

Guía de los Comités de Gestión de Crisis

*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 |
| 1.00 | Julio 2016 | Incorporación de la parte del Comité Tecnológico |  |
| 3.00 | Mayo 2017 | Actualización 2017 |  |
| 3.01 | Noviembre 2017 | Cambios menores |  |
| 3.10 | 31-7-18 | Revisión 2018 del documento |  |
| 3.11 | Octubre 2018 | Premisas de activación de Comités y PCN/PCT |  |
| 3.20 | 20-3-2019 | Revisión 2019 del documento |  |
| 3.30 | 18-11-2019 | Revisión 2019 S2 tras cambios organizativos |  |

ACCIONES PENDIENTES

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

ÍNDICE

[1 INTRODUCCIÓN 5](#_Toc24968936)

[1.1 ALCANCE Y OBJETIVOS 5](#_Toc24968937)

[1.2 SUPUESTOS DE LOS PLANES 6](#_Toc24968938)

[1.2.1 SUPUESTOS DEL PLAN DE CONTINUIDAD DE NEGOCIO (PCN/PCT) 6](#_Toc24968939)

[1.2.2 SUPUESTOS DEL PLAN DE CONTINUIDAD TECNOLÓGICO (PCT) 7](#_Toc24968940)

[1.3 ESCENARIOS De CONTINGENCIA 8](#_Toc24968941)

[1.3.1 QUÉ ES UNA "CRISIS" DESDE EL PUNTO DE VISTA DE CONTINUIDAD 8](#_Toc24968942)

[1.3.2 ESCENARIOS De CONTINGENCIA deL PCN/PCT 8](#_Toc24968943)

[1.3.3 ESCENARIOS De CONTINGENCIA deL PCT 9](#_Toc24968944)

[2 VISIÓN GENERAL DEL COMITE TÁCTICO DE GESTIÓN DE CRISIS 10](#_Toc24968945)

[2.1 PROPÓSITO Y OBJETIVOS DEL COMITÉ TÁCTICO DE GESTIÓN DE CRISIS 10](#_Toc24968946)

[2.1.1 PROPÓSITO 10](#_Toc24968947)

[2.1.2 objetivos del CTGC en el PCN/PCT 10](#_Toc24968948)

[2.1.3 objetivos del ctgc en el PCT (COMITÉ TÁCTICO TECNOLÓGICO) 11](#_Toc24968949)

[3 UBICACIONES DE LOS EQUIPOS PCN/PCT-PCT 13](#_Toc24968950)

[3.1 UBICACIONES ALTERNATIVAS DEFINIDAS POR HRE PARA EL PCN 13](#_Toc24968951)

[3.2 UBICACIONES ALTERNATIVAS DEFINIDAS POR HRE PARA EL PCT 14](#_Toc24968952)

[3.3 DIAGRAMAS ORGANIZATIVOS PARA LA GESTIÓN DE CRISIS Y/O CONTINGENCIAS 15](#_Toc24968953)

[3.3.1 Estructura de LOS COMITÉS DE GESTIÓN DE CRISIS 15](#_Toc24968954)

[3.3.2 PREMISAS PARA LA PUESTA EN MARCHA Y ACTIVACIÓN DEL PCN/PCT 16](#_Toc24968955)

[3.3.3 Estructura y miembros de los Equipos EN EL PCN/PCT 17](#_Toc24968956)

[4 Roles y RESPONSABILIDADES DE los diferentes comités y equipos 19](#_Toc24968957)

[4.1 Comité Estratégico de Gestión de Crisis (CE) 19](#_Toc24968958)

[4.2 Comité Táctico de Gestión de Crisis (CT) 19](#_Toc24968959)

[4.3 EQUIPO DE COMUNICACIÓN CORPORATIVA 19](#_Toc24968960)

[4.4 responsable de continuidad de negocio/TECNOLÓGICO 19](#_Toc24968961)

[4.5 responsabILIDADES DE LOS EQUIPOS DE ÁREAS CRÍTICAS DE NEGOCIO 20](#_Toc24968962)

[4.5.1 responsable deL EQUIPO DE ÁREA CRÍTICA DE NEGOCIO 20](#_Toc24968963)

[4.5.2 COORDINADOR DEL ÁREA DE NEGOCIO (CAN) Y SUSTITUTO (BCAN) 20](#_Toc24968964)

[4.5.3 MIEMBROS CRÍTICOS DE LOS EQUIPOS DE ÁREAS CRÍTICAS DE NEGOCIO 21](#_Toc24968965)

[4.6 RESPONSABILIDADES DE los EQUIPOS DE SOPORTE 21](#_Toc24968966)

[4.6.1 RESPONSABILIDADES DEL EQUIPO DE RRHH Y SERVICIOS GENERALES 21](#_Toc24968967)

[4.6.2 RESPONSABILIDADES DE MARKETING Y COMUNICACIÓN 22](#_Toc24968968)

[4.6.3 RESPONSABILIDADES DEL EQUIPO DE TECNOLOGÍAS DE LA INFORMACIÓN 22](#_Toc24968969)

[4.6.4 RESPONSABILIDADES DEL EQUIPO KAM 23](#_Toc24968970)

[4.6.5 TAREAS EN LOS CENTROS ALTERNATIVOS Y LUGARES DE RECUPERACIÓN 23](#_Toc24968971)

[4.7 RESPONSABILIDADES DE los EQUIPOS TECNOLÓGICOS 23](#_Toc24968972)

[5 ACCIONES DE RESPUESTA INMEDIATA DEL CTGC 25](#_Toc24968973)

[5.1 ACCIONES DE RESPUESTA DEL RESPONSABLE DEL CTGC 25](#_Toc24968974)

[5.2 CRITERIO DE ESCALABILIDAD PARA LA ACTIVACIÓN 26](#_Toc24968975)

[6 ACTIVACIÓN DEL COMITÉ TÁCTICO DE GESTION DE Contingencias 27](#_Toc24968976)

[6.1 NOTIFICACIÓN AL RESPONSABLE DEL CTGC 27](#_Toc24968977)

[6.2 EVALUACIÓN DE LA SITUACIÓN POR EL CTGC 27](#_Toc24968978)

[6.2.1 ejecución del plan de activación de las salas de crisis 27](#_Toc24968979)

[6.2.2 LISTADO DE las salas de crisis 28](#_Toc24968980)

[6.2.3 convocatoria a los miembros del CTGC 28](#_Toc24968981)

[6.2.4 INFORME DEL CTGC 28](#_Toc24968982)

[6.2.5 PROCESO DE EVALUACIÓN DE DAÑOS 29](#_Toc24968983)

[7 DECISIÓN DE DECLARAR LA CRISIS 32](#_Toc24968984)

[7.1 CONSIDERACIONES A TENER EN CUENTA PARA LA TOMA DE LA DECISIÓN 32](#_Toc24968985)

[7.2 ACTIVIDADES UNA VEZ DECLARADA LA CRISIS 32](#_Toc24968986)

[7.3 SUPERVISIÓN DEL PROCESO DE RESPUESTA Y RECUPERACIÓN 33](#_Toc24968987)

[8 GESTIÓN Y VISIÓN GLOBAL DEL PROCESO DE RECUPERACIÓN 34](#_Toc24968988)

[8.1 GESTIÓN Y VISIÓN GLOBAL DEL PROCESO DE RECUPERACIÓN DEL PCN/PCT 34](#_Toc24968989)

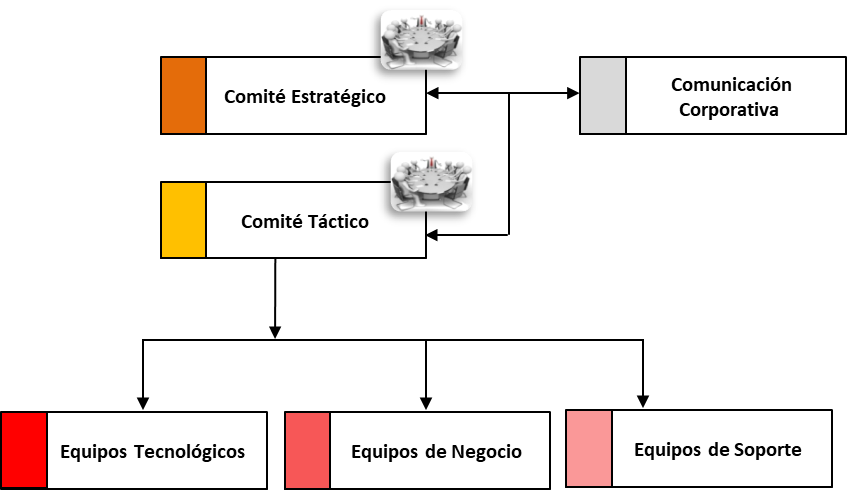
[9 MANTENIMIENTO DE LA GUIA DEL COMITÉ DE GESTIÓN DE CRISIS 36](#_Toc24968990)

[9.1 ACTUALIZAR LA GUÍA DE ACCIÓN DEL CTGC 36](#_Toc24968991)

[9.2 DISTRIBUCIÓN DE LA GUÍA DE ACCIÓN DEL CTGC 36](#_Toc24968992)

1. INTRODUCCIÓN

En el siguiente gráfico se puede observar la estructura organizativa definida para la Gestión de Crisis en HRE.



La presente guía de ayuda se ha desarrollado para dar soporte a los Comités Estratégico y Táctico de Gestión de Crisis.

Durante el año 2019 se ha actualizado el Plan de Continuidad de Negocio, quedando de esta forma reducidos los tiempos de respuesta en caso de contingencia, así como los impactos tangibles e intangibles.

* 1. ALCANCE Y OBJETIVOS

Esta guía es aplicable a todos los departamentos y Áreas de Negocio y su finalidad es proporcionar un marco de trabajo que permita la gestión de las contingencias de modo efectivo y eficaz.

Los objetivos principales de la guía son los siguientes:

* **Proporcionar a los Comités Estratégico y Táctico de Gestión de Crisis,** y los responsables del mismo, **las directrices o pautas a seguir para conseguir una reacción eficiente ante cualquier contingencia**, que derive en una interrupción importante del Negocio.
* **Facilitar el proceso de toma de decisiones** en caso de producirse un incidente que impacte en las personas, funciones críticas de negocio y/o infraestructuras.
* **Realizar un escalado claro y rápido** de acciones a llevar a cabo.
* **Facilitar la comunicación** dentro de la entidad y/o con el exterior.
  1. SUPUESTOS DE LOS PLANES
     1. 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.
  + 1. 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.
  1. ESCENARIOS De CONTINGENCIA
     1. QUÉ ES UNA "CRISIS" DESDE EL PUNTO DE VISTA DE CONTINUIDAD

Una “crisis” es una situación potencialmente catastrófica para cualquier organización o empresa, que no se puede predecir.

Sus características comunes son por tanto, la sorpresa, urgencia, unicidad y descenso en las cualidades de la comunicación.

Las crisis se pueden clasificar de muchas maneras: según la naturaleza, la duración, la gravedad, los efectos, en función de las causas que han originado la crisis (catástrofes, fallos funcionales graves, crisis de honorabilidad, amenazas económico-financieras, crisis internas), es por ello, que el impacto que puede provocar puede ser de diferente tipología:

* Impacto Tangible: gastos adicionales, reglamentario, contractual, exposición financiera, etc.
* Impacto Intangible: servicio al cliente, reputacional, de imagen, etc.
  + 1. ESCENARIOS De CONTINGENCIA deL PCN/PCT

El Equipo de Trabajo ha concretado los escenarios de contingencia a desarrollar en el Plan de Continuidad de Negocio en una propuesta de cuatro escenarios de contingencia, que engloban posibles contingencias de ubicación, de tecnología, de recursos humanos y de proveedores críticos.

En concreto, la propuesta de Escenarios de Contingencias a cubrir en el Plan de Continuidad de Negocio es:

* Afección de todo o parte del personal crítico de un equipo de recuperación imposibilitando su vuelta inmediata al trabajo
  + - Intoxicación,
    - Pandemia, etc.
* Afectación únicamente a los equipos de usuario debido a:
  + - Caída de los sistemas eléctricos y/o infraestructura de red en una ubicación
    - Afectación de malware a equipos locales
* Se excluyen los escenarios propios del PCT
* Actos de terrorismo, vandalismo y/o sabotaje (amenaza de bomba, etc.)
* Incendios
* Agentes atmosféricos (fuertes vientos, nevadas intensas, etc.)
* Terremotos, inundaciones
* Detección de un fallo estructural, etc.
* Fallo del Servicio del Proveedor
* Imposibilidad de prestación del servicio (total y/o parcial)
  + - Agentes atmosféricos (fuertes vientos, nevadas intensas, etc.)
    - Incendios
    - Terremotos, etc.

**INDISPONIBILIDAD DE RECURSOS HUMANOS CRÍTICOS**

**INDISPONIBILIDAD DE INFORMACIÓN CRÍTICA POR FALLOS EN TECNOLOGÍA**

**INDISPONIBILIDAD DE LA UBICACIÓN POR INACCESIBILIDAD O DESTRUCCIÓN**

**INTERRUPCIÓN DE PROVEEDORES CRÍTICOS**

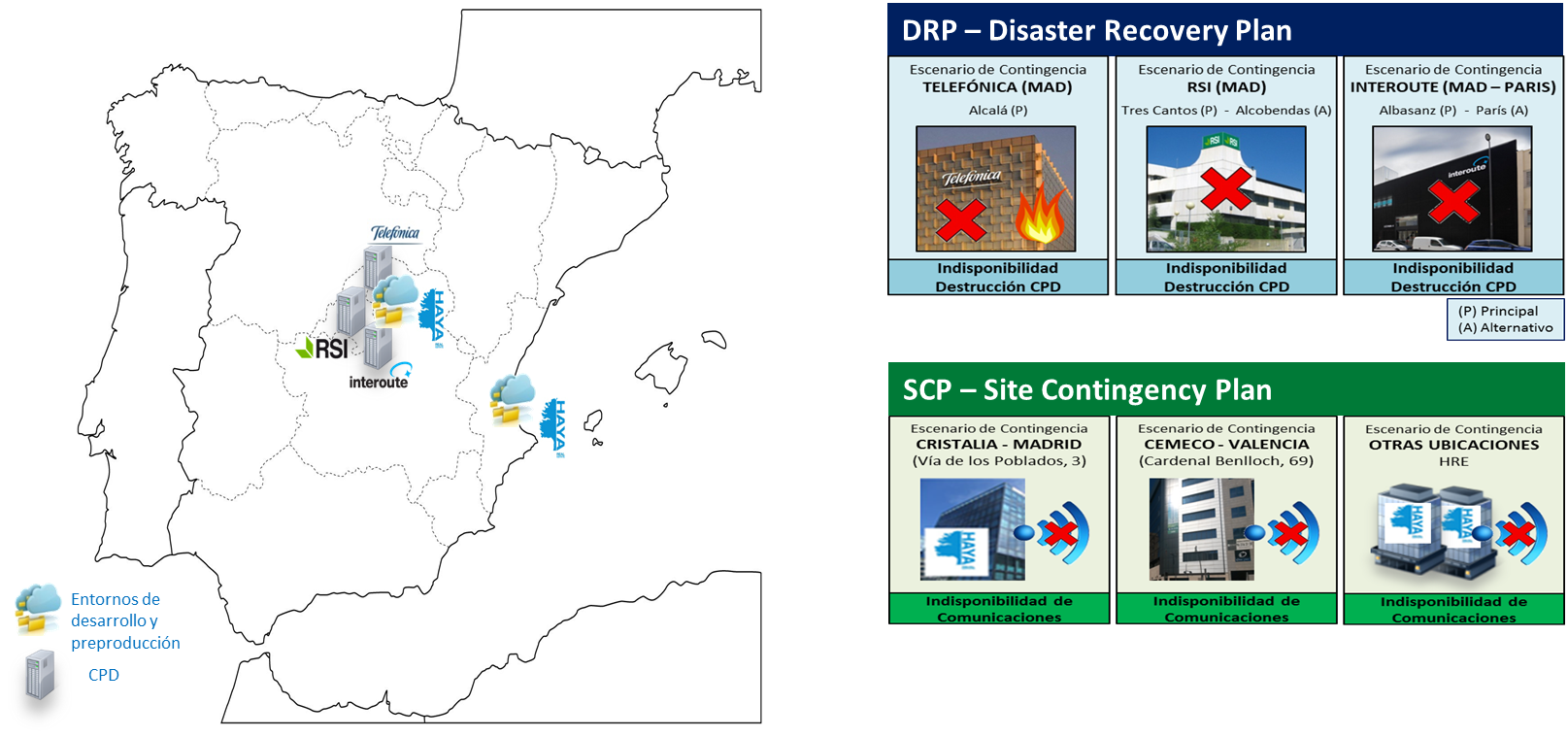


* + 1. ESCENARIOS De CONTINGENCIA deL PCT

El Equipo de Trabajo ha concretado los escenarios de contingencia a desarrollar en el Plan de Continuidad Tecnológico en una propuesta de dos fases, el Disaster Recovery Plan (DRP) y el Site Contingency Plan (SCP), los cuales se identifican a continuación:

* + - 1. ESCENARIOS DeL DISASTER RECOVERY PLAN (DRP)

Una vez estudiadas las potenciales amenazas que aplican sobre la infraestructura de los CPDs así como los diferentes Sistemas de Información disponibles en los mismos, se han definido cuatro escenarios de contingencia que mitigan los principales riesgos. Los escenarios de contingencia cubiertos en el presente DRP se muestran a continuación:

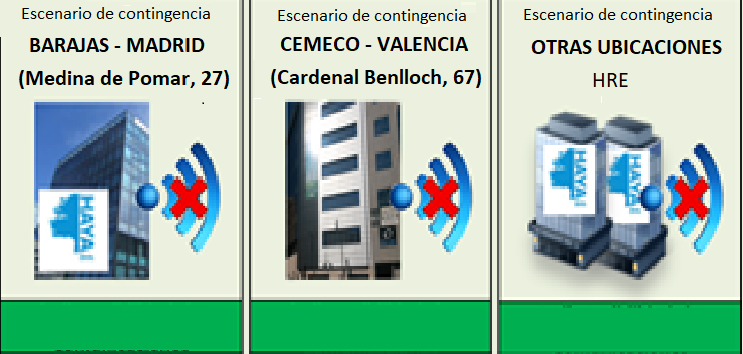


*Imagen <Escenarios de contingencia del DRP cubiertos>*

Existe una serie de contingencias que no quedan recogidas dentro del presente plan y son:

* Contingencias producidas fuera de los CPDs comentados.
* Contingencias que por su impacto limitado o concreto se resuelven dentro del proceso “Gestión de Incidencias”.
* Contingencia total y simultánea en varios de los CPDs de **Madrid**.
  + - 1. ESCENARIOS DeL SITE CONTINGENCY PLAN (SCP)

Una vez estudiadas las potenciales amenazas que aplican sobre la infraestructura de los sites de HRE, se han definido tres escenarios de contingencia que mitigan los principales riesgos. Los escenarios de contingencia cubiertos en el presente SCP se muestran a continuación:



**Indisponibilidad de comunicaciones**

**Indisponibilidad de comunicaciones**

**Indisponibilidad de comunicaciones**

*Imagen <Escenarios de contingencia del SCP cubiertos>*

1. VISIÓN GENERAL DEL COMITE TÁCTICO DE GESTIÓN DE CRISIS
   1. PROPÓSITO Y OBJETIVOS DEL COMITÉ TÁCTICO DE GESTIÓN DE CRISIS
      1. PROPÓSITO

El propósito o finalidad del Comité Táctico de Gestión de Crisis (CTGC) es proteger la “salud” y seguridad de los empleados y dirigir las acciones operativas a realizar durante el momento de la contingencia, por medio de una organización bien estructurada que supervise la reacción o respuesta a esa contingencia, para minimizar el impacto cuantitativo y cualitativo de la misma sobre el negocio del HRE.

De los miembros del CTGC se espera estén localizados las 24 horas del día, los siete días de la semana para responder a las necesidades que se deriven de la interrupción temporal de la operativa normal en la Entidad.

* + 1. objetivos del CTGC en el PCN/PCT

Entre los objetivos del Comité Táctico de Gestión de Crisis se incluyen los siguientes:

* Determinar si algunos impactos negativos como resultado de la contingencia advierten que se ha de activar el Plan de Continuidad de Negocio.
* Informar al Comité Estratégico sobre la contingencia y/o desastre.
* Autorizar la activación de las ubicaciones alternativas para los equipos de recuperación afectados 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.

Para alcanzar estos objetivos, el CTGC debería seguir las **pautas de Gestión de la Contingencia** que se detallan a continuación:

1. Evaluar los daños producidos por la contingencia y analizar el impacto potencial para HRE.
2. Proponer al Comité Estratégico (CE) la activación del Plan de Continuidad de Negocio de HRE en base a los resultados del informe de Evaluación de Daños.
3. Asegurarse de que se actúa conforme a lo escrito en el Plan de Continuidad de Negocio de los distintos equipos implicados en el proceso de recuperación de negocio.
4. Asignar la toma de decisiones en función del nivel de autoridad, a los distintos responsables de los equipos de recuperación.
5. Garantizar un circuito de comunicaciones preciso, eficiente y seguro.
6. Solventar todas las incidencias que puedan plantearse durante las distintas fases del proceso de recuperación, en el Plan de Continuidad de Negocio.
7. Responder siempre a las expectativas públicas y legales a través de los equipos de Comunicación Corporativa.
8. Verificar que el proceso de información pública de la situación de contingencia a terceras partes claves para el negocio de HRE (Socios, Clientes, etc.), minimice los perjuicios para ésta en términos de imagen y en extensión el impacto no tangible.
9. Dar el soporte adecuado, es decir, justificar cada acción de respuesta llevada a cabo durante la contingencia.
   * 1. objetivos del ctgc en el PCT (COMITÉ TÁCTICO TECNOLÓGICO)

Cuando la contingencia es tecnológica, los miembros no permanentes que se ponen en marcha pertenecen a los equipos tecnológicos de HRE. Estos miembros forman Comité Táctico Tecnológico (CTT). Las principales funciones de dicho Comité son:

En situación de Normalidad:

* Conocer la información disponible del CP-DRP-SCP
* Recibir formación práctica para conocer sus responsabilidades en caso de contingencia (activación del DRP-SCP)
* Participar en simulacros de gestión de Crisis

En situación de Contingencia:

* Proteger la salud y seguridad de los empleados ante una contingencia
* Dirigir las acciones tácticas durante la evaluación de la contingencia para minimizar el impacto y el tiempo de respuesta
* Declarar la situación como crítica y proponer al Comité Estratégico la activación del CP-DRP-SCP
* Asegurar durante el transcurso de la contingencia, que los responsables de los Equipos Tecnológicos ponen en marcha su personal crítico así como están coordinados con el resto de responsables de Equipos Tecnológicos
* Mantener informados sobre la situación, si es necesario, a los equipos de “comunicación corporativa”.
* Coordinar y dirigir la reacción inicial y los esfuerzos posteriores para restablecer la vuelta a la normalidad

El Comité Táctico Tecnológico debería seguir las pautas de **Gestión de Contingencias** que se detallan a continuación:

1. Evaluar los daños producidos por la contingencia y analizar el impacto potencial para HRE.
2. Proponer al Comité Estratégico (CE) la activación del DRP-SCP de HRE en base a los resultados del informe de Evaluación de Daños.
3. Asegurarse de que se actúa conforme a lo escrito en los Planes de Continuidad Tecnológicos de los distintos equipos implicados en el proceso de recuperación Tecnológico.
4. Asignar la toma de decisiones en función del nivel de autoridad, a los distintos responsables de equipos tecnológicos.
5. Garantizar un circuito de comunicaciones preciso, eficiente y seguro.
6. Solventar todas las incidencias que puedan plantearse durante las distintas fases del proceso de recuperación, en el Plan.
7. Responder siempre a las expectativas públicas y legales a través de los equipos de Comunicación Corporativa.
8. Verificar que el proceso de información pública de la situación de contingencia a terceras partes claves para el negocio de HRE (Socios, Clientes, etc.), minimice los perjuicios para ésta en términos de imagen y en extensión el impacto no tangible.
9. Dar el soporte adecuado, es decir, justificar cada acción de respuesta llevada a cabo durante la contingencia.
10. UBICACIONES DE LOS EQUIPOS PCN/PCT-PCT

El principal objetivo de las ubicaciones alternativas, es que el Comité Estratégico (CE), el Comité Táctico de Gestión de Crisis (CTGC) y el resto de equipos de recuperación definidos dentro del Plan de Continuidad de Negocio, dispongan de una ubicación alternativa para coordinar sus actividades en caso de contingencia.

El responsable del PCN/PCT ejecutará el Plan de activación de las salas de continuidad una vez le haya sido notificada la contingencia y coordinará con el Equipo de Medios, el acondicionamiento de las salas oportunas, equipándolas con los requerimientos necesarios para facilitar las tareas de gestión y supervisión del Proceso de Recuperación.

* 1. UBICACIONES ALTERNATIVAS DEFINIDAS POR HRE PARA EL PCN

HRE ha definido las siguientes ubicaciones alternativas para la Continuidad de negocio en caso de contingencia, en función del desastre planteado y declarado por el Comité Estratégico (CE):

|  |  |
| --- | --- |
| **ESCENARIO DE CONTINGENCIA**  **UBICACIONES ALTERNATIVAS para el Comité Estratégico (CE) y Comité Táctico de Gestión de Crisis (CTGC)** | |
| Desastre Total | SAREB - Castellana, 89 |
| Desastre Parcial | BARAJAS. Medina de Pomar, 27 |
| Simulacros Periódicos | BARAJAS. Medina de Pomar, 27 o SAREB – Castellana, 89  Según simulacro |

|  |  |
| --- | --- |
| **ESCENARIO DE CONTINGENCIA**  **UBICACIONES ALTERNATIVAS para Equipos de Soporte y Apoyo** | |
| Desastre Total | SAREB - Castellana, 89 |
| Desastre Parcial | BARAJAS. Medina de Pomar, 27 |

|  |  |
| --- | --- |
| **ESCENARIO DE CONTINGENCIA**  **UBICACIONES ALTERNATIVAS para Equipos de Negocio** | |
| Desastre Total | SAREB – Castellana, 89 (Alternativa para Valencia y Almería)  CEMECO – Avda. Cardenal Benlloch, 67 (Alternativa para Madrid) |
| Desastre Parcial | BARAJAS. Medina de Pomar, 27 |
| Pruebas Periódicas | SAREB, BARAJAS-MADRID, CEMECO-VALENCIA, CABO DE GATA-ALMERÍA  Según prueba |

* 1. UBICACIONES ALTERNATIVAS DEFINIDAS POR HRE PARA EL PCT

Con el objetivo de gestionar de una manera coordinada la respuesta ante contingencias es indispensable y así está definido, el disponer de unas salas de crisis donde poder reunir a los diferentes miembros de los diferentes comités así como equipos de soporte para gestionar eficazmente la respuesta.

|  |  |
| --- | --- |
| **ESCENARIO DE CONTINGENCIA**  **UBICACIONES ALTERNATIVAS para el Comité Estratégico (CE) y Comité Táctico Tecnológico (CTT)** | |
| Desastre Total | BARAJAS. Medina de Pomar, 27 |
| Desastre Parcial | BARAJAS. Medina de Pomar, 27 |
| Simulacros Periódicos | BARAJAS. Medina de Pomar, 27 |

|  |  |
| --- | --- |
| **ESCENARIO DE CONTINGENCIA**  **UBICACIONES ALTERNATIVAS para el resto de Equipos** | |
| Desastre Total | BARAJAS. Medina de Pomar, 27 |
| Desastre Parcial | BARAJAS. Medina de Pomar, 27 |

* 1. DIAGRAMAS ORGANIZATIVOS PARA LA GESTIÓN DE CRISIS Y/O CONTINGENCIAS
     1. Estructura de LOS COMITÉS DE GESTIÓN DE CRISIS

A continuación, se muestran los datos de contacto de los miembros de los diferentes comités:

**- Comité Estratégico**



**- Comité Táctico**



A continuación, se presentan los nombres de los responsables del Plan de Continuidad de Negocio y Tecnológico de HRE:

* **Responsable PCT**: Sr. Javier Sánchez Salas

Tlf: 683 297 989

E-mail: jsanchezs@haya.es

* **Sustituto del responsable PCT**: Sr. Luis Alberto Rodrigo Piqueras

Tlf: 627 616 245

E-mail: lrodrigo@haya.es

* + 1. PREMISAS PARA LA PUESTA EN MARCHA Y ACTIVACIÓN DEL PCN/PCT

Para la **activación del Comité Táctico** de Gestión de Crisis o el Comité Tecnológico de Gestión de Crisis:

* El Responsable de Continuidad de Negocio, o su sustituto podrán convocar a los miembros del Comité Táctico que consideren oportunos según el alcance de la contingencia, teniendo en cuenta los miembros que son permanentes en cualquier caso y los que asistirían en función de la contingencia.

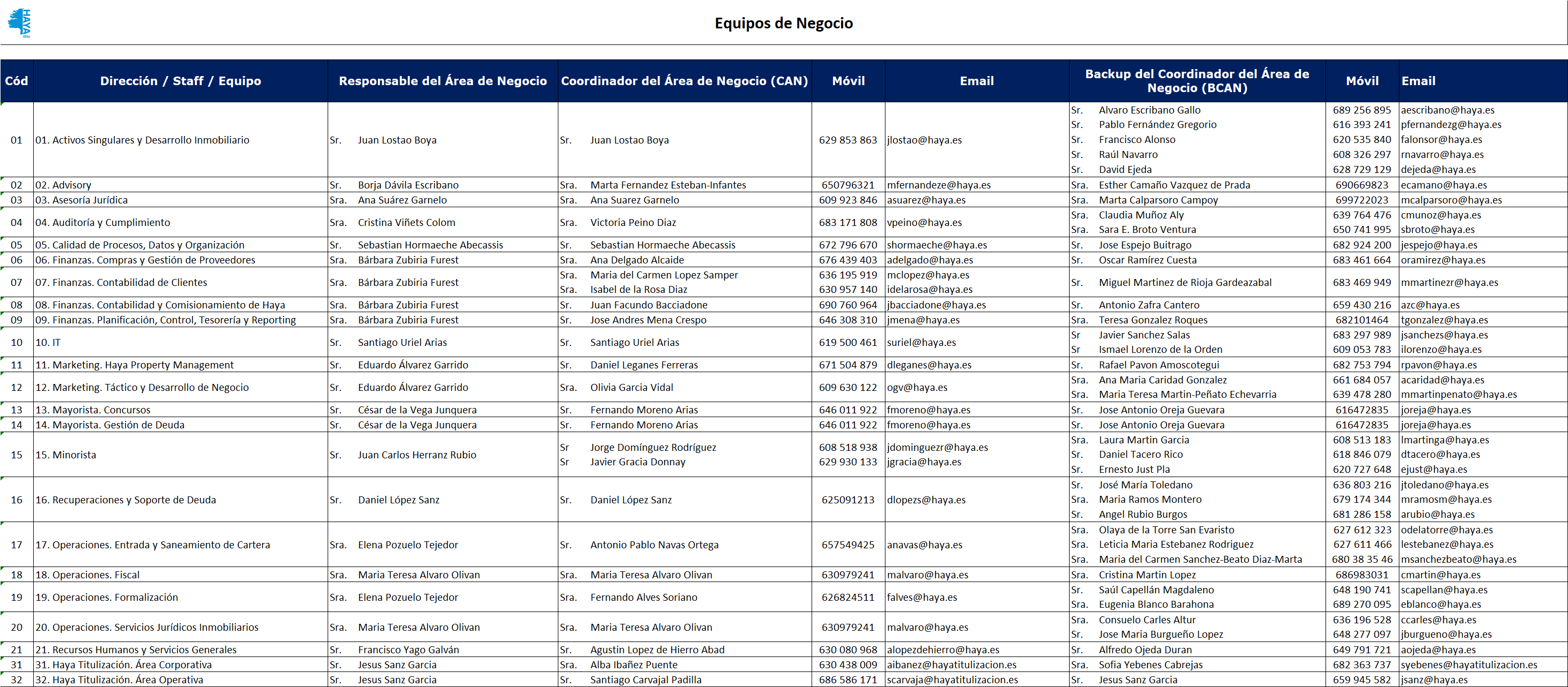
Para la **activación del Comité Estratégico** de Gestión de Crisis:

* Por mayoría simple, los miembros del Comité Táctico de Gestión de Crisis (o Tecnológico) pueden convocar al Comité Estratégico si consideran que la contingencia es lo suficientemente grave como para poder activar el Plan de Continuidad de Negocio y/o Tecnológico, teniendo en cuenta los miembros que son permanentes en cualquier caso y los que asistirían en función de la contingencia.

Para la **activación del Plan de Continuidad de Negocio y/o Tecnológico**:

* Por mayoría simple, los miembros del Comité Estratégico de Gestión de Crisis pueden activar el Plan de Continuidad de Negocio y/o Tecnológico, así como la posterior decisión de estrategias a poner en marcha (ubicaciones alternativas, recursos humanos, tecnología y proveedores críticos)
  + 1. Estructura y miembros de los Equipos EN EL PCN/PCT
       1. Equipos de Negocio

A continuación, se muestra el listado de los Equipos de las Áreas Críticas de Negocio dentro de la organización de HRE, junto a sus responsables y coordinadores PCN/PCT (CAN, BCAN):

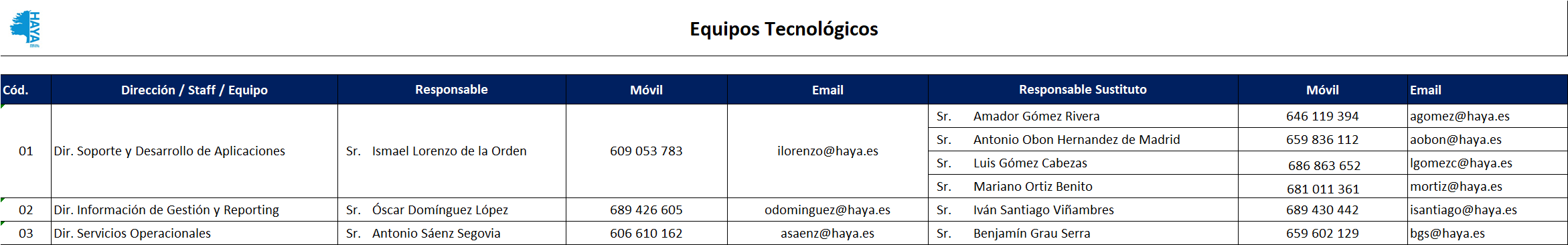


Los responsables o Alternativos de cada uno de los equipos, tienen la responsabilidad de formar a los miembros de sus respectivos grupos para completar así la totalidad de las tareas (asociadas a las funciones críticas) asignadas a su equipo, en cada una de las fases de recuperación. Tales tareas, forman parte de las actividades y procedimientos que constituyen el Plan de continuidad de Negocio de cada uno de estos Equipos claves de recuperación, y establecen las pautas de actuación a seguir en caso de desastre. Los procedimientos del Plan de Continuidad de Negocio se ejecutarán conforme lo determine el CTGC, según el desastre.

* + - 1. Equipos de Recuperación de Soporte Y APOYO

En las siguientes tablas se listan los datos de contacto de los Equipos de Recuperación de Soporte y Apoyo:





1. Roles y RESPONSABILIDADES DE los diferentes comités y equipos

A continuación, se detalla para cada uno de los equipos de recuperación las responsabilidades a poner en marcha en las diferentes etapas de Contingencia.

1. 1. Comité Estratégico de Gestión de Crisis (CE)

Los Roles y Responsabilidades en Continuidad de Negocio/Tecnológico son:

* Declarar la situación como crítica y activar el PCN/PCT.
* 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 están en contacto.
* Marcar la comunicación y acciones a los proveedores, al mercado inmobiliario, clientes y medios de comunicación.
  1. Comité Táctico de Gestión de Crisis (CT)

Los Roles y Responsabilidades en Continuidad de Negocio/Tecnológico son:

* 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 los equipos de recuperación afectados por la contingencia o desastre.
* Coordinar y dirigir la reacción inicial y todos los esfuerzos posteriores para restablecer la vuelta a la normalidad.
* Coordinar los medios de comunicación externos con los internos.
* Seguimiento y supervisión de actividades críticas a llevar a cabo por los Equipos de Negocio.
  1. EQUIPO DE COMUNICACIÓN CORPORATIVA

Los Roles y Responsabilidades en Continuidad de Negocio/Tecnológico son:

* Coordinar la comunicación interna y externa informando de la situación.
* Informar a Entidades HRE.
* Informar periódicamente de la situación a los interesados y a Proveedores.
  1. responsable de continuidad de negocio/TECNOLÓGICO

Los Roles y Responsabilidades en Continuidad de Negocio/Tecnológico en normalidad son:

* Proporcionar la metodología de la gestión de la documentación.
* Hacer cumplir los plazos de generación y revisión de la documentación.
* Dar soporte en las pruebas y el mantenimiento.
* Certificar el cumplimiento de la Política y Normativa del PCN/PCT.
* Coordinar la puesta en marcha de las acciones correctoras de las pruebas.
* Coordinar la gestión de simulacros de gestión de crisis con la Dirección.
* Gestionar la elaboración de seminarios, cursos y workshops.

Los Roles y Responsabilidades en Continuidad de Negocio/Tecnológico en contingencia son:

* Mantener informado al Comité Táctico de la situación de la contingencia.
* Dar apoyo al Comité Táctico en materia de Continuidad de Negocio/Tecnológico para la determinación de la activación o no del Plan.
* Informar de la situación actual de las ubicaciones alternativas y teletrabajo.
  1. responsabILIDADES DE LOS EQUIPOS DE ÁREAS CRÍTICAS DE NEGOCIO
     1. responsable deL EQUIPO DE ÁREA CRÍTICA DE NEGOCIO

Los Roles y Responsabilidades en Continuidad de Negocio en normalidad son:

* Asegurar que el PCN se alinea con los requerimientos de negocio y organizativos.
* Asegurar que la información generada en el PCN se mantiene actualizada.
* Supervisión de las pruebas periódicas.
* Coordinación del seguimiento de las acciones correctoras globales.
* Reciben formación en materia de Continuidad de Negocio.
* Conocen toda la información del PCN.
* Actualizar la información del equipo tras su activación en contingencia.

Los Roles y Responsabilidades en Continuidad de Negocio en contingencia son:

* Mantener informado a los Comités Táctico y Estratégico de los avances de la evaluación y puesta en marcha (si procede) del PCN.
* Informar sobre la evolución del proceso de respuesta y recuperación a dichos Comités.
  + 1. COORDINADOR DEL ÁREA DE NEGOCIO (CAN) Y SUSTITUTO (BCAN)

Los Roles y Responsabilidades en Continuidad de Negocio en normalidad son:

* Responsables de la Continuidad de Negocio del Área.
* Definición y realización de las pruebas y el mantenimiento.
* Puesta en marcha de las acciones de mejora después de las pruebas periódicas.
* Actualización y pruebas de los árboles de llamadas.
* Actualización y pruebas de las Actividades de recuperación.

Los Roles y Responsabilidades en Continuidad de Negocio en contingencia son:

* Atender a las órdenes del responsable del área y de los Comités Táctico y Estratégico para conocer el estado de la activación del PCN.
* En caso de activación del PCN, y según la estrategia establecida en cada caso, utilizar el árbol de llamadas para localizar al personal en contingencia y darle las instrucciones pertinentes.
* Mantener informado al Responsable del Equipo de los avances en la evaluación y puesta en marcha (si procede) del PCN.
* Informar sobre la evolución del proceso de respuesta y recuperación al Responsable del Equipo.
  + 1. MIEMBROS CRÍTICOS DE LOS EQUIPOS DE ÁREAS CRÍTICAS DE NEGOCIO

Los Roles y Responsabilidades en Continuidad de Negocio en normalidad son:

* Conocen la normativa y documentación general de PCN.
* Utilizan la estrategia de recuperación y plan de pruebas.
* Conocen toda la información específica del equipo del PCN.
* Reciben formación en materia de Continuidad de Negocio.
* Reciben información del Plan de Pruebas y Participar y validar las pruebas periódicas.

Los Roles y Responsabilidades en Continuidad de Negocio en contingencia son:

* Puesta en marcha de las funciones identificadas (en función del escenario).
* Mantener informado al Coordinador de Negocio del Equipo de los avances en la evaluación y puesta en marcha (si procede) del PCN.
* Informar sobre la evolución del proceso de respuesta y recuperación al Coordinador de Negocio del Equipo.
  1. RESPONSABILIDADES DE los EQUIPOS DE SOPORTE

Los equipos de soporte que se han definido para dar apoyo a las operaciones de recuperación son:

**Marketing y Comunicación**

**RRHH y Servicios Generales**

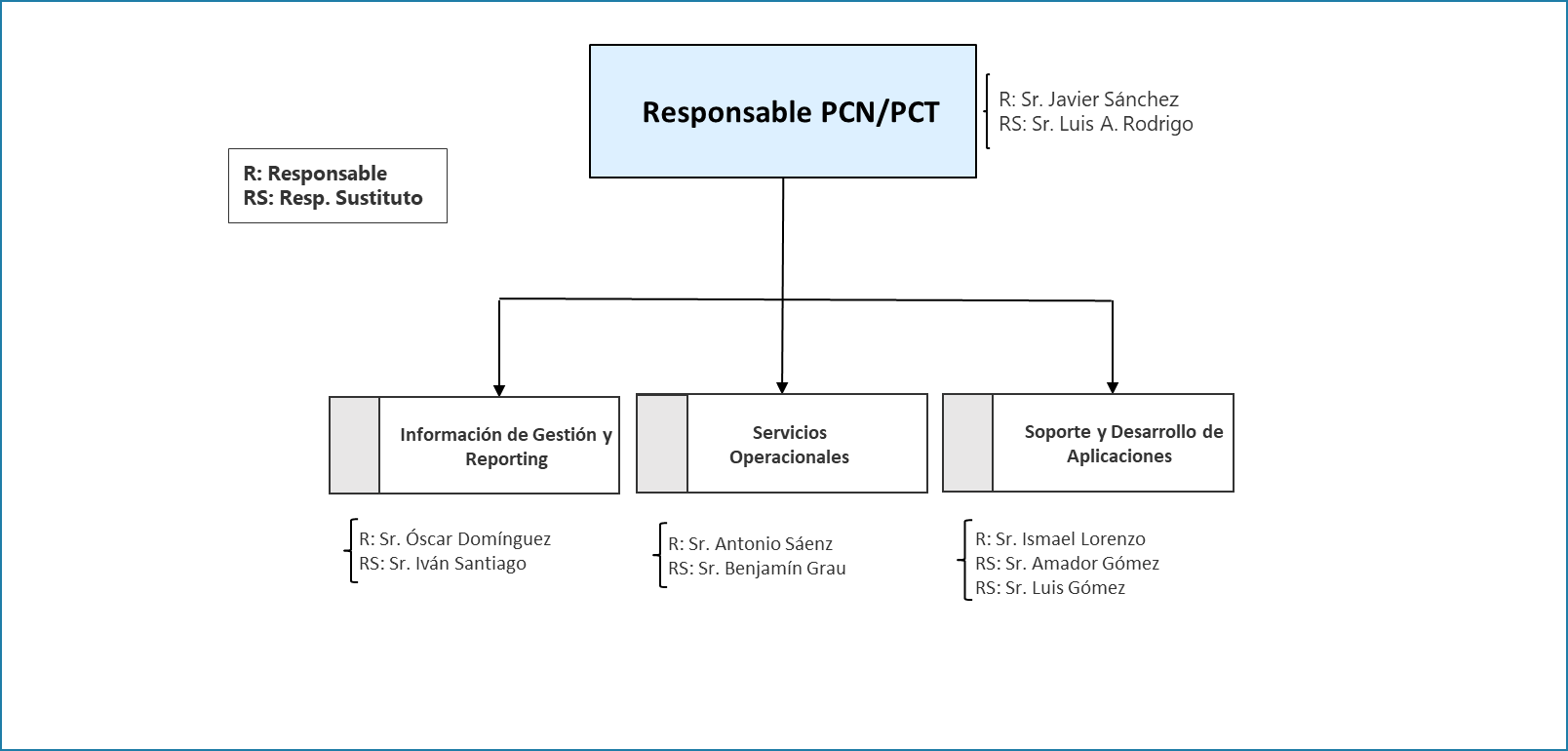
**Tecnologías de la Información**

**Key Account Manager**

Las responsabilidades definidas para cada uno de estos equipos en el proceso de recuperación, se detallan a continuación en los siguientes apartados.

* + 1. RESPONSABILIDADES DEL EQUIPO DE RRHH Y SERVICIOS GENERALES
* Colaborar en la valoración de los daños ocasionados por la crisis.
* Ofrecer los datos de contacto de empleados requeridos para las tareas de recuperación y restauración.
* Si se producen daños personales, habilitar un plan para conocer el estado de los empleados y asistencia a los mismos y familiares.
* Poner en marcha un sistema de información y comunicación con las secciones sindicales y representantes de las instalaciones afectadas
* Colaborar en la valoración de los daños ocasionados por la crisis.
* Coordinar la distribución y puesta en marcha de los recursos necesarios en las ubicaciones de respaldo, contando para ello con la colaboración del Equipo de Intervención de Sistemas.
* Coordinar la relación con los Cuerpos y Fuerzas de Seguridad del Estado, así como con los servicios de emergencia.
* Facilitar el traslado de todo el personal implicado en la crisis a las ubicaciones de respaldo, en su caso, mediante la organización del transporte y del resto de aspectos relacionados (catering, etc.).
* Coordinar la búsqueda de instalaciones y adecuarlas para su instalación
  + 1. RESPONSABILIDADES DE MARKETING Y COMUNICACIÓN
* La preparación de la información de los Comités Estratégico y Táctico que ha de hacerse pública, dando cuenta de la actual o potencial reacción de los medios de comunicación.
* Realizar las comunicaciones desde que se declara la contingencia o desastre por los Comités Estratégico y Táctico y durante todo el proceso de recuperación, de forma breve y concisa para minimizar el riesgo de colapso en el circuito de comunicaciones.
* Verificar el correcto funcionamiento de canales de comunicación (Intranet, email)
* Recopilar la información prioritaria y necesaria. Para informar a empleados y medios de comunicación y transmitir una imagen pública de HRE positiva.
* Redactar y coordinar comunicaciones internas y externas.
* Gestionar las relaciones con los medios de comunicación, socios institucionales, accionistas y clientes.
* Asegurar el mantenimiento y operatividad del portal corporativo: [www.haya.es](http://www.haya.es)
  + 1. RESPONSABILIDADES DEL EQUIPO DE TECNOLOGÍAS DE LA INFORMACIÓN
* Realizar la valoración inmediata de daños causados por la crisis.
* Garantizar la restauración de las comunicaciones corporativas entre sedes y las instalaciones alternativas
* Dar soporte prioritario a la restauración de las aplicaciones de negocio y a las utilizadas por los Equipos de Recuperación
* Poner en marcha los Planes de Contingencia establecidos para el restablecimiento y recuperación de sistemas corporativos.
  + 1. RESPONSABILIDADES DEL EQUIPO KAM
* Realizar la valoración sobre la posible afectación en su cartera.
* Establecer y garantizar la comunicación corporativa entre HRE y carteras.
* Recopilar la información prioritaria y necesaria para informar a sus carteras y transmitir una imagen pública de HRE positiva.
* Redactar, coordinar y gestionar las comunicaciones con las carteras, así como dar soporte prioritario a la restauración de las aplicaciones de negocio y a las utilizadas por los Equipos de Recuperación.
  + 1. TAREAS EN LOS CENTROS ALTERNATIVOS Y LUGARES DE RECUPERACIÓN
* Establecimiento de los puestos de trabajo y los recursos necesarios (Hardware, suministros de oficina, etc.) en el Centro Alternativo y lugares de Recuperación correspondiente al escenario de desastre declarado por el CGC (Comité de Gestión de Crisis), en función de las especificaciones del CGC.
* Comprobar el suministro de luz, calefacción, gas natural, tomas de luz, agua, sistemas de seguridad y demás condiciones ambientales para garantizar que esos lugares de recuperación reúnen unas condiciones mínimas y unos requisitos de seguridad y confort para desarrollar desde allí las actividades críticas de negocio de HRE.
* Avisar al CGC (Comité de Gestión de Crisis), una vez está listo el Centro Alternativo y Lugar de Recuperación, para poder dar paso a la Fase II del Plan de Continuidad de Negocio.
  1. RESPONSABILIDADES DE los EQUIPOS TECNOLÓGICOS

Los equipos tecnológicos que se han definido para dar apoyo a las operaciones de recuperación son:



Las responsabilidades definidas para cada uno de estos equipos en el proceso de recuperación se detallan a continuación en los siguientes apartados:

* Supervisión de los procedimientos de backups de los distintos sistemas y plataformas informáticos (datos y programas) que soportan los servicios críticos de negocio.
* Colaborar con el Comité en el proceso de evaluación de daños de los sistemas informáticos y de telecomunicaciones afectados por la contingencia y que soportan procesos críticos de negocio.
* Participar en el traspaso de los sistemas al lugar alternativo, según se requiera.
* Redireccionamiento de las comunicaciones de voz y datos al centro alternativo correspondiente.
* Coordinar las actividades, según se requiera, con el personal de apoyo y externos.
* Asistir cuanto se necesite, en la adquisición e instalación del equipamiento en el lugar de recuperación.
* Participar en la comprobación de los equipos e instalaciones.
* Coordinar y participar en la restauración o sustitución de PC´s, LANs y otras entradas de comunicación en el lugar dañado.
* Confirmar programa y copias de los ficheros acordados fuera del edificio.
* Revisar cada copia de los archivos del sistema. Restaurar ficheros críticos.
* Definir la configuración mínima que se necesita.
* Supervisar la reanudación de procesos críticos. Asegurarse del estado de los dispositivos de seguridad perimetral, para conseguir un acceso apropiado.

1. ACCIONES DE RESPUESTA INMEDIATA DEL CTGC
2. 1. ACCIONES DE RESPUESTA DEL RESPONSABLE DEL CTGC

A continuación, se detallan las acciones inmediatas que el CTGC deberá seguir **tan pronto como tenga conocimiento de la contingencia y/o desastre**:

1. El Director Autorizado perteneciente al CTGC, se cerciora de inmediato de que la situación es grave a partir de la información preliminar del Responsable del Comité Táctico de HRE y manda activar el PCN/PCT. Si la contingencia se produce dentro del horario laboral, el Responsable del CTGC, se pone en contacto inmediatamente (mediante llamada al teléfono móvil obtenido de la lista de contactos) con cada uno de los miembros del CTGC para organizar una reunión con carácter de **extrema urgencia (si lo estima oportuno)**.
2. El Responsable del CTGC obtiene la información pertinente en base a los datos técnicos suministrados por el Equipo de Evaluación y los equipos de soporte técnico y realiza una evaluación preliminar para delimitar el impacto y los daños en el edificio afectado por la contingencia.
3. Si se considera que la situación es grave y que no puede subsanarse inmediatamente,  **procede a comunicar la situación al Responsable del Comité Estratégico para proceder a la activación del PCN/PCT**, así como de los distintos equipos de recuperación afectados, en base al escenario de contingencia.
4. Si se considera que la situación puede subsanarse en poco tiempo, el *Responsable del proceso de recuperación*, informará a los responsables de los equipos de las distintas áreas críticas, vía teléfono (fijo y/o móvil) o mensaje, según proceda y continuará en estado de alerta, vigilando la secuencia de acontecimientos, que se vayan desarrollando. En caso contrario, será encargado de activar los equipos de recuperación que el Responsable del Comité Táctico estime oportunos en función de la contingencia.

5. El CTGC mantendrá informado al Comité Estratégico de la situación de contingencia así como de su avance en la recuperación.

* 1. CRITERIO DE ESCALABILIDAD PARA LA ACTIVACIÓN

Cuando se esté decidiendo si activar (recomendar) o no el PCN/PCT debería tenerse en cuenta las siguientes cuestiones:

* Tiempo de parada/caída previsto
* Impacto significativo para el negocio (funciones críticas afectadas)
* Daño a la instalación/es y nivel de afectación de la plataforma informática y tecnológica corporativa
* Existencia de víctimas o lesionados críticos (departamentos afectados)
* Peligro para la integridad física o seguridad personal
* Impacto monetario en los ingresos o pérdida de ventas
* Conocimiento de los medios de comunicación de lo sucedido
* Impactos en el servicio al cliente (reputacional)
* Asociados afectados por la estrategia de recuperación
* Dimensión de los daños a terceros

1. [ACTIVACIÓN DEL COMITÉ TÁCTICO DE GESTION DE Contingencias](#_3.1_NOTIFICACIÓN_AL)
2. 1. NOTIFICACIÓN AL RESPONSABLE DEL CTGC

En general, al Responsable del CTGC se le comunicará lo sucedido a través de uno de los diferentes implicados:

1. El Responsable del Plan de Continuidad de Negocio/Tecnológico
2. En primera instancia, la notificación puede llegar de Riesgos Laborales / Tecnología
3. Los miembros del CGC y/o cualquier empleado de HRE
4. Terceras personas del negocio de HRE
5. Autoridades locales
   1. EVALUACIÓN DE LA SITUACIÓN POR EL CTGC

Una vez que la contingencia ha ocurrido, el Responsable del CTGC pondrá en marcha el Equipo de Evaluación para completar el informe inicial de evaluación a utilizar por él y el Responsable de Continuidad de Negocio ha sido avisado, éste último asumirá las siguientes responsabilidades:

1. El Responsable de Continuidad de Negocio/Tecnológico documentará con los siguientes dos informes, en función de la contingencia, toda la información relevante sobre los siguientes aspectos y hará llegar dicha información al Responsable del CTGC y al resto de sus miembros, ubicados en las ubicaciones alternativas designadas:

1. Informe de Evaluación preliminar de Continuidad de Negocio/Tecnológico:



* + 1. ejecución del plan de activación de las salas de crisis

Tras la evaluación de la situación, el responsable del PCN/PCT, comunicará con el **Responsable del Equipo de Recursos Humanos y Medios**, para que active las ubicaciones alternativas correspondientes:

Las instalaciones deberán cumplir los siguientes requisitos:

1. Asegurarse de que todo el equipamiento y aprovisionamientos previstos están preparados (teléfonos, fax, equipamiento informático, etc.).

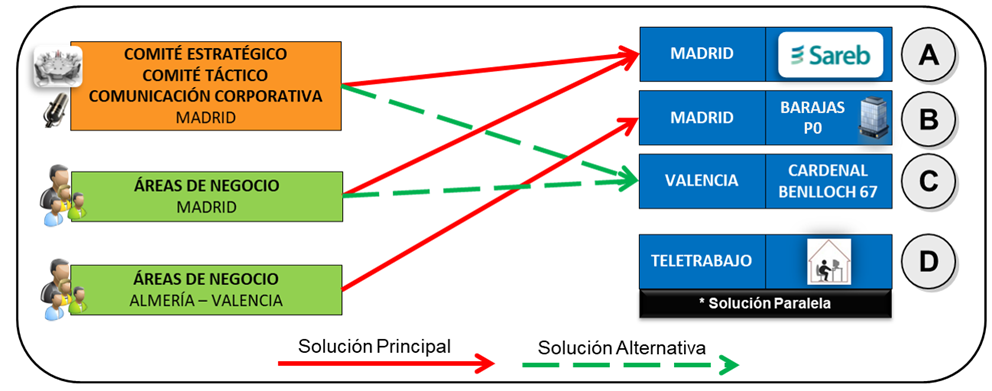
2. Establecer y hacer que se cumpla, un único punto de entrada al recinto y asegurar que los miembros de los equipos implicados tienen autorización de entrada.

3. Comprobar suministros de luz, agua, gas natural, temperatura y demás medios para garantizar un mínimo funcionamiento y la seguridad adecuada para la eficaz ocupación del centro alternativo.

4. Avisar al CE/CTGC una vez los edificios alternativos estén acondicionados.

* + 1. LISTADO DE las salas de crisis

A continuación, se muestra la estrategia de ubicaciones para cada zona:



* + 1. convocatoria a los miembros del CTGC

El Responsable del CTGC en función de la información proporcionada por el Responsable de Continuidad de Negocio así como del informe de evaluación inicial convocará a los miembros permanentes del CTGC así como a los miembros en función de la contingencia establecidos.

* + 1. INFORME DEL CTGC

El Responsable del Comité Táctico de Gestión de Crisis será responsable de realizar el primer informe de situación con los miembros del CTGC usando las siguientes directrices de actuación:

1. Asignar a una persona que tome nota del acta.

2. Revisar la evaluación de la situación presentada por el Responsable de Continuidad de Negocio y/o pedir directamente los informes desde el conocimiento de tal situación que tienen los miembros del CTGC.

3. Iniciar una ronda de conversaciones para comprobar (si aplican) los siguientes aspectos:

* + Seguridad Personal de Empleados.
  + Situación del edificio/s o sedes afectadas por la contingencia.
  + Estimación temporal de la caída.
  + Análisis, planificación y búsqueda de alternativas “urgentes” para la sustitución de la sede original, afectada por la Contingencia, en caso de que se determine que el siniestro dejará indisponible la instalación por un plazo superior a 45 días (período durante el cual las ubicaciones alternativas designadas pueden acoger la restauración de las actividades y servicios de negocio críticos de HRE.
  + Empleados disponibles.
  + Efectos de la respuesta en la implementación de los procedimientos de evaluación de daños.
  + Informes de situación de terceras personas.
  + Informes de situación de la Centralita e infraestructura tecnológica y de comunicaciones (servicios tecnológicos afectados).
  + Impacto en la imagen de HRE.
  + Recursos disponibles.
  + Discernir el motivo principal o raíz del problema.
  + Solución a ese problema y estrategias.

1. Resumen de impacto en el negocio y recursos disponibles
   * 1. PROCESO DE EVALUACIÓN DE DAÑOS

El origen y naturaleza de las eventuales contingencias o desastres que pueden afectar el negocio de HRE es muy heterogéneo, incluyendo los impactos físicos en las instalaciones y daños en los sistemas como resultado de la materialización de una o varias amenazas, como un incendio, inundación, atentado, terremoto y demás sucesos que pueden afectar el normal funcionamiento del sistema informático corporativo, como los fallos generales de hardware o software crítico, virus, hackers y crackers informáticos, apagones en las telecomunicaciones, errores técnicos o errores humanos.

El principal objetivo de realizar una evaluación de daños es el de determinar el impacto de esa contingencia en el negocio y minimizar el tiempo de caída o parada del mismo.

La información de la Evaluación de Daños será utilizada por el CTGC para determinar si declara o no el desastre y por consiguiente, si se deben activar o no, el Plan de continuidad de negocio de los equipos de recuperación definidos dentro de la estrategia de Continuidad.

El Responsable de Continuidad de Negocio/Tecnológico coordinará junto con el Equipo de Soporte correspondiente y algunas terceras partes afectadas por la contingencia o siniestro, las acciones encaminadas a realizar una evaluación de los daños sufridos por los empleados, edificios, equipamientos y recursos informáticos de hardware, software y telecomunicaciones, así como los ficheros y archivos en papel críticos, que soportan los procesos y actividades de negocio críticos.

* + - 1. Aspectos clave de la Evaluación de Daños

| **Aspectos clave** | **Detalles** | **Contacto** |
| --- | --- | --- |
| Daño en proceso crítico | * Duración estimada de la parada. * Recursos o equipamiento necesario para la vuelta a la normalidad | * Pendiente de definir |
| Evaluación lugar afectado | * Impacto (físico) en la estructura de cualquier edificio * Impacto en equipamiento * Estado del acceso a diferentes áreas dentro del edificio * Capacidad para proteger el edificio. | * Pendiente de definir |
| Identificar políticas de sustitución del personal y equipamiento de negocio | * Tiempo estimado necesario para reparar el edificio: * Días * Semanas * Meses * Si es posible, identificar políticas para la restitución de equipamientos personales, etc. desde el lugar afectado | * Pendiente de definir |
| Valoración de los recursos (departamentos afectados) | * Recursos que son recuperables * Recursos que necesitan ser adquiridos. | * Pendiente de definir |
| Establecer acceso temporal para empleados autorizados | * Coordinar con Infraestructura para establecer un método efectivo que permita el acceso temporal a áreas restringidas, si procede. | * Pendiente de definir |
| Hardware/Software Network/Telecomunicaciones | * Naturaleza de la contingencia * Situación actual * Estado de la plataforma informática corporativa * Recursos necesarios para restaurar/recuperación * Duración estimada de la caída o parada   Informe IT sobre:   * Dimensión del Daño * Sistemas afectados * Terceras partes afectadas * Duración prevista de la caída/parada | * Pendiente de definir |
| Observar Impacto Social | * Observar la reacción pública de los medios de comunicación, a través de los canales y recursos habituales. | * Pendiente de definir |

* + - 1. Sesión de Evaluación de Daños

El Responsable del CTGC evalúa los datos disponibles y si lo estima oportuno convocará al resto de miembros del Comité para valorar los datos de los daños y/o contingencia y tomar las siguientes acciones inmediatas según los aspectos que apliquen en función de la misma:

**Evaluación preliminar del alcance de la contingencia**

En base a la información obtenida por parte del Responsable de Continuidad de Negocio (informe inicial de evaluación) y Equipo de Evaluación, de los servicios de emergencia (Policía, bomberos, ambulancias, etc.), puestos en alerta y personados en el edificio siniestrado, se debe disponer de los siguientes datos, con la finalidad de poseer las evidencias suficientes para soportar la toma de decisión de escalar el Plan de Continuidad de Negocio, declarar el desastre y activar el Plan de Continuidad de los Equipos de áreas críticas de negocio:

* Evaluación preliminar de los **daños personales** sufridos por los empleados del edificio siniestrado. Si de la evaluación preliminar de daños, se desprende que existen empleados que pueden ser críticos, para la restauración de las actividades y funciones críticas de negocio de las áreas críticas afectadas por la contingencia o desastre, que se encuentran indisponibles, por haber resultado heridos por el siniestro, el CTGC asignará al Responsable del Equipo de Recursos Humanos y Medios para proveer recursos alternativos, pudiendo solicitar la colaboración del Responsable del Equipo Tecnológico de la unidad o unidades afectadas para verificar si existen empleados que presenten el perfil profesional requerido o si se contrata por agencia de trabajo temporal, o consultora especializada en selección y contratación de personal, el personal especificado para la restauración de las actividades y procesos de negocio críticos de las unidades afectadas, desde los Centros Alternativos definidos.
* Evaluación preliminar de las **causas del incidente**.
* Estimación inicial y aproximada de la dimensión de los daños a las instalaciones, el equipamiento, los sistemas informáticos y los ficheros o registros vitales afectados
* Estimación inicial y aproximada de **cuándo estará disponible nuevamente el edificio** (Si dicha estimación supera los 45 días, el CTGC debe adoptar las medidas necesarias con carácter urgente, para proveer un nuevo espacio que complemente a las Salas de Continuidad, ya que a partir de ese plazo, se hará necesaria la restauración de determinadas actividades y procesos de negocio propios de la operativa normal, que inicialmente no fueron considerados críticos en el análisis realizado.

1. [DECISIÓN DE DECLARAR LA CRISIS](#_4.1_CONSIDERACIONES_A)
2. 1. CONSIDERACIONES A TENER EN CUENTA PARA LA TOMA DE LA DECISIÓN

Según la información obtenida del proceso de Evaluación de Daños, el CTGC deberá tener en cuenta las siguientes consideraciones, con la finalidad de poseer las evidencias suficientes para soportar la toma de decisión de escalar el proceso de toma de decisión, declarar el desastre y activar el Plan de Continuidad/Tecnológico de los diferentes equipos implicados:

* Tiempo de parada/caída previsto.
* Impacto significativo para el negocio.
* Daño a la instalación/es y nivel de afectación de la plataforma informática corporativa.
* Existencia de víctimas o lesionados críticos.
* Peligro para la integridad física o seguridad personal.
* Incumplimiento en obligaciones contractuales.
* Impacto monetario en los ingresos o pérdida de ventas.
* Conocimiento de los Medios de comunicación de lo sucedido.
* Impactos en el servicio al cliente.
* Socios afectados por la estrategia de recuperación.
* Dimensión de daños a terceros.
  1. ACTIVIDADES UNA VEZ DECLARADA LA CRISIS

Una vez se ha tomado la decisión de declarar la crisis, el CTGC debe decir qué componentes del PCN se deben implementar, y para qué dimensión deberían ser implementados (ejemplo: qué escenario de desastre se ha planteado y que curso de acción se va a seguir para la restauración del negocio). Además, también deberían realizarse las siguientes tareas:

* Informar a los responsables de los Equipos correspondientes de la situación actual de la contingencia.
* Transmitir a los Responsables de las unidades afectadas por la contingencia, el mensaje de que activen su PCN/PCT, en base al escenario de desastre declarado.
* Supervisión de las actividades de los diferentes equipos implicados en la contingencia.
* Monitorizar la ejecución del Plan de continuidad de cada uno de los equipos, una vez activados, así como resolución de las posibles incidencias.

* 1. SUPERVISIÓN DEL PROCESO DE RESPUESTA Y RECUPERACIÓN

Gestionar, coordinar y supervisar el proceso de recuperación, es esencial para garantizar el éxito del Plan de Continuidad de Negocio/Tecnológico y de alcanzar la consecución de los fines perseguidos: minimizar el impacto (cuantitativo y cualitativo) de la contingencia y garantizar la supervivencia de la entidad.

Entre las actividades que deberá desarrollar el responsable del CTGC se encuentran las siguientes:

* Solicitar un resumen periódico de las últimas actividades llevadas a cabo por otros miembros del CTGC.
* Mantener una lista continuada con las limitaciones, revelaciones y asunciones encontradas por el CTGC.
* Asegurarse de que las necesidades razonables del CTGC son cubiertas.

1. [GESTIÓN Y VISIÓN GLOBAL DEL PROCESO DE RECUPERACIÓN](#_7.gestion_y_vision)
2. 1. [GESTIÓN Y VISIÓN GLOBAL DEL PROCESO DE RECUPERACIÓN](#_7.gestion_y_vision) DEL PCN/PCT

Gestionar, coordinar y supervisar el proceso de recuperación, es esencial para garantizar el éxito del Plan de Continuidad de Negocio/Tecnológico de HRE y alcanzar la consecución de los fines perseguidos: minimizar el impacto (cuantitativo y cualitativo) de la contingencia y garantizar la supervivencia de la entidad.

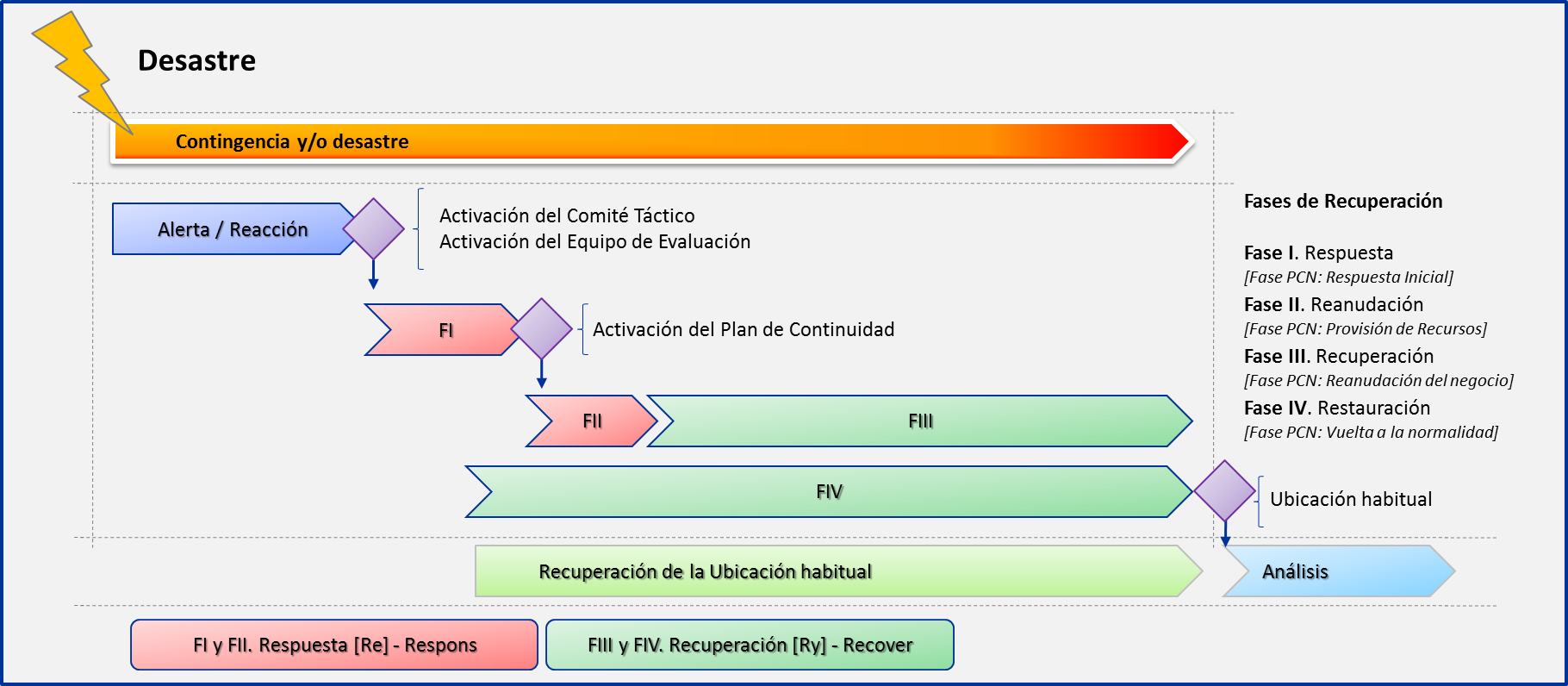
1. Solicitar un resumen periódico de las últimas actividades llevadas a cabo por otros miembros del CTGC.

2. Mantener una lista continuada con las limitaciones, revelaciones y asunciones encontradas por el CTGC.

3. Asegurarse de que las necesidades razonables del CTGC son cubiertas:

En este apartado se describe la cronología lógica de los sucesos que serán coordinados por el CTGC para garantizar una gestión eficiente del proceso de recuperación de negocio de HRE, en caso de contingencia o desastre.

Se sigue la siguiente estructura de fases de recuperación de la actividad de negocio:



1. Ocurrencia de la contingencia o desastre.
2. **Activar la Fase I** (Respuesta) del Plan de Continuidad de los diferentes equipos ubicadas en el edificio que ha sufrido el siniestro.
3. Una vez que se han llevado a cabo las tareas de ejecución del Plan de Evacuación de Emergencia del edificio siniestrado, recuento de empleados, contacto con los servicios de emergencia y securización del acceso al edificio siniestrado, el CTGC inicia las tareas de **evaluación preliminar de daños** (A través de los informes recibidos de los Equipos de Evaluación). Los Responsables de los diferentes equipos implicados ubicados en el edificio afectado se desplazan a la Ubicación Alternativa y realizan las actividades de la Fase I de su PCN/PCT, esperando la indicación del CTGC para escalar y pasar a la **Fase II**.
4. El CTGC, declara el desastre, en base al informe de Evaluación de Daños e informa a los Equipos de Recuperación que pasen a la **Fase II** de su PCN/PCT y activa el Plan de las áreas críticas que están afectadas por la parada de los sistemas y que residen en la sede del edificio siniestrado, indicándole a los responsables que realicen las actividades de las Fases I - II.
5. Al mismo tiempo, el CTGC solicita al Equipo de Medios que pase a la **Fase IV** de su PCN/PCT y a los Responsables de los equipos implicados el traslado a los Centros Alternativos, que lleven a cabo las actividades de la **Fase III**.
6. Cuando todos los equipos hayan realizado las actividades de la Fase III de sus respectivos PCN/PCT, y las actividades de negocio críticas (aplicaciones críticas disponibles), hayan sido reanudadas, el CTGC, tomará la decisión de pasar a la Fase IV y monitorizará la vuelta a la normalidad, y la reanudación de las actividades, ya sea desde el edificio original afectado por la contingencia (si se ha conseguido reparar los daños en menos de 45 días) o desde la nueva sede designada por el CTGC.
7. MANTENIMIENTO DE LA GUIA DEL COMITÉ DE GESTIÓN DE CRISIS
8. 1. ACTUALIZAR LA GUÍA DE ACCIÓN DEL CTGC

Toda la Normativa y documentación del Plan de Continuidad de Negocio/Tecnológico se mantendrá actualizada, para garantizar que cuando tengan lugar cambios o se actualice cualquier dato, se mantenga intacta la funcionalidad de los documentos. A continuación se enumeran algunos ejemplos de sucesos que pueden introducir variaciones en la guía de Acción del CTGC.

1. Adición de nuevas aplicaciones y/o servicios.

1. Reorganizaciones de la Entidad.
2. Cambios de sedes o edificios donde residen las unidades de negocio/soporte críticas.
3. Cambios en los listados de empleados y en otras listas de contacto.
4. Cambios en el lugar de recuperación o ubicaciones alternativas.
5. Problemas y/o debilidades que sean descubiertas durante la ejecución del plan de pruebas.
6. Problemas y/o debilidades surgidos durante la puesta en marcha por contingencia y/o siniestro.
   1. DISTRIBUCIÓN DE LA GUÍA DE ACCIÓN DEL CTGC

La Guía del CTGC se distribuirá al Director Autorizado a declarar el desastre, el Responsable de la Recuperación y, demás miembros del CGC.

La documentación referente a la Continuidad de Negocio/Tecnológico de HRE se alojará en la Intranet.