PLAN DE CONTINGENCIA, CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRE GRUPO REDVOISS

DICIEMBRE 2021

CONTENIDO

Política general de contingencia y continuidad de negocio 3

Objetivos de la política general de contingencia y continuidad de negocio 3

Controles para aplicar la política general de contingencia y continuidad de negocio 3

Controles necesarios para la política general de contingencia y continuidad de negocio 5

Desarrollo de plan de continuidad del negocio y recuperación ante desastre 6

FASE I. Análisis del negocio y evaluación de riesgos 7

FASE II. Estrategia de respaldo 8

FASE III. Desarrollo del plan de continuidad 9

FASE IV. Pruebas y mantenimiento 12

Política general de contingencia y continuidad de negocio

Para Grupo Redvoiss, es primordial el garantizar la seguridad y minimizar los riesgos, por lo que debemos estar preparados y protegernos ante un posible desastre, que pudiera paralizar nuestra actividad y afectar a nuestros clientes. Por ello, estamos conscientes que la información es el activo esencial, tanto los sistemas de información, que se apoyan en tecnologías complejas y novedosas que también pueden estar expuestos a amenazas de seguridad. Por todo ello, estamos convencidos de tener pautas de seguridad basadas en las mejores prácticas del mercado y que indiquen cómo actuar en caso de que haya un fallo que pueda comprometer la continuidad del negocio de nuestra empresa.

Nuestro plan para la continuidad de negocio, contempla las personas responsables de aplicarlo, las operativas a seguir (por ejemplo: implementar un mecanismo de respaldo para nuestra información más crítica), los activos implicados (tanto personales como físicos), indicadores, etc. Este plan de continuidad del negocio, se debe comprobar con cierta frecuencia y de esta forma validar que se puede poner en marcha. Se considera igualmente de ser el caso, cuando contratemos servicios tecnológicos (en la nube o a proveedores externos) o que impliquen el tratamiento de nuestra información. En estos exigimos y comprobamos que tienen planes de contingencia disponibles que se adecuen a nuestra política para la continuidad del negocio.

Objetivos de la política general de contingencia y continuidad de negocio

Diseñar y probar un plan de continuidad de negocio (PCN) que nos permita recuperar en un plazo razonable, la operativa habitual de nuestra empresa para garantizar la continuidad del negocio.

Controles para aplicar la política general de contingencia y continuidad de negocio

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a almacenamiento en la red corporativa.

Los controles se clasificarán en dos niveles de complejidad:

- **Básico (B):** El esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.

- **Avanzado (A):** El esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

- **Procesos (PRO):** Aplica a la dirección o al personal de gestión.
- **Tecnología (TEC):** Aplica al personal técnico especializado.
- **Personas (PER):** Aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Determinar el alcance del PCN** Analizar para que activos y procesos debes garantizar la continuidad.	☐
B	PRO	**Concretar el flujo de responsabilidades** Determinar las responsabilidades de las personas que deben llevar a cabo el plan de continuidad en caso de aparición de desastres.	☐
A	PRO/TEC	**Realización del BIA (Análisis del Impacto en el Negocio)** Elaborar detalladamente el BIA de tu empresa.	☐
B	PRO	**Definir la política de comunicación y aviso a entidades externas** Definir qué tipo de mensajes debe transmitir tu empresa en caso de desastre.	☐
B	PRO	**Caducidad del PCN** Actualizar el plan de continuidad de negocio de tu empresa cada 12 meses	☐
A	PRO/TEC	**Elegir la estrategia de continuidad** Elegir la estrategia de continuidad óptima para tu empresa. Teniendo en cuenta si fuera preciso la implantación de un centro de respaldo.	☐
A	PRO/TEC	**Detallar la respuesta a la contingencia** Detallar los procedimientos y controles específicos a ejecutar ante la aparición de un desastre.	☐
A	PRO/TEC	**Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio**	☐

		Probar y evaluar cada 6 meses del plan de continuidad de negocio de tu empresa.	

Controles necesarios para la política general de contingencia y continuidad de negocio

- **Determinar el alcance del plan de continuidad del negocio.** Se debe seleccionar los activos para los cuales garantizar la continuidad. Para ello nos basaremos en los activos críticos de la clasificación de activos de información.

- **Concretar el flujo de responsabilidades.** Para una correcta ejecución del plan de continuidad del negocio tenemos que determinar quién(es) debe(n) hacerse cargo de la situación en caso de desastre. Definiremos las responsabilidades, la secuencia de decisiones y los canales adecuados para establecer las comunicaciones oportunas.

- **Realización del BIA (Análisis del Impacto en el Negocio)**. Para calcular el riesgo al que estamos sometidos, debemos estudiar las implicaciones de un incidente grave en los activos de información. Para ello determinaremos, entre otros:

    - cuáles son las actividades principales de la organización;
    - las dependencias, con otros procesos o proveedores, de las actividades anteriores;
    - el máximo tiempo que podemos estar sin esa actividad o actividades;
    - el tiempo mínimo de recuperación del servicio a niveles aceptables.

- **Definir la política de comunicación y aviso a entidades externas**. En ciertos casos puede ser necesario determinar qué personas deben notificar las situaciones de desastre a las autoridades pertinentes y a los medios de comunicación. Analizaremos qué tipo de mensaje se debe transmitir y cómo.

- **Caducidad del plan de continuidad del negocio**. Con el fin de mantener actualizado nuestro plan de continuidad de negocio, determinaremos la periodicidad con la cual debería revisarse. Asimismo, analizaremos la necesidad de actualizar nuestro plan tras acometer cambios importantes en nuestros sistemas de información.

- **Elegir la estrategia de continuidad**. Determinaremos que estrategia es la más adecuada para nuestra empresa. Implantaremos políticas de copias de seguridad, donde definiremos la información que debe incluirse en dichas copias, qué tipo de soporte se

utilizará, con qué periodicidad y en qué instalaciones físicas. Asimismo, debemos definir pruebas periódicas para verificar la integridad y la correcta recuperación de la información. Por otro lado, estudiaremos la conveniencia de implantar un centro de respaldo a raíz de los resultados obtenidos durante la elaboración del BIA (Análisis del Impacto en el Negocio). Esto es especialmente importante si el alcance del Plan es el CPD.

- **Detallar la respuesta a la contingencia.** Se debe detallar los procedimientos y controles que aseguren el nivel de continuidad de los procesos y activos esenciales ante una situación adversa.

- **Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio**. Para garantizar que el plan de continuidad del negocio, evaluaremos cada cierto tiempo todos los procedimientos y controles que lo componen, para modificarlos, eliminarlos o añadir nuevos si fuera necesario. Estas actividades se tendrán en cuenta sobre todo tras acometer cambios sustanciales en nuestros sistemas.

Desarrollo de plan de continuidad del negocio y recuperación ante desastre

Para desarrollo de plan de continuidad de negocio con identificar datos relevantes de la empresa: sus productos/servicios, sus objetivos empresariales, procesos internos, etc. El propósito general de un Plan de recuperación es obtener un mapa de acciones que reduzcan “la toma de decisiones” durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costes y aumentando la efectividad.

Podemos dividir un Plan de Continuidad de Negocio en cuatro Fases:

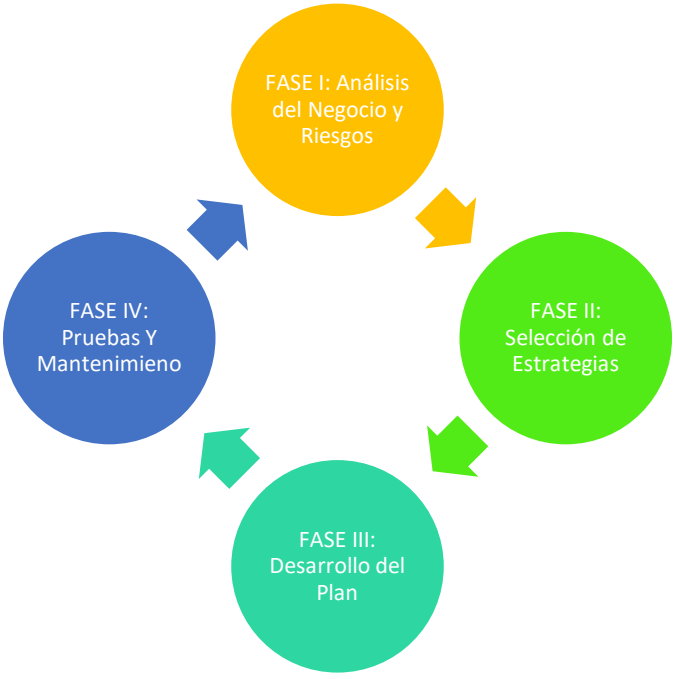

Diagrama de plan de continuidad del negocio y recuperación ante desastre

FASE I. Análisis del negocio y evaluación de riesgos

Dentro de los procesos de negocio que son esenciales para Grupo Redvoiss en los que se van a desarrollar este plan, con el objetivo de asegurar la continuidad operativa están:

¿Cuáles son las actividades más importantes para la compañía?

R.- Grupo Redvoiss, empresa operadora de telefonía local y proveedora de soluciones de telefonía, mensajería, redes de datos, servicios de ciberseguridad y gestión TI.

¿Cómo afectaría económicamente una interrupción de los servicios a medida que va pasando el tiempo sin reanudar el servicio?

R.- El Grupo Redvoiss, entregamos servicios a muchas empresas de distinto tamaño y rubro, siendo estos de carácter crítico o muy relevantes para los clientes, El primer impacto es la provisión de servicios y baja en la facturación, seguido de pérdida de clientes y reputación en el mercado.

¿Cuál sería la capacidad operativa de la empresa a medida que pasa el tiempo?

R.- Contamos con una plataforma de servicios ubicada en 2 Data Centers en modalidad de alta disponibilidad y conexiones redundantes tanto internas como hacia los clientes más relevantes. También las conexiones a Internet se encuentran en ambos Data Centers.

¿Cuál es el plazo máximo para volver a la normalidad sin llegar a incurrir en graves pérdidas?

R.- Los servicios deben ser provistos en forma continua, sin interrupciones. Cualquier indisponibilidad que sobrepase las 4 horas de tiempo ya tiene impacto y no debería pasar de más de 8 horas sin servicios.

FASE II. Estrategia de respaldo

En esta fase mostraremos los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en la empresa. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el análisis de impacto.

Selección de estrategias:

Existen diferentes estrategias para mitigar el impacto de una interrupción. Cada una de estas estrategias tiene unos parámetros de tiempo, disponibilidad y costes asociados que serán más o menos apropiados dependiendo de las funciones de negocio. A continuación, se describen diferentes estrategias para reubicación funcional:

- **No hacer nada:** Este tipo de actuación podría utilizarse en aquellas funciones o actividades que se han clasificado como “no urgentes” en el Análisis de Impacto. En este tipo de estrategia se asume el riesgo.

- **Utilización de espacios propios:** Espacios existentes en la empresa, tales como salas de formación, cafeterías, etc. Este tipo de estrategia requiere una planificación minuciosa.

- **Reutilización de recursos:** Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad.

- **Trabajo Remoto o Teletrabajo:** ya hemos experimentado el trabajo remoto y nos ha resultado eficiente, tomando las medidas de seguridad en las conexiones remotas.

- **Acuerdos Recíprocos:** en este caso tenemos la posibilidad de tener acuerdos entre dos organizaciones (o dos unidades de negocio de la propia compañía diferentes) con características de equipamiento/espacios similares, que permitiría a cada una de las partes recuperar funciones en la otra localización.

- **Sitio alternativo subcontratado a terceros:** esta la contemplada la posibilidad de contratación con empresas especializadas de espacios alternativos para la recuperación de la actividad.

TIEMPO OBJETIVO DE RECUPERACIÓN	INTERNAS	CONTRATADO
Meses	Reconstrucción/ Realojamiento	- - - - - -
Semanas	Edificios prefabricados On-Site	Contratación de unidades móviles o prefabricados
Días	Recuperación “in situ” Trabajo en casa	Subcontratación de procesos en oficinas móviles
Horas	Localizaciones diversas con empleados formados	Re-localización de un grupo de personas
Inmediato	Localizaciones diversas para la misma función	Cambio de funcionamiento a un centro de respaldo subcontratado

Tabla de Estrategias de Recuperación

FASE III. Desarrollo del plan de continuidad

En este apartado describiremos las actividades claves para el Plan de Continuidad. Para ello definiremos:

- Los equipos necesarios para el desarrollo del Plan.
- Las responsabilidades y funciones de cada uno de los equipos.
- Las dependencias orgánicas entre los diferentes equipos.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Los procedimientos de actuación ante incidentes.

- La estrategia de vuelta a la normalidad

Organización de los equipos:

Los equipos de emergencia están formados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan. Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación, los equipos que formar parte del Plan:

- **Comité de Crisis**: Encargado de dirigir las acciones durante la contingencia y recuperación. Está conformado por el Comité de ciberseguridad

- **Equipo de Recuperación:** Su función es restablecer todos los sistemas necesarios (voz, datos, comunicaciones, etc.). Está conformado por el Comité de ciberseguridad y equipo de infraestructura.

- **Equipo Logístico:** responsable de toda la logística necesaria en el esfuerzo de recuperación. Está conformado por el Comité de ciberseguridad

- **Equipo de las Unidades de Negocio:** Encargados de la realización de pruebas que verifiquen la recuperación de los sistemas críticos. Está conformado por el Comité de ciberseguridad y equipo de infraestructura.

Desarrollo de procedimientos:

A continuación, describiremos las funciones que debe desempeñar cada equipo y los procedimientos que se efectuaran serna acordado al momento de la incidencia para cada caso a seguir en cada una de las fases de activación del Plan de Continuidad.

Fase de alerta. Se indican los procedimientos de actuación ante las primeras etapas de un suceso que implique la pérdida parcial o total de uno o varios servicios críticos. Dividiremos esta fase en tres partes:

Notificación: Define cómo y quién debe ser informado en primera instancia de lo ocurrido.

	EVENTO	ACCIÓN
1	Situación de contingencia/incidente	Aviso inmediato con el máximo detalle

	detectado por algún empleado de la compañía. (Fuego, inundación, virus, etc.).	posible al responsable de Personal de turno o a Seguridad.
2	El responsable de turno o de seguridad conoce que ha sucedido una contingencia.	Aviso a la persona de contacto del Comité de Crisis. Aviso a los equipos de emergencia (si procede).

Cuadro Fase de Notificación

Evaluación: Análisis de la situación y valoración inicial de los daños. definición de estrategias.

	EVENTO	ACCIÓN
3	Conocimiento por algún miembro del Comité de incidente ocurrido.	El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad. Será necesario informar de la situación a los siguientes responsables: • Responsable de Seguridad. • Comité de Dirección de la Empresa. • Relaciones Públicas. • Equipo de Recuperación.

Cuadro Fase de Notificación

Ejecución del Plan: Decisión del equipo gerencial de disparar el Plan debido al alcance de los daños.

	EVENTO	ACCIÓN
4	Consideración por parte del Comité de Crisis y ejecución del Plan.	Iniciar el árbol de llamadas. Informar al Comité de Dirección.
5	Paso a la Fase de Transición.	

Cuadro fase de lanzamiento del plan

Fase de transición: esta es la fase previa a la de recuperación de los sistemas. Es importante que en esta fase la coordinación entre los diferentes equipos y equipos de logística, ya que son

éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible.

Podemos dividir la fase de transición en dos partes principalmente:

- Procedimientos de concentración y traslado de personas y equipos.
- Procedimientos de puesta en marcha del centro de recuperación.

Fase de recuperación: Una vez que hemos establecido las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados. Podemos dividir esta fase en dos:

- Procedimientos de restauración.
- Procedimientos de soporte y gestión.

Fase de vuelta a la normalidad: Una vez con los procesos críticos en marcha y solventada la contingencia, se debe activar las diferentes estrategias y acciones para recuperar la normalidad total de funcionamiento. Para ello vamos a dividir esta fase en diferentes procedimientos:

- Análisis del impacto.
- Procedimientos de vuelta a la normalidad

Generación de informes y evaluación:

Una vez solventado el incidente y vuelto a la normalidad, cada equipo deberá realizar un informe de las acciones llevadas a cabo y sobre el cumplimiento de los objetivos del Plan de Continuidad, los tiempos empleados, dificultades con las que se encontraron, etc. Toda esta información servirá para valorar si el plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación de este.

FASE IV. Pruebas y mantenimiento

Plan de pruebas: el plan de continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el plan de pruebas que asegure la viabilidad de las soluciones adoptadas.

El Plan de Pruebas diseñado tiene como objetivos:

- Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la compañía.
- Probar la efectividad y los tiempos de respuesta del plan para comprobar que están alineados con la definición realizada en el diseño.
- Identificar las áreas de mejora en el diseño y ejecución del plan.
- Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.
- Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operativa en situación de contingencia.
- Concienciación y formación para los empleados a través de la realización de pruebas.

Ejercicios técnicos:

Se debe realizar ejercicios requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos verificados durante un ejercicio de simulación son:

- Procedimientos de emergencia.
- Métodos alternativos.
- Líneas de telecomunicaciones de backups.
- Procedimientos de notificación Vendedores / Clientes.
- Capacidad y rendimiento del hardware.
- Portabilidad del software.
- Accesibilidad al centro de respaldo.
- Movilización de los equipos de trabajo.
- Recuperación de ficheros y documentación almacenados en lugar externo.
- Recuperación de datos.

Mantenimiento del plan de continuidad:

Por la propia dinámica de negocio, se van incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos van evolucionando para dar respuesta a las necesidades planteadas. La correcta planificación del mantenimiento del Plan de Continuidad evitará que quede en poco tiempo obsoleto y que en caso de contingencia no pueda dar respuesta a las necesidades.