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.