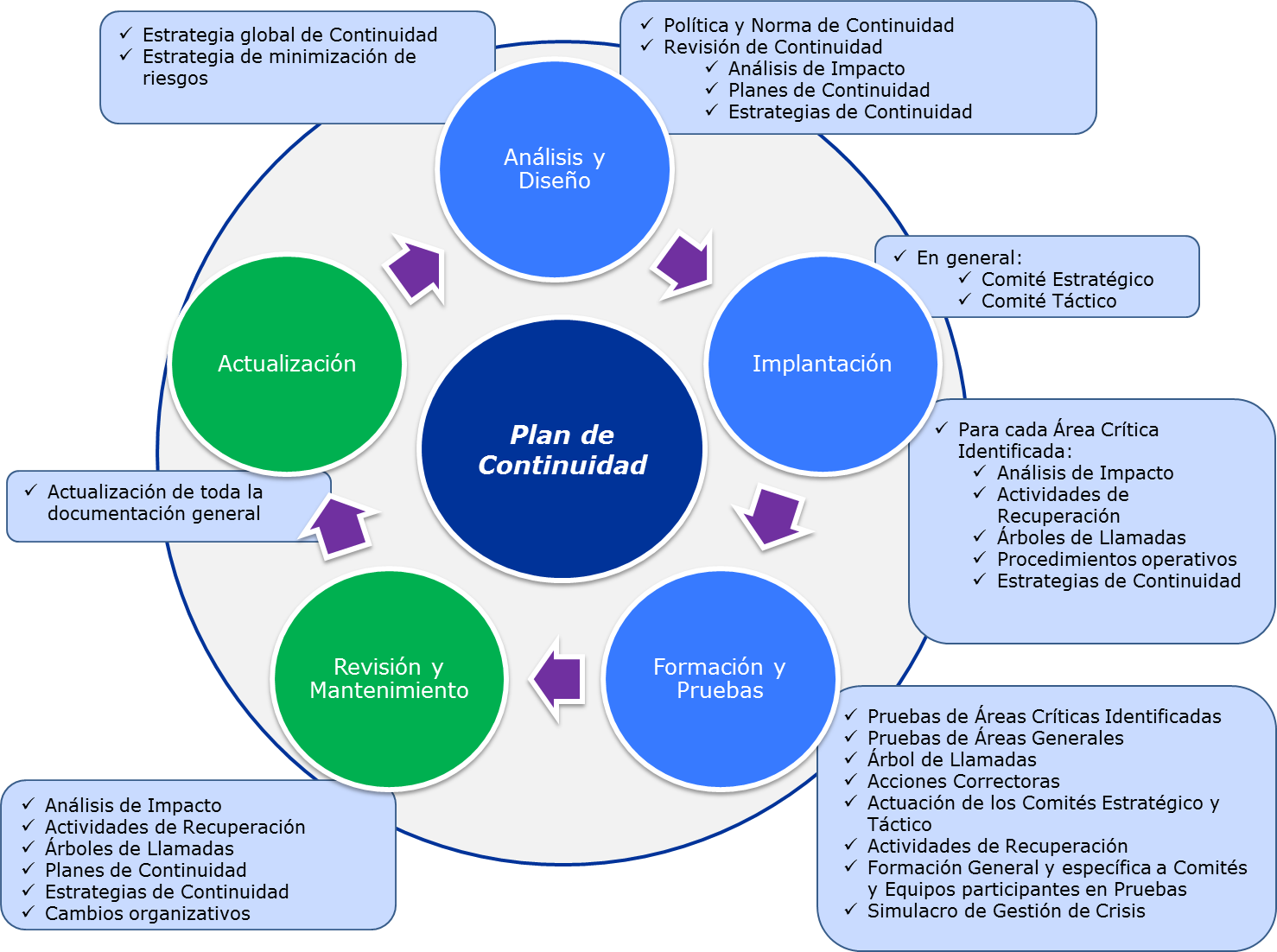
### CICLO DE VIDA DEL PLAN DE CONTINUIDAD

HRE lleva desarrollando desde el año 2015 el Plan de Continuidad de Negocio de la Compañía. Para ello, ha decidido establecer un proceso de gestión basado en el ciclo de vida de la continuidad de negocio. La elaboración de un plan de Continuidad de Negocio no acaba en la ejecución de un único proyecto que se desarrolla en un periodo de tiempo determinado, sino que se trata de **un ciclo permanente de revisión y actualización con una periodicidad determinada.** Este ciclo de mejora continua permite a HRE estar preparado en todo momento ante una posible contingencia o desastre. Siguiendo las mejores prácticas definidas por el estándar ISO22301, en cuanto a Continuidad de Negocio.

El ciclo de vida de un Plan de Continuidad se compone de cinco fases:

* Análisis y Diseño
* Implantación
* Formación y Pruebas
* Revisión y mantenimiento
* Actualización

En el siguiente esquema se muestra cada una de las acciones que se han desarrollado en cada una de las fases del ciclo de vida del Plan de Continuidad de Negocio.



De esta manera, se desarrolla y mantiene un proceso controlado para la continuidad del negocio y tecnológica en toda la organización que trata los requisitos de seguridad de la información necesarios para la continuidad del negocio de la Compañía. En cada una de las fases de realizan las actividades clave para la gestión de la continuidad de negocio y tecnológica:

**Análisis y Diseño**

* Comprender los riesgos que la organización afronta en cuanto a probabilidad y efectos en el tiempo, incluyendo la identificación y la priorización de las actividades críticas de negocio mediante un estudio del análisis de impacto en el negocio y en la tecnología.
* Identificar todos los activos que intervienen en las actividades críticas de negocio y de tecnología.
* Comprender los efectos que las interrupciones causadas por los incidentes de seguridad de la información puedan tener en el negocio y en la tecnología (es importante encontrar soluciones que traten incidentes de menor impacto, así como incidentes graves que pudieran amenazar la viabilidad de la organización) y establecer los objetivos empresariales de las instalaciones de procesamiento de la información.

**Implantación**

* Identificar y considerar la implementación de más controles preventivos o paliativos.
* Identificar suficientes recursos financieros, organizativos, técnicos y del entorno con el fin de afrontar los requisitos de seguridad de la información identificados.
* Garantizar la seguridad del personal y la protección de las instalaciones de procesamiento de la información y de las propiedades de la organización.
* Formular y documentar planes de continuidad de negocio que traten los requisitos de seguridad de la información de acuerdo con las estrategias de continuidad del negocio y tecnológica acordadas.
* Comunicar a las partes interesadas internas y equipos de gestión de las actividades de recuperación los planes de recuperación, así como las estrategias a seguir en caso de activación del plan de continuidad de negocio y tecnológico. Coordinar la activación e implantación del plan de continuidad de negocio y tecnológico con todas las partes implicadas, proveedores externos, personal interno, alta dirección, etc.

**Formación y Pruebas**

* Realizar un plan de formación con el fin de identificar los contenidos y personas implicadas en el Plan de Continuidad de Negocio y Tecnológico de forma que tengan conocimiento de la existencia y de los objetivos del mismo, sepan quiénes son todos los Responsables y Coordinadores y cómo contactar con ellos, conozcan sus responsabilidades particulares y de grupo y conozcan las actividades identificadas para las diferentes fases (Fase I: Respuesta Inicial, Fase II: Provisión de Recursos, Fase III: Reanudación de Operaciones y Fase IV: Vuelta a la Normalidad)
* Probar y actualizar periódicamente los planes y las funciones que se apliquen.
* Además, es necesario, incorporar las lecciones aprendidas en los planes de recuperación, para poder hacer frente a situaciones futuras en caso de ser necesario.

**Revisión y mantenimiento**

* Garantizar que la gestión de la continuidad del negocio y tecnológica se incorpora a las funciones y la estructura de la organización.

**Actualización**

* La responsabilidad del proceso de gestión de la continuidad del negocio y tecnológica debería recaer en un nivel adecuado dentro de la organización para mantener siempre actualizada la documentación y garantizar así la vigencia del plan.

En definitiva, para que la Organización alcance un grado de madurez óptimo en relación a sus necesidades, será necesaria la ejecución de varios ciclos completos (Análisis y Diseño – Implantación - Formación y pruebas – Revisión y mantenimiento – Actualización) a través de los cuales se irá aproximando, de forma progresiva, hacia el nivel deseado en términos de gestión de la continuidad de negocio y tecnológica.

En la estrategia planteada por los Planes de Continuidad por parte de HRE, determina un único marco de referencia, de manera que se garantice que todos los planes parciales son consistentes y así dirigir de una manera coherente los requisitos de seguridad de la información, e identificar las prioridades para las pruebas y el mantenimiento.

### Gestión y revisión de la documentación DEL PLAN DE CONTINUIDAD DE NEGOCIO

A continuación, se muestra el listado de los documentos entregados que forman el Plan de continuidad de negocio de HRE:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Carpeta** | **Nombre del documento** | **Descripción del documento** | **Tipo** | **F. Actualización** |
| 01. Mantenimiento BIA, AcR, ALL | XX. HRE\_PCN\_ BIA\_Equipo | Análisis de Impacto de Negocio-BIA (uno por equipo XX) | Excel | Noviembre 2019 |
| 01. Mantenimiento BIA, AcR, ALL | XX. HRE\_PCN\_ AcR\_Equipo | Actividades de Recuperación-AcR (uno por equipo XX) | Excel | Marzo 2019 |
| 01. Mantenimiento BIA, AcR, ALL y 02. Estrategias de Continuidad | Cada pack de archivos BIA + AcR por equipo + Árbol de llamadas global | Planes de Continuidad de Negocio | Word | Noviembre 2019 |
| 02. Estrategias de Continuidad | 08. HRE\_PCN\_Alcance y estrategias de continuidad | Estrategias de Continuidad de infraestructuras, RRHH | Word | Marzo 2019 |
| 02. Estrategias de Continuidad | 00. HRE\_PCN\_ALL\_Árbol de Llamadas | Árboles de Llamadas Global-ALL | Excel | Noviembre 2019 |
| 02. Estrategias de Continuidad | 08. HRE\_PCN\_Protocolo de SAREB y HRE en caso de Contingencia de HRE | Protocolo de SAREB y HRE en caso de Contingencia de HRE | Word | Noviembre 2019 |
| 02. Estrategias de Continuidad | Protocolos escenarios de contingencia HRE-Sareb | 7 planes de contingencia según los escenarios definidos | Word | Diciembre 2016 |
| 02. Estrategias de Continuidad | 11. HRE\_PCN\_Estrategia de Comunicación Corporativa (2 ficheros) | Estrategia de Comunicación Corporativa en Contingencia (Interna y Externa) | Word | Marzo 2019 |
| 02. Estrategias de Continuidad | 11. HRE\_PCN\_Protocolo de Valija y documentación de contingencia en sites | Estrategia de redirección de valija y de documentación física en sites alternativos | Word | Marzo 2019 |
| 03. Análisis de Riesgos | 07. HRE\_PCN\_AR\_Amenazas | Análisis de riesgos - Amenazas | Excel | Noviembre 2017 |
| 03. Análisis de Riesgos | 07. HRE\_PCN\_AR\_Salvaguardas | Análisis de riesgos - Salvaguardas | Excel | Noviembre 2017 |
| 04. Plan FPM | 12. HRE\_PCN\_Plan de Pruebas | Plan de Pruebas | Word | Marzo 2019 |
| 04. Plan FPM | 12. HRE\_PCN\_Plan de Mantenimiento | Plan de Mantenimiento | Word | Noviembre 2019 |
| 04. Plan FPM | 16. HRE\_PCN\_Plan de Formación | Plan de Formación | Word | Marzo 2019 |
| 05. Pre-Formación y Pruebas | Varios ficheros de formación para los distintos roles | Formación en Continuidad de Negocio para los distintos roles | PPT | Abril-Mayo 2018 |
| 06. Formación y Pruebas | 00. HRE\_PCN\_Modelo Pruebas\_Equipo | Pruebas de Continuidad de Negocio | Varios | Abril-Mayo 2018 |
| 08. Implantación SGCN | 05. HRE\_PCN\_Política Continuidad de Negocio | Política de Continuidad de Negocio | Word | Marzo 2019 |
| 08. Implantación SGCN | 05. HRE\_PCN\_Norma sobre la Continuidad de Negocio y Tecnológica | Norma de Continuidad de Negocio y Tecnológica | Word | Noviembre 2019 |
| 08. Implantación SGCN | 05. HRE\_PCN\_Roles y Responsabilidades de los Equipos participantes en el PCN | Roles y Responsabilidades de los Equipos participantes en el PCN | Word | Noviembre 2019 |
| 08. Implantación SGCN | 09. HRE\_PCN\_Guía del Comité Táctico de Continuidad de Negocio | Guía de los Comités de Gestión de Crisis | Word | Noviembre 2019 |
| 08. Implantación SGCN | 17. HRE\_PCN\_Guía para responsables y coordinadores CAN-BCAN | Guía para Responsables, CAN y BCAN PCN | Word | Noviembre 2019 |
| 09. Informes | 06. HRE\_PCN\_Resumen Ejecutivo BIA | Resumen Ejecutivo BIA | Word | Noviembre 2019 |
| 09. Informes | 07. HRE\_PCN\_Resumen Ejecutivo Riesgos | Resumen Ejecutivo Riesgos | Word | Noviembre 2017 |
| 09. Informes | 14. HRE\_PCN\_Informe Formación y Pruebas | Informe de Resultados de Formación y Pruebas de Continuidad de Negocio | PowerPoint | Julio 2019 |
| 09. Informes | 14. HRE\_PCN\_Informe Simulacro | Informe de Resultados de Simulacros de Continuidad de Negocio | PowerPoint | Noviembre 2019 |
| 09. Informes | 03. HRE\_PCN\_Informe Final PCN | Informe del Plan de Continuidad de Negocio de Haya Real Estate | PowerPoint | Noviembre 2019 |
| 09. Informes | 38. HRE\_PCN\_Análisis diferencial ISO22301 | Análisis diferencial ISO22301 | Word | Noviembre 2019 |

**Documentación utilizada en situación de normalidad y contingencia**

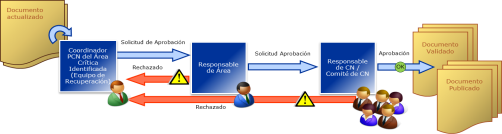
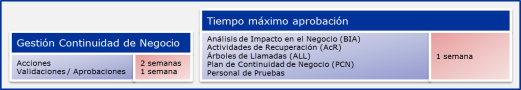


En la gestión del plan de continuidad de negocio, toda aquella documentación que se genera necesita de una revisión y validación por parte del responsable inmediato del Área Crítica de Negocio y del Responsable de la Continuidad de Negocio definidos. La frecuencia de estas revisiones se deberá de ajustar en la fase de pruebas y mantenimiento para que se adecuen a la dinámica del PCN establecida por parte de HRE.

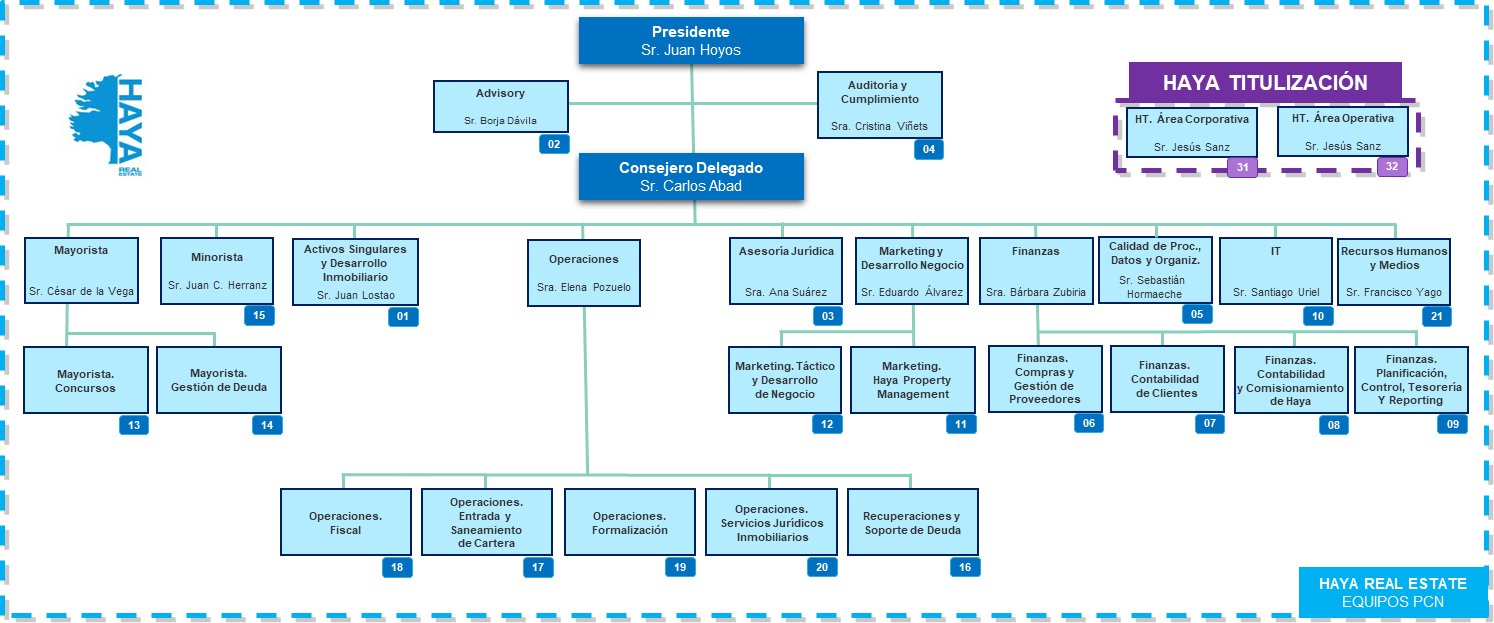
Como recomendación de la frecuencia con la que se deben revisar los documentos para garantizar la actualización del Plan ante cambios de la organización y asegurar la Continuidad del Negocio, la siguiente tabla indica las frecuencias asociadas a cada uno de los documentos:

|  |  |
| --- | --- |
| **Descripción del documento** | **Periodicidad (Mto. programado)** |
| Análisis de Impacto de Negocio-BIA (uno por equipo XX) | Semestral |
| Actividades de Recuperación-AcR (uno por equipo XX) | Anual |
| Árboles de Llamadas-ALL (uno por equipo XX) | Trimestral |
| Análisis de Riesgos de Funciones y Recursos-AR (uno por equipo XX) | Anual |
| Análisis de Riesgos - Amenazas | Anual |
| Análisis de Riesgos - Salvaguardas | Anual |
| Guía de los Comités Estratégico y Táctico | Anual |
| Guía para Responsables, CAN y BCAN PCN | Anual |
| Estrategias y Protocolos de Continuidad | Anual |
| Plan de Comunicación de Crisis | Anual |
| Política de Continuidad de Negocio | Anual |
| Norma de Continuidad de Negocio y Tecnológica | Anual |
| Roles y Responsabilidades de los Equipos participantes en el PCN | Anual |
| Plan de Pruebas | Anual |
| Plan de Mantenimiento | Anual |
| Plan de Formación | Anual |

Como proceso de control de cambios y gestión de la actualización, el siguiente gráfico propone el circuito de aprobación de la nueva documentación (o actualización) generada por parte de los responsables, así como la frecuencia que tiene cada uno de los aspectos de la gestión de la documentación y seguimiento de las estrategias de continuidad de Negocio.



A continuación, se muestra la estructura jerárquica de HRE con los equipos identificados en el Plan de Continuidad de Negocio y sus responsables de área:



### Gestión y revisión de la documentación DEL PLAN DE CONTINUIDAD TECNOLÓGICO

A continuación, se muestra el listado de los documentos entregados que forman el Plan de continuidad tecnológico de HRE:

| **Carpeta** | **Nombre del documento** | **Descripción del documento** |
| --- | --- | --- |
| 01. General | 00. HRE\_PCN\_PCT\_Guía de los Comités de Gestión de Crisis | Guía de los Comités de Gestión de Crisis |
| 01. General | 00. HRE\_PCN\_PCT\_Norma sobre la Continuidad de Negocio y Tecnológica | Norma sobre la Continuidad de Negocio y Tecnológica |
| 01. General | 00. HRE\_PCT\_Acciones puesta en marcha ante situaciones de contingencia | Acciones puesta en marcha ante situaciones de contingencia |
| 01. General | 00. HRE\_PCT\_Amenazas y escenarios cubiertos | Amenazas y escenarios cubiertos del PCT |
| 01. General | 00. HRE\_PCT\_Documentación Plan de Continuidad Tecnológico | Documentación asociada al Plan de Continuidad Tecnológico |
| 01. General | 00. HRE\_PCT\_Plan de Formación, Pruebas, Mantenimiento y Actualización | Plan de Formación, Pruebas, Mantenimiento y Actualización |
| 02. Estructura Organizativa PCT | 00. HRE\_PCT\_Estructura organizativa en contingencia | Estructura organizativa en contingencia de HRE |
| 03. Equipos PCT | XX. HRE\_PCT\_Funciones\_Equipo tecnológico | Funciones de los equipos tecnológicos (1 excel por cada equipo) |
| 04. Documentación Técnica | 00. HRE\_PCT\_Afectación y Seguimiento Secuencias de Recuperación | Afectación y Seguimiento Secuencias de Recuperación |
| 04. Documentación Técnica | 00. HRE\_PCT\_Infraestructura Tecnológica | Infraestructura Tecnológica HRE |
| 04. Documentación Técnica | 00. HRE\_PCT\_Tipos de Contigencias de los Sistemas de Información | Tipos de Contigencias de los Sistemas de Información |
| 04. Documentación Técnica | XX. HRE\_PCT\_Diagrama de flujo\_Secuencia de recuperación | Diagrama de flujo de la secuencia de recuperación (1 visio por secuencia) |
| 04. Documentación Técnica | XX. HRE\_PCT\_Sistemas de Información\_sistema\_Esquema | Esquema del sistema de información (1 ppt por sistema de información) |
| 04. Documentación Técnica | 00. HRE\_PCT\_Protocolo ante Indisponibilidad de Comunicaciones en Sites | Protocolo ante Indisponibilidad de Comunicaciones en Sites |
| 04. Documentación Técnica | 00. HRE\_PCT\_Protocolo ante Indisponibilidad y-o destrucción de CPDs de Madrid | Protocolo ante Indisponibilidad y-o destrucción de CPDs de Madrid |
| 04. Documentación Técnica | 00. HRE\_PCT\_Protocolo de Secuencias de Recuperación de Comunicaciones (voz y datos) | Protocolo de Secuencias de Recuperación de Comunicaciones (voz y datos) |
| 04. Documentación Técnica | 00. HRE\_PCT\_Protocolo de Secuencias de Recuperación de los Sistemas de Información | Protocolo de Secuencias de Recuperación de los Sistemas de Información |
| 04. Documentación Técnica | XX. HRE\_PCT\_Sec\_Recuperación ante contingencia | Secuencia de recuperación de la contingencia identificada (1 word por cada secuencia) |
| 05. Proveedores | XX. Documentación referente a contratos y tecnología de proveedores críticos tecnológicos | Documentación referente a contratos y tecnología de proveedores críticos tecnológicos |
| 06. Contactos | 00. HRE\_PCT\_Información Miembros Comités, Negocio, Soporte, Tecnológico y Com.Clientes | Información Miembros Comités, Negocio, Soporte, Tecnológico y Com.Clientes |
| 07. Anexos | Varios anexos de soporte utilizados para la elaboración del PCT | Varios anexos de soporte utilizados para la elaboración del PCT |
| 08. Pruebas | 00. HRE\_PCT\_Alcance y Seguimiento Pruebas | Alcance y Seguimiento Pruebas |
| 08. Pruebas | 00. HRE\_PCT\_Consolidado Resultados Participantes Pruebas | Consolidado Resultados Participantes Pruebas |
| 08. Pruebas | 00. HRE\_PCT\_Planteamiento pruebas PCT | Planteamiento pruebas PCT |
| 08. Pruebas | 00. HRE\_PCT\_Prueba\_XXXX\_Participante | Modelo de pruebas PCT para participantes (1 excel para cada participante) |
| 09. Informes | 00. HRE\_PCT\_CP-DRP-SCP | Disaster Recovery Plan y Site Contingency Plan de HRE |
| 09. Informes | 00. HRE\_PCT\_Informe Final PCT | Informe Final del PCT |

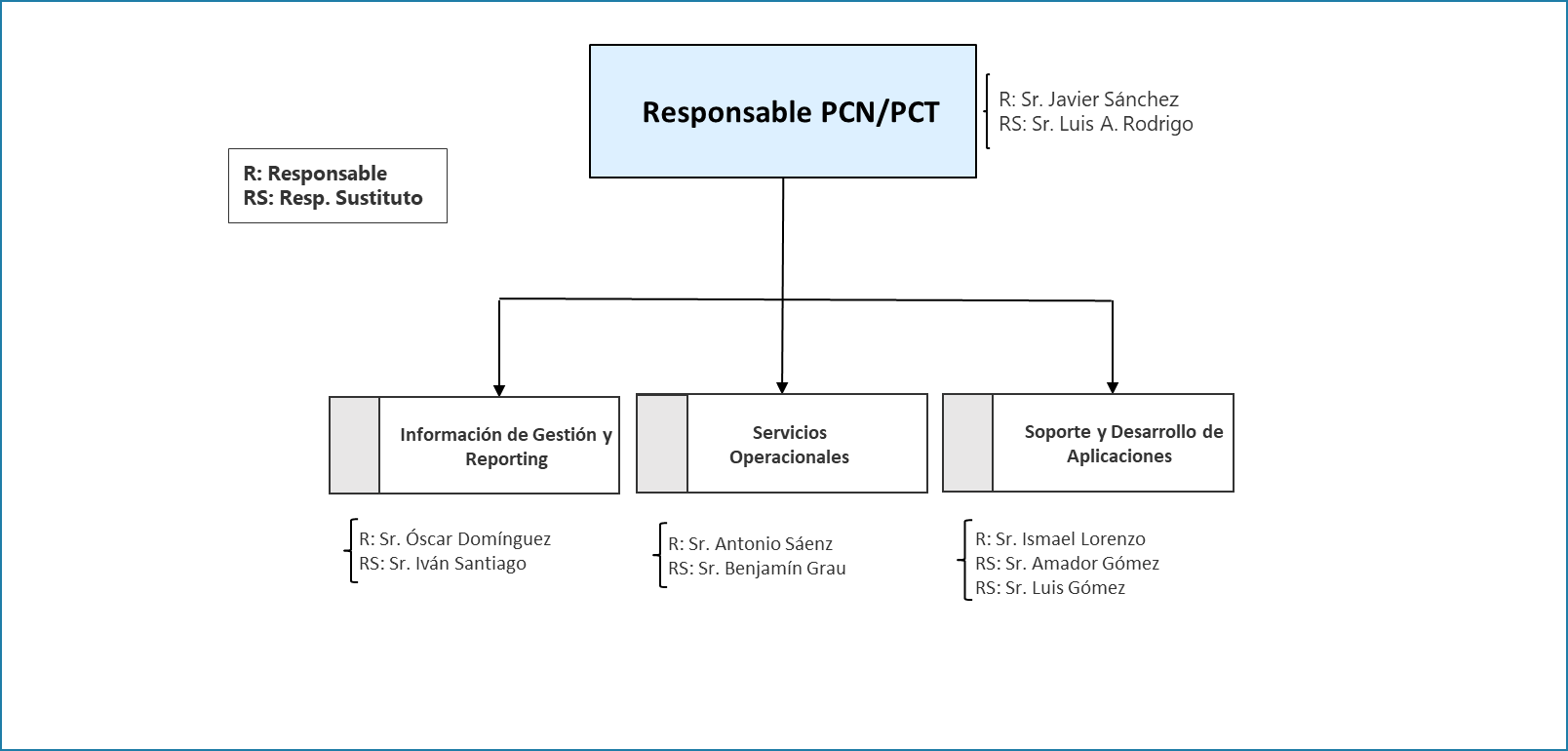
**Documentación utilizada en situación de normalidad y contingencia**



En la gestión del plan de continuidad tecnológico, toda aquella documentación que se genera necesita de una revisión y validación por parte del responsable inmediato del Área Crítica Tecnológica y del Responsable de la Continuidad Tecnológica definidos. La frecuencia de estas revisiones se deberá de ajustar en la fase de pruebas y mantenimiento para que se adecuen a la dinámica del PCT establecida por parte de HRE.

Como recomendación de la frecuencia con la que se deben revisar los documentos para garantizar la actualización del Plan ante cambios de la organización y asegurar la Continuidad Tecnológica es **anual.**

A continuación, se muestra la estructura jerárquica de HRE con los equipos identificados en el Plan de Continuidad Tecnológico y sus coordinadores:



### ROLES Y RESPONSABILIDADES

Para el correcto funcionamiento del plan de continuidad de negocio es necesario definir una serie de responsabilidades y roles asociado a la gestión del ciclo de vida del Plan. Se recomiendan los siguientes roles para HRE:

* **Comité Estratégico de Gestión de Crisis:** Se define un Comité de Gestión de Crisis Estratégico para la Compañía.
* **Comité Táctico de Gestión de Crisis:** Se define un Comité de Gestión de Crisis Táctico para la Compañía.
* **Comité Táctico Tecnológico:** Se define un Comité de Gestión de Crisis Táctico Tecnológico para la Compañía.
* **Responsable de Continuidad de Negocio de HRE:** Se define un responsable único para todas las Áreas de la Compañía.
* **Responsable del Equipo del Área Crítica de Negocio/Tecnológica:** Persona responsable jerárquicamente de diversas Áreas de Negocio, en algunos casos el Coordinador del Área Crítica de Negocio y el responsable son la misma persona.
* **Coordinador/es del Equipo del Área Crítica de Negocio/Tecnológica (CAN):** Persona/s identificada/s como responsable/s del Área de Gestión encargada de completar la información del cuestionario de continuidad de Negocio/Tecnológica en General.
* **Backup/s (sustituto/s) del Coordinador del Equipo del Área Crítica de Negocio/Tecnológica (BCAN):** Persona/s sustituta/s del Coordinador del Área Crítica de Negocio/Tecnológica.
* **Personal de Pruebas:** Personal encargado de planificar, ejecutar y elaborar las acciones correctoras.
* **Auditoría**: Responsable de la revisión de los plazos de ejecución de las diferentes actividades del ciclo de vida.
* **El resto del Personal de la Organización:** Todas las personas de la organización deben de conocer las estrategias de continuidad y las normas existentes relacionadas con el Plan de Continuidad de Negocio y Tecnológico.

A continuación, se especifican las principales responsabilidades de cada uno de estos roles en referencia a la Continuidad del Negocio y Tecnológica dentro de HRE:

* **Comité Estratégico de Gestión de Crisis:** 
  + Activar el Plan de Continuidad de Negocio/Tecnológico.
  + Autorizar la activación de las ubicaciones alternativas para las Áreas Críticas de Negocio/Tecnológicas afectadas por la contingencia o desastre.
  + Coordinar y dirigir la reacción inicial y todos los esfuerzos posteriores de HRE para restablecer la vuelta a la normalidad.
  + Coordinar los medios de comunicación externos con los internos de HRE.
  + Dirigir todas las acciones iniciales durante las primeras 72 horas siguientes al momento en que se activó el plan.
* **Comité Táctico (o Táctico Tecnológico) de Gestión de Crisis:**
  + Evaluar la situación de la contingencia.
  + Declarar la situación como crítica y activar al Comité Estratégico de Gestión de Crisis.
  + Seguimiento y supervisión de actividades críticas a llevar a cabo por los Equipos de las Áreas Críticas de Negocio/Tecnológicas.
* **Comité de Continuidad de Negocio:** 
  + Aprueba la Norma de Continuidad de Negocio y Tecnológica.
* **Responsable de Continuidad de Negocio/Tecnológica de HRE:**
  + Generar Norma, Plan de Pruebas e Informe de pruebas.
  + Valida y publica el BIA, Funciones Críticas y en Contingencia, Actividades de Recuperación, Árboles de llamadas y Estrategias de Continuidad.
  + Publica manuales.
  + Utiliza toda la información en general.
  + Gestiona la elaboración de seminarios cursos y workshops.
  + Coordina el seguimiento de acciones correctoras globales.
* **Responsable del Área Crítica de Negocio/Tecnológica:** 
  + Utiliza toda la información en general.
  + Asigna Coordinador/es al Área Crítica de Negocio/Tecnológica (CAN) y Backup/sustituto/s (BCAN).
  + Valida toda la documentación PCN del Área Crítica de Negocio/Tecnológica.
  + Conoce las estrategias de continuidad.
* **Coordinador/es del Área Crítica de Negocio/Tecnológica (CAN) y Backup/Sustituto/s (BCAN):** 
  + Genera BIA (Análisis de Impacto en el Negocio), Funciones Críticas y en Contingencia, Actividades de Recuperación, Modelo de Valor del Análisis de Riesgos y Árbol de llamadas.
  + Participa en pruebas.
  + Utiliza toda la información en general.
  + Recibe formación.
  + Coordina la recuperación de las actividades críticas de Negocio/Tecnológicas.
  + Realiza el seguimiento de acciones correctoras de Negocio/Tecnológicas.
* **Personal de Pruebas:** 
  + Utilizan las Estrategias de Continuidad, plan de pruebas.
  + Participan y validan las pruebas periódicas.
  + Reciben información del plan de pruebas.
  + Conocen la normativa de los Planes de Continuidad.
* **Auditoría:** 
  + Evaluación del Modelo de Gestión de Continuidad de Negocio/Tecnológica.
  + Revisión de los documentos de Continuidad de Negocio/Tecnológica generados.
  + Informar a los Comités Estratégico y Táctico y coordinación de la Seguridad de la Información de los aspectos que puedan ser relevantes.
* **El resto del Personal de la Organización:**
  + Conocen las Estrategias de Continuidad.
  + Conocen la normativa del Plan de Continuidad de Negocio y Tecnológico.

### PlanES DE FORMACIÓN, pruebas y mantenimiento

Las diferentes áreas y sus responsables deben de tener en cuenta las siguientes directrices generales para realizar las pruebas y el mantenimiento del Plan de Continuidad de Negocio y Tecnológico.

Existen tres documentos específicos que recogen el detalle de estos planes, con el fin de asegurar el éxito de dichos Planes:

* Formación
* Pruebas periódicas y simulacros de gestión de crisis
* Mantenimiento



**Formación**

El objetivo principal del “Plan de Formación” es identificar los contenidos y personas implicadas en los Planes de Continuidad de forma que:

* Tengan conocimiento de la existencia del Plan de Continuidad de Negocio y Tecnológico y de los objetivos del mismo.
* Sepan quiénes son todos los Responsables y Coordinadores y cómo contactar con ellos.
* Conozcan sus responsabilidades particulares y de grupo.
* Conozcan las actividades identificadas en el Plan de Continuidad para las diferentes fases (Fase I: Respuesta Inicial, Fase II: Provisión de Recursos, Fase III: Reanudación de Operaciones y Fase IV: Vuelta a la Normalidad)

Se establece que debe formarse a todo el personal de la Compañía según sus responsabilidades en un período de 2 años.

**Pruebas periódicas y simulacros de gestión de crisis**

Deben de incluir la evaluación y los procedimientos operativos alternativos, así como validar los tipos de respuesta de las actividades críticas y la información asociada teniendo en cuenta:

* Verificar los flujos de entrada y de salida de la información.
* Probar todas las aplicaciones y sistemas identificados como críticos.
* Implicar en las pruebas a los responsables de las Áreas Críticas de Negocio y Tecnológicas y a los miembros de los mismos que necesiten más entrenamiento y preparación para llegar a un nivel aceptable de familiaridad con sus responsabilidades dentro del proceso de Recuperación de su Equipo.
* Asegurar que el escenario de la prueba, plantea la indisponibilidad, no solo de recursos tecnológicos, sino de registros vitales necesarios para la iniciación de las actividades de negocio de las Áreas Críticas de Negocio y Tecnológicas afectadas para la eventual contingencia.
* Garantizar que solo se utilizan los recursos disponibles desde el Centro Alternativo o Hot Sites de los proveedores tecnológicos, para verificar la disponibilidad de todos los recursos críticos desde una ubicación diferente de la que surja la contingencia o desastre.
* Probar nuevamente componentes del Plan que tuvieron deficiencias de recuperación en anteriores pruebas.
* Preparar y entrenar a los Comités Estratégico y Táctico, los Equipos de Negocio y Tecnológicos, Soporte y Comunicación Corporativa para una posible contingencia.
* Garantizar la óptima comunicación entre los Comités Estratégico y Táctico y los Equipos de Negocio y Tecnológicos, Soporte y Comunicación Corporativa.

Se tendrán que probar todos los escenarios abarcados por el Plan de Continuidad de Negocio y Tecnológico de forma rotativa en un período de 3 años, así como participar en las mismas todo el personal identificado como crítico.

**Mantenimiento**

Las acciones que se tienen que llevar a cabo para realizar el mantenimiento son:

* Contactar y planificar reuniones con los interlocutores adecuados que desarrollen un papel clave en el proceso de recuperación (responsables de las Áreas Críticas), con la finalidad de garantizar que cada uno de ellos está adquiriendo la responsabilidad del mantenimiento de la documentación generada.
* Revisar toda la documentación de las pruebas y actualizar el PCN/PCT para mostrar la situación real de cada uno de los Equipos de Negocio y Tecnológicos críticos implicados en los Planes. Dichos Planes deberán de actualizarse, como mínimo anualmente. Cualquier componente individual de los Planes que sea probado con una periodicidad inferior a un año necesitará una tarea de mantenimiento más frecuente para garantizar que los Planes estén totalmente actualizados.
* El mantenimiento de los Planes de Continuidad es necesario para garantizar que los planes de las diferentes Áreas Críticas implicadas en las Estrategias de Continuidad de la Compañía se mantengan actualizados. El mantenimiento regular asegura que los Planes de Continuidad responden a las necesidades de los requerimientos de cada una de las Áreas Críticas de Negocio y Tecnológicas.

Existen dos tipos de mantenimiento: **regular programado** y **no programado**:

* El **mantenimiento regular programado (anual)** contempla la conducta de las revisiones del PCN/PCT para facilitar la detección de Cambios, que podrían impactar significativamente en el actual proceso del Plan de Recuperación. Estas revisiones se centran en situaciones conocidas que han ocurrido para asegurar que las actualizaciones se han incorporado a la documentación de los Planes de Continuidad.
* El **mantenimiento no programado** es necesario cuando se obtienen resultados de situaciones específicas no planificadas. **Estas revisiones se realizarán cuando se produzcan las siguientes situaciones:**
  + Cambios organizativos y/o de los coordinadores (o de sus sustitutos) de las áreas críticas.
  + Cambios después de las pruebas periódicas.
  + Cambios en los sistemas operativos o utilidades de programas.
  + Cambios en el diseño de las bases de datos de aplicaciones de producción.
  + Cambios en el diseño de la red de comunicaciones (voz y datos).
  + Cambios en los elementos externos de las instalaciones de las Ubicaciones Alternativos y material de instalación.
  + Resultados de las evaluaciones periódicas del impacto en el Negocio/Tecnología que podrían necesitar modificaciones en la prioridad de restauración de los procesos y/o sistemas.
  + Cambios en las Áreas Críticas de Negocio/Tecnológicas identificadas, Equipos de Soporte y/o en su personal.
  + Cambios en los requerimientos mínimos de las Ubicaciones Alternativas.
  + Nuevas Aplicaciones desarrolladas o compradas.
  + Cambios en los vendedores y/o proveedores del servicio.
  + En general, después de cualquier cambio de documentación en el PCN/PCT.

## GLOSARIO DE TÉRMINOS

* **Actividad Crítica**: Servicio o función prioritaria llevada a cabo en la empresa cuya parada, más allá de unas franjas de tiempo determinadas (4h, 24h, etc.), supone un impacto económico y/o de imagen muy grave para la compañía.
* **Actividad de Recuperación**: Descripción de las acciones que un equipo debe llevar a cabo con un fin concreto dentro de la secuencia de tareas que el Plan de Continuidad contempla para la recuperación de las actividades críticas.
* **Amenaza:** causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
* **Análisis de Impacto en el Negocio (AIN):** Procesos de análisis de funciones de negocio y el efecto que una interrupción de negocio podría tener en dichas funciones.
* **Árbol de Llamada**: Listado con los datos de contacto de los responsables, el personal crítico y los sustitutos de un área del Plan de Continuidad.
* **BIA**: Documento de trabajo en el que se determinan las actividades críticas, los impactos de su parada, las personas y los recursos críticos (equipamientos y sistemas) que la compañía necesita para proceder su la recuperación. Normalmente se crea uno por unidad/departamento/Área de Negocio.
* **Comité de Continuidad de Negocio:** Equipo normalmente formado por Altos Directivos de la Organización, que son responsables últimos de la Gestión de la Continuidad de Negocio y movilizan los recursos necesarios para su correcta ejecución.
* **Continuidad de Negocio**: Capacidad estratégica y táctica de la organización de planificar y responder ante incidentes e interrupciones para continuar las operaciones de negocio en un nivel aceptable predefinido.
* **Backup/sustituto del Coordinador PCN del Área Crítica de Negocio/Tecnológica (BCAN) persona** que, en ausencia del Coordinador del PCN del Área, colabora en todas las cuestiones relacionadas con el Plan de Continuidad, hasta que el Coordinador está disponible de nuevo.
* **Coordinador PCN del Área Crítica de Negocio/Tecnológica (CAN):** Persona/s identificada/s como responsable/s del Área de Gestión encargada de completar la información del cuestionario de continuidad en general.
* **Ciclo de Vida de Gestión de Continuidad**: Serie de actividades de continuidad de negocio/tecnológica que cubren todos los aspectos y fases del programa de gestión de continuidad.
* **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
* **Equipo del Área Crítica de Negocio/Tecnológica**: Equipo formado por el personal crítico identificado encargado de la recuperación de una o más de las funciones críticas.
* **Equipo de Soporte**: Equipo formado por el personal crítico identificado encargado de de asistir al resto de equipos que forman parte del Plan para que puedan desempeñar sus funciones lo mejor y más rápidamente posible.
* **Escenarios de Contingencia:** Supuestos de desastre que tiene un gran impacto en la Organización y que se cubrirán dentro del Plan de Continuidad de Negocio. Se desarrollarán las actividades de recuperación dando una mayor cobertura a estos escenarios así como planificando las acciones a poner en marcha en cada caso.

Para cada escenario se identifican las amenazas que causan mayor impacto en la disponibilidad de las funciones y actividades.

* **Estrategias de Continuidad**: Conjunto de acciones encaminadas a dar solución a las contingencias contempladas dentro del Plan de Continuidad de Negocio.
* **Fase de Recuperación**: Unidad temporal en la que se divide el Plan de Continuidad de Negocio, y en la que se desarrolla un conjunto de acciones con un objetivo concreto.
* **Funciones Críticas:** Aquellas que tendrán que llevarse a cabo para entregar los productos y servicios fundamentales que permiten a una organización cumplir sus objetivos más importantes y sensibles al cumplimiento de plazos.
* **Impacto:** El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
* **Incidente:** Evento único o serie de eventos de seguridad inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad.
* **OTR**: Objetivo en tiempo de Recuperación. Tiempo máximo admisible de parada de una actividad crítica, por encima del cual el impacto económico o de imagen de la compañía se vería muy dañado. Definido por la compañía.
* **OPR**: Objetivo en punto de Recuperación. Marca la pérdida admisible de datos ligados con una actividad crítica, es decir, marca cada cuanto debe hacerse una copia de seguridad de los datos de la actividad, según los requerimientos indicados por negocio.
* **Plan de Continuidad del Negocio (PCN):** Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de que un evento imprevisto las ponga en peligro.
* **Plan de Continuidad Tecnológico (PCT):** Plan orientado a permitir la continuación de la tecnología en el caso de que un evento imprevisto la deje indisponible.
* **Recursos:** Todos los activos, personal, aptitudes, información, tecnología (incluyendo maquinaria y equipos), locales, y suministros e información (ya sea electrónica o no) que una organización tenga que tener disponibles para su uso, cuando sea necesario, para operar y cumplir sus objetivos.
* **Registro Vital**: Registros en formato físico (papel, CD, etc.) al que se tiene que tener acceso en todo momento, incluso con el Plan de Continuidad de Negocio activo. Se establece una estrategia para asegurar el acceso al mismo, normalmente redundándolo y almacenándolo en una segunda ubicación.
* **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
* **Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo.