INTRODUCCIÓN A LA CONTINUIDAD DEL NEGOCIO

ING. FREDY BUSTAMANTE

INTRODUCCIÓN

- Tornados, inundaciones, terremotos… La mayoría de nosotros temenos, 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 amenzas 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 "Recuparación 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 inversion.

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 equilibro 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 equilibro 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 explosión
  - 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.

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 respalde 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 verificarse	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	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	Las actividades de gestión del riesgo se reautorizan o reacreditan periódicamente o cuando existe un cambio importante en un sistema (como agregar nuevas interfaces)
5. Desecho	Esta fase puede implicar la disposición de información, hardware y software. Puede incluir mover, archivar, descartar o destruir la información y el hardware.	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 eliminen adecuadamente, que los datos residuales se manejen adecuadamente y que la migración del sistema se realice de manera segura y sistemática.

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 RECOPILACIÓN 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 x 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 (cualitativo 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 utilizara 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.

Análisis de Impacto

ING. FREDY BUSTAMANTE

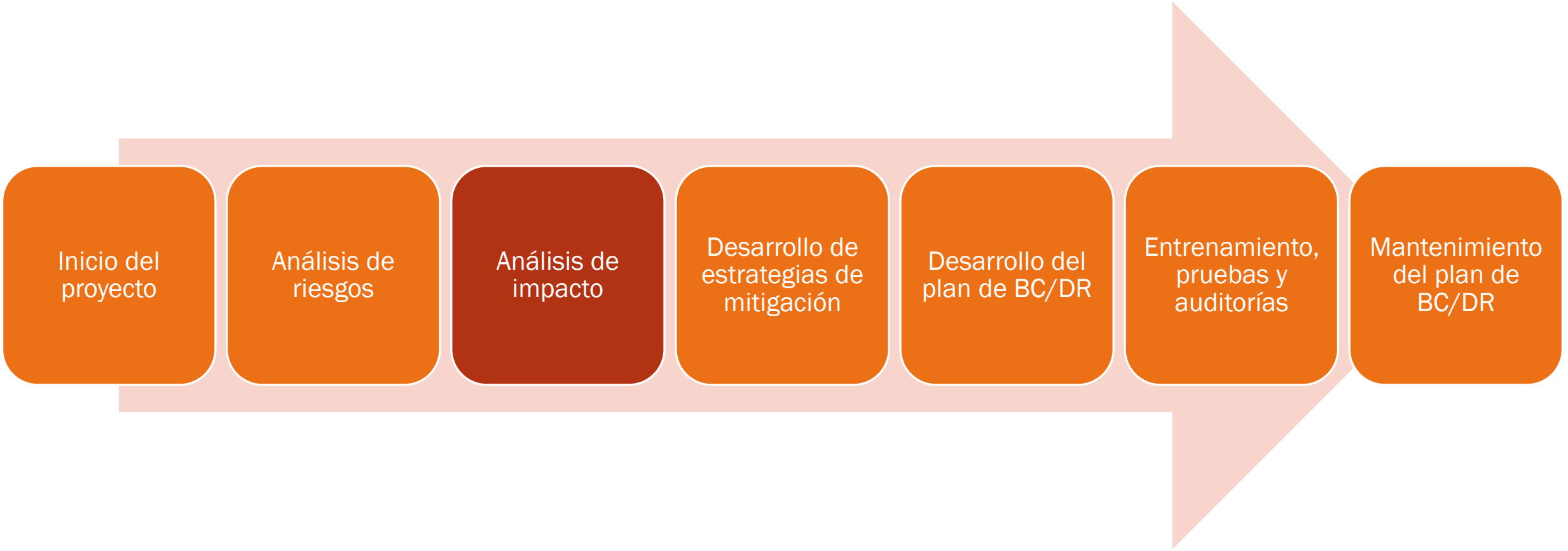
Análisis de Impacto

- 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

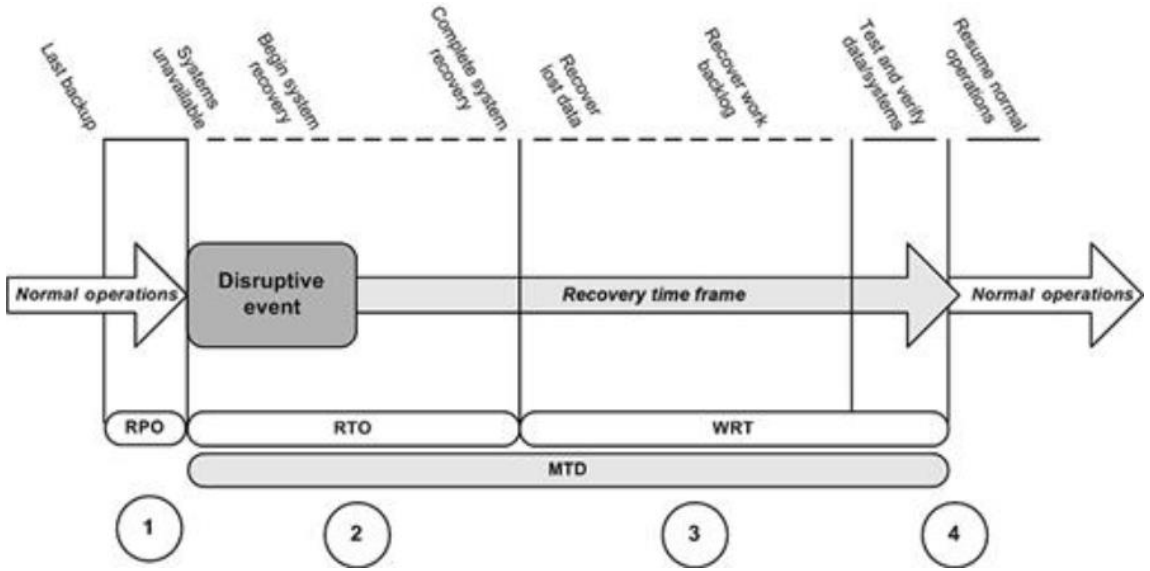
- Requisitos de tiempo de recuperación
  - Relacionado a la criticidad del impacto están los requisitos de tiempo de recuperación.
- Veamos la definición de algunos términos que nos servirán para entender mejor:
- Tiempo de inactividad máximo tolerable (Maximum tolerable downtime, MTD)
  - Como se indica 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

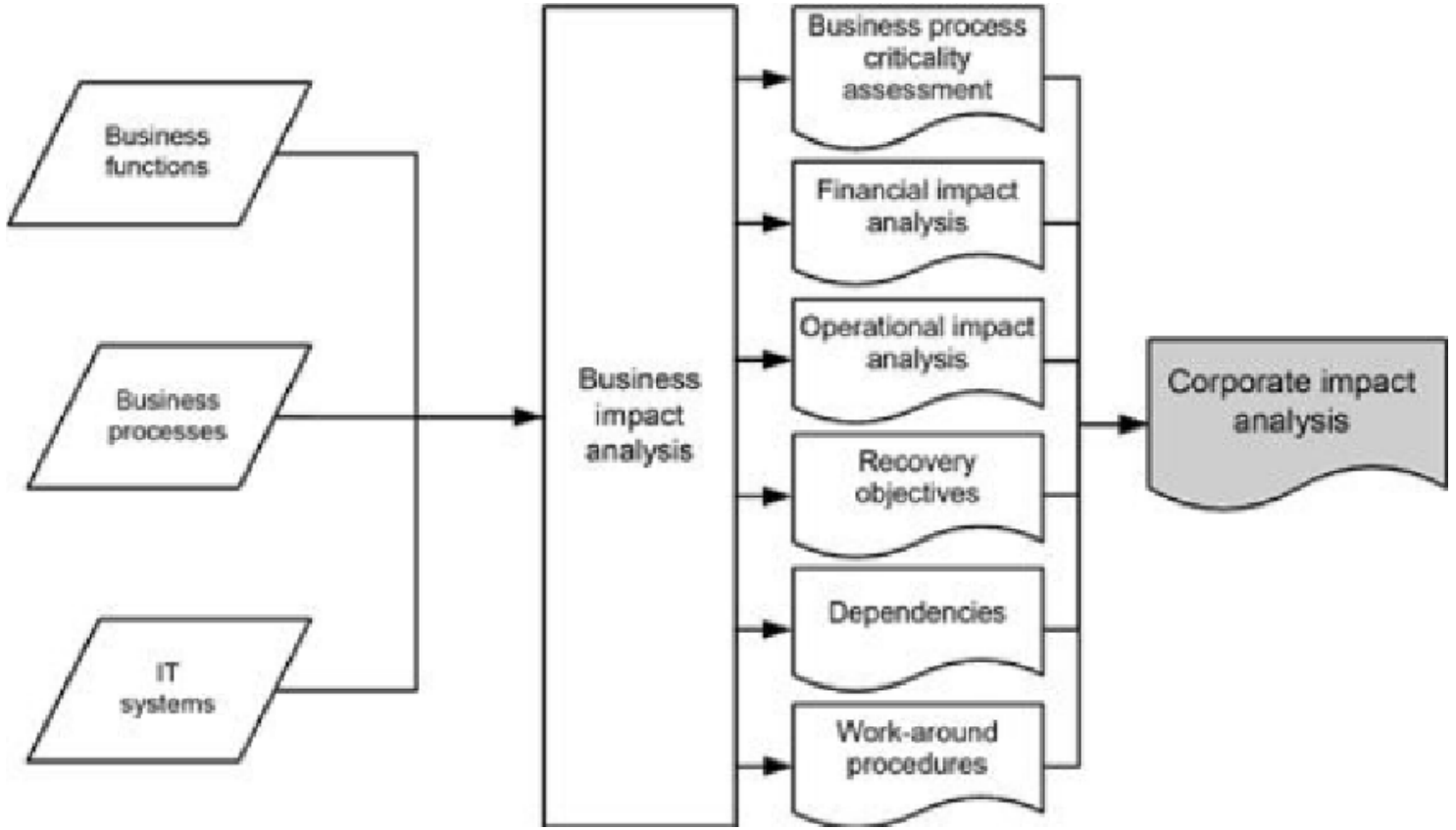
- MTD = RTO + WRT
- Recovery time objective (RTO)
  - El tiempo objetivo de recuperación se refiere al tiempo en que, por ejemplo, un sistema esté nuevamente accesible para los usuarios, por ejemplo, puede tomarnos 1 hora tomar una imagen de una máquina virtual, realizar configuraciones y recuperar el 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:

* Listado en orden alfabét ico en inglés.

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)

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 “llamarían” 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 equilibro 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
Escritorios, 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? Según 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 que 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)