

INTRODUCCIÓN A LA CONTINUIDAD DEL NEGOCIO

ING. FREDY BUSTAMANTE

INTRODUCCIÓN

- Tornados, inundaciones, terremotos... La mayoría de nosotros tememos, por lo menos, una experiencia cercana a este tipo de desastres naturales.
- Incendios, robos, cyber ataques... O hemos vivido o escuchado sobre desastres provocados por otras personas.
- Muchas empresas tienen un seguro contra este tipo de amenazas y pagan por este tipo de protección.
- Pero muchas veces no tienen ni siquiera una política de backup
- ¿Por qué?

INTRODUCCIÓN

- ¿Es suficiente con tener un backup de los datos y sistemas en un lugar remoto?
- Antes del año 2000 se pensaba que esto era suficiente y en muchos casos realmente lo era, principalmente porque no se dependía tanto de la tecnología, si no había sistema para imprimir facturas, se hacían de forma manual y posteriormente se ingresaban al sistema.
- El avance de la tecnología y de la dependencia en la misma en nuestra vida cotidiana así como experiencias de otro tipo de desastres como pandemias o cyber ataques nos han demostrado que esto ya no es suficiente.

INTRODUCCIÓN

- Por naturaleza tendemos a evitar pensar en desastres que pongan en peligro incluso nuestra vida, sería demasiado estresante mantenerse pensando en un desastre como un terremoto.
- Sin embargo las empresas suelen tener planes para este tipo de eventos, puntos de reunion, personas encargadas de coordinar una evacuación, etc.
- Además un plan de continuidad del negocio o un plan de recuperación de desastres requiere fondos que podrían ser utilizados para otros proyectos.
- Aunque este tipo de proyectos no debería ser liderado por IT sino por la alta gerencia, la realidad es que el impacto de un desastre será desproporcionadamente mayor en los servicios informáticos por lo que suele ser este departamento quien haga los principales esfuerzos.

DEFINICIONES

- Se suele mezclar o confundir los términos “Continuidad del negocio” y “Recuperación ante desastres”
- La realidad es que estos se traslapan y se complementan, pero no son lo mismo.
- **Plan de continuidad del negocio** (BCP por sus siglas en inglés) es una metodología utilizada para crear y validar un plan para mantener funcionando las operaciones de una empresa antes, durante y después de un desastre o un evento disruptivo.
- La continuidad del negocio se refiere a mantener una empresa funcionando, a pesar del riesgo potencial, amenaza o la causa de una interrupción

DEFINICIONES

- **Disponibilidad continua o alta disponibilidad** es un subconjunto de la continuidad del negocio y se refiere a mantener un servicio activo sin permitir su inactividad por ningún motivo, entre más nos queramos acercar a un 0% de inactividad el costo crece exponencialmente.
- El factor clave para un BCP es qué grado de interrupción puede tolerar el negocio y cuánto está dispuesto a pagar para evitar dicha interrupción, se debe buscar el equilibrio entre estas dos.
- Por ejemplo, si debemos invertir \$1M en un BCP y la empresa obtiene ganancias de \$50M al año, sería totalmente viable, por el contrario si las ganancias fueran de \$1.5M al año deberíamos buscar reducir el costo de dicha inversión.

DEFINICIONES

- **Recuperación ante desastres** es parte del BCP y se ocupa del impacto inmediato de un evento.
 - Recuperarse de una interrupción de los servidores, una violación de seguridad, inundación, etc.
- La recuperación ante desastres implica detener los efectos del desastre tan pronto como sea posible y abordar las consecuencias inmediatas.
 - Apagar equipos en riesgo, mover equipos de lugar, etc.
 - Habilitar servicios en otros equipos y/o localidades, recuperar información, etc.

COMPONENTES DEL NEGOCIO

- Personas
 - Procesos
 - Tecnología
-
- Para un ingeniero en sistemas es normal entender la importancia de estos tres componentes.
 - La tecnología es tan buena como las personas que la diseñaron e implementaron y los procesos desarrollados para utilizarla.
 - Cada empresa es distinta por lo que no existe un efoque único que sirva para todos, por esto se señalan los elementos principales para que cada empresa complete los detalles específicos.

COMPONENTES DEL NEGOCIO

- Las personas en la planificación de BC/DR:
 - Son quienes realizan la planificación y la implementación del BCP y DR.
 - Existen muchos aspectos relacionados con este elemento que a menudo se pasan por alto durante la planeación.
 - Son las responsables del diseño, implementación y monitoreo de los procesos destinados a salvaguardar los datos. Sin embargo, la gente comete errores todos los días.
 - Se necesita de personas de toda la organización para que el BC/DR sea efectivo.
 - Crear un plan sin el aporte de toda la empresa es casi una garantía de fracaso en la planificación y peor aún, en la ejecución.
 - Durante un desastre las personas pueden responder de diferentes formas (bloquearse totalmente, estresarse, liderar, etc.) o no estar disponibles 😞

COMPONENTES DEL NEGOCIO

- Procesos en la planificación de BC/DR:
 - Existen dos fases: Planificación e Implementación.
 - Tener procesos simples y bien probados en los que confiar cuando ocurre un desastre suele ser la diferencia entre una eventual recuperación y un fracaso de toda la empresa.
 - Por ejemplo, un proceso que nos indique qué hacer en caso de que el servidor del sistema de planillas tenga un fallo, este debería incluir la posibilidad de que aún no se haya realizado el pago del bono 14.
 - No hablamos únicamente de cómo recuperar el servidor o instalar uno nuevo, sino qué debería hacer el departamento de RRHH, contabilidad y cualquier otro involucrado para garantizar que el personal reciba el pago a tiempo.
 - ¿Esto en realidad debería ser parte de un BCP? Tomemos en cuenta que la nómina no es un proceso crítico...

COMPONENTES DEL NEGOCIO

- Tecnología en la planificación de BC/DR:
 - Es el componente con el que más estamos relacionados y la razón principal por la que estamos involucrados e incluso iniciamos este tipo de proyectos.
 - Parte de la razón para planificar BC/DR es analizar la tecnología utilizada por la empresa y entender qué elementos son vulnerables a los diferentes tipos de desastres.
 - Si los servidores, equipos de red y PCs están conectados a un UPS y este a un generador de energía, pero pasamos por alto los equipos de aire acondicionado, de igual forma tendríamos un problema en caso de que la temperatura subiera mientras no tenemos energía eléctrica.

MÁS INFORMACIÓN...

- The Business Continuity Institute (UK): www.thebci.org
- DRI International (USA): www.drii.org/DRII/index.htm
- Department of Homeland Security Business Readiness (USA):
www.ready.gov/business/index.html
- Disaster Recovery Journal (USA): www.drj.com

EL COSTO DE LA PLANIFICACIÓN VS EL COSTO DEL FRACASO

- Línea superior: Ingresos (ventas)
- Línea inferior: Utilidades (ingresos – egresos)
- Enfocarse en la línea superior significa aumentar su participación de mercado (acaparandolo o haciéndolo crecer), esto puede causar que sus utilidades se vean afectadas.
- Por otro lado, enfocarse en la línea inferior significa aumentar su utilidad, pero algunas veces se puede reducir costos por medio de acciones no sostenibles a mediano o largo plazo o incluso cerrando operaciones en algunos lugares.
- Lo más común es buscar el equilibrio entre estos dos enfoques.

EL COSTO DE LA PLANIFICACIÓN VS EL COSTO DEL FRACASO

- Pero ¿esto qué tiene que ver con la planificación de BC/DR?
- Conocer el enfoque que tiene su empresa en el momento de proponer una planificación BC/DR le puede dar herramientas para lograr los fondos requeridos.
- Dado que los costos de planificación en términos de personal y recursos necesarios afectarán su costo de operación.
 - Si la empresa está enfocada en la línea superior estos costos no serán tan importantes en dicho momento e incluso puede apoyarse en el hecho de que la empresa esté buscando nuevos clientes para argumentar los beneficios de esta planificación.
 - Por el contrario, si la empresa está enfocada en su línea inferior, el reto de conseguir los fondos necesarios será mayor, deberá buscar justificar esta planificación con eficiencias operativas, costos adicionales que pudieran surgir en el momento de un evento, etc.
 - En cualquier caso, puede estar seguro de que el hecho de no mitigar el impacto de un desastre definitivamente afectará su línea superior e inferior y pondrá en peligro incluso la existencia de su empresa.

EL COSTO DE LA PLANIFICACIÓN VS EL COSTO DEL FRACASO

- Por lo tanto, cuando se compara el costo de la planificación vs el costo del fracaso, la única opción con sentido para el negocio es buscar el equilibrio financiero que nos indique hasta dónde llegar.
- Los desastres pueden resultar en pérdidas enormes, no solo directamente financieras sino también la pérdida de confianza de los inversionistas y la imagen corporativa, además de problemas legales dado que la tendencia es que los datos privados de nuestros clientes son capturados, guardados y transmitidos utilizando redes públicas.
- Muchas personas utilizan el argumento que se gasta demasiado dinero en un plan y en recursos que jamás se utilizarán, aunque esto puede ser cierto no deja de ser necesario, similar a la contratación de un seguro para su automóvil.

UN MAL PLAN VS NINGÚN PLAN

- Un plan mal realizado o incompleto muchas veces es peor que no tener ningún plan.
- El tener un mal plan puede causar que las personas asuman que, en el caso de una emergencia, todos saben qué hacer y cómo hacerlo o al menos existe la documentación necesaria que indique cómo recuperarse de dicha emergencia.
 - Este falso sentido de seguridad puede llevarnos a problemas incluso mayores de los que pueda causar el evento por sí mismo.
- Cuando los desastres ocurren existen muchas prioridades y muchas empresas no son una de ellas, por ejemplo, de necesitarse atención médica el personal de emergencia prestará atención a hospitales, colegios, etc. La mayoría de las empresas tendrán que valerse por sí mismas para evacuaciones, atenciones médicas inmediatas, etc. Un plan mal realizado y/o mal implementado puede causar incluso problemas legales al no haber tenido procesos y recursos básicos como salidas de emergencia bien señalizadas, medicina básica, etc. O incluso por perder información valiosa para nuestros clientes a pesar de haber tenido un plan para evitarlo.

OPTIMISMO VS PESIMISMO

- Se debe buscar un balance entre el optimismo y el pesimismo.
- Optimismo: puede descartar riesgos potenciales y, a menudo, minimizará el impacto potencial de los acontecimientos.
- Pesimismo: hace pensar que todo posible riesgo ocurrirá y tendrá un gran impacto, incluso mayor del que realmente podría ocurrir.
- Ninguno de los dos extremos es correcto, se debe buscar el equilibrio y ser realista.
- Se puede llegar a planificar para eventos muy grandes y no estar preparados para eventos pequeños y que son más comunes de forma que algo simple nos puede afectar más de lo que debería.
- Se debe buscar el mejor camino para avanzar en la planificación, los planes para eventos pequeños suelen servir como base para los eventos más grandes.

TIPOS DE DESASTRES A CONSIDERAR

- Por lo general pensamos en desastres comunes, pero es muy probable que pasemos por alto algunos que pueden tener impacto en la empresa, por esto es necesario analizar y revisar bibliografía que nos de ideas adicionales.
- El listado puede ser muy extenso, es importante pensar en las operaciones de la empresa, sus localidades y la industria a la que pertenece para determinar cuáles de ellos son importantes como para ser considerados.

TIPOS DE DESASTRES A CONSIDERAR

- Las amenazas o peligros se dividen en tres categorías básicas:
 - Peligros naturales
 - Peligros causados por el hombre
 - Accidentes y peligros tecnológicos

NATURALES

- Cold weather-related hazards
 - Avalanche
 - Severe snow
 - Ice storm and hail storm
 - Severe or prolonged wind
- Warm weather-related hazards
 - Severe or prolonged rain
 - Heavy rain and/or flooding
 - Floods
 - Flash flood
 - River flood
 - Urban flood
 - Drought (can impact urban, rural, and agricultural areas)
 - Fire
 - Forest fire
 - Wild fire—urban, rural, agricultural
- Urban fire
- Tropical storms
- Hurricanes, cyclones, and typhoons (name depends on location of event)
- Tornado
- Wind storm
- Geological hazards
 - Earthquake
 - Tsunami
 - Volcanic eruption
 - Volcanic ash
 - Lava flow
 - Mudflow (called a lahar)
 - Landslide (often caused by severe or prolonged rain)
 - Land shifting (subsidence and uplift) caused by changes to the water table, man-made elements (tunnels, underground building), geological faulting, extraction of natural gas, and so on

CAUSADOS POR EL HOMBRE

-
- Human-caused hazards, also known as anthropogenic hazards, are a bit more diverse in their nature.
 - Terrorism
 - Bombs
 - Armed attacks
 - Hazardous material release (biohazard, radioactive)
 - Cyber attack
 - Biological attack (air, water, food)
 - Transportation attack (airports, water ports, railways)
 - Infrastructure attack (airports, government buildings, military bases, utilities, water supply)
 - Kidnapping (nonterrorist)
 - Bomb
 - Bomb threat
 - Explosive device found
 - Bomb explosion
 - Explosion
 - Fire
 - Arson
 - Accidental
 - Cyber attack
 - Threat or boasting
 - Minor intrusión
 - Major intrusión
 - Total outage
 - Broader network infrastructure impaired (Internet, backbone, etc.)
 - Civil disorder, rioting, and unrest
 - Protests
 - Broad political protests
 - Targeted protests (specifically targeting your company, for example)
 - Product tampering
 - Radioactive contamination
 - Embezzlement, larceny, and theft
 - Kidnapping
 - Extortion
 - Subsidence (shifting of land due to natural or man-made changes causing building or infrastructure failure)

ACCIDENTES Y PELIGROS TECNOLÓGICOS

- Similar a los causados por el hombre pero estos son no intencionales.
 - Transportation accidents and failures
 - Highway collapse or major accident
 - Airport collapse, air collision, or accident
 - Rail collapse or accident
 - Water accident and port closure
 - Pipeline collapse or accident
 - Infrastructure accidents and failures
 - Electricity—power outage, brownouts, rolling outages, failure of infrastructure
 - Gas—outage, explosion, evacuation, collapse of system
 - Water—outage, contamination, shortage, collapse of system
 - Sewer—stoppage, backflow, contamination, collapse of system
- Information system infrastructure
- Internet infrastructure outage
- Communication infrastructure outage (undersea cables, satellites, etc.)
- Major service provider outage (Internet, communications, etc.)
- Systems failures
- Power grid or substation failure
- Nuclear power facility incident
- Dam failure
- Hazardous material incident
- Local stationary source
- Nonlocal or in-transit source (e.g., truck hauling radioactive or chemical waste crashes)
- Building collapse (various causes)

ELEMENTOS BÁSICOS DE LA PLANIFICACIÓN DE BC/DR

- Nuestro rol como profesional de TI en BC/DR es único pues aún no necesariamente siendo los responsables integrales de la planificación de BC/DR somos responsables del aspecto tecnológico y este está tan inmerso en todas las operaciones de las empresas que resulta imposible separarlo como un tema independiente.
- Por esta razón siempre tendremos que abordar BC/DR de forma integral y se deberá determinar el rol específico del departamento de TI según sea apropiado para la empresa correspondiente.
- El equipo para este proyecto se debe conformar incluyendo personal experto de las diferentes áreas de la empresa.

ELEMENTOS BÁSICOS DE LA PLANIFICACIÓN DE BC/DR

- Diseño de sistema confiable
- Punto único de fallo
- Estos conceptos son bien conocidos por un profesional de TI que abarca desde el diseño de alguno de los equipos (servidor con dos fuentes, raid, cambio de ciertas piezas sin necesidad de apagarlo, etc.) hasta el diseño de la red, data center, etc. Y se refiere básicamente a construir redundancias y backups que permitan mantener servicios funcionando a pesar de algún fallo en algún componente.
- Estos pueden ser el inicio de un plan de BC/DR, ya sea que estén implementados o se implementen como parte de este proceso.

PASOS BÁSICOS EN LA PLANIFICACIÓN DE BC/DR

1. Inicio del Proyecto
2. Evaluación de riesgos
3. Análisis de impacto del negocio
4. Desarrollo de estrategias de mitigación
5. Desarrollo del plan
6. Capacitación, pruebas y auditorías
7. Mantenimiento del plan

INICIO DEL PROYECTO

- El inicio del proyecto es muy importante, acá es donde se empieza a involucrar y a buscar el apoyo de toda la empresa.
- Obtener el apoyo de los ejecutivos y de toda la empresa en general es determinante en el éxito del proceso de planificación BC/DR.
- El lanzamiento del proyecto con los principales involucrados debe notarse, todos deben enterarse, se puede utilizar los diferentes medios de comunicación (formal e informal) e incluso asambleas generales para informar de la importancia, los pasos, lo que se requiere del personal, etc.

EVALUACIÓN DE RIESGOS

- En este paso se debe analizar con cada uno de los miembros claves de su empresa (estén o no en el equipo del proyecto) cuáles son los potenciales riesgos a los que se podrían enfrentar.
- Como profesional de TI, usted juega un papel clave al explicarles los efectos de los diferentes riesgos sobre la tecnología para que se pueda tomar en cuenta no solo lo que les afecta directamente (como lluvias al transporte) sino también la falta o limitación de la tecnología frente a estos u otros riesgos.

ANÁLISIS DE IMPACTO DEL NEGOCIO

- Una vez listados los riesgos debe prestar atención al potencial impacto de estos.
 - En este paso un profesional de TI necesita información de los expertos de cada área.
-
- Usted puede determinar el costo de reposición de un equipo o de tener un equipo de respaldo para emergencias, pero, por ejemplo, ¿cuánto cuesta el no poder vender en línea durante 1 hora? ¿quién debería calcular esto?

DESARROLLO DE ESTRATEGIAS DE MITIGACIÓN

- Para cada riesgo identificado que tenga un impacto significativo se deben analizar las opciones.
- ¿Qué tanto se puede tolerar, reducir, evitar o transferir el riesgo y el impacto?

DESARROLLO DEL PLAN

- Luego de los pasos de análisis estarán listos para desarrollar el plan, para lo cual se debe determinar:
 - Requerimientos técnicos y del negocio
 - Alcance
 - Presupuesto
 - Cronograma
 - Métricas de calidad
 - Etcétera

CAPACITACIÓN, PRUEBAS Y AUDITORÍA

- Después de haber desarrollado el plan se debe entrenar a todo el personal en cómo implementarlo.
- Realizar simulacros y ejercicios, especialmente para aquellos riesgos con mayor probabilidad de ocurrir.
- Pruebas de evacuación, de restauración de backup, de levantar servicios en un sitio remoto, etc.

MANTENIMIENTO DEL PLAN

- Si no se le da un mantenimiento adecuado, se actualiza y se revalida cada cierto tiempo el plan puede volverse inútil al momento de la ocurrencia de un desastre.
- Tan simple como que las instrucciones para levantar un servicio pertenezcan a una versión anterior del software o que los datos de contacto para personas o empresas clave ya no sean válidos hasta tener procesos completos que ya no se realicen o departamentos que ya no existen.

Mantenimiento del plan de BC/DR

Ing. Fredy Bustamante

Temas a tratar



Gestión de cambios en el plan de BC/DR



Estrategias para gestionar cambios



Auditoría del plan de BC/DR



Actividades de mantenimiento del plan de BC/DR



Cierre del proyecto

Introducción

Mantener el plan que se ha desarrollado puede ser uno de los mayores desafíos en el proceso de continuidad del negocio y recuperación de desastres. Si se ha experimentado falta de entusiasmo o resistencia al proceso de BC/DR, es probable que el apoyo para mantener el plan desaparezca rápidamente. Muchos asumen que, una vez que el proyecto se completa, pueden darlo por concluido y seguir adelante. Sin embargo, la realidad es que el mantenimiento del plan es esencial para una preparación continua.

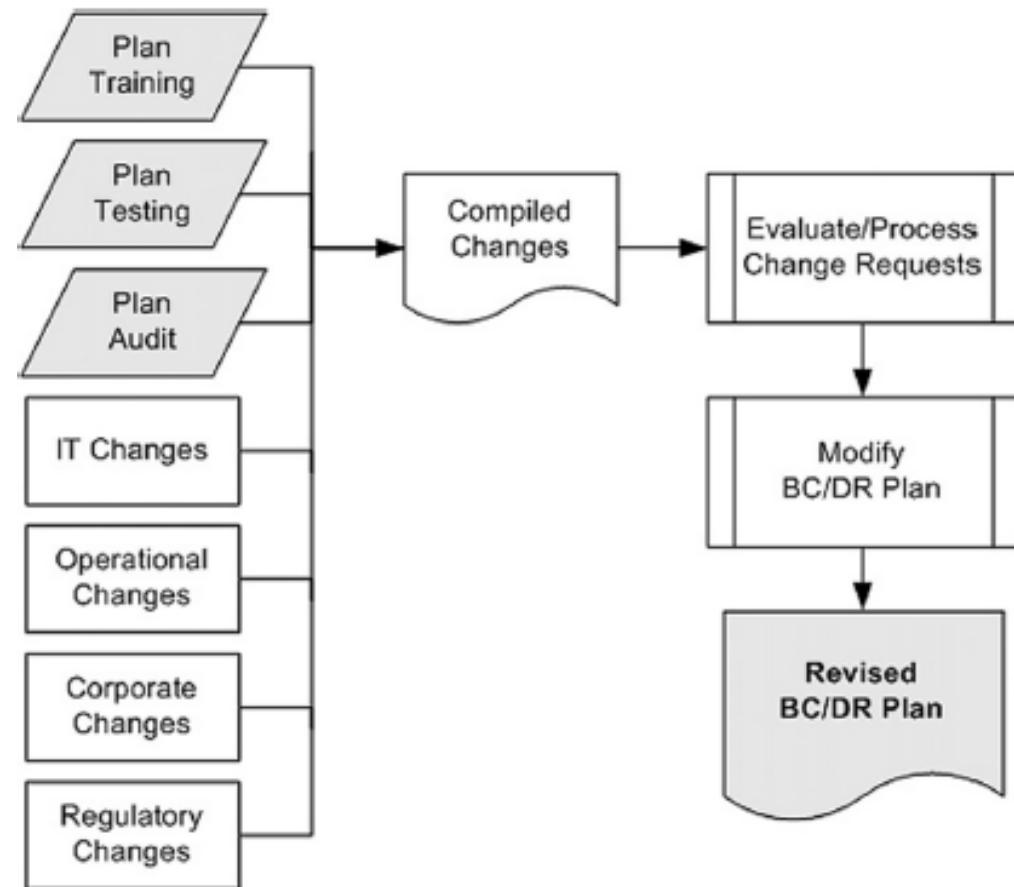
La ventaja es que, en este punto, el plan ya existe y varias personas han apoyado a realizarlo, se han cambiado procesos introduciendo el plan a lo largo de la organización.

Introducción



Gestión de cambios en el plan de BC/DR

- El cambio es constante en las organizaciones:
 - Cambios en operaciones, tecnología, personal, regulaciones, etc.
- ¿Cómo reflejar estos cambios en el plan de BC/DR?
 - Estrategias para reducir la complejidad de actualizar el plan sin un equipo dedicado.



Gestión de cambios en el plan de BC/DR

- Podemos resumir los pasos en:
 1. Monitorear cambios: Identificar fuentes de cambio.
 2. Evaluar el impacto: Determinar si el cambio afecta el plan de BC/DR.
 3. Adaptar el plan: Ajustar el plan si el cambio tiene impacto.
- Esto puede requerir un análisis de riesgos y desarrollo de nuevas estrategias de mitigación.

Gestión de cambios en el plan de BC/DR

- Capacitación, Pruebas y Auditorías
 - Las actividades de capacitación y prueba revelan áreas de mejora en el plan.
 - Es fundamental capturar y revisar las solicitudes de cambios derivadas de estas actividades.
- Cambios en tecnologías de la información
 - Revisar los cambios en la infraestructura tecnológica.
 - Evaluar el impacto de cada cambio tecnológico en el plan de BC/DR.
 - Se recomienda agregar dos pasos en los proyectos de TI:
 - Fase de planificación: Evaluar el alcance de cambios en el plan BC/DR.
 - Cierre de proyecto: Actualizar la documentación del plan BC/DR.
 - Ejemplo: "Evaluar el impacto de la renovación de equipo en el plan de BC/DR".
 - Mantener una lista de cambios en IT y evaluar su impacto en el BC/DR.
 - Preguntas clave:
 - ¿El cambio mejora o empeora la capacidad de recuperación de la organización?
 - Balancear el impacto del cambio en el BC/DR antes de su implementación.

Gestión de cambios en el plan de BC/DR

- Cambios en las Operaciones
 - Las funciones críticas determinadas en la evaluación de riesgos deben estar actualizadas.
 - Cambios operativos:
 - Reorganización, expansión, nuevos departamentos, instalaciones o estructuras de gestión.
 - Auditoría del plan BC/DR: Ayuda a identificar ajustes necesarios en respuesta a cambios operativos.
 - Por ejemplo: un cambio paulatino entre la venta en locales a venta en línea puede causar cambios importantes en la operación pero estos pueden pasar desapercibidos por irse generando a lo largo de mucho tiempo.

Gestión de cambios en el plan de BC/DR

- Cambios Corporativos
 - Impacto de fusiones, adquisiciones, escisiones o reestructuraciones.
 - Estos cambios pueden desafiar significativamente el plan de BC/DR.
 - Evaluación continua: Integrar el plan de BC/DR en operaciones y planificación de IT.
 - Tratar de no depender de la orden directa de un gerente
- Cambios Legales, Regulatorios o de Cumplimiento
 - Adaptar el plan de BC/DR a nuevas leyes o regulaciones.
 - Impacto en la seguridad de datos y otros procesos operativos o tecnológicos.
 - Evaluación de cumplimiento: Asegurar que el plan actual cumple con los nuevos requerimientos.

Estrategias para gestionar cambios

- 2 estrategias clave para gestionar el cambio
 - Tener un proceso para monitorear los cambios.
 - Tener un proceso para evaluar solicitudes de cambio.
- Es más fácil monitorear los cambios y responder conforme sea necesario, en lugar de hacerlo una vez al año y tener que recordar qué ha cambiado desde la última revisión del plan.
- La forma más sencilla de monitorear el cambio en toda la organización, en relación con los planes de BC/DR, es añadir uno o dos pasos en los procedimientos operativos estándar, como: “Determinar el impacto, si lo hay, en el plan de BC/DR.” “Si existe impacto, enviar solicitud de cambio BC/DR a [posición responsable].”

Estrategias para gestionar cambios

- Monitoreo del cambio
 - Implementar procesos de monitoreo facilita el mantenimiento del plan de BC/DR.
 - Desarrollar procesos que se integren en los flujos de trabajo diarios para evaluar rápidamente el impacto potencial de los cambios en el plan de BC/DR.
 - Si el cambio no tiene impacto, se puede ignorar desde la perspectiva de BC/DR.
 - Si tiene impacto, se debe enviar una solicitud de cambio al equipo de BC/DR.
 - Por ejemplo, una solicitud de cambio puede ser simplemente anotar que el líder del Equipo de Respuesta a Emergencias ha cambiado. Este cambio debe activar la revisión del plan BC/DR (nombres de contacto, teléfonos y lista de equipo).

Estrategias para gestionar cambios

- Monitoreo de cambios en tres áreas clave
 - Personas
 - Revisar periódicamente cambios de personal que impacten en el plan.
 - Esto puede ser parte de una auditoría del plan de BC/DR.
 - Procesos
 - Asignar expertos o miembros del equipo BC/DR para monitorear cambios en procesos clave y marcarlos para revisión.
 - Tecnología
 - Monitorear cambios tecnológicos, con mayor énfasis en equipo especializado, para asegurar que el plan BC/DR se mantenga actualizado.

Estrategias para gestionar cambios

- Evaluación e incorporación de cambios
 - El proceso de revisión de cambios debe estar bien definido y debe asignarse a alguien responsable.
 - Recuerde la regla de gestión de proyectos: cada tarea necesita un responsable. Sin alguien designado, no se completará la tarea, y es clave para mantener actualizado el plan de BC/DR.
 - Algunos cambios pueden requerir una revisión muy profunda del plan, por ejemplo, una mudanza a un nuevo edificio, cambio de la infraestructura a la nube.

Estrategias para gestionar cambios

Puntos clave para un proceso periódico de gestión de cambio:

1. Compilar todas las solicitudes de cambio y priorizar según riesgo, vulnerabilidad e impacto.
2. Determinar si alguna solicitud es obligatoria por ley o regulación, de ser así, marcarla como “cambio requerido”.
3. Revisar las solicitudes para eliminar redundancias y asegurar relevancia.
4. Priorizar la lista final y evaluar cada cambio en función de:
 - Riesgos y amenazas seleccionadas
 - Vulnerabilidad ante amenazas
 - Análisis de impacto en el negocio
 - Estrategias de mitigación de riesgos
5. Evaluar costos, perfil de riesgo (si aumenta o reduce el riesgo), deseabilidad y viabilidad.
6. Decidir si la solicitud se incorpora, se retrasa, se rechaza o se cierra.
7. Documentar el impacto en el plan BC/DR para cada cambio aprobado y notificar a los solicitantes.
8. Determinar si se necesita entrenamiento o pruebas adicionales para cada cambio aprobado.
9. Para cada cambio “retrasado”, documentar la razón y cómo se procesará después y notificar a los interesados.
10. Para cada cambio “rechazado” o “cerrado”, documentar la razón de denegar el cambio y notificar a los interesados.
11. Para cada cambio “aprobado”, revisar el plan de BC/DR, realizar los cambios y notificar a los interesados.

Auditoría del plan de BC/DR

¿Por qué auditar el plan BC/DR?

- La auditoría del plan BC/DR consiste en revisar el plan contra requisitos específicos.
- Permite verificar si el plan cumple con las prácticas comerciales, objetivos, estrategias, y situación financiera de la organización.
- También se revisa el plan en función de restricciones externas, como requisitos legales o regulatorios (ej., ISO).
- La auditoría no prueba ni entrena sobre el plan; es una revisión imparcial.
- La auditoría no garantiza que los pasos y procesos del plan funcionen en práctica.
- El objetivo es evaluar si el plan satisface las necesidades generales de la organización.

Auditoría del plan de BC/DR

Una auditoría debe realizarse como un proyecto estándar con un plan de auditoría que incluya, al menos:

- Alcance, cronograma, requisitos y limitaciones de la auditoría
- Revisión de riesgos corporativos y estrategias de gestión de riesgos, incluyendo BC/DR
- Revisión del impacto en el negocio
- Revisión de actividades de desarrollo del plan de BC/DR
- Revisión de planes y actividades de pruebas del plan de BC/DR
- Revisión de planes y actividades de entrenamiento del plan de BC/DR
- Revisión de procesos de gestión de cambios y mantenimiento del plan de BC/DR

Auditoría del plan de BC/DR

Propósito de la auditoría en el mantenimiento del plan:

- La auditoría ayuda a mantener el plan al identificar brechas o debilidades en estos procesos.
- Al revisar estos elementos, es posible generar solicitudes de cambio que debe gestionar el equipo de BC/DR.
- Crear una lista de verificación de auditoría facilita revisar el plan periódicamente y usar un método estandarizado cada vez.

Actividades de mantenimiento del plan de BC/DR

Existen diversas actividades, además de la gestión de cambios, que pueden ayudar a mantener el plan actualizado y listo para activarse:

1. Notificar actualizaciones: Si el plan se revisa, notificar a los miembros del equipo de BC/DR oportunamente.
2. Sistema de numeración de revisiones: Utilizar un sistema para que los miembros sepan si tienen la última versión del plan.
3. Actualizar información de contacto: Revisar y actualizar información de contacto clave regularmente (personal, proveedores, clientes, sitios alternos, etc.).
4. Lista de distribución: Crear una lista de distribución del plan limitada a personal autorizado, incluyendo sitios remotos y fuera de la oficina.
5. Copias fuera de sitio: Asegurarse de tener copias actualizadas del plan fuera de sitio o en la nube, con acceso seguro.

Actividades de mantenimiento del plan de BC/DR

6. Copias físicas en el sitio: Mantener copias en papel o en medios físicos (CDs, DVDs, USBs) para uso si los sistemas de TI fallan. Si contienen información sensible, cifrarlas o mantenerlas en un lugar seguro.
7. Gestión de versiones antiguas: Implementar un proceso para destruir o archivar versiones antiguas y reemplazarlas con la nueva.
8. Revisión de copias remotas: Cada vez que se modifique el plan, revisar y actualizar copias en almacenamiento remoto o en sitios alternos.
9. Pruebas ante cambios significativos: Probar el plan tras cambios importantes para identificar problemas y capacitar al personal en las modificaciones.
10. Integración en procesos operativos: Integrar consideraciones de BC/DR en procesos operativos para reducir el esfuerzo de mantenimiento.

Actividades de mantenimiento del plan de BC/DR

11. Asignación de responsabilidad: Asignar la responsabilidad de gestionar notificaciones y solicitudes de cambio a un miembro del equipo de BC/DR.
12. Documentar procedimientos: Documentar los procedimientos de mantenimiento y seguirlos para evitar riesgos adicionales en el proyecto.
13. Capacitación ante cambios: Incorporar capacitación en el proceso de cambios para que las modificaciones en personas, procesos o tecnología reflejadas en el plan de BC/DR también actualicen los planes de entrenamiento.
14. Presupuesto para actividades de BC/DR: Incluir actividades de prueba, capacitación, auditoría y mantenimiento del plan de BC/DR en el presupuesto de TI o corporativo.

Cierre del proyecto de BC/DR

- En este punto tienen el conocimiento suficiente para crear el proyecto del plan de BC/DR, al seguir cada paso y tomar en cuenta los puntos importantes en cada uno podrán desarrollar un plan de BC/DR claro, que sea comprensible y razonable incluyendo las principales amenazas y mitigación de riesgos para las funciones críticas.
- Por último considerar las siguientes actividades de cierre.

Cierre del proyecto de BC/DR

1. Completar documentación: Asegurar que toda la documentación esté finalizada.
2. Distribución del plan: Distribuir el plan BC/DR al personal adecuado.
3. Anunciar la finalización: Comunicar la finalización del plan al patrocinador del proyecto y a las partes interesadas; obtener aprobación formal.
4. Comunicar a la empresa: Anunciar la finalización del plan en la empresa para aumentar la conciencia y **celebrar el éxito**.
5. Informar a autoridades: Comunicar la finalización a las autoridades regulatorias, si corresponde.
6. Anunciar planes de capacitación o pruebas.

Cierre del proyecto de BC/DR

7. Revisión de lecciones aprendidas: Realizar una sesión de revisión para discutir lecciones aprendidas e incorporarlas al proceso. Esta debe ser una reunión de trabajo para capturar prácticas y lecciones aprendidas, no un cierre o celebración.
8. Reunión de cierre: Celebrar la finalización y reconocer el esfuerzo del equipo, si es apropiado.
9. Revisiones de personal: Completar cualquier revisión de personal relacionada con el trabajo del proyecto.
10. Informe de cierre: Enviar un informe de cierre al patrocinador del proyecto, equipo ejecutivo u otros interesados, según corresponda.
11. Actualizar documentación legal o de cumplimiento: Reflejar la preparación BC/DR en la documentación legal o de cumplimiento, según sea necesario.
12. Establecer fecha de auditoría: Programar la fecha para la próxima auditoría, revisión, prueba o capacitación del BC/DR.

ENTRENAMIENTO, PRUEBAS Y AUDITORÍA

ING. FREDY BUSTAMANTE

TEMAS A TRATAR

- Capacitación para respuesta a emergencias, recuperación ante desastres y continuidad del negocio
- Pruebas del plan de continuidad del negocio y recuperación ante desastres
- Realización de auditorías de sistemas de TI

INTRODUCCIÓN



Si el plan de BC/DR no se mantiene actualizado y no es entendido por todos los que puedan participar en la respuesta a una emergencia y su recuperación se vuelve **inútil**.



Por eso es crítico el entrenamiento periódico, pruebas y auditoría del plan como parte de las tareas administrativas regulares.



INTRODUCCIÓN



ENTRENAMIENTO PARA RECUPERACIÓN DE DESASTRES Y CONTINUIDAD DEL NEGOCIO

Dos enfoques del entrenamiento BC/DR:

- Respuesta física ante una emergencia.
- Implementación del plan BC/DR.

El entrenamiento en recuperación de desastres (DR) y continuidad del negocio (BC) se enfoca en dos áreas. La primera es cómo reaccionar físicamente ante emergencias (como incendios o inundaciones). La segunda es entrenar a los equipos responsables de implementar el plan de BC/DR, asegurando que tengan las habilidades necesarias para restaurar sistemas y seguir protocolos.

RESPUESTA ANTE EMERGENCIAS

- El equipo de respuesta ante emergencias (ERT) debe estar identificado y entrenado.
- Especialización según la ubicación y riesgos.
- Capacitación en primeros auxilios y RCP.

Cada empresa debe contar con un equipo de respuesta ante emergencias (ERT) entrenado en las actividades necesarias según los riesgos geográficos (inundaciones, terremotos, etc.). Además, es recomendable incluir capacitación en primeros auxilios y RCP para todos los empleados.

PLANIFICACIÓN DEL ENTRENAMIENTO BC/DR

- Definir objetivos y alcances.
- Evaluar necesidades de capacitación.
- Desarrollar, programar y monitorear el entrenamiento.

El entrenamiento para BC/DR debe seguir un enfoque estructurado. Primero se definen los objetivos, luego se realiza un análisis de necesidades para detectar brechas de habilidades, se desarrolla el plan de entrenamiento, y finalmente se monitorea la efectividad de este proceso.

ALCANCE Y OBJETIVOS DEL ENTRENAMIENTO

- El entrenamiento debe estar alineado con el plan BC/DR.
- Definir cronogramas y objetivos para cada equipo.
- Considerar entrenamiento cruzado para roles múltiples.

El plan de entrenamiento debe estar alineado con el plan de BC/DR, asignando objetivos específicos a cada equipo, como el equipo de respuesta ante crisis (CMT) o el equipo de recuperación de desastres. El cronograma debe considerar las responsabilidades cruzadas de algunos miembros que pertenezcan a varios equipos.

A continuación un ejemplo...

ALCANCE Y OBJETIVOS DEL ENTRENAMIENTO

Entrenamiento del Equipo de Respuesta a Incidentes de Computación (CIRT)

Alcance: Capacitar a todos los administradores de red para monitorear el tráfico en busca de problemas de seguridad. No incluye la configuración de auditorías o habilitación de archivos de log.

Objetivos:

1. Desarrollar conciencia sobre amenazas de seguridad actuales.
2. Entender qué archivos de log monitorear.
3. Identificar qué buscar en los archivos de log.
4. Saber investigar entradas sospechosas en los logs.
5. Responder a actividad sospechosa en la red.

Cronograma:

- Capacitación inicial dentro de 30 días.

- Sesión inicial de 2 horas.
- Refrescos trimestrales de 30 minutos.

Requisitos:

1. Localizar información sobre amenazas y tendencias.
2. Ubicar archivos de log especificados.
3. Interpretar entradas de log.
4. Detectar tendencias.
5. Tomar acciones ante actividad sospechosa.

EVALUACIÓN DE NECESIDADES DE CAPACITACIÓN

- Análisis de brechas de habilidades.
- Identificación de nuevas habilidades requeridas durante las pruebas del plan.
- Evaluaciones periódicas de las habilidades del personal.

Un análisis de brechas de habilidades permite identificar las áreas donde el equipo necesita entrenamiento adicional. Este análisis debe actualizarse periódicamente para asegurar que el personal esté preparado para implementar el plan BC/DR.

DESARROLLO DEL ENTRENAMIENTO

- Capacitación específica y medible.
- Uso de materiales variados (teoría, práctica, ejercicios).
- Importancia de la experiencia práctica.

El entrenamiento debe tener resultados medibles. Para asegurar la absorción de conocimientos, se deben usar diferentes métodos de enseñanza, como clases teóricas, ejercicios prácticos, y simulaciones. Una evaluación final debe verificar que los empleados comprendan los conceptos clave.

No todo el entrenamiento es igual, no es lo mismo entrenar a alguien sobre presionar un botón y parar una máquina que entrenar a alguien para restaurar un sistema que puede tener varios componentes.

PROGRAMACIÓN Y ENTREGA DEL ENTRENAMIENTO

- Desafíos en la programación del entrenamiento.
- Uso de sistemas de aprendizaje flexibles (online o presenciales).
- Importancia de verificar la calidad del entrenamiento.

Programar el entrenamiento puede ser un desafío. Las empresas pueden optar por sistemas flexibles de aprendizaje en línea, pero es importante verificar la calidad de estos programas y que el personal haya aprendido los conceptos clave.

MONITOREO Y MEDICIÓN DEL ENTRENAMIENTO

- Desarrollo de objetivos claros.
- Verificación de habilidades con pruebas teóricas y prácticas.
- Seguimiento de asistencia y cumplimiento del entrenamiento.

Para garantizar la efectividad del entrenamiento, es fundamental desarrollar objetivos claros y evaluar las habilidades adquiridas a través de exámenes y demostraciones prácticas. También se debe monitorear la asistencia y actualizar el entrenamiento según sea necesario.

ENTRENAMIENTO Y PRUEBAS PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

Existen cuatro métodos básicos para entrenar al personal y, al mismo tiempo, probar el plan de BC/DR:

- Ejercicios en papel o de escritorio (paper walk-throughs)
- Ejercicios funcionales (functional exercises)
- Ejercicios en campo (field exercises)
- Interrupciones completas (full interruptions)

Los cuatro métodos principales para entrenar al personal y probar los planes de continuidad y recuperación de desastres. Los métodos varían en complejidad, desde simulaciones simples en papel hasta interrupciones completas de las operaciones para verificar la preparación ante emergencias.

ELEMENTOS CLAVE DEL ENTRENAMIENTO PARA LOS PLANES DE BC/DR

- El entrenamiento debe asegurar que los líderes del equipo sepan:
- Cómo y cuándo activar el plan.
- Notificar, reunir y gestionar a sus equipos.
- Operar como parte de un equipo multidisciplinario.
- Comunicar efectivamente en situaciones de estrés.

Estos son los aspectos fundamentales que los líderes del equipo deben dominar para manejar eficazmente una crisis. El entrenamiento se enfoca en habilidades críticas como la activación del plan, la gestión del equipo y la comunicación efectiva bajo presión.

EL PAPEL DEL ENTRENAMIENTO EN BC/DR

- El entrenamiento tiene dos objetivos principales:
- Familiarizar al personal con el plan de BC/DR.
- Reforzar el conocimiento de los procedimientos básicos.

El propósito del entrenamiento no es solo que los empleados conozcan el plan, sino que también estén capacitados para aplicarlo en una emergencia, asegurando que todos los procedimientos sean claros y comprendidos por el personal.

ENTRENAMIENTO PERSONALIZADO PARA ROLES ESPECÍFICOS

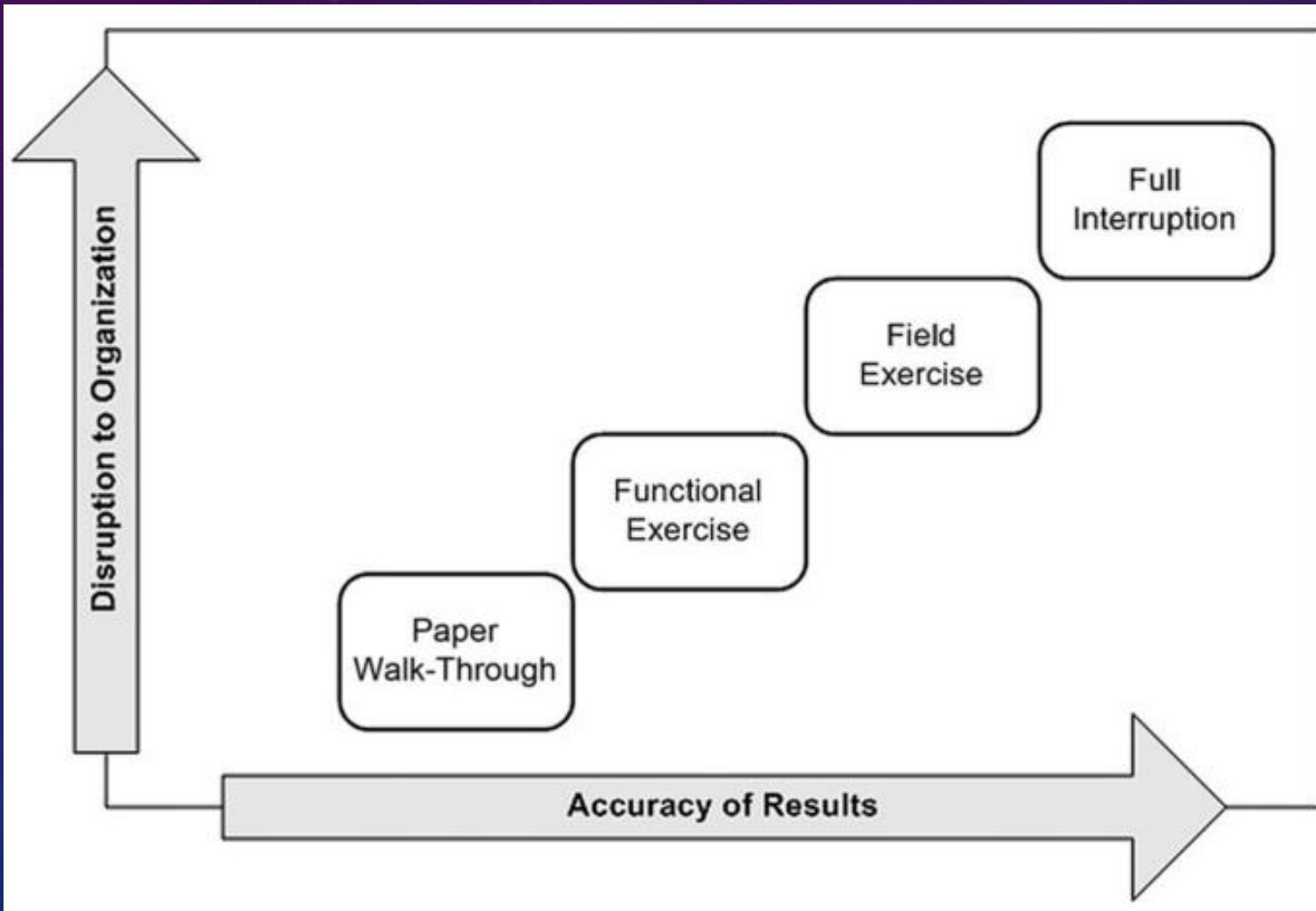
- El entrenamiento debe ser específico para los roles de los participantes.
Por ejemplo:
 - Un administrador de bases de datos (DBA) necesita capacitación en evaluación de daños en TI.
 - Un coordinador de crisis debe aprender a utilizar equipo de comunicación de emergencia.

El entrenamiento debe adaptarse a las responsabilidades específicas de cada rol. Cada miembro del equipo tiene tareas únicas en una emergencia y requiere la capacitación adecuada para cumplir con sus funciones durante la crisis.

TRABAJO EN EQUIPO MULTIDISCIPLINARIO EN BC/DR

- El equipo de gestión de crisis (CMT) puede incluir líderes de diferentes departamentos que normalmente no interactúan entre sí.
 - Durante una crisis, es probable que los equipos de diversos departamentos deban trabajar juntos de manera fluida. Es importante que todos los líderes estén familiarizados con la estructura de mando y sepan cómo colaborar con otros, independientemente de sus roles habituales.
- La comunicación durante una crisis puede requerir la implementación de planes de contingencia si las herramientas tradicionales de comunicación no están disponibles.
 - La comunicación efectiva es esencial en una crisis. Es importante tener planes alternativos de comunicación en caso de que las herramientas tradicionales, como teléfonos o correos electrónicos, no estén disponibles durante la emergencia.

MÉTODOS DE PRUEBAS DEL PLAN: DISRUPCIÓN VS EXACTITUD



MÉTODOS DE ENTRENAMIENTO: EJERCICIOS EN PAPEL

- Este método de entrenamiento involucra una revisión detallada del plan de BC/DR en un entorno de oficina, donde los participantes discuten cada paso del plan sin activarlo realmente.

Este tipo de ejercicio permite a los equipos repasar el plan sin realizar interrupciones operativas. Es un método sencillo y eficaz para asegurarse de que todos comprendan sus roles y las acciones necesarias ante una emergencia.

MÉTODOS DE ENTRENAMIENTO: EJERCICIOS EN PAPEL

Existen ocho pasos discretos que puedes seguir para realizar una caminata en papel efectiva. Estos pasos también se aplican a otros tipos de entrenamiento (funcional, de campo, etc.).

1. Desarrollar Escenarios Realistas

Crea escenarios basados en los riesgos determinados por tu evaluación que tengan la mayor probabilidad e impacto. Comienza con un incendio en el edificio, ya que estadísticamente es el desastre más probable que afecta a las empresas.

2. Desarrollar Criterios de Evaluación

Define criterios para evaluar el éxito del entrenamiento, tales como:

- Cómo siguieron los participantes el plan.
- La comunicación entre los equipos.
- Efectividad de las listas de verificación.
- Confianza de los participantes en la implementación del plan.

3. Proporcionar Copias del Plan

Entrega las copias más recientes del plan a los miembros del equipo antes de la caminata. Considera crear un diagrama de flujo para ayudar a los miembros a entender su rol dentro del plan (ver imagen siguiente).

4. Dividir a los Participantes por Equipos

Si hay miembros de diferentes equipos, agrúpalos para facilitar la comunicación y reducir interrupciones.

5. Usar Listas de Verificación

Proporciona copias de las listas de verificación de los procesos clave para asegurar que se mantenga la dirección durante la caminata.

6. Tomar Notas

Asigna a alguien la tarea de llevar notas sobre el flujo general, niveles de preparación, brechas en el plan, etc.

7. Identificar Necesidades de Entrenamiento

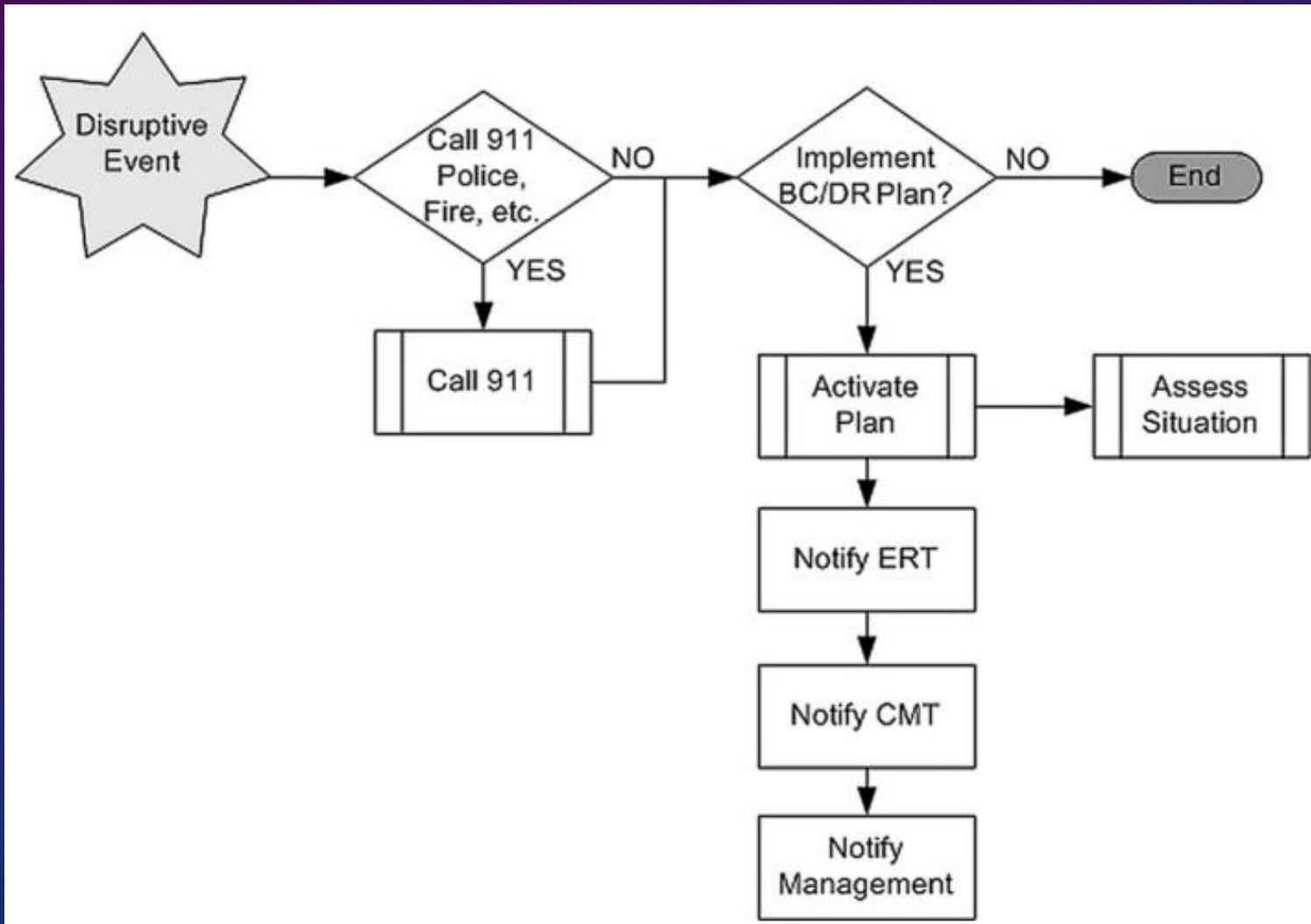
Mantén un registro de las habilidades que los participantes consideran necesarias para implementar el plan de manera efectiva.

8. Desarrollar Resumen y Lecciones Aprendidas

Compila y resume las notas recogidas, programando una reunión de seguimiento para discutir los resultados y las lecciones aprendidas.

MÉTODOS DE ENTRENAMIENTO: EJERCICIOS EN PAPEL

Ejemplo parcial de un flujo de proceso del plan de BC/DR



MÉTODOS DE ENTRENAMIENTO: EJERCICIOS FUNCIONALES

Se utilizan para probar realmente algunas de las funcionalidades del plan. A menudo es útil y adecuado realizar una revisión en papel junto con ejercicios funcionales. Estos entrenan al personal en procedimientos críticos o funciones necesarias para responder y manejar la interrupción.

- Suelen utilizar guiones basados en escenarios y tienen una duración de 2-3 horas.
- El equipo se divide en dos grupos: el equipo principal y los alternos. Los alternos sirven como un segundo grupo para fines de entrenamiento.
- Un guion inicia la secuencia de eventos, que típicamente toma unos 15-20 minutos.
- Los equipos (ERT y CMT) deben responder a los eventos guionizados utilizando su entrenamiento y el plan BC/DR.
- Los alternos actúan como empleados comunes, simulando comportamientos como el pánico o no seguir instrucciones, o pueden tener lesiones simuladas que el equipo de respuesta debe atender.
- El objetivo es que los miembros trabajen en equipo, comprendan sus roles y responsabilidades, y se comuniquen eficazmente bajo condiciones de estrés.
- Se deben definir los objetivos específicos de un ejercicio, por ejemplo:
 - Determinar cuándo es necesario restaurar una base de datos.
 - Acceder a respaldos en bóvedas de datos remotas.
 - Restaurar los datos y verificar la restauración (nombre de archivos, tamaños, ubicaciones).
 - Probar funciones específicas del plan BC/DR mediante instrucciones paso a paso.

Los ejercicios funcionales son una excelente herramienta de entrenamiento y ayudan a probar las capacidades del equipo bajo condiciones simuladas.

MÉTODOS DE ENTRENAMIENTO: EJERCICIOS DE CAMPO

Implican simulaciones bastante realistas basadas en escenarios probables. Estos ejercicios son similares a los que realizan los equipos de respuesta a emergencias en situaciones simuladas, que muchas veces se ven en las noticias locales. Si deseas practicar tu respuesta ante emergencias y recuperación de desastres con ejercicios a gran escala, podrías coordinar estos ejercicios con los equipos de respuesta a emergencias locales.

Beneficios:

- Los equipos de respuesta a emergencias locales pueden estar dispuestos a participar, brindando una excelente oportunidad para probar y afinar habilidades.
- Estos ejercicios no solo pondrán a prueba las habilidades del equipo, sino que también proporcionarán retroalimentación valiosa para la planificación de desastres.

Consideraciones:

- Muchas empresas apenas tienen tiempo o recursos para realizar una revisión anual en papel de su plan, por lo que puede ser difícil realizar un escenario realista completo.
- Sin embargo, si tu empresa trabaja en una industria peligrosa (químicos peligrosos, explosivos, energía, etc.), podrías querer (o estar legalmente obligado) a realizar ejercicios en campo para evaluar y mejorar la preparación.
- Aunque los recorridos en papel y los ejercicios funcionales son útiles, pueden dejar brechas de conocimiento o problemas en el plan que solo se detectan ante una situación real.
- Los ejercicios en campo pueden reducir el riesgo de estas brechas, pero requieren una inversión significativa de tiempo y recursos.
- Para algunas empresas, esta inversión es justificada.

MÉTODOS DE ENTRENAMIENTO: PRUEBA DE INTERRUPCIÓN TOTAL

Al igual que un ejercicio en campo, una prueba de interrupción total puede aplicarse a toda la organización o a sistemas específicos dentro de ella.

Objetivo: Activar todos los componentes del plan y detener todas las funciones críticas de la empresa.

- Incluye la activación de sitios de trabajo alternativos, instalaciones fuera de la sede y almacenamiento externo.
- Puede ser una prueba **anunciada** o **no anunciada**.
 - Las pruebas **no anunciadas** simulan de manera más realista una interrupción o desastre, pero son más disruptivas.
- La mayoría de las empresas son reacias a interrumpir sus operaciones lo suficiente para realizar una prueba completa.
- Sin embargo, en algunas situaciones, interrumpir una unidad de negocio puede ser aceptable para lograr una preparación más realista.

PRUEBAS DEL PLAN DE BC/DR

Razones para probar el plan:

- Asegurar que el plan funcionará en una interrupción real.
- Verificar la comprensión de los procesos por los implementadores del plan.
- Validar la integración de tareas entre unidades de negocio y funciones de gestión.
- Confirmar los pasos desarrollados para cada fase de implementación.
- Identificar los recursos necesarios.
- Familiarizar a las partes involucradas con el flujo de información.
- Detectar fallos o debilidades en el plan.
- Evaluar costos y factibilidad.

COMPRENSIÓN DE LOS PROCESOS

- Las pruebas deben asegurar que los miembros del equipo entiendan los procesos, procedimientos y pasos del plan.
- Deben descubrir procesos faltantes y confirmar dependencias.
- Las funciones críticas deben restaurarse primero, y el plan debe priorizarlas adecuadamente.
- Entender los procesos también incluye el entender las soluciones alternativas y procesos manuales que deben ser implementados durante la recuperación y continuidad del negocio.
 - Y estos deben ser probados.

VALIDACIÓN DE LA INTEGRACIÓN DE TAREAS

- Las pruebas deben involucrar al personal clave de funciones críticas y al equipo de BC/DR.
- Los expertos deben verificar la secuencia correcta de tareas, dependencias y recursos.
- La falta de integración de tareas puede ocasionar un fallo en la implementación del plan.
- **Ejemplo:** Identificar tareas de recuperación de sistemas IT y su interdependencia con otros sistemas y procesos.

CONFIRMACIÓN DE LOS PASOS

- La prueba debe confirmar que los pasos necesarios están listados y en el orden correcto.
- Las pruebas paso a paso ayudan a descubrir errores u omisiones.
- **Ejemplo:** Verificar que el orden de los pasos para iniciar un servicio de TI sea lógico y ejecutable.

CONFIRMACIÓN DE LOS RECURSOS

- Durante las pruebas, es clave preguntar: "¿Qué recursos son necesarios para ejecutar este paso?"
- Recursos pueden incluir personal, habilidades, equipos y suministros.
- **Ejemplo:** Asegurar que dos equipos no requieran simultáneamente los mismos recursos.

FAMILIARIZACIÓN CON EL FLUJO DE INFORMACIÓN

- Las comunicaciones son críticas durante interrupciones.
- Las pruebas identifican quién necesita qué información y cuándo, además de identificar cómo se mueve.
- También debemos identificar cómo fluyen los datos a través de los sistemas de TI para poder estar seguros que un servicio estará realmente funcionando con los datos que necesita.
- **Ejemplos:**
 - Verificar cómo se intercambia información entre equipos de respuesta ante emergencias.
 - Verificar cómo fluyen los datos para alimentar un sistema de venta en línea.

IDENTIFICACIÓN DE DEBILIDADES

- Las pruebas con listas de verificación y simulaciones revelan fallos o debilidades.
- Los escenarios realistas ayudan a detectar problemas que no aparecen en teoría.
- **Ejemplos:**
 - Descubrir omisiones como números de contacto
 - Licencias necesarias para la recuperación
 - Máquinas virtuales que no funcionan correctamente en servidores de recuperación

EVALUACIÓN DE COSTOS Y FACTIBILIDAD

- Las pruebas ayudan a comprender mejor los costos de implementación del plan.
- Identificar la factibilidad de los pasos del plan en situaciones reales.
- Ejemplos:
 - Determinar si un proveedor hará cargos extras por tareas no descritas detalladamente en un contrato.
 - Gastos adicionales de transporte, alimentación, etc.

CRITERIOS DE EVALUACIÓN

- Crear criterios claros para evaluar las pruebas.
- Utilizar preguntas para evaluar la efectividad de cada fase del plan.
- Se puede utilizar las listas o pasos del plan de BC/DR para generar los criterios.
- Ejemplo:
 1. ¿Pudo el miembro principal del equipo comenzar el proceso de notificación con éxito?
 2. ¿Cuántos miembros del equipo fueron contactados?
 3. ¿Cuánto tiempo tomó notificar a los miembros del equipo?
 4. ¿Faltaban números de teléfono o había números incorrectos?
 5. ¿Cuántos miembros del equipo fueron contactados a través de sus métodos principales vs. métodos alternativos?
 6. ¿Cuántos miembros del equipo no estaban en la lista de notificación?
 7. ¿Había nombres en la lista de notificación que no debían estar?
 8. ¿Funcionaría esto si los sistemas telefónicos estuvieran fuera de servicio?

RECOMENDACIONES BASADAS EN RESULTADOS DE PRUEBAS

- Desarrollar recomendaciones a partir de los resultados de las pruebas.
- Las recomendaciones pueden implicar modificaciones al plan o entrenamiento adicional.
- Ejemplo:
 - Actualización de listas de contacto o inclusión de nuevas áreas de negocio en el plan.
 - Verificación de medios alternos de comunicación.

REALIZACIÓN DE AUDITORÍAS DE SISTEMAS Y SEGURIDAD DE TI

- **Una auditoría es un examen sistemático basado en criterios definidos.**
- Cumplimiento de leyes o regulaciones
 - Si la empresa debe cumplir con leyes o normativas, seguramente ha pasado por auditorías rigurosas.
- Relación con BC/DR
 - Las auditorías que se realizan para cumplir con normativas pueden ser útiles en la planificación de BC/DR y deben incluirse en el plan.
- Una auditoría debe incluir tanto la continuidad del negocio como auditorías de sistemas.
- Ejemplo:
 - Si tu empresa debe cumplir con los estándares ISO/IEC 27001 (Seguridad de la información) o el Decreto 22-2008 (Ley de acceso a la información pública), los planes de BC/DR deben abordar estos temas y la auditoría del plan debe incluir esos parámetros.

AUDITORÍAS DE SISTEMAS DE TI Y SEGURIDAD

Las auditorías de sistemas de TI implican un conjunto de tareas que ayudan a reducir el riesgo de intrusión o ataque. Las auditorías se centran principalmente en asegurar la confidencialidad, integridad y disponibilidad de los datos de la empresa, áreas que comúnmente son blanco de ataques.

EVALUACIÓN SISTEMÁTICA DE SEGURIDAD

- Una auditoría de sistemas de TI se enfoca en:
 - Evaluar la seguridad de varios sistemas de TI.
 - Revisar la configuración física y del entorno de la red.
 - Revisar la configuración del software y el manejo de datos, especialmente los sensibles.
 - Verificar los controles de accesos de los usuarios.
- Estas están asociadas al cumplimiento de estándares por temas legales o exigencias de clientes.
 - Se recomienda realizar auditorías de este tipo incluso si no fuese obligatorio.

FORTALECIMIENTO DE LA SEGURIDAD DE LOS SISTEMAS

El fortalecimiento de la seguridad de los sistemas es una estrategia de mitigación de riesgo que minimiza el área de ataque mediante:

- Eliminación de protocolos de red no utilizados.
- Desactivación de puertos y servicios no utilizados.
- Reducción de permisos al mínimo necesario.
- Eliminación de usuarios no utilizados.
- Automatización de actualizaciones de antivirus y antispyware.
- Etcétera.

AUDITORÍA DEL PLAN BC/DR

La auditoría de sistemas en la planificación BC/DR incluye:

- Asegurar que las estrategias de mitigación de riesgos de TI estén implementadas y configuradas correctamente.
- Asegurar que los sistemas identificados en el plan de BC/DR sigan en funcionamiento y operativos.
- Identificar áreas donde se haya implementado nueva tecnología y que puede no estar incorporada en el plan de BC/DR.
- Identificar áreas donde la tecnología ha sido retirada o modificada, lo que resulta en la necesidad de revisar el plan de BC/DR.
- Revisar los procesos identificados en el plan de BC/DR en relación con los sistemas de TI para garantizar que los pasos y procesos sean aún correctos, completos y relevantes.
- Verificar que el equipo de respuesta a incidentes de TI (CIRT, CERT, o cualquier otro término utilizado) esté operativo y tenga una comprensión clara de roles, responsabilidades y cómo implementar los segmentos específicos de TI del plan de BC/DR.
- Revisar los datos de varios sistemas para garantizar que aún cumplen con los planes de BC/DR. Estos sistemas incluyen sistemas operativos, equipos de redes y telecomunicaciones, bases de datos y aplicaciones, respaldos de sistemas, controles de seguridad, integración y pruebas. Cualquiera de estas áreas está sujeta a cambios frecuentes. Una auditoría puede ayudar a asegurar que el plan de BC/DR funcionará si se implementa

IMPORTANCIA DE LA AUDITORÍA PERIÓDICA

- Las auditorías periódicas son una excelente práctica para mantener actualizado el plan BC/DR.
- Es más sencillo añadir pasos a las auditorías regulares que realizar una auditoría BC/DR separada.
- También facilita encontrar cambios graduales que pueden impactar significativamente la implementación del plan BC/DR.

Respuesta y recuperación ante emergencias

Ing. Fredy Bustamante

Introducción

- La regla básica sobre planificación para emergencias es:
Mantenerlo simple
- Cuanto más complicados sean sus planes de respuesta a emergencias, menos probabilidades habrá de que sean eficaces en una emergencia real.
- Los planes más complejos podrán utilizarse para la recuperación.

Temas

- Descripción general de la gestión de emergencias
- Planes de respuesta a emergencias
- Gestión de crisis
- Recuperación de TI

Descripción general de la gestión de emergencias

Descripción general de la gestión de emergencias

- Independientemente de cómo esté organizada su empresa debe **asignar roles claros**.
 - Todos deben saber quién está a cargo o quién toma las decisiones.
 - No puede permitir que en una emergencia varias personas piensen que pueden tomar decisiones pues generará caos.
 - A gran escala, cuando ocurre un desastre que afecta a toda una comunidad, es importante conocer las entidades que estarán a cargo de diferentes tareas como rescatar personas, atenderlos, darles comida, etc.
 - No asuma que una entidad llegará a rescatar o apoyar al personal de la empresa, en su planificación incluya **encargados y tareas que permitan cubrir las emergencias sin ayuda externa**.

Planes de respuesta a emergencias

Planes de respuesta a emergencias

- Como personal de TI, solemos participar y tener un rol en específico dependiendo del tipo de emergencia.
- Los planes de emergencia surgen de los riesgos identificados con anterioridad.
- Recordemos que la respuesta a emergencias es la respuesta inmediata al incidente.
 - En un incendio, la respuesta a la emergencia consiste en evacuar el edificio, llamar al departamento de bomberos y, dependiendo el caso, algunos empleados podrán utilizar extintores para intentar controlar el incendio.
 - No debe crear un plan para cada tipo de emergencia, por el contrario, tener pocos planes de respuesta generales de los cuales se toma lo que corresponde a la emergencia que ocurre en un momento dado.

Planes de respuesta a emergencias

- Un conjunto básico de tareas de respuesta a emergencias son las siguientes:
 - Proteger al personal
 - Contener el incidente
 - Implementar comando y control (intervención del ERT y del CMT)
 - Respuesta y triaje de emergencias (médicas, evacuación, búsqueda y rescate)
 - Evaluar el impacto y el efecto
 - Notificación
 - Próximos pasos
- Las 3 primeras tareas son las más importantes pues se protege a las personas, se contiene la emergencia y se evalúa la situación.

Planes de respuesta a emergencias

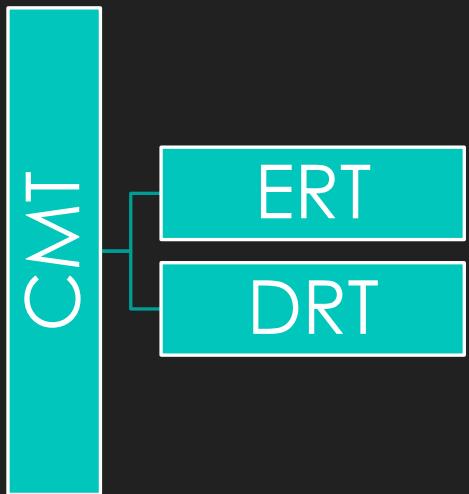
○ Cada plan debe incluir:

- Roles y responsabilidades: quién y qué debe hacer cada uno.
- Herramientas y equipos: extintores, kits de primeros auxilios, cascos, radiocomunicadores, llaves, etc.
- ERT debe tener un inventario de estos, revisarlos y darles mantenimiento periódicamente.
- Recursos: recursos humanos como saber quién es experto en qué (relacionado a emergencias), agua, alimentos, otros medicamentos, etc.
- Acciones y procedimientos: procedimientos de evacuación, qué hacer en caso de derrame químico, inundación, protocolos de comunicación.

Gestión de crisis

ERT: Equipos de respuesta a emergencias

- El ERT debe estar definido con sus roles y responsabilidades, cada persona debe conocer los límites de su autoridad y a quién debe recurrir por ayuda o escalamiento.
- El equipo de gestión de crisis (CMT) puede o no ser el mismo que el ERT.
- CMT
 - Toma decisiones de alto nivel y dirige los recursos de la empresa durante la crisis
 - Coordina entre empleados y partes externas, equipos ERT y DR
 - Único portavoz para empleados y todas las partes externas durante la crisis
 - Implementa el Plan de Continuidad del Negocio (BC) y Recuperación ante Desastres (DR)
 - Mantiene el registro de eventos
- ERT
 - Gestiona, prueba y se prepara solo para la respuesta a emergencias
 - Entrenado para abordar emergencias específicas
- DRT (Equipo de DR)
 - Implementa procedimientos de recuperación de TI y de negocios



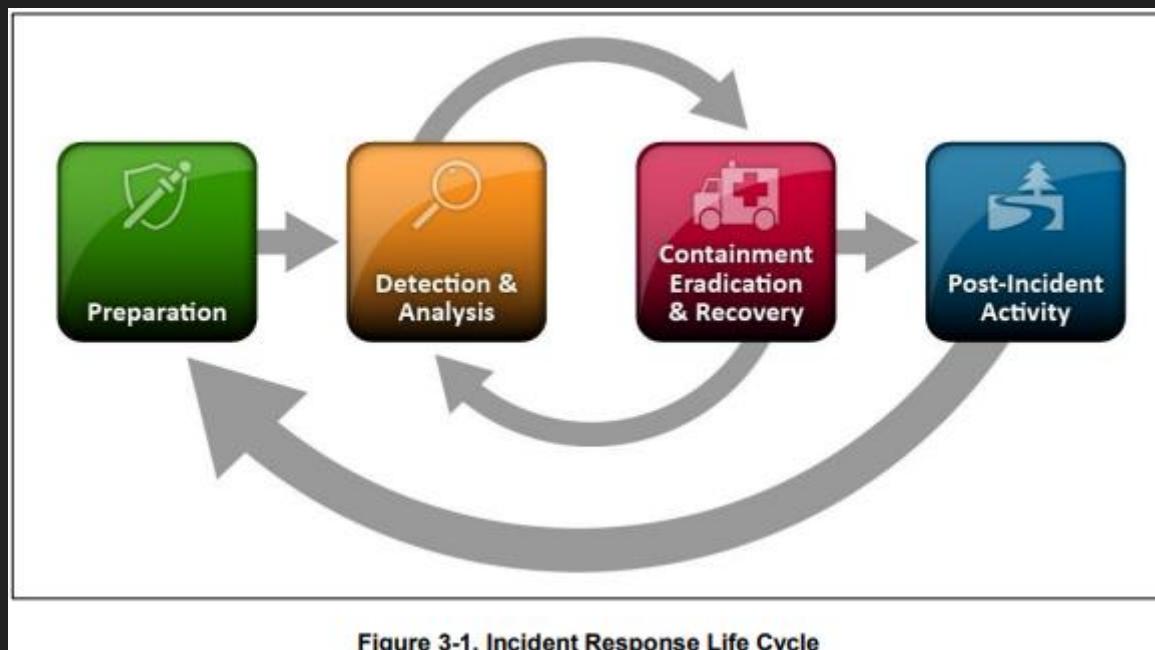
Recuperación de TI

CIRT: Computer Incident Response

- Dentro de TI debe existir un equipo que, similar al ERT, pueda dar respuesta ante una emergencia relacionada con o que afecte el hardware y software.
 - Debe cumplir con los mismos requisitos que un ERT pero enfocados en hardware y software.
- Deben tener procedimientos ordenados de cómo restaurar los servicios, las dependencias, los proveedores, passwords, etc.
- Sus principales responsabilidades son:
 - Monitorear
 - Alertar y movilizar
 - Evaluar y estabilizar
 - Resolver
 - Revisar

CIRT: Computer Incident Response

○ Más información en <https://csrc.nist.gov/pubs/sp/800/61/r2/final>



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.**

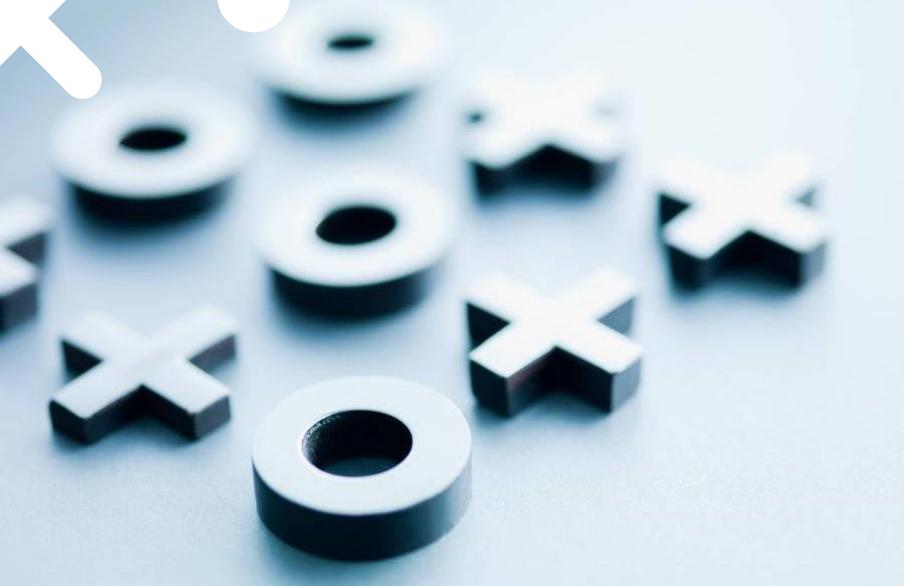
Si se analiza el plan de manera integral, se puede ver que en un extremo del espectro se encuentra la mitigación de riesgos y en el otro extremo, la recuperación ante desastres.

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

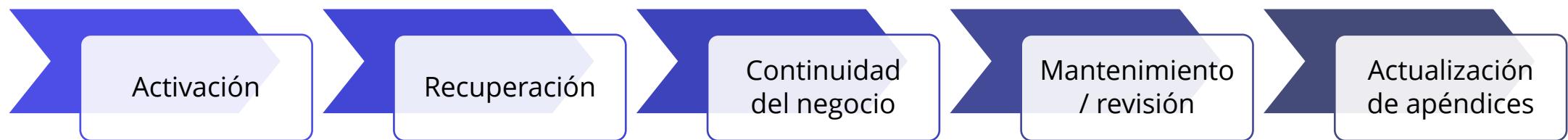
Introducción





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.
 - Despues 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.
 - Despues 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

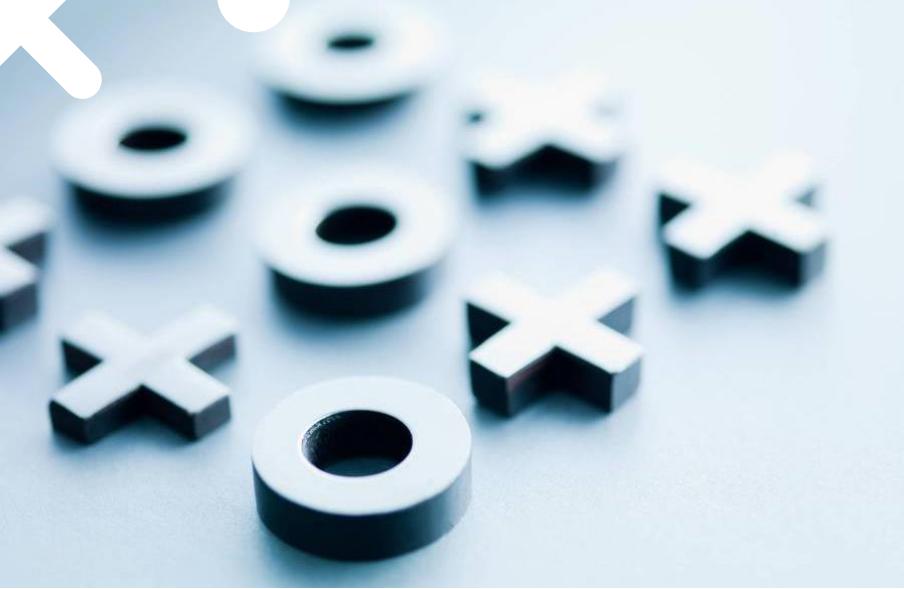
Fase de continuidad del negocio

- 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.
- Despues 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.

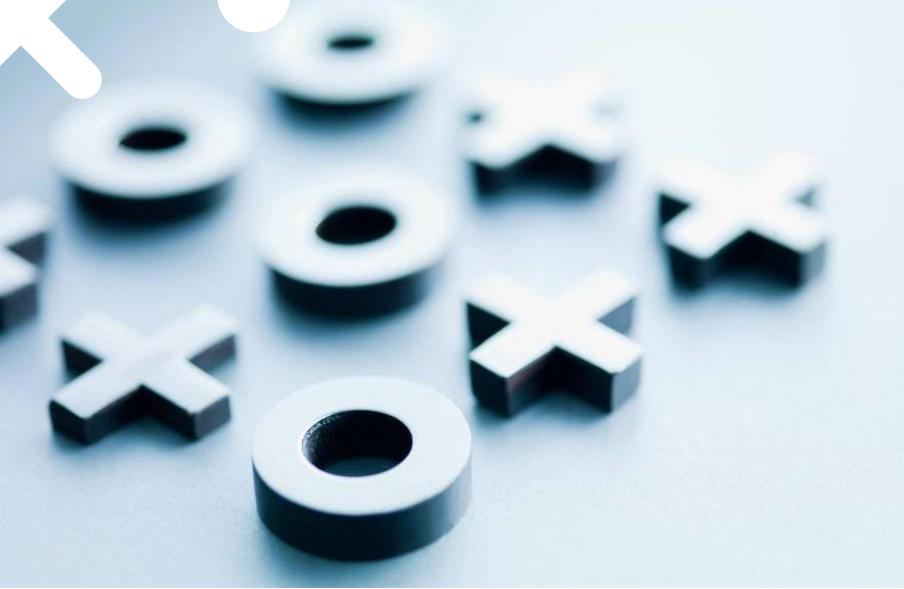
Definición de equipos de BC/DR y personal clave

- **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 alterno.

Recordemos que debemos definir cuáles son las condiciones bajo las cuales moveremos servicios hacia un sitio alterno, 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 operacionalmente 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 alterno 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 alterno, 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 alterno, 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



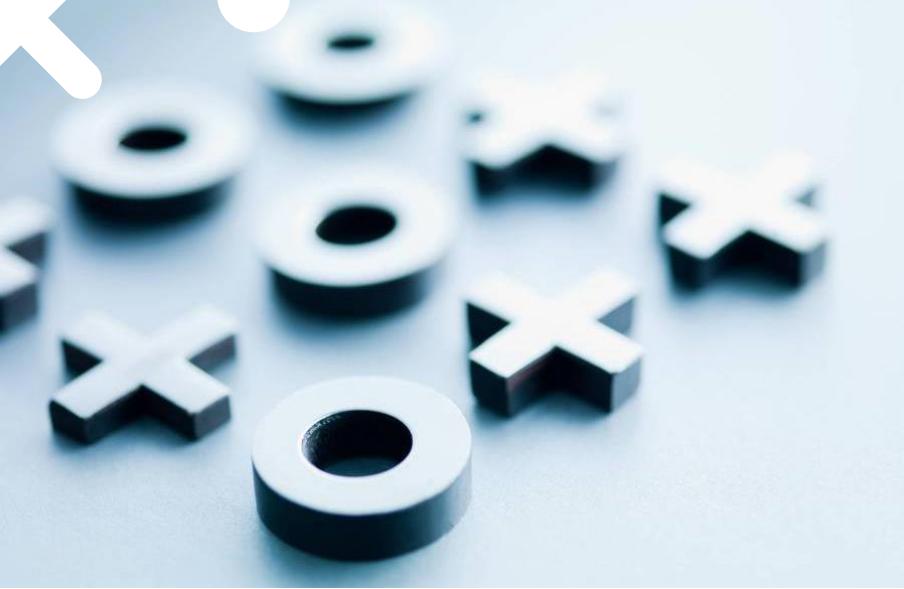
- **Interno**
 - El plan de comunicación interna es realmente parte del plan de activación e implementación de BC/DR.
 - Si ocurre una interrupción, debe tener un proceso establecido para notificar a los miembros del equipo de BC/DR, esto como parte de la activación del plan.
 - Este plan debe poder 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 activations de planes de BC/DR (o no activations)
 - 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 alterno 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

Desarrollo de la estrategia de mitigación de riesgos

Ing. Fredy Bustamante



Desarrollo de la estrategia de mitigación de riesgos

- Tipos de estrategias de mitigación de riesgos
- Proceso de mitigación de riesgos
- Mitigación de riesgos de TI
- Consideraciones sobre respaldo y recuperación

Desarrollo de la estrategia de mitigación de riesgos

- Mitigación de riesgos: **adopción de medidas para reducir los efectos adversos.**
 - En esta fase se desarrollan estrategias para **aceptar, evitar, reducir o transferir** riesgos relacionados con posibles interrupciones del negocio.
 - La mitigación de riesgos es común utilizarla en diferentes ámbitos de la empresa, por ejemplo, en administración de proyectos se debe evitar o minimizar los efectos de eventos que puedan afectar el buen término de estos.
 - El enfoque que veremos es específico para la continuidad de negocios y recuperación de desastres y veremos aspectos únicos relacionados con TI.

Desarrollo de la estrategia de mitigación de riesgos



Desarrollo de la estrategia de mitigación de riesgos

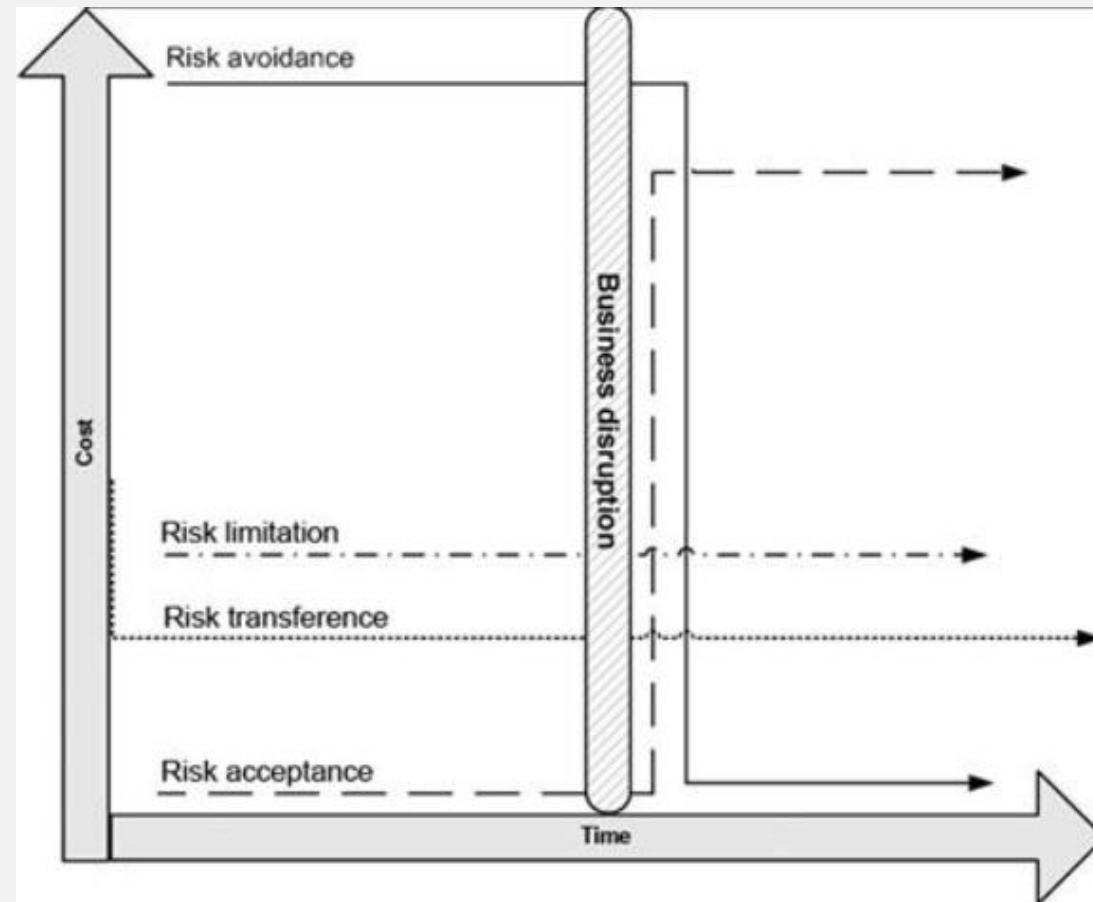
- Es importante tomar en cuenta que la estrategia de mitigación de riesgos debe ir acorde al perfil de la empresa, por ejemplo, si su empresa es aversa al riesgo y desea evitarlo a casi cualquier costo, sus estrategias deberán ser apropiadas a este objetivo.
- Debe mantenerse enfocado en las prioridades, como ya se habrá dado cuenta, este proceso es exhaustivo por lo que una de sus tareas es priorizar y cubrir los elementos clave.

Tipos de estrategias de mitigación de riesgo

Tipos de estrategias de mitigación de riesgo

- Las 3 opciones estándar son:
 - Aceptar
 - Evitar
 - Limitar
 - Transferir

Relación entre tiempo y costo para las opciones de mitigación



Tipos de estrategias de mitigación de riesgo

- **Aceptar el riesgo**
 - No es realmente una estrategia de mitigación pues no se está reduciendo de ninguna forma el efecto sino simplemente se está aceptando.
 - Sin embargo, el aceptar un riesgo es una opción legítima cuando administramos el riesgo.
 - La razón más común para tomar esta opción es que el costo de reducir en alguna medida el riesgo es más caro que el efecto que este tiene.
 - No vale la pena gastar \$10,000 en un segundo servidor si el estar sin el servicio asociado tiene un costo de \$1,000 mensuales.
 - Esta opción es prácticamente la opción de “no hacer nada” que se utiliza en varios ámbitos de toma de decisiones.
 - Para esta opción el costo antes de un evento es el más bajo y suele ser el más alto después de este (comparando entre estrategias para el mismo riesgo).
 - El problema de esta opción es que suele ser la que más utilizan las empresas sin realizar un verdadero análisis, por esto es importante que en la elaboración de su plan de BC/DR se analicen las diferentes opciones de forma correcta.

Tipos de estrategias de mitigación de riesgo

- **Evitar el riesgo**
 - Tomar medidas para que el riesgo se aborde por completo y no pueda ocurrir.
 - Esta opción es la opuesta a la anterior y se trata de evitar totalmente el riesgo.
 - Por ejemplo, si en la entrada de la empresa hay un árbol que, en caso de lluvia muy fuerte, puede botar una rama y caer sobre una persona o un vehículo, la opción anterior es aceptar que podría pasar y si pasa pagar los gastos y demanda correspondiente, mientras en esta opción se quitaría el árbol por completo para evitar cualquier riesgo.
 - Por ejemplo, en TI, tener un sitio totalmente redundante que sea capaz de sostener todos los servicios de la empresa y que los datos sean actualizados en el instante en que estos cambian en el sitio original.
 - Esta opción suele ser la más cara de implementar y mantener antes de un evento y es la que suele tener menor costo adicional después de este (costo de estar fuera y de recuperarse).
 - Evitar el riesgo suele no ser factible para todos los riesgos y/o todas las empresas por diferentes razones (no solo la financiera) pero debe ser analizada para poder determinarlo y no tomar decisiones sin tener la información correspondiente.
 - La decisión suele centrarse en determinar si se debe gastar tiempo y dinero hoy (mitigar) o después (remediar).

Tipos de estrategias de mitigación de riesgo

- Limitar el riesgo
 - Es la estrategia más comúnmente utilizada y consiste en limitar la exposición al riesgo tomando una serie de acciones.
 - Por ejemplo, realizar backup de los datos todos los días es una estrategia de mitigación pues limita la pérdida de datos (efecto) a causa de algún evento (riesgo), realmente no estoy evitando quedarme sin un disco por un fallo, pero limito el efecto.
 - Esta opción está entre aceptar y evitar tanto en el tema de costo antes como después de un evento.

Tipos de estrategias de mitigación de riesgo

- Transferir el riesgo
 - Implica transferir el riesgo a un tercero dispuesto a hacerlo.
 - Muchas empresas subcontratan ciertas operaciones como servicio al cliente, nómina, entrega de productos, etc. Aunque normalmente lo hacen para enfocarse en sus competencias básicas, pero también pueden hacerlo como parte de la gestión de riesgos.
 - Un ejemplo de transferencia es la contratación de seguros a empresas que están dispuestas a aceptar el riesgo a cambio de dinero o contratos de servicio que incluyen atención a emergencias a cualquier hora y el cambio de piezas si fuera necesario.
 - Una diferencia importante entre limitar y transferir es que limitar suele incluir un pago inicial (compra de equipo) y pagos recurrentes (por mantenimiento, licencias, etc.) mientras que transferir suele ser un gasto fijo cada periodo (mes, año, etc.)
 - Se debe considerar que normalmente el transferir el riesgo es únicamente la parte de costos, no podrán ser incluidos efectos como la reputación ante los clientes.

Proceso de mitigación de riesgos



Proceso de mitigación de riesgos

- Para desarrollar una estrategia de mitigación de riesgos debemos analizar las opciones.
 - Ya hemos visto que existen varios tipos de riesgos, amenazas, fuentes de amenazas, vulnerabilidad e impacto.
 - Luego tenemos que analizar el perfil de recuperación que incluye los requerimientos y opciones de recuperación, tiempos (MTD) y costos contra las opciones.
 - A partir de esto podemos seleccionar las opciones apropiadas y una vez conocidos estos elementos, se puede diseñar una estrategia integral.

Proceso de mitigación de riesgos

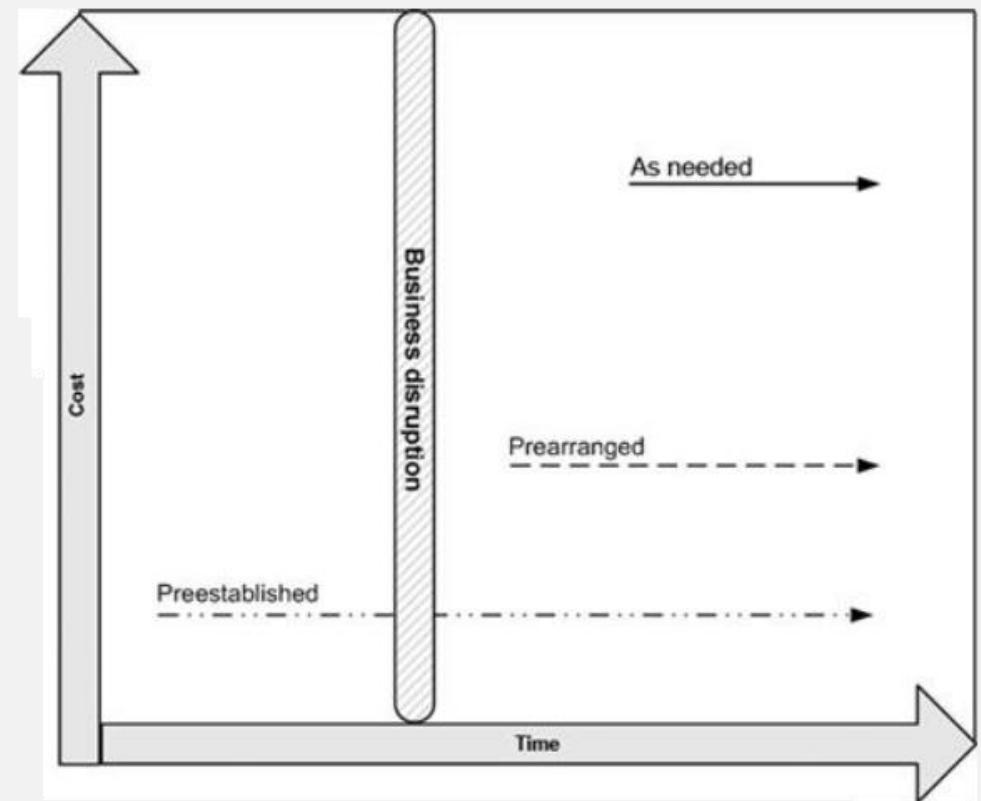
- Requerimientos de recuperación
 - Los requisitos de recuperación generalmente se desglosan por áreas funcionales, incluidas instalaciones y áreas de trabajo, sistemas de TI e infraestructura, fabricación y producción (operaciones) y datos críticos/registros vitales, en general, cualquier requisito importante que tenga su empresa.
 - Estos requerimientos de recuperación se desarrollan para los procesos críticos identificados en el BIA, lo que nos ayuda a identificar los recursos que deben ser el foco de la estrategia de recuperación.
 - Si un proceso no es de misión crítica o esencial no será un buen candidato para gastar tiempo y esfuerzo en este proceso de mitigación.
 - Se pueden clasificar respecto a las áreas funcionales, por ejemplo, para el área de Instalaciones (edificios), un requerimiento de recuperación puede ser un espacio alterno para las oficinas o un centro de comando para gestionar la crisis y las comunicaciones.

Proceso de mitigación de riesgos

- Opciones de recuperación
 - Para desarrollar una variedad de opciones de recuperación se debe tomar en cuenta el impacto en la organización, dependencias con otras funciones, dependencias de TI, puestos clave, las habilidades y los conocimientos necesarios, el tiempo necesario de recuperación y cualquier otra información que haya identificado en el BIA.
 - Estas opciones tendrán distintos plazos, costos y capacidades, por lo que, en este punto, solo debe preocuparse de desarrollar la lista de **opciones viables** en función de los datos obtenidos.
 - Por ejemplo, si necesita un sitio alterno podría listar una nube pública, nube privada, co-location, sitio alterno propio, sitio alterno alquilado, después se deberá evaluar cada opción.

Proceso de mitigación de riesgos

- Opciones de recuperación
 - Existen 3 opciones básicas de recuperación:
 - **Según sea necesario:** generalmente toma más tiempo para implementar después de un evento y cuesta más, pero puede tener un costo menor si se toma en cuenta los costos acumulados durante un tiempo largo.
 - **Con antelación:** suelen ser de un costo intermedio e implementarse en menor costo pues ya está pactado, para estas opciones debe evaluar de forma exhaustiva a sus proveedores para asegurarse que podrán cumplir con lo ofrecido.
 - **Preestablecida:** se podrá implementar de forma casi inmediata, pero suelen tener un costo mayor, recurrente e irrecuperable antes del evento. En algunos casos se busca minimizar el impacto de estos costos aprovechando de alguna forma, por ejemplo, un sitio alterno puede ser frío, tibio o caliente.



Proceso de mitigación de riesgos

- Tiempo de recuperación de las opciones
 - Una vez listados los requerimientos y las opciones de recuperación se deberán observar los tiempos de recuperación de cada opción.
 - Dado que ya está definido el MTD puede compararlo con estos tiempos, las opciones que no cumplen con esto deberán ser eliminadas del listado.
- Costo vs capacidad de las opciones de recuperación
 - Ahora cuenta con una lista reducida de opciones de recuperación en función de las que cumplen con los requisitos de recuperación y el MTD.
 - A esta lista debe agregar la evaluación del costo y las capacidades de cada una, el listado de atributos a considerar es:
 - Costo: Costo de la opción de mitigación o recuperación.
 - Capacidad: las capacidades de la opción (características vs necesidades).
 - Esfuerzo: la cantidad de esfuerzo que tomará implementar y administrar la opción.
 - Calidad: atributos de calidad del producto, servicio o datos asociados con la opción.
 - Control: cantidad de control que retendrá la empresa sobre el proceso crítico.
 - Seguridad física (safety): en los casos que aplique, se debe indicar una calificación de la seguridad física que esta opción ofrece para luego poder hacer una comparación con otras opciones (seguridad para las personas y equipos en las instalaciones).
 - Seguridad (security): se refiere a la seguridad de los datos y recursos (que no sean robados, eliminados, etc.).
 - Conveniencia: suele ser un atributo cualitativo basado, de preferencia, en datos cuantitativos, se debe documentar los datos y razones para calificar la conveniencia, por ejemplo, como alta, neutra o baja.

Proceso de mitigación de riesgos

- Costo vs capacidad de las opciones de recuperación
 - Puede crear una matriz para evaluar estos atributos y poder tomar una decisión, por ejemplo:
 - Opciones para adquirir un sistema crítico de TI

Opción	Costo	Capacidad	Esfuerzo	Calidad	Control	Seguridad física	Seguridad	Deseabilidad
Según sea necesario	Alto	Desconocido	Alto	Bajo	Bajo	N/A	N/A	Bajo
Con antelación	Medio	Cumple requisitos	Medio	Medio	Medio	N/A	N/A	Medio
Preestablecida	Bajo	Cumple requisitos	Bajo	Alta	Alta	N/A	N/A	Medio

- Opciones para establecer un data center alterno

Opción	Costo	Capacidad	Esfuerzo	Calidad	Control	Seguridad física	Seguridad	Deseabilidad
Sitio frío pagado por la empresa	Medio	Cumple requisitos	Medio	Bajo	Alta	Media	Media	Media
Sitio caliente con proveedor externo	Alto	Cumple requisitos	Bajo	Alta	Baja	Alta	Alta	Media
Servicio de nube pública	Bajo	Cumple requisitos	Bajo	Media	Baja	Alta	Media	Media

Proceso de mitigación de riesgos

- SLA de recuperación
 - Cualquier acuerdo de servicio de recuperación debe incluir métricas específicas que lo definan, por ejemplo:
 - Tiempo de respuesta
 - Capacidades técnicas: espacio de almacenamiento, velocidades, etc.
 - Acceso a las áreas y equipos
 - Acceso a áreas de trabajo para el personal
 - Procedimientos y garantía de seguridad
 - Soporte técnico y funcional

Los SLA que tenga con servicios contratados le pueden servir de referencia para evaluar los de recuperación.

Proceso de mitigación de riesgos

- Revisión de controles existentes
 - En algunos casos ya tendrá implementadas algunas de las opciones de recuperación, es necesario revisar que cumplan con los requisitos correspondientes pues seguramente no fueron implementadas con estos en mente.
 - Además, el hecho de estar ya implementadas, pueden ser una ventaja vs otras opciones y hacer más fácil su aceptación o realizarle mejoras.

Proceso de mitigación de riesgos

- Desarrollo de la estrategia de mitigación de riesgos
 - Los pasos para desarrollar la estrategia de mitigación de riesgos son:
 1. Reunir los datos de recuperación
 2. Comparar costos, capacidades y SLAs de las opciones
 3. Determinar si las opciones restantes se clasifican en aceptar, evitar, limitar o transferir el riesgo y cuál es más deseable de estas.
 4. Seleccionar las opciones que mejor se adapten a las necesidades de la empresa.
 - Estos datos y el proceso realizado deben quedar documentados, el resultado final puede documentarlo utilizando tablas o cualquier formato que la empresa utilice siguiendo el mismo estilo que los pasos anteriores.

Proceso de mitigación de riesgos

- Ejemplo de opciones para la estrategia de mitigación de pérdida de datos críticos:

Categoría	Opción	Costo, Capacidad, SLAs	Mitigación de Riesgos	Implementar
Frecuencia de respaldo de datos	Continua	Costoso, ningún tiempo de inactividad, excede el MTD	Solución potencial, dependiendo del costo de implementación.	
	Diario	Moderado, hasta 8 horas de pérdida potencial de datos, 3 horas para restaurar, cumple con MTD	Implementar un proceso de respaldo diario para reducir la probabilidad de pérdida significativa de datos y para reducir el tiempo de recuperación para cumplir con MTD.	X
	Semanal	Moderado, hasta 5 días de pérdida potencial de datos, 12 horas para restaurar, puede cumplir con MTD		
	Mensual	Bajo, no cumple con MTD		
Tipo de Respaldo de Datos	Completo	Mayor tiempo de respaldo, menor tiempo de recuperación, cumple con MTD		
	Incremental	Tiempo de respaldo medio, mayor tiempo de recuperación, excede MTD		
	Diferencial	Tiempo de respaldo medio, tiempo de recuperación medio, cumple con MTD	El respaldo diferencial cumple con MTD al menor costo.	X

Proceso de mitigación de riesgos

- Ejemplo de opciones para la estrategia de mitigación de pérdida de datos críticos:

Categoría	Opción	Costo, Capacidad, SLAs	Mitigación de Riesgos	Implementar
Método de Respaldo de Datos	Cintas de respaldo	Mayor tiempo de recuperación, menos costoso, puede no cumplir con MTD		
	Vaulting electrónico	Tiempo de recuperación largo, algo costoso, puede no cumplir con MTD		
	Replicación de datos	Tiempo de recuperación medio, gasto medio, puede cumplir con MTD		
	Sombreado de discos	Recuperación rápida, gasto medio, puede cumplir con MTD	Basado en restricciones de costo, esta opción puede cumplir con MTD. Este y el sombreado de discos serán explorados en términos de costo, tiempo y viabilidad.	X
	Espejo de discos	Recuperación rápida, gasto medio, puede cumplir con MTD	Basado en restricciones de costo, esta opción puede cumplir con MTD. Este y el sombreado de discos serán explorados en términos de costo, tiempo y viabilidad.	X
	Virtualización de Almacenamiento	Tiempo de recuperación rápido, alto costo, elimina el riesgo de fallos localizados, cumple con MTD		
	Almacenamiento en Red	Tiempo de recuperación rápido, mayor costo, elimina el punto único de fallo, puede eliminar el riesgo de fallos localizados, cumple con MTD		
	Clúster de Alta Disponibilidad en Área Amplia	Tiempo de recuperación rápido, mayor costo, elimina el punto único de fallo, puede eliminar el riesgo de fallos localizados, cumple con MTD		
	Espejo Remoto	Disponibilidad continua, tiempo de recuperación cero, costo más alto, elimina el punto único de fallo y el riesgo de fallos localizados, excede MTD		

Mitigación de riesgos de TI

Mitigación de riesgos de TI

- Hasta el momento hemos hablado bastante sobre el análisis de impacto y la mitigación de riesgos a nivel empresa.
- Vamos a centrarnos en la mitigación de riesgos específicamente para TI.
- El riesgo con respecto a los datos incluye, además de los **desastres naturales** de los que hemos estado hablando, las **interrupciones en el centro de datos** (incendios, energía, humedad, etc.), **fallas de hardware** (por antigüedad, accidentes, etc.) o **software** (bugs), **violaciones de seguridad** que pueden incluir pérdida, robo o modificaciones de datos críticos, e interrupciones debido a que los **datos críticos no están disponibles** para los usuarios (DDoS, malware, etc.).
- Los análisis de riesgos y de impacto deben cubrir estos, por lo que es un buen momento para revisarlos con más detalle.

Mitigación de riesgos de TI

- Datos y registros críticos
 - Al analizar el MTD y el costo de las interrupciones (pérdida de productividad, pérdida de ingresos, etc.), tendrá una sólida comprensión del impacto que tendría la pérdida de varios datos críticos en la organización.
 - Si no lo tiene claro, debe regresar a su análisis de riesgo, vulnerabilidad e impacto para obtener en **dónde se guarda sus datos críticos, quién los genera, qué se hace con ellos y qué harían sin ellos**.
- Además, deberá analizar los requerimientos legales y regulatorios asociados con los datos críticos, por ejemplo, datos médicos, financieros, etc. que sean afectados de alguna forma por la ley.
 - Es necesario consultar con abogados sobre esto y que nos mantengan informados sobre cambios en las leyes y regulaciones que puedan afectarnos.
- Finalmente debe revisar todos sus controles existentes, así como las soluciones propuestas a la luz de la recuperación ante desastres y continuidad del negocio.
- Normalmente encontraremos que nuestros controles cubren partes de los posibles riesgos, pero seguramente no hayamos considerado todas las posibilidades al analizarlos contra estos.



Mitigación de riesgos de TI

- Sistemas e infraestructura críticos
 - A partir de las necesidades de protección y administración de datos dentro del alcance del proceso de planificación de BC/DR, puede comenzar a evaluar soluciones de hardware y software, proveedores y costos.
 - No existe una fórmula única para solucionar esto, deberá utilizar los conocimientos y experiencia propia y de su equipo, así como proveedores que puedan asesorarlo.
 - Las convenciones, visitas de o a proveedores, desayunos y demás invitaciones son buena fuente de actualización para estar enterados de los últimos avances y servicios ofrecidos por los diferentes fabricantes.
 - A partir de analizar los controles actuales vs los que necesita, podrá determinar si puede **complementar o debe cambiar por completo algunos de ellos**.
 - A partir de este proceso se dará cuenta que debe tener proveedores, hardware y software que le **solucionen a mediano plazo**, 3 a 5 años, y no simplemente buscar las soluciones más baratas, imagine una solución de backup de la que no tenga seguridad que estará vigente y funcionando un año después.
 - Además, se recomienda que **no se enfoque en soluciones a largo plazo**, más de 10 años, pues seguramente tendrá que invertir mucho tiempo y recursos en buscar la solución perfecta y, dado que la tecnología y los requerimientos cambian, podría malgastar estos recursos.
 - Esto depende mucho de la solución y situación específicas, debe analizar todas las aristas antes de tomar decisiones.
 - Debe evaluar el **costo de adquisición, implementación y administración de la solución**. Tendrá que hacer algunas concesiones, pero si tiene en cuenta las **limitaciones de datos y el presupuesto**, podrá **diseñar una solución aceptable (o incluso óptima)** que se ajuste a esos parámetros.

Mitigación de riesgos de TI

- Revisión de las prioridades críticas del sistema
 - A través de su análisis de impacto empresarial, debería haber desarrollado una **evaluación de los sistemas de TI críticos que incluya una priorización** de los activos.
 - Debería tener un listado de los activos y sus prioridades, por ejemplo:
 - Cluster de servidores virtuales: Alto
 - Acceso a Internet: Alto
 - Acceso a correo electrónico: Bajo
 - NAS: Alto
 - CRM: Alto
 - Aplicación de administración de inventario: Medio
 - Sistema financiero: Medio
 - Basado en este análisis debe revisar sus estrategias de mitigación de riesgo para asegurarse que cumplen o exceden los requerimientos de recuperación en función de estas prioridades.
 - No se olvide de las dependencias, algunas veces nos centramos en los sistemas principales y nos olvidamos de que estos pueden depender de componentes que no estén clasificados como prioritarios.
 - Por ejemplo, podemos tener un servidor clasificado como importancia alta, tener un reemplazo, pero no tomar en cuenta el switch al que este se conecta, de forma que, al momento de la recuperación, no cumpliríamos con lo establecido debido a una dependencia.
 - Debemos documentar el orden de recuperación, algunos pueden ser intuitivos, como recuperar el servidor antes de instalar el SO, pero en algunos casos este orden podrá no ser tan obvio, por ejemplo, que un sistema deba acceder a Internet para verificar una licencia o un sistema que dependa del Active Directory para identificar a los usuarios.

Consideraciones sobre backups y recuperación

Consideraciones sobre backups y recuperación

- Como profesionales de TI estamos conscientes de la importancia de los backups y su respectiva recuperación, esto suele asociarse únicamente a datos, pero es aplicable a toda la infraestructura y software.
- Existen varias opciones y la idea es que revisemos algunas de ellas para tenerlas en mente en el momento de desarrollar nuestra estrategia.

Consideraciones sobre backups y recuperación

- Procesos de negocio alternos
 - En el análisis realizado hasta el momento usted tendrá los procesos de negocio clave y métodos alternativos para manejar estos procesos durante una interrupción, ya sea de los sistemas de TI, el edificio, el área en donde este se encuentra, etc.
 - En base a este análisis debe revisar cada proceso para determinar si existe un método alternativo para proveer los datos necesarios para que estos procesos funcionen de forma correcta.
 - Datos de órdenes de producción
 - Datos de clientes para atenderles en caso de dudas
 - Datos financieros
 - Nómina

Consideraciones sobre backups y recuperación

- Sistemas de recuperación de TI
 - Analice si tiene algún sistema de recuperación y si estos están actualizados, podría ser el momento adecuado de cambiarlos o mejorarlos.
 - Este proceso de análisis debe realizarlo de forma periódica, no puede depender de sistemas con una antigüedad de 5 años sin haberlos revisado previamente.
- Sitios Alternos
 - Esta es una de las decisiones más importantes, debe considerar que estos sitios suelen tener un costo alto, ya sea al inicio o como un gasto recurrente (o ambos).
 - Una clasificación de los sitios alternos puede ser:

Consideraciones sobre backups y recuperación

- Una clasificación de los sitios alternos puede ser:
 - Sitio alterno espejo: es un sitio alterno que tiene exactamente las mismas características y datos que el sitio primario, es el más costoso, aunque puede utilizarse como sitio de acceso rápido según donde estén localizados sus usuarios.
 - Sitio caliente: similar a un sitio espejo, pero no tiene una configuración idéntica siendo capaz de replicar los servicios más importantes.
 - Sitio tibio: un sitio alterno que está equipado para soportar algunos servicios se puede utilizar en el día a día como un sitio para servicios de menor importancia y en el momento de una interrupción tomarse para montar los servicios más importantes.
 - Sitio móvil: son datacenters que pueden transportarse a un lugar alterno y operar desde cualquier sitio.
 - Sitio frío: un sitio que no está en funcionamiento normal, pero existen los procesos necesarios para ponerlo en funcionamiento en el momento de una interrupción, es posible que se deba complementar parte de la infraestructura antes de que pueda funcionar completamente; en este sitio se podría guardar una copia física de los backups.
 - Sitio recíproco: es un acuerdo con algún proveedor o empresa que de alguna forma tenga relación con la suya para establecer un sitio temporal en caso de una disrupción, se le llama recíproco pues el acuerdo es en ambas vías.

Consideraciones sobre backups y recuperación

- Sistemas de almacenamiento
 - Considere opciones de almacenamiento que tengan capacidad para mitigar riesgos y procedimientos de recuperación entre sus características.
 - Por ejemplo:
 - Servidores con sistema de arreglo de discos
 - Discos de repuesto (instalados y no instalados)
 - SAN
 - NAS
 - Protocolos de datos distribuidos
 - Backup automático
 - Contrato de reemplazo de partes

Consideraciones sobre backups y recuperación

- Soluciones para desktops
 - Normalmente se suele no tomar en cuenta los equipos de usuarios, en parte porque puede ser más costoso tener soluciones de mitigación de pérdida de datos y recuperación.
 - Sin embargo, algunos usuarios podrían tener información incluso más sensible que la almacenada en un servidor.
 - Idealmente debería tener una réplica de todos los datos almacenados en un equipo de escritorio, pero los usuarios suelen realizar acciones fuera de lo establecido que hacen de esto una tarea muy complicada.
 - Algunas opciones pueden ser:
 - Apuntar el directorio My Documents a un servidor
 - Utilizar soluciones de nube que repliquen archivos automáticamente
 - Soluciones de backup para sistemas de usuario
 - Equipos virtuales
 - En todo caso deberá identificar los equipos más importantes según la criticidad de los datos que se manejan en ellos.
 - No olvide que estos equipos pueden ser robados por lo que debe preocuparse por asegurar los datos para que estos no puedan ser leídos por personas no autorizadas.

Consideraciones sobre backups y recuperación

- Licenciamiento y software
 - También debe considerar tener un backup de los instaladores del software (SO, Office, servidor de base de datos, CRM, etc.) así como sus respectivas licencias.
 - Aunque hoy en día las licencias suelen estar en línea, aún existen licencias físicas ya sea por medio de códigos o dispositivos de hardware.
 - Tome en cuenta también las contraseñas asociadas a los servicios que se van a instalar, así como de las licencias si estas se encuentran en línea.
 - Además, cuando se habla de licenciamiento no olvide que tendrá que mantener tanto las licencias del sitio primario como el o los sitios alternos.
 - Por último, la configuración necesaria para que los servicios funcionen correctamente también deben mantenerse seguros, en algunos casos es necesario guardar un archivo de configuración o identificar settings específicos que deben cambiarse para que algún servicio funcione correctamente.
 - La configuración de seguridad puede pasarse por alto en el proceso de recuperación así que no olvide, no solo tener la configuración respaldada, sino establecer procesos que eviten el olvidarse de esto.



Análisis de Impacto

ING. FREDY BUSTAMANTE

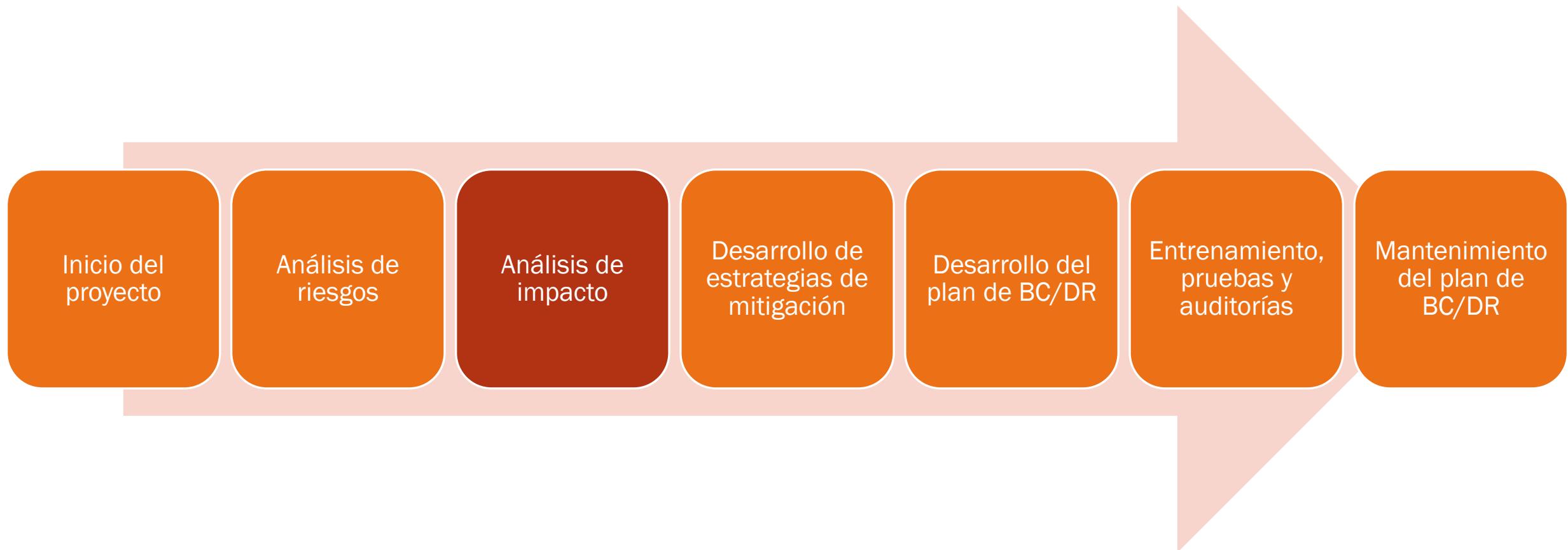
Análisis de Impacto

- Es uno de los aspectos más críticos del plan de BC/DR.
- Al terminar esta fase podrá entender el impacto de varias amenazas e interrupciones sobre el negocio y desarrollará métodos que, de forma sistemática, reducirán el riesgo y mitigarán el impacto.
- Los puntos que veremos son:
 - Descripción general
 - Comprender la criticidad del impacto
 - Identificar funciones y procesos empresariales
 - Recopilar datos para el análisis de impacto empresarial
 - Determinar el impacto
 - Puntos de datos del análisis de impacto empresarial
 - Preparación de informe

Análisis de Impacto

- En el tema anterior hablamos sobre la administración del riesgo y el proceso para el análisis de este. Para eso hablamos de amenazas que una empresa puede enfrentar y de cómo debemos documentarlas.
- El análisis de impacto (BIA) analiza las funciones comerciales (procesos de negocio) críticas y el impacto de no tener esas funciones disponibles para la empresa.
- El análisis de riesgo empieza desde el lado de las amenazas y el análisis de impacto comienza desde el lado de los procesos de negocio.
 - Cuando se habla en general de riesgo empresarial puede que se inicie con el análisis de impacto, pero al realizar el plan de BC/DR hace más sentido tener una imagen general de las amenazas para luego analizar su impacto.
 - Sin embargo, lo importante es que, antes de desarrollar la estrategia de mitigación se cuente con el ambos análisis.

Análisis de Impacto



Análisis de Impacto

- La principal tarea del análisis de impacto es comprender que procesos en su negocio son vitales para sus operaciones en curso y comprender el impacto que la interrupción de estos procesos tendría en su negocio.
- Desde el punto de vista de IT, según NIST:
 - El propósito de BIA es correlacionar componentes específicos del sistema con los servicios críticos que brindan y, en base a esa información, caracterizar las consecuencias de una interrupción en los componentes del sistema.
 - Dos partes esenciales: Entender los procesos críticos y correlacionarlos a los servicios de TI.

Análisis de Impacto

- Como profesionales de TI entendemos la importancia de los servicios de TI, pero debemos entender cuáles son los procesos críticos que dependen de nuestros sistemas para que, en caso de una interrupción, tengamos definido qué servicios y en qué orden debemos recuperar con mayor urgencia.
 - En el momento de la crisis todos los departamentos de la empresa solicitarán con urgencia el restablecimiento de los servicios que utilizan, ¿a quién le hacemos caso?
- Como Ingenieros en Informática y Sistemas estamos en la capacidad de ser Gerentes de Sistemas (CIO) e incluso, con estudios y experiencia adicional, estamos en la capacidad de ser Gerente General (CEO), por esto, debemos pensar como administradores de la empresa en forma general cuando tomamos decisiones y manejar conceptos de finanzas, producción, administración, recursos humanos, etc. Ahora es normal que cualquier proceso de la empresa, crítico o no, requiera tecnología para funcionar (correo electrónico, hardware, software específico, etc.)
 - Cadena de valor, razones financieras, ciclo de conversión de efectivo, estrategia, etc, son conceptos con los que podemos analizar a la empresa y comunicarnos con nuestros pares.

Análisis de Impacto

- De acuerdo con el Instituto de Continuidad de Negocio (BCI, www.thebci.org), existen 4 propósitos principales del BIA:
 - Comprender los objetivos críticos de la organización, la prioridad de cada uno y el plazo para la reanudación de estos, luego de una interrupción no programada.
 - Informar una decisión de gestión sobre la interrupción máxima tolerable (MTO) para cada función.
 - Proporcionar la información de recursos (equipos, instalaciones, tecnologías, proveedores, personal) a partir de la cual se puede determinar/recomendar una estrategia de recuperación adecuada.
 - Delinear las dependencias que existen tanto interna como externamente para lograr objetivos críticos.

Análisis de Impacto

- BIA en pasos más detallados:
 1. Identificar procesos y funciones comerciales clave.
 2. Establecer requisitos para la recuperación empresarial.
 3. Determinar las interdependencias de recursos.
 4. Determinar el impacto en las operaciones.
 5. Desarrollar prioridades y clasificación de procesos y funciones de negocio.
 6. Desarrollar requisitos de tiempo de recuperación.
 7. Determinar el impacto financiero, operativo y legal de la interrupción.

Análisis de Impacto

- Los dos puntos de impacto principales de cualquier interrupción del negocio son el **impacto operativo** y el **impacto financiero**.
 - Impacto Operativo: aborda el efecto no monetario, incluyendo cómo las personas, los procesos y la tecnología se ven afectados por una interrupción del negocio y cuál es la mejor manera de abordar ese impacto.
 - Impacto Financiero: aborda los impactos monetarios y cómo una interrupción del negocio afectará los ingresos, los costos y la viabilidad general de la empresa, tanto a corto como a largo plazo.

Análisis de Impacto

- El DRI identifica los siguientes tópicos a considerar:

1. Impacto en el cliente

- ¿Qué tan pronto se darán cuenta los clientes de tu problema?
- ¿Qué tan rápido llevarán su negocio a tu competidor?
- ¿Qué tan rápido se moverán los proveedores contractuales (quienes brindan servicio a tus clientes en tu nombre) a un competidor?
- ¿Cuál es el impacto en tus acuerdos de nivel de servicio contractual?
- ¿Cuál es el impacto en la cadena de suministro para tus clientes clave?
- ¿Cuáles son las implicaciones aguas arriba y aguas abajo para tus clientes clave?

2. Impacto financiero

- Pérdida de ingresos y ganancias
- Costos para recuperarse de un desastre:
 - Horas extras y mano de obra temporal
 - Viajes y gastos para consultores y proveedores
 - Deducibles de seguros
 - Gastos de bolsillo no cubiertos por el seguro
 - Equipos, materiales y suministros perdidos
- Costos de limpieza y restauración
- Costos de mejora durante la nueva construcción
- Impacto en la cuota de mercado
- Impacto en el precio de las acciones o valoración a corto y largo plazo
- Multas y sanciones contractuales o regulatorias
- Potenciales demandas (todos los honorarios asociados)

Análisis de Impacto

3. Impacto reputacional

- Junta directiva
- Accionistas
- Clientes
- Comunidad
- Atención de los medios y redes sociales
- Competidores aprovechando tu desastre

4. Impacto operativo

- Niveles de servicio o producción reducidos
- Aumento de costos de materiales (pedidos de emergencia)
- Aumento de costos de horas extras o mano de obra con producción reducida
- Disrupciones en el flujo de trabajo (soluciones

manuales, etc.) y reducción de eficiencias

- Pérdida de control (calidad)
- Incapacidad para cumplir con plazos y entregables claves
- Disrupción de proyectos y/o procesos en curso
- Disrupción de la cadena de suministro

5. Impacto humano

- Pérdida de vidas y lesiones graves
- Impacto en las funciones comunitarias
- Estrés (impacto en la familia, el trabajo y la comunidad)
- Aumento del uso de servicios comunitarios o sociales
- Impacto emocional a largo plazo en la familia, el trabajo y la comunidad

Análisis de Impacto

- **Pérdidas aguas arriba y aguas abajo**

- Adicional al impacto directo de una interrupción, existen impactos indirectos que debemos considerar.
- Pérdidas aguas arriba: El término aguas arriba se refiere a las etapas anteriores de un proceso de producción o cadena de suministro, por lo que las pérdidas aguas arriba son aquellas que sufrirá si uno de sus proveedores clave es afectado por un desastre.
- Pérdidas aguas abajo: Aguas abajo se refiere a las etapas posteriores de un proceso de producción o cadena de suministro (por ejemplo, distribución, venta y servicio al cliente), por lo que las pérdidas aguas abajo ocurren cuando los clientes clave o las vidas de la comunidad se ven afectados.
- En ambos casos pueden existir pérdidas aun cuando nuestro negocio no ha sufrido un desastre, pero sí la comunidad, clientes o proveedores.
 - Tome en cuenta que las personas, negocios y comunidades están interrelacionados.

Análisis de Impacto

- Impacto humano

- Un desastre puede impactar en la vida de las personas produciendo heridas o incluso muertes.
- A medida que se evalúen las funciones y los procesos de negocio, también necesitará identificar **puestos clave, conocimientos clave y habilidades clave** necesarias para BC/DR.
- En cierto sentido, esto comienza a entrelazarse con lo que llamamos **planificación de sucesión**.
 - Por ejemplo, en algunas empresas no se permite a dos personas clave o sustituto uno del otro viajar juntos.
- Posiciones clave: las empresas deben tener un plan en el que se identifica a los posibles sucesores en puestos clave, de forma que, si existe una renuncia, despido o muerte, se tenga ya un plan para reemplazar a la persona, para esto es necesario determinar las responsabilidades, conocimientos y habilidades con las que debe contar el sucesor de forma que esté capacitado o al menos tener el plan de capacitación correspondiente.
 - Tome en cuenta que se definen las responsabilidades, conocimientos y habilidades necesarias para el puesto, no las que tiene una persona en específico.
- Estos sucesores de posiciones clave, son quienes podrían realizar tareas específicas durante un desastre y/o en el proceso de recuperación si la persona en la posición clave no estuviera disponible.
- En el departamento de TI podemos identificar al SA o DBA que pueda, por ejemplo, reinstalar un servidor y volver a dejar operacional un servicio (note que no siempre será el jefe o coordinador quien esté en la posición clave)

Análisis de Impacto

- Necesidades Humanas

- Más allá de identificar reemplazos temporales o definitivos, habilidades, etc. Es importante tomar en cuenta que durante y después de un desastre las personas reaccionarán de formas distintas, por ejemplo, algunos podrían evacuar e inmediatamente estar bromeando en el área de reunión, otros podrían tener ataques de pánico, algunos podrían parecer estar normales y horas o días después tener alguna reacción tardía.
- Un buen plan de BC abordará los factores humanos por dos razones:
 1. Es lo correcto: no todos los empleados estarán listos para continuar sus labores de forma normal, algunos tendrán hijos o familiares que atender, otros podrán requerir atención médica o psicológica, etc.
 2. Tiene sentido empresarial: si los empleados deben decidir entre familia y trabajo, lo normal es que se inclinen por lo primero, aun así, algunos tendrán un sentido de responsabilidad hacia el trabajo que los haga reincorporarse antes de estar listos, lo cual puede ocasionar errores o accidentes, por lo que, tener un plan para suplir temporalmente al personal que no está listo ayudará a evitar estos problemas.

Análisis de Impacto

- Criticidad del impacto

- Durante el proceso de determinar las funciones críticas del negocio debe tener en mente una escala de calificación.
- Más adelante, una vez que haya compilado su lista, podrá asignar una "calificación de criticidad" a cada función comercial.
- **Categorías de Criticidad:** Se puede utilizar la clasificación que desee, solo asegúrese de que esté bien definida, bien delimitada y sea entendida por todos, por ejemplo:
 - Categoría 1: Funciones críticas – de misión crítica
 - Categoría 2: Funciones esenciales – Vitales
 - Categoría 3: Funciones necesarias – Importantes
 - Categoría 4: Funciones deseables – Menores

Análisis de Impacto

- Funciones críticas – de misión crítica

- Los procesos y funciones comerciales de misión crítica son aquellos que tienen el mayor impacto en las operaciones y la necesidad de recuperación de su empresa.
- La tolerancia a una interrupción que impida la realización de este tipo de funciones será muy pequeña en comparación del resto de funciones, normalmente se hablará de pocas horas.
- Se debe responder a la pregunta ¿Cuáles son los procesos que deben estar presentes para que la empresa pueda funcionar?

- Funciones esenciales – Vitales

- Algunas funciones estarán entre las críticas y las importantes, así que se utiliza esta categoría para este tipo de funciones (más importantes que el resto de las funciones, pero no son de misión crítica).
- Si no le es posible determinar cuáles funciones no son críticas puede ser que esta categoría quede vacía.
- Piense en las funciones que son extremadamente importantes pero que deben ser atendidas después de las funciones críticas.
- La recuperación de estas funciones podría variar entre varias horas a un par de días.

Análisis de Impacto

- Categoría 3: Funciones necesarias – Importantes

- Las funciones y procesos importantes no impedirán que el negocio funcione en el corto plazo, pero generalmente tienen un impacto a largo plazo si faltan o se desactivan.
- Desde el punto de vista de TI piense en servicios como el correo electrónico, acceso a internet.
- La recuperación de estas funciones podría tomar días o semanas.

- Categoría 4: Funciones deseables – Menores

- Los procesos de negocio menores suelen ser aquellos que se han desarrollado a lo largo del tiempo para abordar problemas o funciones pequeños y recurrentes.
- No se les extrañará en el corto plazo y definitivamente no mientras se recuperen las operaciones.
- Incluso, algunas de estas funciones podrían nunca recuperarse.
- Puede considerar no tener una opción de recuperación de estas funciones o servicios.
- La recuperación de estas funciones podría tomar semanas o meses.

Análisis de Impacto

- Funciones estacionales y ocasionales

- Cuando realice sus entrevistas de BIA, asegúrese de pedir a los participantes que piensen en todos los procesos comerciales a lo largo del año (o años). Algunas funciones y procesos ocurren solo durante ciertas épocas del año, como la temporada de impuestos, fin de año y días festivos, y es posible que se omitan durante el proceso. Si son procesos lo suficientemente importantes, hay muchas posibilidades de que se incluyan, pero las mejores prácticas de gestión de proyectos no dependen de la suerte: dependen del proceso. Asegúrese de preguntar sobre cualquier proceso especial que ocurra a lo largo del año calendario y que tal vez no se les ocurra de inmediato a los participantes.

Análisis de Impacto

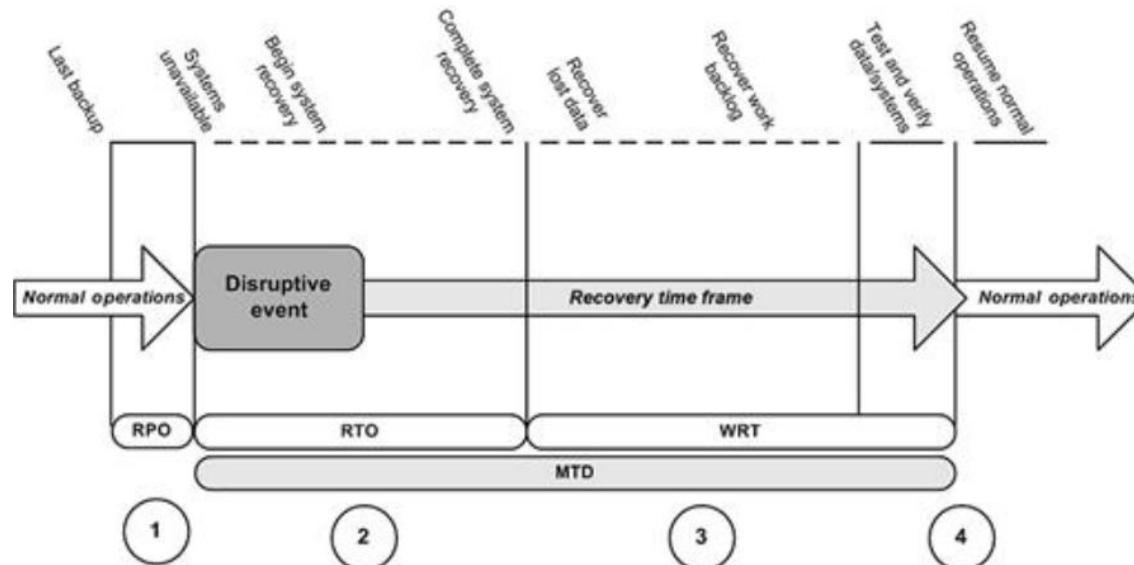
- Requisitos de tiempo de recuperación
 - Relacionado a la criticidad del impacto están los requisitos de tiempo de recuperación.
- Veamos la definición de algunos términos que nos servirán para entender mejor:
- Tiempo de inactividad máximo tolerable (Maximum tolerable downtime, MTD)
 - Como se indica en el nombre el tiempo máximo que una empresa puede tolerar la ausencia o indisponibilidad de una función comercial particular.
 - En algunos casos se utiliza Maximun Tolerable Outage (MTO)
 - Entre más alta la criticidad de la función menor será el MTD.
 - El tiempo de inactividad consta de dos elementos:
 - Tiempo de recuperación del sistema
 - Tiempo de recuperación del trabajo
 - Es decir: $MTD = RTO + WRT$

Análisis de Impacto

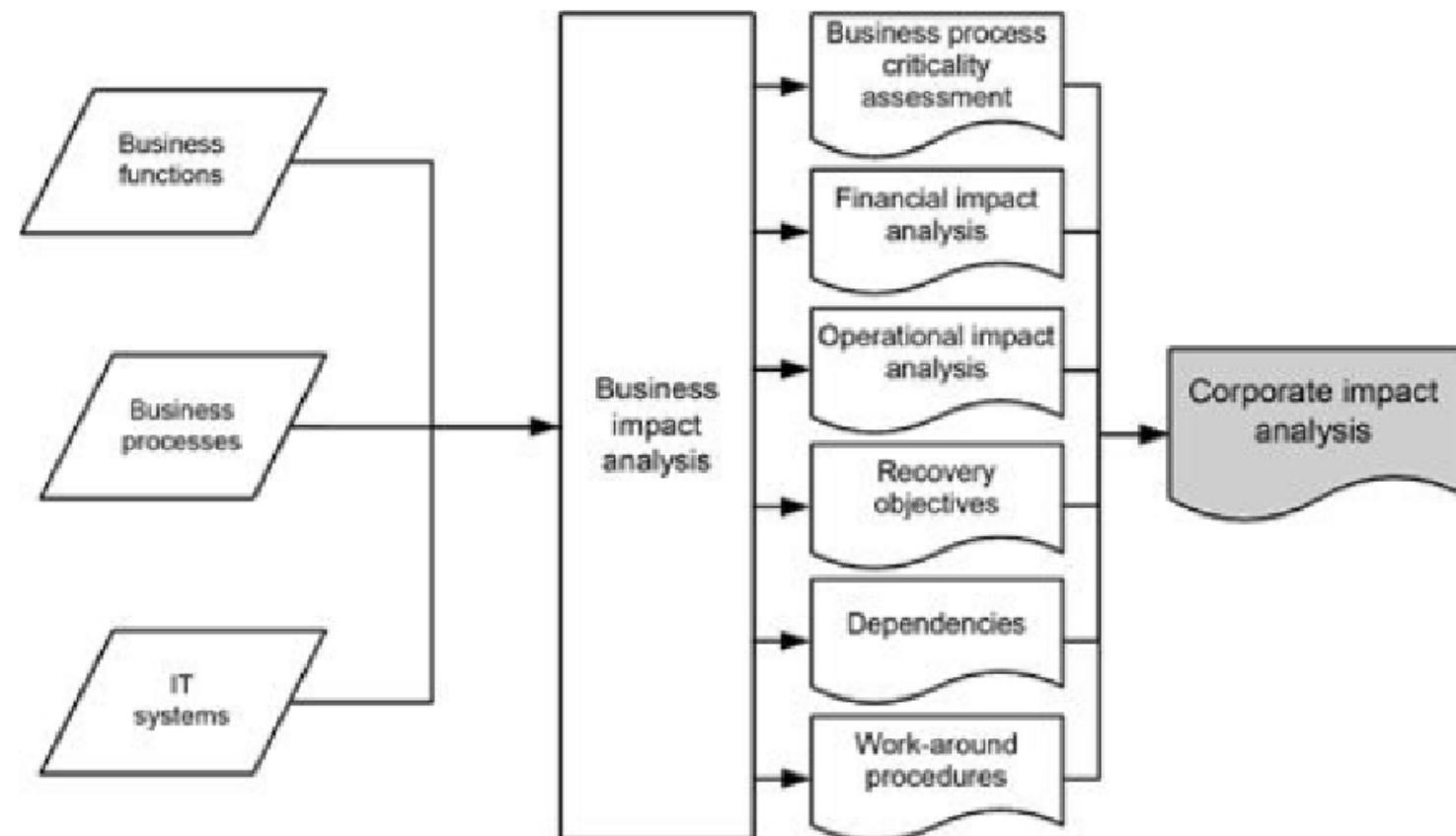
- MTD = RTO + WRT
- Recovery time objective (RTO)
 - El tiempo objetivo de recuperación se refiere al tiempo en que, por ejemplo, un sistema esté nuevamente accesible para los usuarios, por ejemplo, puede tomarnos 1 hora tomar una imagen de una máquina virtual, realizar configuraciones y recuperar el último backup de la base de datos.
- Work recovery time (WRT)
 - El tiempo de recuperación del trabajo es el tiempo que toma para revisar que los servicios estén funcionando de forma correcta, se realicen sincronizaciones y otras tareas previas a la operación, así como que los usuarios ingresen y se preparen para regresar al punto en el que estaban antes de la interrupción.
 - El no tomar este tiempo en cuenta puede afectarnos y no cumplir con el MTD establecido.

Análisis de Impacto

- Objetivo de punto de recuperación (Recovery point objective, RPO)
 - El punto de recuperación es la cantidad de datos perdidos que se puede tolerar por el sistema o función.
 - Desde la perspectiva de TI, a esto debe responder nuestra política de backups.



Análisis de Impacto



Análisis de Impacto

• Identificar funciones

- Debe iniciar por listar todas las funciones que su equipo tenga en mente no importando si, en principio, no les encuentre mayor importancia a algunas.
- Es importante poder incluir a los expertos de cada área de la empresa para que este análisis pueda incluir aquellos detalles que pueden escapar al resto de personas.
- Puede iniciar con la siguiente lista y agregar o eliminar las que no correspondan a su empresa:
 1. Instalaciones y seguridad
 2. Finanzas
 3. Recursos Humanos
 4. Tecnología de la información
 5. Legal/cumplimiento
 6. Fabricación (montaje)
 7. Marketing y ventas
 8. Operaciones
 9. Investigación y desarrollo
 10. Almacén (inventario, cumplimiento de pedidos, envío y recepción)

* Listado en orden alfabético en inglés.

Análisis de Impacto

- Al analizar estas funciones empresariales, piense en cómo funciona su negocio y los procesos clave que ocurren en cada una de estas.
- Estos procesos clave serán los que categorice según lo visto con anterioridad.
- Además de listar y describir las funciones y procesos se recomienda documentar las posiciones clave, habilidades y conocimientos correspondientes.

Análisis de Impacto

- Instalaciones y seguridad

- ¿Cuántas localidades tiene la empresa, tamaños, características generales?
- ¿Cuáles de estas localidades son necesarias para la operación?
- ¿Qué debería hacer para trasladar alguna operación o recuperarlas en caso de desastres?
- ¿Cómo establecemos la seguridad para el ingreso del personal? ¿esto podría ser secundario?

- Finanzas

- Por definición Finanzas es una función crítica de la empresa, pero no todas las funciones financieras de la empresa con de misión crítica.
- Son críticas o esenciales: ¿pagos y cobros a corto plazo? ¿facturación? ¿pago de nómina?*
- Es necesario pensar en aquello que pueda generarnos una demanda legal, aunque no parezca tan importante para el funcionamiento de la empresa.
- Al verificar estas funciones y sus posibles estrategias de mitigación tendrá una oportunidad para innovar con tecnología y hacer que las personas salgan de su zona de confort.

* Una parte de este proceso es del departamento de finanzas, aunque en general será un proceso de RRHH

Análisis de Impacto

- Recursos Humanos

- Durante un desastre y en los primeros momentos del proceso de recuperación RRHH debería ser un centro de información, el personal debe estar informado para ser la comunicación oficial.
 - ¿Cuándo y dónde se deberá presentar a trabajar? ¿las personas de la empresa y la comunidad se encuentran bien? ¿Cuál es el estado general de la empresa?
 - ¿Cuándo y cómo se les pagará? ¿el sueldo completo?
- RRHH estará afectada y afectará a muchas funciones, se debe analizar con cuidado y no dejar fuera ninguna función hasta que se haga el listado completo por prioridades.

- Tecnología de la información

- Todas las funciones de TI parecen ser críticas, más si las analizamos desde el punto de vista de qué tanto nos “llamarán” los usuarios si alguno de los servicios no está disponible.
- Generalmente serán las demás funciones de la empresa las que determinen qué servicios son críticos para operar, es decir, se clasificarán las funciones de TI en base a las demás funciones de la empresa.
- Si analizamos individualmente cada servicio con las funciones a las que sirven, todos serán críticos.
- También debemos determinar aquellas funciones que ocurren dentro del área de TI y que pueden ser esenciales para la recuperación ante un desastre, como los backups o la seguridad de la información que puede quedarse para un segundo plano y tener mayores problemas a corto, mediano o largo plazo.

Análisis de Impacto

- Legal/cumplimiento

- No suele ser un área que toda empresa tenga, por lo que habrá que determinar quién o quiénes son los encargados de estas funciones.
- Se debe pensar qué funciones son críticas para mantenerse en “cumplimiento” tanto para los contratos firmados como la ley en general, tomando en cuenta las leyes locales y extranjeras según nos afecten por clientes o proveedores.

- Fabricación (montaje)

- Si la empresa tiene esta función (fabricación directamente, ensamblaje o cualquier forma de producción de bienes), definitivamente será crítica pues es a lo que su empresa se dedica.
- Dentro de todas las funciones de esta área se tendrán que determinar cuáles no son críticas y clasificarlas según corresponda.
- Se debe analizar no solo las funciones internas sino también aguas arriba y aguas abajo, como la pérdida de un proveedor clave o no poder entregar a tiempo al cliente porque la aerolínea que traslada los bienes producidos no esté funcionando.

Análisis de Impacto

- Marketing y ventas

- Se puede pensar que ventas es una función crítica y que marketing no lo es, aunque esto puede ser cierto para la mayoría de las empresas, no podemos dejar de analizar si marketing pueda tener funciones que sí lo sean o se vuelvan críticas durante o después de un evento.
- En general las funciones de ventas serán críticas, aunque algunas podrían no serlo tanto, por ejemplo, para algunas empresas un canal de ventas en línea puede ser secundario.
- Algunas empresas necesitan estar en contacto constante con sus clientes por medio del marketing, al no tener esta función activa podrían perderse ventas importantes. Además, nos puede ayudar a evitar rumores o que falsa información se difunda.

- Operaciones

- Si la empresa no fabrica bienes seguramente se dedicará a algún tipo de servicio (servicios, desarrollo de software, investigación, análisis, etc.). No importa lo que haga, el fin de la empresa será vender para generar ingresos, esta área es la que se encarga de coordinar todas las actividades que hacen que el producto o servicio pueda ser vendido al cliente.
- Cada empresa determina cómo implementa esta función, podría ser un área que engloba todos los procesos necesarios (logística, producción, administración de recursos, control de calidad, cadena de suministros, etc.), en algunos otros casos cada función tiene un área de operaciones.
- Independientemente de esto, las funciones asociadas a operaciones suelen ser críticas por lo que es un caso similar a Fabricación.

Análisis de Impacto

- **Investigación y desarrollo**

- Algunas empresas podrían estar dedicadas a realizar investigación, siendo esta su fuente de ingreso, si este fuera el caso, definitivamente tendremos funciones críticas en esta área.
- De lo contrario, tendremos que analizar si, por ejemplo, la empresa depende del desarrollo de algún nuevo producto o servicio y que pueda tener algún tiempo de entrega específico, o sí se hace investigación con animales, etc.

- **Almacén (inventario, cumplimiento de pedidos, envío y recepción)**

- Estas funciones pueden estar dentro de otras áreas como logística, producción, etc. y estas pueden ser analizadas en conjunto con dichas funciones, o podrían estar separadas como un proveedor interno o externo (subcontrato) ya sea completa o algunas partes.
- En todo caso, habría que analizar las funciones que no se hayan incluido en las otras áreas para determinar su criticidad y colocarlas en la categoría correspondiente.

Análisis de Impacto

- En este análisis nos podemos encontrar con resistencia por parte de las diferentes áreas, de la alta gerencia y hasta de nosotros mismos, pues se pondrá en evidencia procesos mal diseñados, no documentados, no legales, etc.
- Si se afronta con resistencia puede no ser completado de forma correcta y recordemos que es peor tener un mal plan que no tener ningún plan.

Análisis de Impacto

- Recopilación de datos para el análisis del impacto
 - Al igual que en el análisis del riesgo utilizaremos herramientas como cuestionarios, entrevistas, documentación e investigación.
 - Para saber que preguntar debemos contar con el apoyo de los SMEs (subject matter expert), ya sea que ellos diseñen las herramientas, nos apoyen con información para diseñarlas o sean quienes nos den toda la información requerida.
 - Para prepararnos para realizar este análisis debemos entender que los líderes de la empresa estarán muy ocupados con todo tipo de trabajo crítico, por lo que no debemos esperar mucho entusiasmo en tomarse el tiempo de apoyarnos, por el contrario, asumamos que estarán muy renuentes a ayudar por lo que debemos tratar de ser concisos y “quitarles” el menor tiempo posible.

Análisis de Impacto

- Desde un punto de vista de TI, antes de hacer una entrevista o cuestionario, debemos tener claro y a la mano lo siguiente:
 1. Descripción detallada de los sistemas clave, bases de datos y procesos, organizados por área funcional.
 2. Identificación de los propietarios de las aplicaciones de TI y sus contrapartes operativas. (propietarios en TI y en las áreas funcionales)
 3. Descripción clara de las interdependencias de los sistemas, interfaces y sistemas upstream/downstream. (una descripción y un mapa serían muy valiosos para mejor entendimiento)
 4. Descripciones cualitativas y cuantitativas de los costos del tiempo de inactividad.

Análisis de Impacto

- Algunas preguntas que se pueden realizar son las siguientes:

1. ¿Cómo operaría el departamento si los equipos de cómputo, servidores, correo electrónico y acceso a internet no estuvieran disponibles?
2. ¿Qué puntos únicos de fallo existen?
3. ¿Cuáles son las relaciones y dependencias subcontratadas críticas?
4. Si se produjera una interrupción, ¿qué soluciones alternativas utilizaría para sus procesos empresariales clave?
5. ¿Cuál es la cantidad mínima de personal que necesitaría y qué funciones tendrían que llevar a cabo?
6. ¿Cuáles son las habilidades, conocimientos y experiencia clave necesarios para la recuperación?
7. ¿Qué controles operativos o de seguridad críticos se necesitan si los sistemas no funcionan?
8. ¿Cómo funcionaría esta empresa en un sitio de respaldo? ¿Qué personal, equipo, suministros comunicaciones, procesos y procedimientos necesitaría?

Análisis de Impacto

- Determinando el impacto

- Al llegar a este paso tendremos el análisis de riesgo y un listado de puntos de impacto potenciales.
- El impacto de cualquier interrupción en el negocio puede incluir:
 1. Financiero: Pérdida de ingresos, costos adicionales, responsabilidad legal con sanciones financieras.
 2. Clientes y proveedores: pérdida de clientes y proveedores por la interrupción de nuestro negocio o por un desastre que les afecte.
 3. Empleados y personal: pérdida de personal por muerte, lesiones, estrés o abandono de la empresa.
 4. Relaciones públicas y credibilidad: las compañías que experimentan fallos en sus sistemas pueden tener serios problemas de credibilidad.
 5. Aspectos legales: es necesario evaluar las normativas relativas a la salud y seguridad de los trabajadores, la privacidad y la seguridad de los datos y otras limitaciones legales.
 6. Requisitos reglamentarios: puede ser que incumpla algunos requisitos y que no esté exenta de estos según el tipo de desastre sufrido.

Análisis de Impacto

7. Aspectos medioambientales: Algunas empresas podrían enfrentar problemas medioambientales si experimentan fallos en determinados sistemas.
8. Operacional: claramente las operaciones de la empresa pueden verse afectadas por una interrupción.
9. Recursos humanos: ¿cómo se verá afectado el personal? ¿cuál será el impacto de la respuesta del personal en las operaciones? ¿cuáles serán los inconvenientes cualitativos (moral, confianza, etc.)?
10. Exposición a pérdidas: no solo las pérdidas financieras sino de propiedades y cualquier tipo de activos.
11. Imagen social y corporativa: ¿cómo verán a su empresa los clientes, proveedores, socios y la comunidad? ¿se verá afectada su imagen?
12. Credibilidad de la comunidad financiera: ¿cómo verán a su empresa posibles o actuales inversionistas, bandos o entidades crediticias?

Análisis de Impacto

- Matriz de funciones del negocio y criticidad

- Se debe procesar la información sobre las funciones y ordenar por criticidad, al realizarlo puede utilizar una matriz similar a la siguiente:

Función	Proceso	Criticidad
Recursos Humanos	Nómina Verificación de antecedentes de los empleados	Misión crítica Importante
Finanzas	Cuentas por cobrar Cuentas por pagar Declaración de impuestos trimestrales Pagos de deudas/préstamos	Misión crítica Misión crítica Misión crítica Vital
Marketing y Ventas	Llamadas de ventas a clientes Análisis del historial de compras del cliente	Misión crítica Vital

Análisis de Impacto

- Puntos de datos del análisis de impacto

- Dependiendo del tamaño de su empresa así será la cantidad de puntos de datos que recolectará en su análisis.
- Enfoque su análisis para no perderse en muchos puntos de datos que sean innecesarios, busque el equilibrio para tener la suficiente información que le permita a su empresa navegar por los desastres sin naufragar, pero evite ahogarse en muchos datos.
- Para recolectar los puntos de datos se puede guiar con la siguiente tabla, una vez realizado esto, tendrá una comprensión integral de su negocio, sus funciones clave y qué pasaría si esas funciones fueran interrumpidas.

Análisis de Impacto

- Puntos de datos del análisis de impacto

Punto de Datos	Descripción	Dependencias de TI
Financiero	Si esta función no ocurriera, ¿cuál sería el impacto financiero para el negocio? ¿Cuándo se sentiría o notaría el impacto financiero? ¿Sería único o recurrente? Describa el impacto financiero de que esta función no ocurra.	Descripción de cómo un retraso en esta función impactaría en los sistemas de TI y otros sistemas de soporte relacionados.
Atrasos	¿En qué punto el trabajo comenzaría a acumularse?	Descripción de cómo un retraso impactaría en los sistemas de TI y otros sistemas de soporte relacionados.
Recuperación	¿Qué tipos de recursos se necesitarían para apoyar la función? ¿Cuántos recursos se necesitarían y en qué plazo (teléfonos, escritorios, computadoras, impresoras, etc.)?	¿Qué recursos, habilidades y conocimientos serían necesarios para recuperar los sistemas de TI relacionados con esta función de negocio?
Tiempo de recuperación	¿Cuál es el tiempo mínimo necesario para recuperar esta función de negocio si se interrumpe? ¿Cuál es el tiempo máximo que esta función de negocio podría estar indisponible?	¿Cuánto tiempo tomaría recuperar, restaurar, reemplazar o reconfigurar los sistemas de TI relacionados con esta función de negocio?
Acuerdos de nivel de servicio (SLAs)	¿Existen acuerdos de nivel de servicio (SLAs) relacionados con esta función de negocio? ¿Cuáles son los requisitos y métricas asociados con estos SLAs? ¿Cómo se verán impactados los SLAs por la interrupción de esta función de negocio?	¿Cómo se verían afectados los niveles de servicio de TI por la interrupción o falta de disponibilidad de esta función de negocio? ¿Cómo impactan los SLAs externos en los sistemas de TI?
Tecnología	¿Qué hardware, software, aplicaciones u otros componentes tecnológicos son necesarios para apoyar esta función? ¿Qué sucedería si algunos de estos componentes no estuvieran disponibles? ¿Cuál sería el impacto? ¿Qué tan severamente se vería afectada la función de negocio?	¿Qué activos de TI se requieren para apoyar/mantener esta función de negocio?

Análisis de Impacto

- Puntos de datos del análisis de impacto

Punto de Datos	Descripción	Dependencias de TI
Función o proceso de negocio	Breve descripción de la función o proceso de negocio (usaremos “función” de aquí en adelante).	Descripción de los sistemas de TI primarios utilizados para esta función de negocio.
Dependencias	Descripción de las dependencias de esta función. ¿Cuáles son los puntos de entrada y salida de esta función? ¿Qué debe suceder o estar disponible para que esta función ocurra? ¿Qué entrada se recibe, ya sea de fuentes internas o externas, que se requiere para realizar esta función? ¿Cómo impactaría la interrupción de esta función a otras partes del negocio? ¿Cómo y cuándo ocurriría esta interrupción en otras funciones?	Descripción de los sistemas de TI que impactan o son impactados por esta función de negocio. ¿Hay alguna dependencia de TI interna o externa?
Dependencias de recursos	¿Esta función de negocio depende de alguna función clave de trabajo? Si es así, ¿cuál y en qué medida? ¿Esta función de negocio depende de algún recurso único? Si es así, ¿cuál y en qué medida (contratistas, equipo especial, etc.)?	Descripción de los sistemas informáticos/IT secundarios o de soporte requeridos para que ocurra esta función de negocio.
Dependencias del personal	¿Esta función depende de habilidades, conocimientos o experiencia especializados? ¿Cuáles son los roles o posiciones clave asociados con esta función? ¿Qué sucedería si las personas en estos roles no estuvieran disponibles?	Descripción de los roles clave, posiciones, conocimientos, experiencia y certificaciones necesarias para trabajar con este sistema o función de TI.
Perfil de impacto	¿Cuándo ocurre esta función? ¿Es de forma horaria, diaria, trimestral o estacional? ¿Hay un momento específico del día/semana/año en que esta función esté más en riesgo? ¿Hay un momento específico en el que el negocio esté más en riesgo si esta función no ocurre (p. ej., época de impuestos, períodos de nómina, inventario de fin de año)?	Descripción de la línea de tiempo crítica relacionada con esta función/proceso y sistemas de TI relacionados, si los hay.
Operacional	Si esta función no ocurriera, ¿cuándo y cómo impactaría al negocio? ¿El impacto sería único o recurrente? Describa el impacto operativo de que esta función no ocurra.	Descripción del impacto en TI si esta función de negocio no ocurre. Descripción del impacto en las operaciones si esta función de negocio no ocurre.

Análisis de Impacto

- Puntos de datos del análisis de impacto

Punto de Datos	Descripción	Dependencias de TI
Escrítorios, laptops y estaciones de trabajo	¿Esta función de negocio requiere el uso de equipos informáticos de "usuario"?	¿Cuál es la configuración de datos requerida para el equipo informático?
Servidores, redes e Internet	¿Esta función de negocio requiere el uso de equipos informáticos de back-end? ¿Requiere conexión a la red? ¿Necesita acceso a o uso de Internet u otras comunicaciones?	¿Cuál es la configuración de datos requerida para los servidores y equipos de infraestructura?
Procedimientos alternativos	¿Existen procedimientos alternativos manuales que hayan sido desarrollados y probados? ¿Permitirían estos la realización de la función de negocio en caso de fallos de TI o sistemas? ¿Cuánto tiempo podrían operar estas funciones en modo manual o alternativo? Si no se han desarrollado, ¿parece factible desarrollar dichos procedimientos?	¿Existen procedimientos alternativos relacionados con TI para esta función de negocio? Si es así, ¿cuáles son y cómo podrían implementarse?
Trabajo remoto	¿Puede realizarse esta función de negocio de manera remota, ya sea desde otra ubicación de la empresa o por empleados trabajando desde casa u otras ubicaciones fuera de la oficina?	¿Puede realizarse esta función de negocio de manera remota desde la perspectiva de TI? Si es así, ¿qué se necesitaría para habilitar el acceso remoto o la capacidad de realizar esta función de negocio de manera remota?
Desplazamiento de carga de trabajo	¿Es posible trasladar esta función de negocio a otra unidad de negocio que podría no verse afectada por la interrupción? Si es así, ¿qué procesos y procedimientos están en marcha o se necesitan para habilitar esa función?	¿Existen otros sistemas o recursos de TI que podrían asumir la carga en caso de una interrupción grave?
Registros de negocio/datos	¿Dónde se almacenan o archivan los registros de negocio relacionados con esta función? ¿Están actualmente respaldados? Si es así, ¿cómo, con qué frecuencia y dónde?	¿Cómo y dónde se almacenan los respaldos? Segundo los datos proporcionados, ¿es óptima la estrategia actual de respaldo en función de los riesgos e impactos?

Análisis de Impacto

- Puntos de datos del análisis de impacto

Punto de Datos	Descripción	Dependencias de TI
Informes	¿Existen requisitos legales o regulatorios de informes para esta función de negocio? Si es así, ¿cuál es el impacto de una interrupción de esta función en los requisitos de informes? ¿Existen procedimientos alternativos de informes o podrían desarrollarse e implementarse?	¿Existen otras formas en las que los datos de informes podrían generarse, almacenarse o informarse si las funciones clave del negocio o los sistemas estuvieran deshabilitados?
Experiencia en interrupciones de negocio	¿Alguna vez se ha interrumpido esta función de negocio antes? Si es así, ¿cuál fue la interrupción y cuál fue el resultado? ¿Qué se aprendió de este evento que se pueda incorporar en este esfuerzo de planificación?	¿Ha experimentado TI alguna vez la interrupción de esta función de negocio en el pasado? Si es así, ¿cuál fue la naturaleza y duración de la interrupción? ¿Cómo se abordó y qué se aprendió del evento?
Impacto competitivo	¿Cuál sería el impacto competitivo para la empresa si esta función de negocio se interrumpiera? ¿Cuál sería el impacto, cuándo ocurriría y cuándo se produciría la posible pérdida de clientes o proveedores?	¿Qué otros problemas podrían ser relevantes al discutir esta función de negocio en particular? ¿Existen otros problemas relacionados con TI que deberían incluirse o discutirse?

Análisis de Impacto

• Impacto en TI

- Como se dará cuenta en la tabla anterior, las funciones de TI pueden correlacionarse a las funciones de negocio y procesos en cada paso.
- Al obtener todos estos datos necesitará estar continuamente analizando y correlacionando las funciones de TI que afectan o se ven afectadas. Los usuarios y SMEs le podrán apoyar con este análisis, pero no podrán determinar todas las relaciones necesarias.
 - Por ejemplo, el SME de Marketing y Ventas podrá indicarle que el CRM es vital para sus operaciones, pero no sabrá que interfaces o sobre qué hardware está funcionando el mismo o si es necesario pagar licencias, certificados, etc.
- Se recomienda que mapee las funciones empresariales con las funciones, servicios y recursos de TI, para esto puede utilizar diagramas de arquitectura empresarial.
 - En el libro Enterprise Architecture As Strategy de Jeanne W. Ross se habla sobre este tema.

Análisis de Impacto

- Elaboración del informe de análisis de impacto
 - Para realizar este informe debe utilizar formatos de la empresa y deberá incluir al menos: Funciones empresariales, criticidad y análisis de impacto y MTD (Maximum Tolerable Downtime)
 - Puede incluir las tablas realizadas acompañadas de textos o anexos según lo considere necesario
 - Realice un borrador del documento y pida a los SMEs y equipo general de BC/DR que lo revise y le dé retroalimentación.
 - Recuerde incluir los siguientes elementos:

Análisis de Impacto

- Recuerde incluir los siguientes elementos:

- Procesos y funciones clave
- Interdependencia de procesos y recursos
- Dependencias de TI
- Criticidad e impacto en las operaciones
- Información sobre acumulación de trabajo
- Roles clave, posiciones, habilidades, conocimientos y experiencia necesarios
- Requisitos de tiempo de recuperación
- Recursos de recuperación
- Acuerdos de nivel de servicio (SLAs)

- Tecnología (tecnología de TI y no TI)
- Impactos financieros, legales, operativos, de mercado y en el personal
- Procedimientos alternativos
- Trabajo remoto y redistribución de la carga de trabajo
- Datos de negocio y registros clave
- Informes
- Impacto competitivo
- Impacto en inversores/mercado
- Impacto en la percepción del cliente
- Otros (datos específicos del negocio no incluidos anteriormente)

ANÁLISIS DE RIESGOS

ING. FREDY BUSTAMANTE

ANÁLISIS DE RIESGOS

- El análisis de riesgos se debe realizar para poder tomar en cuenta la forma única en que su empresa manejará las posibles amenazas y su riesgo asociado tomando en cuenta factores como localización, tipo de industria, cultura organizacional, estructura organizacional, objetivos estratégicos, entre otros.
- El análisis de riesgos en TI puede respaldar una variedad de actividades de gestión de riesgos en toda la empresa que incluyen:
 - Desarrollo de una arquitectura de infraestructura de TI
 - Desarrollo de una arquitectura de seguridad de TI
 - Definición de requisitos de interfaz para funciones de TI
 - Implementación y mantenimiento de soluciones de seguridad
- No podemos crear un plan de BC/DR hasta que sepamos las amenazas específicas que enfrenta la empresa.

ANÁLISIS DE RIESGOS

- Una de las objeciones comunes hacia la planificación de BC/DR es que hay **demasiadas cosas que pueden salir mal** que no se puede planificar para todas ellas.
- Esto es parcialmente correcto pues es cierto que hay demasiadas cosas que pueden salir mal pero un número reducido de ellas tienen una **opción real de suceder**.
- Se debe crear el plan para lo que tiene una opción real de suceder.
- Esto sin dejar de revisar aquello que no parece tener una opción real de suceder pero que el **impacto** puede ser muy grande.

ANÁLISIS DE RIESGOS

- Por ejemplo, todos los días salimos a la calle en nuestro vehículo, lo que significa tener riesgo de un accidente de tránsito, la única forma de bajar a 0 la posibilidad de que nos ocurra es no salir, pero esto no es viable por lo que tomamos acciones para mitigarlo como tomar clases de manejo y obedecer las leyes de tránsito, además, podemos adquirir un seguro de automóvil para transferir el riesgo de costos altos por reparaciones u hospitalizaciones.
- Aun así, seguimos estando en riesgo de sufrir un accidente y tener costos asociados a ello, pero estamos dispuestos a correr dicho riesgo.
- Esto es un ejemplo de **evitar, reducir, aceptar y transferir el riesgo**.

GESTIÓN DEL RIESGO

- La gestión de riesgos debe ajustarse a las limitaciones financieras de la empresa para que sea viable, en otras palabras, debe ser **razonable**.
- Es un tema **general** que analiza cómo se gestionan todos los riesgos en **toda la empresa**.
- Tres aspectos clave en el proceso de gestión de riesgos:
 - Análisis de riesgos: ¿cómo se realizará la evaluación?
 - Enfoque de evaluación: ¿optará por un enfoque cuantitativo, cualitativo o semicualitativo?
 - Enfoque de análisis: ¿Quiere analizar su riesgo desde una orientación de amenaza, una orientación activo-impacto o una orientación de vulnerabilidad? Puede utilizar cualquiera, pero mantener un método consistente es importante para realizar un buen plan.

GESTIÓN DEL RIESGO

- Cuatro pasos básicos en la gestión de riesgos:
 - Evaluación de amenazas
 - Evaluación de vulnerabilidades
 - Evaluación de impacto
 - Desarrollo de estrategias de mitigación de riesgos
- Nos centraremos en las primeras dos, pero no podemos dejar de mencionar la gestión del riesgo cuando hablamos del análisis de riesgos.

GESTIÓN DEL RIESGO

- Certificaciones: si es de su interés personal o para su empresa existen diferentes certificaciones para la gestión del riesgo como:
- **Certified in Risk and Information Systems Control from ISACA (ISACA CRISC).**
- Además, puede encontrar otras certificaciones no enfocadas en IT.

GESTIÓN DEL RIESGO

- Proceso de gestión del riesgo: Incluye evaluar el potencial y también analizar las compensaciones (trade-offs) o el costo de oportunidad.
 - Trade-offs: se refiere a que gastar en la mitigación de riesgos significa quitar presupuesto de otras actividades.
- Dos conceptos útiles son **magnitud** y **frecuencia**:
 - Por ejemplo, el impacto de un terremoto tendría una alta magnitud, sin embargo, en muchos lugares incluso algunos que son propensos a estos, la frecuencia es relativamente baja.

GESTIÓN DEL RIESGO

- Cada amenaza y posible estrategia de mitigación tienen un costo y un beneficio
 - Analizaremos los costos en cifras en alguna moneda, en vidas humanas y operaciones comerciales.
 - También existe el beneficio de la mitigación, que idealmente debería compensar con creces el costo del evento.
- Por ejemplo, supongamos que el costo de instalar un sistema de extinción de incendios en un edificio pueda ser de \$15,000. Comparando este costo contra (1) daños al edificio, (2) daños a los equipos y mobiliario, (3) daños a los equipos de TI y (4) lesiones y vidas humanas, dichos \$15,000 parecen una inversión excelente pues supondrá evitar un costo mucho mayor en caso de un incendio.

EVALUACIÓN DE AMENAZAS

- Hemos utilizado las palabras **riesgo** y **amenaza** en varias ocasiones, casi indistintamente. Esto, en un contexto general, es correcto, pero no del todo en un contexto de administración del riesgo.
- **Riesgo del negocio:** Proceso de **identificar, controlar y eliminar o minimizar** eventos inciertos que puedan afectar al negocio. Incluye análisis de riesgos, análisis de costos y beneficios, selección, implementación y prueba de estrategias seleccionadas y mantenimiento de estas a largo plazo.

EVALUACIÓN DE VULNERABILIDADES

- La evaluación de vulnerabilidades **analiza que tan vulnerable, susceptible y expuesto está un negocio o sistema a una amenaza particular.**
 - Debe incluir una evaluación de **qué tan vulnerable** es un sistema en particular a una amenaza, así como la **probabilidad de que esa amenaza ocurra**.
 - La parte de la probabilidad de ocurrencia puede ser una evaluación aparte, considero que es mejor realizarse en conjunto dado que están muy relacionadas pues no es lo mismo evaluar una vulnerabilidad a una amenaza con mucha probabilidad de ocurrencia que una vulnerabilidad a una amenaza con muy poca probabilidad.

EVALUACIÓN DEL IMPACTO

- La evaluación del impacto analiza **que tan grande o pequeño será el impacto de la ocurrencia de una amenaza** en el negocio o sistema.
- Por ejemplo, un terremoto tiene un enorme impacto sobre empresas que estén localizadas cerca del epicentro, tendrá menor impacto sobre aquellas que están más lejos del mismo sin olvidar la evaluación del impacto indirecto como proveedores clave que se encuentren cerca del epicentro o el colapso de infraestructura de comunicación, transporte y otros servicios.

DESARROLLO DE ESTRATEGIAS DE MITIGACIÓN DE RIESGOS

- Es el **proceso de decidir cuáles riesgos deberíamos abordar y de qué manera**.
- Los insumos para este proceso son el análisis de evaluación de riesgos o los informes que delinean qué amenazas existen, qué tan vulnerables son sus sistemas y qué probabilidad hay de que ocurra la amenaza, así como el impacto de estos en el negocio.
- Recordemos que podemos reducir, evitar, aceptar o transferir riesgos. En muchos casos, es mucho más costoso evitar completamente un riesgo que reducir su impacto.
- Por ejemplo, para evitar en su totalidad un incendio, podemos construir un edificio con material no inflamable, así como comprar todo el mobiliario, cableado, etcétera, con esta misma característica. Pero tendríamos costos muy altos, para ciertas empresas en ciertas ubicaciones esto puede ser necesario, pero no para la mayoría.
- No existe una solución perfecta, **su trabajo en esta fase es tomar decisiones inteligentes y hacer concesiones** (trade-offs) a la luz de los datos recopilados.

PERSONAS, PROCESOS, TECNOLOGÍA E INFRAESTRUCTURA EN LA GESTIÓN DE RIESGOS

- Ya habíamos hablado sobre personas, procesos y tecnología, en el ámbito de la planificación de BC/DR debemos agregar una cuarta categoría: **infraestructura**
- Claro que infraestructura está incluida en tecnología, pero no debemos olvidar los edificios, sus instalaciones, servicios públicos, transporte público, calles, etcétera. Toda vez sean relevantes para el negocio (de forma directa o indirecta por medio de clientes y proveedores)
- Por esta razón se recomienda separar infraestructura como una categoría adicional y no dejarla en tecnología.

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

- En TI tenemos **riesgos únicos** que no existen en ninguna otra parte de la empresa
- Estos incluyen el desarrollo de estándares y procesos técnicos, físicos, administrativos y de gestión para proteger la **confidencialidad, integridad y disponibilidad (CIA)** de la información de toda la empresa.
- Se debe **balancear** las necesidades tecnológicas de la empresa (especialmente la disponibilidad) con las capacidades y costos tecnológicos actuales.
- Todo riesgo se puede mitigar con grandes gastos, **el objetivo de la gestión de riesgos es reducirlos de la manera más rentable posible.**

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

- Parte de su trabajo como líder de TI es asegurarse que la empresa entienda el riesgo específico de TI y le respalte en los esfuerzos por mitigarlos.
- Por ejemplo, el departamento de finanzas puede entender ciertos riesgos relacionados con aceptar tarjeta de crédito en un punto de venta, pero no entenderá el riesgo relacionado a utilizar algún nivel o tipo de encripción, no tener actualizadas licencias para su firewall o SO del servidor, etc.
- Información adicional:
 - National Institute of Standards and Technology Resources (NIST)
 - <http://csrc.nist.gov/publications/index.html>

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

- El mayor riesgo al que nos enfrentamos está relacionado con la seguridad de la información.
- El objetivo de la gestión del riesgo de TI es mantener los siguientes 3 elementos relacionados con CIA:
 - Asegurar completamente los sistemas de TI
 - Permitir a la gerencia tomar decisiones bien informadas con respecto a la compra e implementación de sistemas de TI
 - Permitir a la gerencia autorizar los sistemas de TI sobre la base de la documentación de respaldo que resulte de las actividades de gestión de riesgos de TI

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

Fases del desarrollo o adquisición de software	Descripción	Apoyo de las actividades de gestión del riesgo
1. Iniciación	Se expresa la necesidad de un sistema, se documenta el propósito y alcance de este.	Los riesgos identificados se utilizan para respaldar el desarrollo de los requisitos del sistema.
2. Desarrollo o adquisición	El sistema se diseña, compra, desarrolla o de alguna forma se construye.	Los riesgos identificados durante esta fase pueden ser utilizados para soportar el análisis de seguridad del software lo que puede llevarnos a concesiones en la arquitectura o diseño de este.
3. Implementación	Las características de seguridad del sistema deben configurarse, habilitarse, probarse y verificararse	El proceso de gestión de riesgos respalda la evaluación de la implementación del sistema frente a sus requisitos y dentro de su entorno operativo. Las decisiones sobre los riesgos identificados deben tomarse antes de la operación del sistema.

GESTIÓN DEL RIESGO ESPECÍFICO DE TI

Fases del desarrollo o adquisición de software	Descripción	Apoyo de las actividades de gestión del riesgo
4. Operación / mantenimiento	<p>El sistema está funcionando. Por lo general, el sistema será modificado de forma continua mediante la adquisición de nuevo hardware y software y debido a cambios en los procesos, políticas y procedimientos de la empresa</p>	<p>Las actividades de gestión del riesgo se reautorizan o reacreditan periódicamente o cuando existe un cambio importante en un sistema (como agregar nuevas interfaces)</p>
5. Desecho	<p>Esta fase puede implicar la disposición de información, hardware y software. Puede incluir mover, archivar, descartar o destruir la información y el hardware.</p>	<p>Se realizan actividades de gestión del riesgo para los componentes del sistema que se eliminarán o reemplazarán para garantizar que el hardware y software se eliminan adecuadamente, que los datos residuales se manejen adecuadamente y que la migración del sistema se realice de manera segura y sistemática.</p>

COMPONENTES DE LA EVALUACIÓN DEL RIESGO

- **Amenazas y fuentes de amenazas** son términos que podemos utilizar sin distinguir alguna diferencia, pero en la evaluación del riesgo es importante realizar la distinción entre la amenaza y su fuente.
- Por ejemplo, un corte de energía es una amenaza que nos afecta a todos, la causa del corte de energía (fuente de la amenaza) podría ser un accidente en una subestación, falta de agua en una represa o un accidente en un poste cercano, tomar en cuenta las posibles causas nos ayuda a evaluar de mejor forma el riesgo determinando de mejor forma su probabilidad e impacto.

COMPONENTES DE LA EVALUACIÓN DEL RIESGO

- En lugar de realizar un análisis exhaustivo para cada amenaza que encontremos, se debe primero realizar la evaluación integral de amenazas para luego decidir en dónde enfocaremos nuestros esfuerzos en la evaluación de vulnerabilidades, en lugar de esforzarnos desde el inicio y desperdiciar recursos en una amenaza en específico.

MÉTODOS DE RECOLLECTACIÓN DE INFORMACIÓN

- Métodos más utilizados:
 - Cuestionarios: Permiten obtener datos específicos y estandarizados.
 - Entrevistas: Permiten descubrir información necesaria por medio de un diálogo.
 - Revisión de documentos: Revisión de la documentación de la empresa (manuales, procesos, etc.) nos puede ayudar en identificar amenazas, sus fuentes y vulnerabilidades.
 - Investigación: Investigar sobre diferentes amenazas, estadísticas asociadas a estas, procesos y recomendaciones durante un desastre, datos públicos de policía, bomberos, hospitales u otras organizaciones.
- Aunque se verá tentado a buscar la mayor cantidad de datos, recuerde que debe establecer un límite para no verse inmerso en una gran cantidad de datos que después no pueda analizar de forma correcta.

LISTA DE VERIFICACIÓN DE AMENAZAS

- Amenazas naturales/ambientales
 - Inundación
 - Tormenta invernal severa
 - Tormenta eléctrica
 - Sequía
 - Terremoto
 - Tornado
 - Huracán
 - Tsunami
 - Volcán
 - Pandemias
- Amenazas causadas por humanos
 - Incendio, incendio provocado
 - Robo, sabotaje, vandalismo
 - Disputas laborales
 - Violencia en el trabajo
 - Terrorismo
 - Peligros químicos y biológicos
 - Guerra, guerra civil
- Amenazas a la infraestructura
 - Fallas en edificios
 - Equipos no informáticos / sistemas
 - Calefacción / refrigeración, energía
- Interrupción de transporte público
- Falta de combustible
- Contaminación de comida o agua
- Cambios legales
- Amenazas específicas de TI
 - Amenazas cibernéticas (amenazas a CIA)
 - Fallos en sistemas y hardware
 - Fallos en equipos de línea de producción
 - Pérdida de datos

EVALUACIÓN DEL RIESGO

- De esta fase se obtiene un documento listando todas las amenazas potenciales y sus fuentes que se han analizado para la empresa.
- Solo se deberían eliminar aquellas amenazas que claramente no aplican para su empresa, el resto se utilizará como entrada para la fase de evaluación de vulnerabilidades.
- Ejemplo: esta matriz es solo una guía y puede ser modificada según las necesidades específicas:

No.	Amenaza	Fuente	Vulnerabilidad	Probabilidad	Controles existentes	Impacto	Calificación
1	Fuego	Interna	%	%	Extintores, ...	%	%
2	Fuego	Externa	%	%	Extintores, ...	%	%
3	Inundación	Interna	%	%	Sensores de humedad	%	%

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Revisaremos algunas metodologías de evaluación de amenazas que nos pueden servir para esta fase.
- Existen dos enfoques esenciales:
 - Cuantitativo
 - Cualitativo
- Recuerde seleccionar uno de los dos enfoques y quedarse con este.

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Enfoque Cuantitativo
 - Se busca utilizar números concretos para representar amenazas, vulnerabilidades e impactos (\$, %).
 - Por ejemplo, “el servidor cuesta \$1,500 más que una workstation” es una declaración cuantitativa, mientras “el servidor es más caro que una workstation” sería una declaración cualitativa “más” no es específico ni medible.
- Veamos el siguiente ejemplo

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Amenaza: Corte de energía
- Fuente: Rayo
- Probabilidad de ocurrencia: datos recabados indican que ocurre 1 vez cada 4 años por lo que la probabilidad será **0.25 anual**. No solo tomamos en cuenta rayos que caigan directamente sobre el edificio sino aquellos que caigan en el área y que puedan causar un corte de energía.
- Vulnerabilidad: Si cada vez que cae un rayo en el área tenemos un corte de energía la vulnerabilidad a esta amenaza será de 1 (100%) anual.
- Valor de riesgo: Probabilidad de ocurrencia x Vulnerabilidad = $0.25 \times 1 = 0.25$.
- Impacto: Asumamos que cada vez que esto ocurre la empresa eléctrica se tarda en llegar y reparar la falla por lo que el tiempo entre la ocurrencia y la reparación es de 2 días. ¿Cuánto nos cuesta estar sin energía 2 días?
 - Pérdidas en ventas: Q18,000 diarios, Q36,000 por ocurrencia.
 - Costos fijos: Q4,200 diarios, Q8,400 por ocurrencia.
 - Daño por mala reputación: arbitrariamente se asignó Q2,000 diarios, Q4,000 por ocurrencia. Este dato puede ser muy subjetivo (cuantitativo por naturaleza), si su empresa puede realizar un cálculo objetivo utilícelo. Puede utilizar el mismo costo diario para cualquier amenaza para ser consistente, pero recuerde que no es lo mismo estar cerrado por 2 días que 1 mes.
 - Impacto total: $Q36,000 + Q8,400 + Q4,000 = Q48,400$
- **Valor total del Riesgo: $Q48,400 * 0.25 = Q12,100$ anual.**
- Si sabe que el costo del riesgo de un corte de energía eléctrica debido a un rayo es de Q12,100 al año, es más fácil evaluar las posibles inversiones para mitigarlo, como un generador de energía que cueste Q50,000, equipo de protección contra rayos por Q5,000, seguro que cubra parte de la pérdida asociada por Q3,000 anuales, etc.
 - Para evaluar inversiones recuerde que, por ejemplo, el generador de energía tiene una inversión inicial, costo de operación y tiempo de vida que puede ser mucho mayor a 1 año. Tampoco olvide que puede tener beneficios adicionales que le generen otros ahorros o ingresos.

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Enfoque Cualitativo

- Se busca definir las amenazas, vulnerabilidades e impactos relativos utilizando lenguaje, por ejemplo, “alto”, “medio” y “bajo”.
- Se debe utilizar un sistema cualitativo con una escala que le permita ser consistente.
- Por ejemplo:

Numérico	Frecuencia	Impacto
6	Constante	Extremadamente alto
5	Muy frecuente	Muy alto
4	Frecuente	Alto
3	Poco frecuente	Bajo
2	Muy poco frecuente	Muy bajo
1	Nunca	Extremadamente bajo

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Otro ejemplo:

Nivel de probabilidad	Descripción
Alto	La fuente de la amenaza está altamente motivada y es suficientemente capaz y los controles para evitar que se ejerza la vulnerabilidad son ineficaces
Medio	La fuente de la amenaza está motivada y es capaz, pero existen controles que pueden impedir el ejercicio exitoso de la vulnerabilidad
Bajo	La fuente de la amenaza carece de motivación o capacidad o existen controles para impedir, o al menos impedir significativamente que se ejerza la vulnerabilidad

- Tabla realizada por NIST (National Institute of Standards and Technology) específicamente para vulnerabilidades asociadas a la seguridad informática.
- Trate de utilizar valores pares como en el primer ejemplo, para obligarse a realizar una elección y no tender a ir al medio.
- Al utilizar el enfoque cualitativo debe asegurarse que todas las personas involucradas tienen un claro entendimiento y están de acuerdo con las escalas; no todos le damos el mismo significado a las palabras.

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Veamos el ejemplo anterior con un enfoque cualitativo:
- Amenaza: Corte de energía
- Fuente: Rayo
- Probabilidad de ocurrencia: Ocurre 1 vez cada 4 años, le asignaremos un valor de 3, es decir, “Poco frecuente”.
- Vulnerabilidad: Si cada vez que cae un rayo en el área tenemos un corte de energía le asignaremos un valor de 6, es decir, “extremadamente alta”.
- Impacto: Asumamos que cada vez que esto ocurre la empresa eléctrica se tarda en llegar y reparar la falla por lo que el tiempo entre la ocurrencia y la reparación es de 2 días. Supongamos que esto es un impacto “bajo” (3) pues no nos pone en mucha desventaja frente a nuestros competidores, clientes y proveedores por lo que son pérdidas que podemos soportar.
- **Valor total del riesgo:** promedio del valor de Probabilidad de ocurrencia + Vulnerabilidad + Impacto = $(3 + 6 + 3)/3 = 4$, según nuestra tabla: Alto

METODOLOGÍA DE EVALUACIÓN DE AMENAZAS

- Podemos buscar mayor detalle, por ejemplo, en Impacto podríamos determinar diferentes valores para diferentes problemas, no es lo mismo que una PC ya no funcione después de un apagón a que sea el servidor de base de datos, quedará en usted la decisión de qué tanto detallarlo y qué escala utilizar (6 elementos, calificación de 1 a 100, etcétera)
- Puede indagar más al respecto en: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- En el apéndice G de este documento puede encontrar diferentes tablas para la probabilidad de ocurrencia, incluso utilizando diferentes escalas dependiendo si la amenaza es intencional o no.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

EVALUACIÓN DE VULNERABILIDADES

- Una vulnerabilidad se define como la debilidad, susceptibilidad o exposición a peligros o amenazas.
- Estas pueden ser explotadas intencionalmente o activarse involuntariamente.
- El resultado de la evaluación de amenazas se convierte en el insumo para la evaluación de vulnerabilidades.
- Esta evaluación se puede dividir en probabilidad de ocurrencia y vulnerabilidad basada en la probabilidad de ocurrencia.
 - La ventaja de separarlos es tener visibilidad de aquellas amenazas que son poco probables pero que la empresa es muy vulnerable a ellas, como a los terremotos, y hacer un análisis especial para estas.
- Para realizar esta evaluación se recomienda dividir las amenazas para que diferentes equipos puedan encargarse de esta evaluación, queda a su criterio la forma que pueda funcionar mejor según el caso específico. Por ejemplo,
 - Clasificar las amenazas utilizando la estructura de Personas, Procesos, Tecnología e Infraestructura.
 - Clasificarlas como Externas e Internas.
 - O por área de la empresa como IT, Instalaciones, Finanzas, RRHH, Operaciones, etc.
- La evaluación no será exclusiva del grupo encargado, por el contrario, tendrán que trabajar en conjunto con personal de toda la empresa.
- Asegúrese de establecer metas, fechas de entrega y hacer revisiones cruzadas entre equipos de forma que estén seguros de seguir un estándar.

EVALUACIÓN DE VULNERABILIDADES

- Revisemos nuevamente la estructura Personas, Procesos, Tecnología e Infraestructura desde el punto de vista de una evaluación de vulnerabilidades.
- Personas: debemos evaluar qué tan vulnerables son las personas a las fuentes de amenazas, por ejemplo, phishing o ingeniería social. No solo evaluar pensando en las personas que trabajan en la empresa sino la comunidad que nos rodea.
- Procesos: ¿Qué tan vulnerables son nuestros procesos (de negocio y de TI) a las fuentes de amenazas identificadas? Por ejemplo:
 - El proceso de toma de pedidos que se ejecuta en un área con 10 computadoras, 10 teléfonos y un sistema que lo facilita, ¿qué tan vulnerable es a una fuente de amenaza que no permita utilizar este espacio?
 - A la vez que estemos evaluando esta vulnerabilidad seguramente estemos pensando en formas de mitigar el riesgo.
 - Entre más estandarizados y documentados tengamos nuestros procesos, más fácil será el poder evaluarlos y crear estrategias de mitigación.

EVALUACIÓN DE VULNERABILIDADES

- **Tecnología:** Claro está que la tecnología es vulnerable a muchas fuentes de amenazas, nosotros como Ing. En Sistemas podemos pensar rápidamente en los más comunes. ¿Qué tan vulnerables estamos a un ataque interno o externo? ¿Qué tan vulnerable es nuestro servidor web?
- No asuma que sus procesos estándares ya han abordado las vulnerabilidades, tampoco asuma que sus planes de emergencia actuales serán adecuados para todas las fuentes de amenazas.
- Por el contrario, asuma que no tiene nada al respecto o trate de verlo desde “fuera de la caja” para realizar una evaluación detallada.
 - Por ejemplo, pudo haber tomado en cuenta una inundación pensando en algún río cercano o por alcantarillado con problemas, pero no por una tubería defectuosa dentro del edificio y esta última fuente hace que se deba tratar por separado.
 - Por último, recuerde incluir la tecnología que no esté a su cargo pero que puede de igual forma ser vulnerable como TV por cable, sistema de alarmas y cámaras, etc.

EVALUACIÓN DE VULNERABILIDADES

- Infraestructura: Por supuesto que la infraestructura es vulnerable a ciertas fuentes de amenazas y no a otras; una inundación solo si estamos a nivel de un río o lago, inundación interna, etc.
- Será el experto, como un Ing. Civil o Arquitecto, quien pueda apoyarnos con esta evaluación.
- No olvidemos evaluar la infraestructura externa a la empresa, como carreteras, instalaciones de las empresas que nos brindan servicios (telecomunicaciones, energía, etc.), etc.

EVALUACIÓN DE VULNERABILIDADES

- Una evaluación de vulnerabilidades puede ser cuantitativa, cualitativa o semicuantitativa.
- Muchas veces se utiliza la semicuantitativa con tablas como las que ya revisamos con anterioridad.
- Al igual que en la evaluación de amenazas y sus fuentes, debemos recabar información por medio de cuestionarios, entrevistas, etc.
- Por ejemplo, fuentes de amenaza de daño por agua a los sistemas informáticos:

Descripción	Alto	Medio	Bajo
1. Si la tubería del edificio se dañara y dejara escapar gran cantidad de agua, ¿qué tan vulnerables son nuestros sistemas informáticos?			
2. Si en el edificio hubiera un incendio, ¿qué tan vulnerables son nuestros sistemas informáticos al agua que el sistema de supresión de incendios utilizará para apagarlo?			
3. Si el edificio se viera afectado por ingreso de agua por fuertes lluvias, ¿Qué tan vulnerable son nuestros sistemas informáticos?			

EVALUACIÓN DE VULNERABILIDADES

- Con esta tabla evaluamos qué tan vulnerables están los sistemas informáticos a estas fuentes de amenaza, ahora se debe determinar la probabilidad de ocurrencia para obtener un valor de riesgo (subtotal pues aún falta el impacto) utilizando los datos cuantitativos, cualitativos o semicuantitativos.
- Finalmente se deberá analizar todos los datos recabados y ajustarlos de ser necesario para que sean consistentes.
- Al finalizar este proceso obtendremos un listado de:
 1. Todas las fuentes de amenazas potenciales.
 2. La probabilidad de ocurrencia de estas.
 3. Vulnerabilidad de su empresa y sistemas informáticos a estas.
 4. Valor de riesgo provisional.
- El documento puede ser un entregable que pueda dar una mejor idea a la alta gerencia sobre avances e importancia de este proyecto. Si fuera necesario, debería obtener una aprobación formal de este.