FINTEC-NOV-001

POLITICA DE CONTINUIDAD DEL NEGOCIO

Historial de versiones.

Versión	Fecha	Modificado por	Descripción breve
V0.1	NOV.2024	Auditores Consultores Recad Limitada	Política Continuidad del Negocio
V0.1	NOV.2024	Directores y Abogado	Política Continuidad del Negocio
V0.1.	NOV.2024	Gerente General	Política Continuidad del Negocio

Aprobada por Directorio 30/11/2024

C.4.2. CONTINUIDAD DEL NEGOCIO

C.4.2.1 DISPOSICIONES GENERALES

En el ámbito de continuidad de negocio, la gestión de riesgo operacional deberá tomar en cuenta los siguientes elementos y adaptarlos de acuerdo con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Contar con una política de continuidad de negocio que considere a lo menos lo siguiente:

- Procedimientos de respuesta ante la ocurrencia de eventos internos o externos que pudieran crear una interrupción en la continuidad de las operaciones del negocio. Para las entidades clasificadas en el Bloque 3, estos procedimientos se deberán referir al menos a la ejecución de un análisis de impacto de negocio (BIA, por su sigla en inglés) y un Análisis de Impacto de Riesgo (RIA, por su sigla en inglés).
- Establecer las principales funciones y responsabilidades sobre la materia, en especial, cuáles serán las instancias encargadas de definir, diseñar, ejecutar y mejorar los procedimientos y metodologías para la gestión de continuidad de negocio. Las políticas de continuidad del negocio formarán parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizada y aprobada al menos anualmente por el directorio u órgano equivalente o con una periodicidad menor en caso de cambios significativos.

b) Contar con personas con conocimientos o experiencia comprobables en estándares de continuidad de negocio y experiencia en la gestión de los riesgos asociados, cuyas actividades principales serán el desarrollo y mejora de las políticas, procedimientos y controles para la gestión de continuidad de negocio.

c) Políticas y procedimientos de capacitación y concientización para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de los riesgos del sistema de continuidad de negocio.

d) El directorio u órgano equivalente deberá mantenerse informado sobre la gestión de continuidad de negocio, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

C.4.2.2 PROCEDIMIENTOS PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIOS

Las entidades que presten los servicios considerados en esta letra E deberán implementar los siguientes elementos para la gestión de la continuidad de negocios, adaptándolos en relación con el modelo de negocios, volumen de operaciones, y número y tipo de clientes:

a) Disponer de un sitio secundario físico o en la nube que permita a la entidad reanudar la operación en caso de que esta se vea interrumpida en el sitio principal, permitiendo restablecer los procesos de mayor relevancia del negocio, tales como plataformas, infraestructura, sistemas y procesamiento de datos.

b) Contar con un Plan de Continuidad de Negocio y Recuperación de Desastres, aprobado anualmente por el directorio u órgano equivalente, que contenga:

- Los procedimientos para la gestión de eventos de continuidad, con un nivel de detalle que permita a las

distintas instancias afectadas determinar las actividades a desarrollar en cada escenario definido.

- Los criterios para la activación del Plan y para la vuelta a la normalidad. Esto incluye evaluar oportunamente los riesgos asociados a la continuidad de negocios que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.

- Roles y responsabilidades del personal.

La periodicidad de actualización de este Plan podría ser mayor dependiendo de la normativa propia de la entidad, o a requerimiento de esta Comisión.

c) Las entidades clasificadas en el Bloque 3 deberán realizar o actualizar, al menos anualmente, ante eventos que amenacen la continuidad de las operaciones del negocio, un BIA con el objeto de identificar los procesos de mayor relevancia para la continuidad de negocio, el impacto que tendría una interrupción de esos procesos, y los tiempos y recursos necesarios para la continuidad y recuperación de estos. El BIA deberá realizarse a nivel estratégico, táctico y operativo. De esos procesos, y considerando los niveles de apetito por riesgo definidos, se deberá determinar:

1) Los tiempos máximos tolerables de interrupción (MTPD por sus siglas en inglés);

2) Los tiempos objetivos de recuperación (RTO por sus siglas en inglés);

3) Los puntos objetivos de recuperación (RPO por sus siglas en inglés);

4) Los niveles mínimos aceptables de operación; y

5) Los recursos humanos, tecnológicos y de infraestructura e información necesarios para su continuidad y recuperación.

Los resultados del BIA deberán ser aprobados por el directorio u órgano equivalente.

d) Las entidades clasificadas en el Bloque 3, definido más abajo, deberán realizar o actualizar, al menos anualmente, una evaluación de impacto de riesgos (RIA) que permita identificar y analizar los riesgos de continuidad de negocio que, de materializarse, provocarían una interrupción en los procesos de mayor relevancia de la entidad. Para lo anterior, se deberá considerar escenarios internos y externos, contemplando, entre otros, la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder o utilizar las instalaciones físicas; y la falta de provisión de los servicios críticos contratados a proveedores.

e) Las entidades clasificadas en el Bloque 3, en consideración de los resultados del BIA y el RIA, deberán definir una estrategia de continuidad de negocio que tenga por objetivo mantener la continuidad de los procesos de mayor relevancia, considerando medidas preventivas para reducir la probabilidad de materialización de daños, minimizar el tiempo de recuperación y limitar el impacto en las operaciones del negocio de la entidad.

f) Se deberá implementar un Plan de Crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las partes interesadas y a esta Comisión, respecto de información relevante respecto del evento de continuidad, las medidas adoptadas para resolverlo y para coordinar una respuesta adecuada dentro de los puntos objetivos y tiempos objetivos de recuperación previstos en el BIA (entidades clasificadas en el Bloque 3 al que se refieren las secciones anteriores).

g) Contar con un procedimiento para el mejoramiento continuo de las políticas, planes y procedimientos de continuidad del negocio con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y

disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.

h) El Plan de Continuidad de Negocio y Recuperación de Desastres deberá ser probado anualmente, de forma de asegurar que es adecuado y efectivo, sin perjuicio de que esta Comisión pueda solicitar una periodicidad diferente para las entidades clasificadas en el Bloque 3. Estas pruebas deberán considerar a lo menos lo siguiente:

1) Deberán ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.

2) Estar basadas en escenarios de riesgo que se asimilen a eventos reales incluyendo escenarios severos pero plausibles. Lo anterior, para demostrar que los procedimientos de continuidad de negocio funcionarán en caso de ser necesarios, incluyendo ataques cibernéticos, desastres naturales y contingencias sanitarias.

3) Las entidades del Bloque 1 y 2, definidas en las secciones anteriores, podrán utilizar indicadores de continuidad del negocio distintos de los establecidos en la Sección B.2.c.

Se deberán emitir reportes de los resultados de las pruebas realizadas al directorio u órgano equivalente, que contengan recomendaciones y acciones para implementar mejoras al Plan de Continuidad de Negocio y Recuperación ante Desastres.

1. Objetivos

Fincap Soluciones Financieras SPA determino que el objetivo de este plan es implementar mecanismos, procedimientos basados en personas, infraestructura, tecnología, procesos, y cultura organizacional que permitan asegurar dentro de los parámetros consensuados con nuestros procedimientos y clientes internos la normal operación del negocio en situaciones extremas.

2. Alcance

El Plan de Continuidad del Negocio o BCP (Business Continuity Planning), debe considerar todas las áreas de la empresa de manera integral incluso desde la estrategia, incorporando el Plan de Recuperación de la Información o DRP (Data Recovery Planning) en conjunto con los elementos mínimos requeridos para continuar con la operación del negocio.
El alcance y su aplicación se encuentra sujeto a los lineamientos establecidos en los diversos manuales de continuidad o relacionados:

- Política de la Seguridad de la Información y Ciberseguridad
- Política de Continuidad de Negocio
- Plan de Continuidad de Negocio y Recuperación de Desastres
- Política de Externalización de Servicios
- Procedimiento de Determinación de Servicios Críticos
- Política de Tratamiento de Excepciones a los Limites de Exposición de los Diversos Riesgos
- Matriz de Riesgo
- Política que Contemple el Funcionamiento del Comité de Riesgo
- Política y Procedimientos de Capacitación (relacionado a contingencias del negocio)

3. Responsabilidades

La empresa definió diferentes roles y responsabilidades.

- **Comité de Riesgo**

  - ✓ Evaluar la contingencia detectada y tomar, en consecuencia, la decisión final de activar o no un

determinado procedimiento de contingencia o una serie de ellos.

- ✓ Evaluar el curso de la contingencia a fin de establecer nuevas necesidades de activación.
- ✓ Evaluar el curso de la contingencia a fin de establecer la desactivación de un determinado procedimiento o un conjunto de ellos.
- ✓ Evaluar el curso de la contingencia y tomar la decisión sobre la finalización de la misma con la posterior notificación sobre la vuelta a la "normalidad".
- ✓ Mantener una fluida comunicación con los coordinadores de Recuperación del Negocio a fin de que puedan mantener informado al comité y que puedan recibir las instrucciones para cada caso.

➢ **Líder del equipo del Plan de Continuidad**

- ✓ Discernir con criterio de negocio y operación la crisis en cuestión y es el responsable de activar el Plan de Contingencia.
- ✓ Contar con la autoridad y el conocimiento necesario para administrar la crisis.
- ✓ Definir el responsable de ejecución del backup y hacer seguimiento de su efectividad.
- ✓ Asegurarse de que se encuentren actualizados los contenidos del plan.
- ✓ Informar al Comité de Crisis sobre nuevas necesidades asociadas al plan.
- ✓ Identificar nuevos escenarios de riesgo potenciales.
- ✓ Coordinar las pruebas del plan de contingencias.

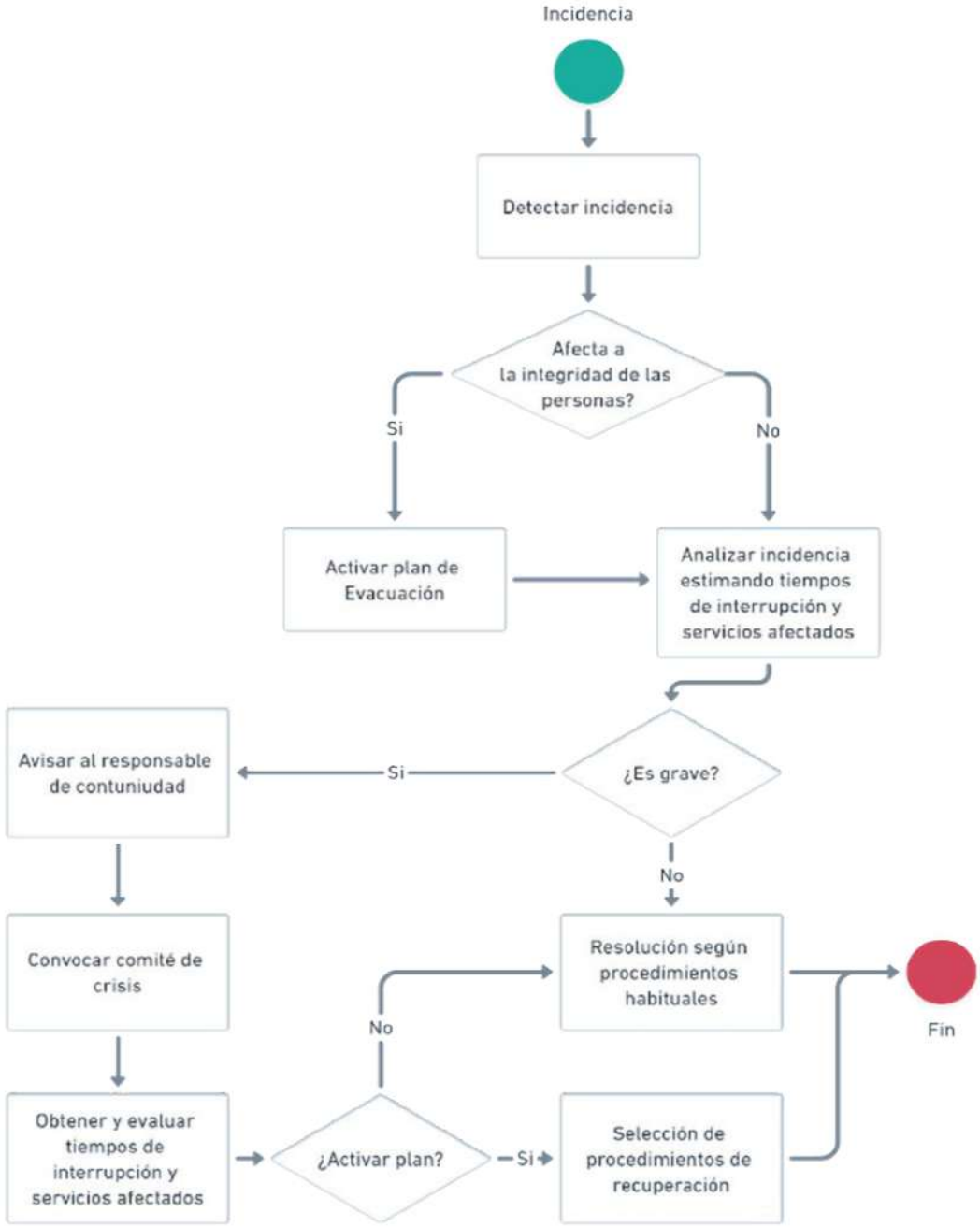
➢ **Miembros del equipo de Continuidad**

- ✓ Mantener fluida comunicación con el comité de crisis informando el curso de la contingencia.
- ✓ Mantener fluida comunicación con el comité de crisis para recibir instrucciones y difundirlas a las líneas.
- ✓ Asegurarse de que la restauración se lleve a cabo en forma efectiva y en función a las necesidades de información de las diferentes partes.
- ✓ Informar y monitorear necesidades especiales y/o desvíos.
- ✓ Asegurarse de que el mapa de proceso se ejecuta conforme a lo establecido en el presente documento.

Ilustración 1

Prioridades del Plan de Continuación de

4. Grafica de Nuestro Plan de Continuidad



5. Etapas de Nuestro plan de Continuidad

- Plan de Continuidad de Negocio (PCN)
- Plan de Continuidad TIC (o Plan de Contingencia TIC, PCTIC)
- Plan de Recuperación ante Desastres (PRD)

6. Fases de un Plan de Continuidad de Negocio

Los planes de continuidad de negocio pueden ayudarnos a:

Ilustración 2
Objetivos del Plan de Continuación de Negocio

Por todo ello, debemos considerar, desde un punto de vista formal, aquellos factores que pueden garantizar la continuidad de una empresa en circunstancias adversas. Este proceso implica las siguientes fases:

- **Fase 0. Determinación del alcance.**
- **Fase 1. Análisis de la organización.**
- **Fase 2. Determinación de la estrategia de continuidad**
- **Fase 3. Respuesta a la contingencia.**
- **Fase 4. Prueba, mantenimiento y revisión.**
- **Fase 5. Concienciación.**

➢ **Fase 0. Determinación del alcance.**
Esta fase es la de menor duración y consume un menor número de recursos.

Según esto, podemos plantear el enfoque desde el punto de vista del activo, o del proceso:

- El enfoque por activo asume la mejora de la continuidad de un conjunto de activos, y a partir de estos obtiene la información de los procesos que los utilizan. Este enfoque es más propio de un PRD o cuando nuestro proyecto lo va a abordar el departamento técnico.
- El enfoque por proceso pretende mejorar la continuidad de un determinado proceso, con independencia de los activos de informática que le den soporte. Este enfoque es más propio del negocio.

➢ **Fase 1. Análisis de la organización.**

Esta fase conlleva la obtención, elaboración y comprensión de las circunstancias, tecnologías, procesos y recursos de nuestra organización. Es importante que involucremos a múltiples actores para que el resultado sea lo más cercano posible a la realidad.

a) Mantener Reuniones

b) Análisis de Impacto Sobre el Negocio

Ilustración 3
Análisis de impacto sobre el negocio

Para cada proceso que hayamos analizado, debemos haber obtenido los siguientes datos:

1. **Tiempo de recuperación o RTO (Recovery Time Objective).**
2. **Recursos humanos y tecnológicos empleados en el proceso**.
3. **Tiempo máximo tolerable de caída o MTD (Maximum Tolerable Downtime).**
4. **Niveles mínimos de recuperación de servicio o ROL (Revised Operating Level).**
5. **Dependencias de otros procesos internos o proveedores externos.**
6. **Grado de dependencia de la actualidad de los datos o RPO (Recovery Point Objective).**

c) Análisis de Riesgo

Para ello, realizaremos los siguientes pasos:

1. Determinar las amenazas a las que está expuesta la organización: robo de información sensible, inundación, pérdida de suministro eléctrico, caída del servidor de correo, etc. A diferencia de otros casos, en este tipo de proyectos nos centraremos en aquellas amenazas que implican una indisponibilidad de los procesos del alcance.

2. Una vez tenemos el listado de las amenazas, determinaremos la probabilidad y el impacto de cada una de esas amenazas. Esto puede hacerse utilizando una escala variable cualitativa, por ejemplo, de uno a cinco: de Muy baja a Muy alta.
   En este caso, nos interesan especialmente aquellos riesgos que impliquen un mayor impacto (y una probabilidad no despreciable), ya que son los que pueden poner en riesgo la continuidad de la organización. Nuestro propósito será identificar aquellos riesgos que pueden poner en peligro la continuidad o la información de los procesos críticos de la organización.

3. Por último, realizaremos el producto de la probabilidad por el impacto de cada amenaza, que nos servirá para identificar aquellos riesgos que debemos tratar con mayor prioridad. De esta manera obtenemos un listado de los riesgos de la organización, donde cada registro será una amenaza, un valor de impacto y uno de probabilidad.

   Aunque estos tres pasos nos proporcionarán el conjunto de amenazas a las que estamos más expuestos, existen metodologías que permiten obtener resultados menos subjetivos y más fiables, pues tienen en cuenta variables como el valor de los activos, sus vulnerabilidades, etc.

   Aunque lo mejor es poder establecer rangos de impacto asociados a valores temporales, de manera que nos sea posible relacionar el MTD/RTO con los tiempos de impacto de una amenaza, este aspecto es complejo de evaluar y determinar por la incertidumbre de la valoración de las amenazas.

"Una vez establecidos los principales riesgos, es decir aquellos con mayor impacto, debemos tratarlos de manera adecuada mediante una de las siguientes estrategias"

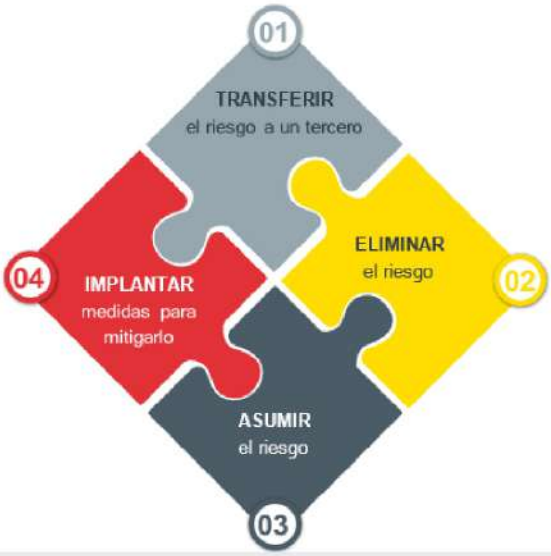


Ilustración 4
Estrategias para el tratamiento de los riesgos

Como respuesta a los riesgos, generaremos un plan de tratamiento de riesgos para cada uno de aquellos que superen el umbral determinado. En algunas ocasiones parte de estas medidas podrán ser consideradas posteriormente para la mejora de la continuidad.

Para cada medida, determinaremos:

- ✓ Descripción de la medida o iniciativa, entendida ésta como un conjunto de controles de la misma naturaleza;
- ✓ Riesgo o riesgos que mitiga;
- ✓ Fecha de la implantación límite;
- ✓ Responsable de la implantación;
- ✓ Recursos necesarios para su implantación.

➢ **Fase 2. Determinación de la estrategia de continuidad.**

Tras los pasos anteriores, deberemos disponer de la siguiente información:

Ilustración 5
Información necesaria para establecer la Estrategia de Continuidad

Algunos elementos potencialmente afectables por una contingencia son los siguientes:

- **Personal.** Según el personal crítico identificado en el BIA, debemos evaluar las diferentes opciones para mitigar su ausencia.
- **Locales.** Deben evaluarse situaciones en las que no se disponga de ubicación para trabajar.
- **Tecnología.** Para las diferentes tecnologías (Prosystem, Cobi, Dicom) implicadas en los activos que dan soporte al proceso se deben valorar posibles alternativas de funciona miento o medidas complementarias.
- **Información.** Debemos considerar todos aquellos aspectos relacionados con la disponibilidad y salvaguarda de la información relacionada con los procesos críticos. (bases de datos)
- **Proveedores.** Debemos garantizar que los proveedores críticos tienen unos tiempos de respuesta acordes a las necesidades de nuestra empresa, y que no estamos expuestos a que nos trasladen sus posibles contingencias. Como resultado de dicho proceso determinaremos las estrategias de recuperación más adecuadas a cada caso, teniendo en cuenta que algunos procesos pueden requerir varias estrategias de recuperación en función de su naturaleza y características.

➢ **Fase 3. Respuesta a la contingencia.**

Una vez hemos definido, en el punto anterior, las estrategias de recuperación para cada uno de los elementos implicados en los procesos críticos afectados por una contingencia, esta fase es la encargada de implementar dicha estrategia. Este proceso comienza con la implantación de las iniciativas identificadas en la anterior fase, y seguirá una fase de clasificación y priorización de medidas, en función del proceso afectado por su implantación y la criticidad de éste.

Durante la implantación, podemos abordar la fase de documentación de respuesta a la contingencia, y a partir de este punto nos centraremos en los elementos más relacionados con la tecnología, aunque son también aplicables a elementos que no sean tecnológicos. Esta documentación se ejecuta en forma de árbol jerárquico, donde el elemento superior gestiona el momento crítico inmediatamente posterior a la crisis, los elementos intermedios ponen las bases para la recuperación de la infraestructura, y los nodos inferiores establecen los procedimientos técnicos detallados para dicha recuperación.

Este proceso lo organizamos en torno a los siguientes elementos que se detallan a continuación.

- **Plan de Crisis (o incidentes)**

Este plan contiene todos los elementos necesarios para la gestión de los momentos iniciales de una crisis:

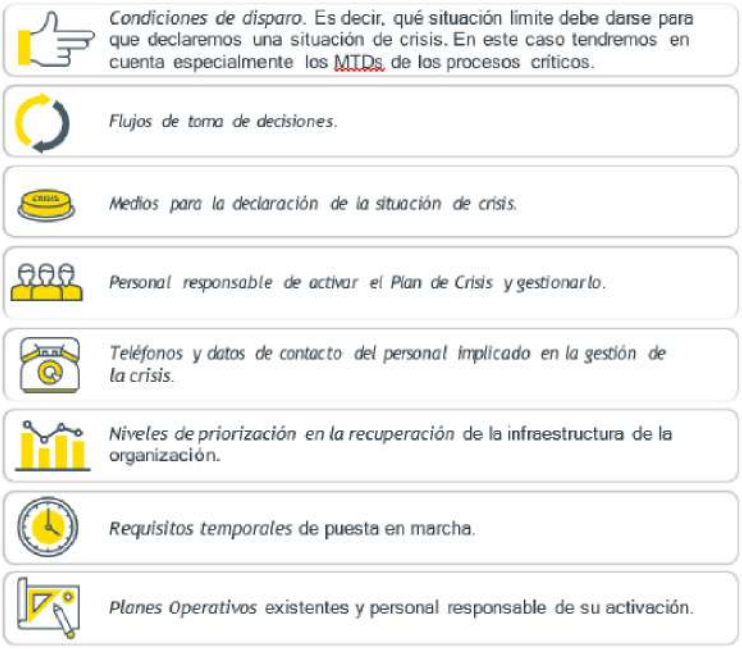


Ilustración 6
Elementos para la gestión inicial de una crisis

- **PLANES OPERATIVOS DE RECUPERACIÓN DE ENTORNOS**
- **PROCEDIMIENTOS TÉCNICOS DE TRABAJO (O DE INCIDENTES)**

➢ **Fase 4. Prueba, mantenimiento y revisión.**

En la ejecución de las pruebas, es necesario llevar a cabo una planificación previa que tenga en cuenta los siguientes aspectos:

- Personal técnico implicado en la prueba;
- Usuario del aplicativo implicado en la prueba;
- Personal externo implicado en la prueba: clientes, proveedores, etc.;
- Descripción de la prueba a realizar;
- Descripción del resultado esperado tras la ejecución de la prueba;
- Hora y fecha de realización; debemos tener en cuenta que siempre que la prueba pueda implicar una pérdida de servicio, ya sea ejecutada con éxito o no, debe planificarse ésta en un horario de mínimo impacto.

Tras la prueba, deberá elaborarse un informe que recoja los resultados y describa las posibles incidencias surgidas durante ésta:

- Resultados no esperados.
- Tiempos estimados superados.
- Mala comunicación con el personal.
- Indisponibilidad de proveedores.
- Etc.

Algunas posibles pruebas que pueden realizarse, siempre teniendo en cuenta que éstas dependen de la idiosincrasia de cada organización y que deben analizarse y plan ficarse cuidadosamente, son las siguientes:

- Realizar la comprobación de que, ante una caída del suministro eléctrico, el sistema de alimentación ininterrumpida y el grupo electrógeno (de existir) entra en funcionamiento.
- Verificar los tiempos de recuperación de los posibles repositorios documentales de la organización en una máquina de pruebas. Los permisos de los servidores deben ser los que cada servidor tenía antes de la recuperación.
- Recuperación de las aplicaciones críticas del negocio (y los datos asociados) en máquinas instaladas durante la prueba.
- Acceso remoto a la infraestructura desde una ubicación remota.
- Si disponemos de entornos replicados o en configuración de servidores, debemos garantizar que

ambos elementos pueden funcionar de manera independiente, y que, ante la caída de uno de ellos, el otro dispositivo funciona correctamente.

- **PLAN DE MANTENIMIENTO**
- **PLAN DE PRUEBAS**

Esto permite:

- Garantizar que la información del plan se mantiene actualizada;
- Garantizar que, en situación de contingencia, la organización podrá recuperarse en los tiempos establecidos, aspecto que puede determinar la continuidad de la organización;
- Incrementar la cohesión del personal implicado en una potencial contingencia;
- Mejorar el conocimiento de los usuarios en relación con las pruebas de continuidad;
- Incrementar la confianza de los usuarios en la organización.

➢ **Fase 5. Concienciación.**

En concreto, debemos plantear un proceso de concienciación que contemple la descripción de los elementos que utilizamos en la continuidad:

- Análisis de impacto sobre el negocio
- Plan de crisis
- Estrategias de recuperación

- **Resumen.**

Tal y como hemos visto, podemos resumir las tareas para realizar un Plan de Capacitación y Continuidad TIC en los siguientes pasos:

- Determinar el alcance de los servicios y procesos objeto de la mejora de su continuidad.

✓ Realizar reuniones con los departamentos implicados y determinar sus necesidades y requerimientos.

✓ Realizar reuniones con personal técnico y determinar con qué capacidades y recursos cuentan.

✓ Identificar los servicios y procesos críticos junto con los activos tecnológicos que los sustentan y sus dependencias.

✓ Obtener los riesgos a los que están ex- puestos los servicios y procesos.

✓ Identificar qué medidas o iniciativas llevar a cabo para que las capacidades tecnológicas sean superiores a las demandas de negocio.

- ✓ Elaborar el plan de crisis para identificar las primeras acciones a realizar cuando ocurre un accidente.
- ✓ Elaborar los planes de recuperación para cada entorno implicado en el alcance.
- ✓ Elaborar las instrucciones técnicas de trabajo para poder llevar a cabo el plan de recuperación.
- ✓ Elaborar el plan de mantenimiento e implantarlo.
- ✓ Elaborar el plan de pruebas e implantarlo, realizando comprobaciones periódicas para verificar que son correctas.
- ✓ Realizar la formación al personal implicado en el Plan de Continuidad de Negocio.

7. CONTROL DE DISTRIBUCIÓN

Fecha	Responsable	Canales de distribución
30/12/2024	Oficial de Cumplimiento	Comunicado Vía BUK y envío por correo electrónico.

8. MODIFICACIONES

No aplica

Rol	Área	Nombre y Contacto
Comité de Crisis	Operaciones	Alvaro Mericq G
Líder del equipo	Area Afectada	Nombre y Contacto
Miembros del equipo de continuidad	Soporte TI Operaciones	Yeison Gonzalez Carlos Ramirez