

Desarrollo del plan de BC/DR

Ing. Fredy Bustamante





Temas

- + Fases de la continuidad del negocio y recuperación ante desastres
- + Definición de equipos de BC/DR y personal clave
- + Definición de tareas y asignación de recursos
- + Planes de comunicación
- + Registro de eventos, control de cambios y apéndices

Introducción

El **análisis de riesgo** nos permitió realizar la evaluación de **vulnerabilidades**, esos datos nos ayudaron a desarrollar una evaluación del **impacto** que los distintos riesgos tendrían en el negocio, por último, tomamos todos los datos e identificamos las **estrategias de mitigación** (evitar, reducir, transferir o aceptar) para los riesgos encontrados. Con esto, ahora tenemos que desarrollar un plan que tome las estrategias de mitigación e **identifique** tanto los **métodos** para implementar esas estrategias como las **personas**, los **recursos** y las **tareas** necesarias para completar estas actividades.



Introducción

Existen muchos métodos para crear el plan de BC/DR, cada empresa tendrá estándares de documentación de procesos y otros temas por lo que puede basarse en cualquier método que se apegue a lo que su empresa utilice.

Sin embargo, los dos propósitos principales de crear el plan son:

1. Pensar en los riesgos y las implicaciones de una interrupción.
2. Garantizar que se cuente con una hoja de ruta lógica a seguir después de un evento de este tipo.

Puede adoptar algún marco de referencia como ISO o COBIT.

Introducción

Podemos dividir el plan en dos partes esenciales:

1. **Conjunto de tareas que puede llevar a cabo para reducir sus riesgos antes de un evento.** Esto puede o no considerarse parte formal del plan de BC/DR, en este caso sí lo tomamos como parte de este.
2. **Pasos que se deben seguir si se produce un desastre o una interrupción del negocio.**

Si se analiza el plan de manera integral, se puede ver que en un extremo del espectro se encuentra la mitigación de riesgos y en el otro extremo, la recuperación ante desastres.

Su estructura se verá más o menos así:

1. Identificar los riesgos
2. Evaluar la vulnerabilidad a los riesgos
3. Determinar el impacto potencial en el negocio
4. Identificar las funciones empresariales de misión crítica
5. Desarrollar estrategias de mitigación para las funciones de misión crítica
6. Desarrollar equipos
7. Implementar estrategias de mitigación
8. Desarrollar pautas de activación del plan
9. Desarrollar pautas de transición del plan
10. Desarrollar procedimientos de capacitación, prueba y auditoría del plan
11. Desarrollar procedimientos de mantenimiento del plan

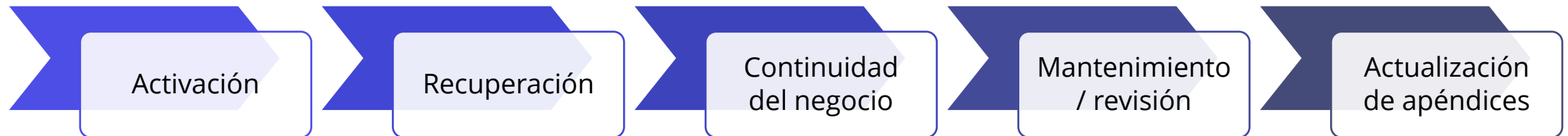
Introducción





Fases de la continuidad del negocio y recuperación ante desastres

Fases de BC/DR



Fases de BC/DR - Activación

Fase de Activación:

- Esta fase aborda el tiempo durante e inmediatamente después de una interrupción.
- Se define:
 - Las condiciones para activarlo, no queremos activarlo ante cualquier evento pequeño, sino cuando realmente sea necesario.
 - Cómo se activa:
 - Quién o quiénes tienen la autoridad para activarlo
 - Qué pasos deberían tomarse para iniciar las actividades de BC/DR
- Incluye:
 - Respuesta y notificación inicial
 - Evaluación del problema y escalamiento
 - Declaración de desastre
 - Implementación del plan

Fases de BC/DR - Activación



Fase de Activación:

Debe definir varios niveles de desastre o interrupción para que usted sepa cuándo, si y cómo implementar su plan.

Puede optar por utilizar un sistema de clasificación de 3 niveles:

- Desastre o interrupción **menor**:
 - Ocurren a menudo y rara vez se activan planes completos.
 - Podemos definir esta categoría con lo siguiente:
 - Normalmente, los efectos se limitan a un componente, un sistema, una función empresarial o solo un segmento de una función empresarial crítica.
 - Las operaciones normales pueden continuar, casi sin interrupciones, ante una interrupción menor.
 - Las funciones empresariales críticas siguen funcionando durante un período de tiempo después de este tipo de interrupción.
 - La falla de un solo sistema o servicio normalmente se puede abordar durante el curso normal de la actividad comercial.

Fases de BC/DR - Activación



- Desastre o interrupción **intermedia**:
 - La probabilidad de ocurrencia es media y el impacto también medio.
 - Podemos definir esta categoría con lo siguiente:
 - Este tipo de interrupción o desastre interrumpe o afecta a una o más funciones o unidades de negocio críticas para la misión, pero no a todas ellas.
 - Las operaciones experimentarán una interrupción significativa; sistemas completos o múltiples sistemas pueden fallar o no estar disponibles, pero no todos.
 - Un evento intermedio podría incluir un incendio o inundación en el edificio que afecte a los sistemas y equipos de TI, daño estructural a la parte del edificio donde se realizan operaciones críticas o donde se ubica el equipo vital.
 - Un evento intermedio también podría incluir un evento con un impacto limitado, pero de larga duración, como un desastre menor donde la recuperación excede el RTO establecido.

Fases de BC/DR - Activación



- Desastre o interrupción **mayor**:
 - La probabilidad de ocurrencia es menor y el impacto es muy alto.
 - Podemos definir esta categoría con lo siguiente:
 - Este evento altera la totalidad o la mayor parte de las operaciones comerciales normales de la empresa y la totalidad o la mayor parte de sus procesos comerciales críticos.
 - Las interrupciones ocurren porque todos o la mayoría de los sistemas y equipos han fallado o son inaccesibles.
 - Esto incluye la destrucción de toda la instalación, de una parte importante de la instalación o de redes, subredes o secciones completas de la empresa.

Fases de BC/DR - Activación

Después de definir el nivel y lo que implica cada uno de ellos, debe definir el proceso para determinar qué partes de su plan de BC/DR deben activarse y a qué miembros del equipo se debe convocar.

Esto dependerá los sistemas, funciones y operaciones que, cuando sean afectadas, causarán una interrupción.

- Activación de equipos de BC/DR
 - Una o más personas deberán evaluar adecuadamente la situación y determinar si es necesario activar el plan o parte de este.
 - Estos equipos pueden ser:
 - Equipo de gestión de crisis
 - Equipo de evaluación de daños
 - Equipo de notificación
 - Equipo de respuesta a emergencias
 - Coordinador o líder de continuidad empresarial
 - Equipo de comunicación de crisis
 - Equipo de recursos y logística
 - Gerente de evaluación de riesgos

Fases de BC/DR - Activación



- Desarrollando triggers
 - Los triggers son los que nos indican cuándo y cómo se activa un plan.
 - Son una serie de condiciones/eventos que nos indican que una interrupción ha ocurrido y dependiendo de estos se determina la respuesta asociada
 - Por ejemplo:
 - Correo de alerta de un servicio que no responde
 - Llamada de un usuario o una persona que indique la falla de algún servicio o la falta de información o algún sistema
 - Correos adicionales de alertas de servidor que no responde
 - Evaluación de los servicios asociados con dicho servidor
 - Verificación visual de una persona o un sistema de vigilancia
 - Al tener la información correspondiente podrá determinar el nivel y si debe o no activar el plan o parte de este.

Fases de BC/DR - Activación

- Por ejemplo:
 - Si una interrupción parece ser intermedia en la evaluación inicial, dentro de las 2 horas siguientes:
 - Intente recopilar información de los servicios de emergencia, si corresponde.
 - Active el equipo de evaluación de daños.
 - Notifique al equipo de gestión de crisis para que esté en alerta.
 - Después de 2 horas desde la notificación del evento, recopile la evaluación inicial del equipo de evaluación de daños. Analice los datos y determine:
 - Tome medidas correctivas y resuelva el problema.
 - Activación parcial o total del plan BC/DR.
 - Después de 3 horas, notifique al equipo de gestión de crisis y siga con los próximos pasos (retirarse, activar completamente).
 - Dentro de las 3 horas posteriores a la notificación del evento, se debe implementar el plan BC/DR si la evaluación indica una interrupción intermedia o importante.

Fases de BC/DR - Activación



Transición a fase de recuperación:

Por último, se debe definir cuándo se cambia de fase, esto suele pasar naturalmente, pero es necesario tenerlo documentado para estar conscientes de la fase en que se está o cuándo cambiar si fuera necesario.

Por ejemplo:

- La evaluación inicial del equipo de evaluación de daños indica una situación de interrupción intermedia.
- Se ha llamado al equipo de gestión de crisis y éste se encuentra en el lugar.
- Se ha detenido o contenido la causa inmediata del incidente.
- Se ha activado el plan intermedio BC/DR.

Se debe tener en cuenta el MTD y requisitos de recuperación por lo que esta información debe estar al alcance del personal en todo momento.

Fases de BC/DR - Recuperación

Fase de Recuperación

- Es la primera fase de trabajo inmediatamente después de la interrupción.
- Esta fase generalmente presupone que la causa de la interrupción ha remitido, se ha detenido o se ha contenido, pero no siempre es así.
 - Dependiendo el evento, se podrá requerir algunas tareas de recuperación mientras este aún está pasando.
- **Podemos decir que los esfuerzos de recuperación tienen que ver con la recuperación de las consecuencias inmediatas del evento, independientemente de que el evento aún esté ocurriendo o no.**
- Esta fase podría incluir tareas como evacuación de las instalaciones, remover equipo que se pueda rescatar rápidamente, evaluación de la situación o de los daños y la determinación de los pasos de recuperación necesarios.

Triggers de transición

- Se deben desarrollar los triggers que nos ayuden a saber cuándo realizar la transición a la fase de continuidad del negocio.
- Por lo general, estos factores tendrán que ver con determinar si los efectos de la interrupción se han abordado y no están empeorando.

Fases de BC/DR - Continuidad

Fase de continuidad del negocio

- En esta fase se definen los pasos necesarios para regresar a una operación “normal”.
- Por ejemplo, en la fase de recuperación podíamos movernos a un lugar temporal y comprar algunos equipos como servidores y PCs, la fase de continuidad del negocio inicia con los pasos necesarios para empezar a operar en la localidad temporal, seguramente con servicios ejecutándose a cierta capacidad menor de lo habitual, y finalizaría con el regreso al sitio principal, para lo cual, se deben definir los pasos a seguir para, por ejemplo, sincronizar datos o ingresarlos a los sistemas correspondientes.
- Después de un desastre es posible que las operaciones o las condiciones cambien de alguna forma por lo que esta fase terminará cuando las operaciones sean totalmente normales dadas las nuevas condiciones.
- Por ejemplo, si el edificio fue destruido, no se esperará a su reconstrucción, sino esta fase terminará cuando estén ubicados en un lugar en donde permanecerán por un largo tiempo.

Fases de BC/DR - Mantenimiento



Fase de mantenimiento / revisión

- Esta fase debe ocurrir se haya o no activado el plan de BC/DR.
- Periódicamente, debe revisar su plan de BC/DR para asegurarse de que aún esté actualizado y sea relevante.
- Después de la fase de continuidad del negocio también es importante realizar esta revisión y mantenimiento pues se debe aprender de la experiencia y corregir o agregar información según corresponda.



Definición de equipos de BC/DR y personal clave

Definición de equipos de BC/DR y personal clave

Definición de equipos y personal clave

- Deben definirse los equipos para satisfacer diferentes necesidades antes, durante y después de una interrupción.
- Debe especificar el puesto o rol particular que satisfaga la necesidad en lugar de especificar individuos.
 - Si asignamos nombres propios tendríamos que estar pendientes de cualquier cambio, además no nos debemos basar en una persona en específico sino en lo que requiere el puesto (acá se puede ver la importancia de la descripción de puestos y planes de carrera dentro de la empresa)
- Se recomienda realizar un documento como descripción de puesto para cada uno de los equipos, para esto puede apoyarse del departamento de RRHH.

Definición de equipos de BC/DR y personal clave

- Una buena descripción del equipo identificará los siguientes atributos:
 - Puestos o funciones laborales incluidas en el equipo (gerente de instalaciones, director de recursos humanos, etc.)
 - Líder del equipo e información de contacto
 - Declaración de misión del equipo o conjunto de objetivos
 - Alcance de las responsabilidades (defina qué es y qué no es parte de la misión de este equipo)
 - Delineación de responsabilidades en cada fase de BC/DR (es decir, ¿cuándo se activará y desactivará el equipo?)
 - Ruta y criterios de escalamiento
 - Y otros datos que considere necesarios

Definición de equipos de BC/DR y personal clave

Veamos algunos equipos comúnmente utilizados y cómo puede incorporarlos a su plan BC/DR.

- **Equipo de gestión de crisis:** Debe contar con representantes de toda la organización y reunir a miembros que tengan la experiencia y la autoridad para lidiar con las secuelas de una interrupción importante. Son quienes dirigen y supervisan todas las acciones del plan y los recursos necesarios.
- **Gestión:** Cada empresa tiene un equipo de gestión que supervisa sus operaciones, es necesario identificar qué miembros de este equipo deben estar involucrados en el plan, de estas personas se debe decidir quién o quiénes tienen la autoridad para activar el plan, pasar de la fase de recuperación a la de continuidad y cómo y cuándo se realizan las pruebas del plan.
- **Equipo de evaluación de daños:** Son quienes evalúan las instalaciones después de un desastre, por esto, debe estar conformado por puestos clave de diferentes áreas como RRHH, Instalaciones, Operaciones y TI, si existen múltiples localidades puede definir partes del equipo de forma local y partes móviles por si fuera necesario la visita de alguien externo al lugar en donde ocurrió el desastre.

Definición de equipos de BC/DR y personal clave

- **Equipo de evaluación de operaciones:**
Puede decidir formar un equipo separado para la evaluación del estado de las operaciones que esté conformado por expertos en el área de forma que puedan dedicar especial atención a esta área.
- **Equipo de TI:** Se necesita un equipo de TI que pueda evaluar el estado de los sistemas y pueda iniciar la fase de recuperación y continuidad. Este equipo debe trabajar de la mano con los equipos de evaluación de daños para determinar el impacto sufrido. Deben participar los coordinadores expertos en recuperación de:
 - Servidores y sistemas operativos
 - Almacenamiento
 - Bases de datos
 - Operaciones de red (LAN, WAN, Telecomunicaciones)
 - Aplicaciones y datos
 - Hardware
 - Sitios alternativos
 - Recuperación/restauración del sitio original
 - Equipo de pruebas
 - Equipo de seguridad de la información

Definición de equipos de BC/DR y personal clave

- **Equipo de apoyo administrativo:** encargado de las actividades administrativas como compras de suministros, logística de entregas con proveedores, resguardo de papeles, etc.
- **Equipo de transporte y reubicación:** Transporte de recursos a una localidad diferente (personas, equipos, suministros, etc.)
- **Equipo de relaciones con los medios:** Dependiendo de la empresa y su relación con el público y los medios, será necesario un equipo que esté en constante comunicación informando a los interesados sobre la situación.
- **Equipo de recursos humanos:** Después de un desastre el personal tendrá necesidades especiales por lo que la administración de personal debe adecuarse a la situación.

Definición de equipos de BC/DR y personal clave

- **Equipo de asuntos legales:** No podemos olvidar que durante y después de un desastre se pueden generar problemas legales por la forma en que se estaba preparados, la forma en que se maneja y la forma en que se recupera el negocio, este equipo debe estar pendiente de cualquier problema legal que se deba abordar.
- **Equipo de seguridad física/personal:** Este equipo debe velar por la seguridad física del personal, tanto por problemas generados durante el desastre como por las actividades de recuperación y continuidad del negocio.
- **Equipo de adquisiciones (equipos y suministros):** Se encargará de administrar el proceso de compra para equipos y suministros que se necesiten derivado del desastre y de la recuperación y continuidad del negocio.

Definición de equipos de BC/DR y personal clave

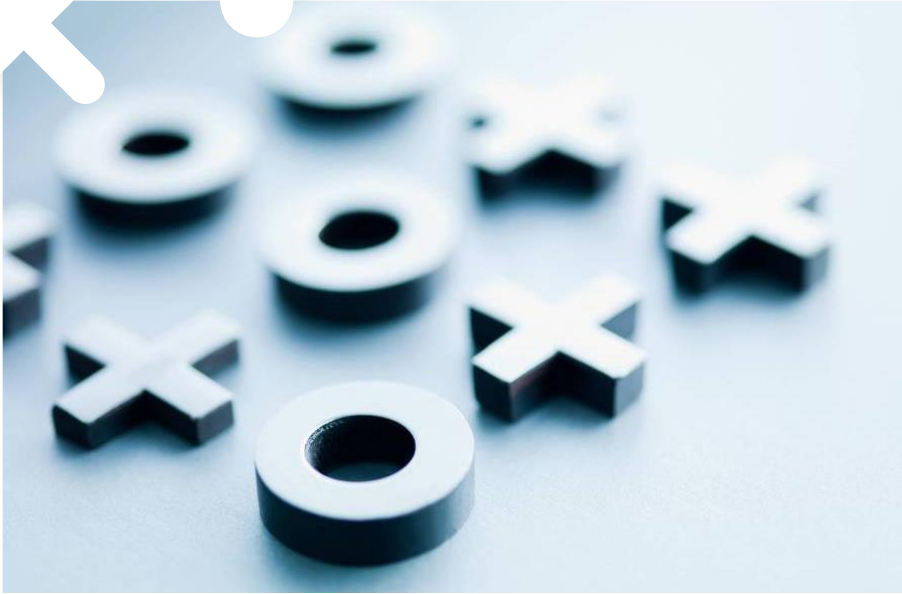
- **Aspectos generales:**

- La conformación de equipos debe realizarse por puestos, roles y necesidades.
- Aun realizándolo de esta forma, se debe revisar que las personas que ocupan los puestos sean las idóneas para el equipo basados en sus habilidades, conocimiento y experiencia, así como su perfil personal.
 - Por ejemplo, una persona demasiado nerviosa no puede estar a cargo de tomar decisiones en una situación muy estresante.
- Algunos miembros o equipos completos pueden ser subcontratados si no existen las personas idóneas dentro de la empresa o si no existe suficiente personal para cubrir todas las actividades.

Definición de equipos de BC/DR y personal clave

- **Información de contacto:**

- La información de contacto de todos los miembros de los diferentes equipos debe estar disponible especialmente cuando se produce un desastre mayor, debe definir en qué medios y lugares mantendrá las diferentes copias y actualizarlas ante cualquier cambio.
- Incluya también proveedores clave, números de emergencia y cualquier otro contacto que pueda necesitarse durante e inmediatamente después de un desastre.
- Debe buscar la forma de que esta información esté disponibles para todas las personas que puedan dar aviso de un desastre sin darles información sensible.
 - Por ejemplo, el número personal del CEO podría ser necesario tenerlo en la lista, pero no todos deberían tener acceso a este.



Definición de tareas y asignación de recursos

Definición de tareas y asignación de recursos

Es fundamental asegurar que las estrategias para mitigar los riesgos se implementen adecuadamente, lo que puede requerir crear planes de proyecto, asignar tareas, recursos y definir cronogramas.

- Asegurar la implementación adecuada de estrategias de mitigación de riesgos.
- Crear planes de proyecto con tareas, recursos y cronogramas.
- Completar actividades críticas antes de una interrupción (UPS, sistemas contra incendios).
- Definir equipos, roles, responsabilidades y desencadenantes de fases.
- Seguir buenas prácticas de gestión de proyectos:
 - Tareas claras en formato verbo/sustantivo.
 - Descomposición de grandes tareas en subtareas manejables.
 - Definir duración, hitos y responsables.
 - Asignar recursos y requisitos.
 - Establecer criterios de finalización y dependencias.

Definición de tareas y asignación de recursos

Sitios Alternos

Vamos a dedicar un poco de tiempo en definir la tarea de implementar un sitio alternativo.

Recordemos que debemos definir cuáles son las condiciones bajo las cuales moveremos servicios hacia un sitio alternativo, para esto debemos tomar en cuenta el MTD, costo de activar el sitio, costo de tener los servicios fuera de línea y otros factores que considere importantes.

- **Criterio de selección:**
 - Debe tomar en cuenta factores como costo, requerimientos técnicos y funcionales, tiempos, calidad, disponibilidad, localización, conectividad, comunicaciones, entre otros.
 - Debe encontrar el balance entre riesgo y mitigación, para esto no puede olvidar el MTD para los servicios críticos y los costos asociados.
 - Priorice los factores o haga una matriz de decisión.

Definición de tareas y asignación de recursos

- **Términos contractuales:**

- Normalmente los proveedores tienen contratos y paquetes de servicio estándar con un costo asociado, algunos tienen mayor flexibilidad y pueden dar servicios especializados.
- Trate de eliminar aquellas opciones que no cumplen con lo mínimo requerido o aquellas que no sean viables por costo, legal, etc.
- Pida que le detallen operativamente todas las opciones y condiciones, si puede hable con clientes actuales o anteriores.
- Comparta las opciones viables con el personal financiero y legal para que las evalúen a detalle.
 - Evalúen en conjunto cada párrafo y asegúrense de entenderlo solicitando aclaraciones y ejemplos.
 - Si encuentra términos vagos, confusos o contradictorios, solicite los cambios que crean necesarios.
 - Nunca confíe en los compromisos verbales, todo debe quedar por escrito con anticipación.

Definición de tareas y asignación de recursos

- **Proceso de comparación:**
 - Asegúrese de especificar qué proceso utilizará para seleccionar al proveedor.
 - Esto puede incluir una lista de requerimientos técnicos, evaluación de la ubicación geográfica, historial financiero, estabilidad y experiencia entre otros.
 - Puede utilizar una matriz de decisión, no solo para tomarla sino también documentarla.
 - Verifique referencias con otros clientes.
 - Pregunte cómo ha respondido la empresa ante diferentes problemas (comunicación, energía, etc.), aunque no se espera que tenga muchos problemas, es normal que tenga algunos y lo importante es cómo responde ante ellos.

Definición de tareas y asignación de recursos

- **Adquisición y pruebas:**

- Una vez haya seleccionado su sitio alternativo o proveedor de almacenamiento externo deberá realizar los arreglos adicionales necesarios para desarrollar la solución de modo que esté completamente lista en el plazo que haya designado.
- Esto podría incluir la compra de hardware y software adicionales, configuración de canales de comunicación y la prueba de todas las soluciones implementadas.
- Debe documentar toda la solución incluyendo cualquier compra y configuración necesarias para implementar el sitio alternativo, así como las pruebas realizadas, esto le ayudará al momento de necesitar el sitio, evaluarlo y probarlo.

Definición de tareas y asignación de recursos

- **Servicios de nube:**
 - Los servicios de nube que ofrecen los diferentes proveedores suelen ser una buena opción para mitigar riesgos.
 - Los servicios en la nube abarcan muchas ofertas de servicios diferentes, entre ellas:
 - IaaS (Infrastructure as a Service)
 - PaaS (Platform as a Service)
 - STaaS (Storage as a Service)
 - DRaaS (Disaster Recovery as a Service)
 - SaaS (Software as a Service)
 - Algunos riesgos asociados a los servicios de nube son:
 - Seguridad en el acceso a sus datos por personal del proveedor
 - Falsa sensación de alta disponibilidad (se debe analizar lo contratado)
 - Cobros adicionales por uso excesivo de algún recurso
 - Problemas legales, por ejemplo, respecto a la propiedad de los datos

Definición de tareas y asignación de recursos

- **Contrato de servicios BC/DR:**
 - Como cualquier contrato, debe involucrar a los departamentos de compras, finanzas y legal, además de entender todos los aspectos técnicos.
 - Al igual que al contratar un servicio de nube o sitio alternativo, tenga en cuenta su MTD, costos y pérdidas potenciales.
 - Realice un análisis financiero para comparar entre los costos de este contrato y las pérdidas potenciales.
 - Desarrolle los requisitos funcionales y técnicos de forma clara
 - Al igual que en el desarrollo de software, sin requisitos claros no podremos tener éxito.
 - Esto ayuda a filtrar proveedores y sus respectivas propuestas.
 - Liste los requisitos obligatorios y opcionales como listas separadas.
 - Determine los niveles de servicio requeridos
 - Aunque esto suele ser parte de los requisitos técnicos, muchas veces los requisitos técnicos se quedan en palabras y no en determinantes de cobro o de penalización, por lo que debe existir una sección de SLA con sus respectivas medidas y consecuencias.

Definición de tareas y asignación de recursos

- **Contrato de servicios BC/DR:** (continuación)
 - Compare la propuesta del proveedor con los requisitos
 - Es necesario que este proceso quede documentado y se pueda indicar de forma objetiva si cumple o no con lo solicitado o a qué nivel.
 - Identificar los requisitos que no cumple la propuesta
 - De la comparación anterior obtenga un listado de los requisitos que no cumple la propuesta
 - Esto le servirá para comparar entre proveedores y propuestas, puede ser que algún requisito no sea fácil de cumplir y se deba evaluar de nuevo
 - Identificar opciones de proveedores no especificadas en los requisitos
 - Identifique y valore las opciones adicionales que ofrecen los proveedores, algunas de ellas pueden volverse relevantes
 - Esto le ayuda a enfocarse en las opciones importantes, pero también en tener un listado de adicionales que pueda servirle para seleccionar algún proveedor



Planes de comunicación

Planes de comunicación



- Es necesario desarrollar varios planes de comunicación, vamos a definir varios de ellos e identificar algunos elementos que deben contener.
- Para cada plan se debe definir lo siguiente:
 - Nombre del equipo de comunicación, miembros del equipo, líder del equipo o cadena de mando
 - Responsabilidades y resultados de este equipo
 - Los límites de las responsabilidades (qué deben y qué no deben hacer)
 - Tiempo y coordinación de los mensajes de comunicación (dependencias, desencadenantes)
 - Ruta de escalamiento
 - Otra información, según corresponda
- Si la empresa tiene un departamento de comunicación, este debe encargarse de estos planes, de lo contrario, es recomendable definir el equipo que se encargará de estos.

Planes de comunicación



- **Interno**

- El plan de comunicación interna es realmente parte del plan de activación e implementación de BC/DR.
- Si ocurre una interrupción, debe tener un proceso establecido para notificar a los miembros del equipo de BC/DR, esto como parte de la activación del plan.
- Este plan debe poder responder a preguntas como ¿Cómo se notificará y actualizará a los miembros del equipo? ¿Qué procesos, herramientas y tecnología se necesitan? ¿Están incluidos en su plan?
 - Recuerde que cualquier recurso debe estar documentado en su plan y asegurarse de tenerlo antes de que ocurra una interrupción.

- **Empleado**

- Es también una comunicación interna, pero difiere del anterior en que es toda comunicación hacia los empleados que no son parte de los equipos de activación y respuesta de BC/DR.
- Si ocurre una interrupción se debe saber cómo informar a todos los empleados, incluyendo respuesta a lo más básico: ¿Qué pasó? ¿Qué se está haciendo para enfrentar el problema? Y ¿A quién deberían acudir para obtener más información?
- Normalmente se define un árbol de comunicación para llegar a todos los niveles con la información correcta.

Planes de comunicación



- **Clientes y proveedores**

- Los clientes y proveedores necesitarán tipos de información diferente pero seguramente similares.
- Se les debe notificar sobre la interrupción, los pasos básicos que se están tomando para resolver el problema, el tiempo estimado para recuperarse y cualquier solución alternativa que sea necesaria mientras tanto.
- La comunicación de este tipo es algo que se debe aprender y practicar para causar el menor impacto negativo o consecuencias de cualquier tipo debido la información o forma de comunicarla, normalmente se le asignará este plan a personas expertas en comunicación.

- **Accionistas**

- Si la empresa tiene accionistas de cualquier tipo, debe comunicarles la naturaleza y el alcance de la interrupción.
- Deberá abordar temas como el impacto financiero a corto plazo, posibles consecuencias legales, viabilidad del negocio.
- Normalmente este plan de comunicación estará a cargo del CEO o algún ejecutivo.

Planes de comunicación

- **La comunidad y el público**

- Por último, en algunos casos se deberá informar a la comunidad y público en general sobre la interrupción.
- Puede ser necesario informar a la prensa local, nacional e internacional.
- Miembros de la comunidad local pueden tener un interés en la interrupción si esto les afecta de alguna forma, sea por el desastre, los servicios que la empresa presta o por actividades secundarias como restaurantes que se llenan por los trabajadores o visitantes de nuestra empresa.
- Este plan de comunicación también de ser ejecutado por personas expertas en relaciones con la prensa y el público.



Registro de eventos, control de cambios y apéndices

Registro de eventos, control de cambios y apéndices

- Al igual que tenemos logs de sistemas operativos o algún equipo de red, debemos mantener un log de las actividades de BC/DR.
- Por ejemplo, para activar un plan debemos tener eventos que disparan el mismo, ya sea que los definamos como eventos durante un tiempo establecido o un evento después de otro (por ejemplo, se va la energía, no regresa por 10 minutos: activar plan x) estos eventos deberían estar en un log para poder justificar por qué activamos un plan que puede significar un gasto y/o consecuencias legales.
- Dado este ejemplo, este registro de eventos es muy importante para nuestra gestión.

Registro de eventos, control de cambios y apéndices

- **Log de eventos en BC/DR**
 - Los logs de eventos no son solo digitales
 - Pueden ser secuencias de notas manuales
 - Sirven para rastrear activaciones de planes de BC/DR (o no activaciones)
 - Registros cronológicos ayudan a tomar decisiones

Registro de eventos, control de cambios y apéndices

- **Aspectos legales de los logs de eventos**
 - Pueden convertirse en documentos legales
 - Consideraciones para equilibrar información y litigios
 - Consulta con consejeros legales

Registro de eventos, control de cambios y apéndices

- **Recomendaciones para los logs de eventos**
 - Registrar solo información relevante
 - Evitar conjeturas, apegarse a los hechos
 - Cumplir con requisitos legales de registro

Registro de eventos, control de cambios y apéndices

- **Control de cambios**
 - Actualización de planes por cambios organizativos
 - Monitorear cambios para minimizar riesgos adicionales

Registro de eventos, control de cambios y apéndices

- **Control de versiones**

- Mantener un historial de revisiones
- Distinción entre revisiones mayores y menores
- Ejemplo de tabla de historial de revisiones:

Número de revisión	Fecha de revisión	Detalle
1.0	22-08-2023	Finalización de primera versión de plan BC/DR
1.1	10-12-2023	Modificación a diagramas de red en sección 4.2
2.0	05-01-2024	Revisión de plan para incluir adquisición de X.
2.1	15-05-2024	Inclusión de nuevos requisitos técnicos en sitio alternativo y cambio de proveedor

Registro de eventos, control de cambios y apéndices

- **Distribución del plan de BC/DR**
 - Métodos seguros de distribución
 - Evitar filtraciones o accesos no autorizados
 - Mantener copias en papel y fuera del sitio

Registro de eventos, control de cambios y apéndices

- **Apéndices en BC/DR**
 - Información relevante pero no central
 - Detalles técnicos, contratos, plantillas
 - Información crítica accesible en un solo lugar

Registro de eventos, control de cambios y apéndices

- **Conclusión**

- Los logs, control de cambios y apéndices son elementos clave
- Aseguran trazabilidad, actualización y soporte documental
- Implementar buenas prácticas para la gestión de BC/DR