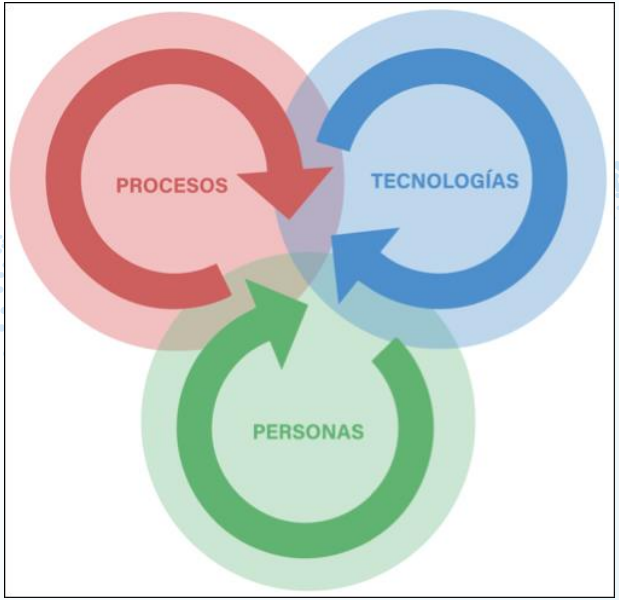
ORACLE®

Continuidad de Negocio

Roberto Gómez Cárdenas

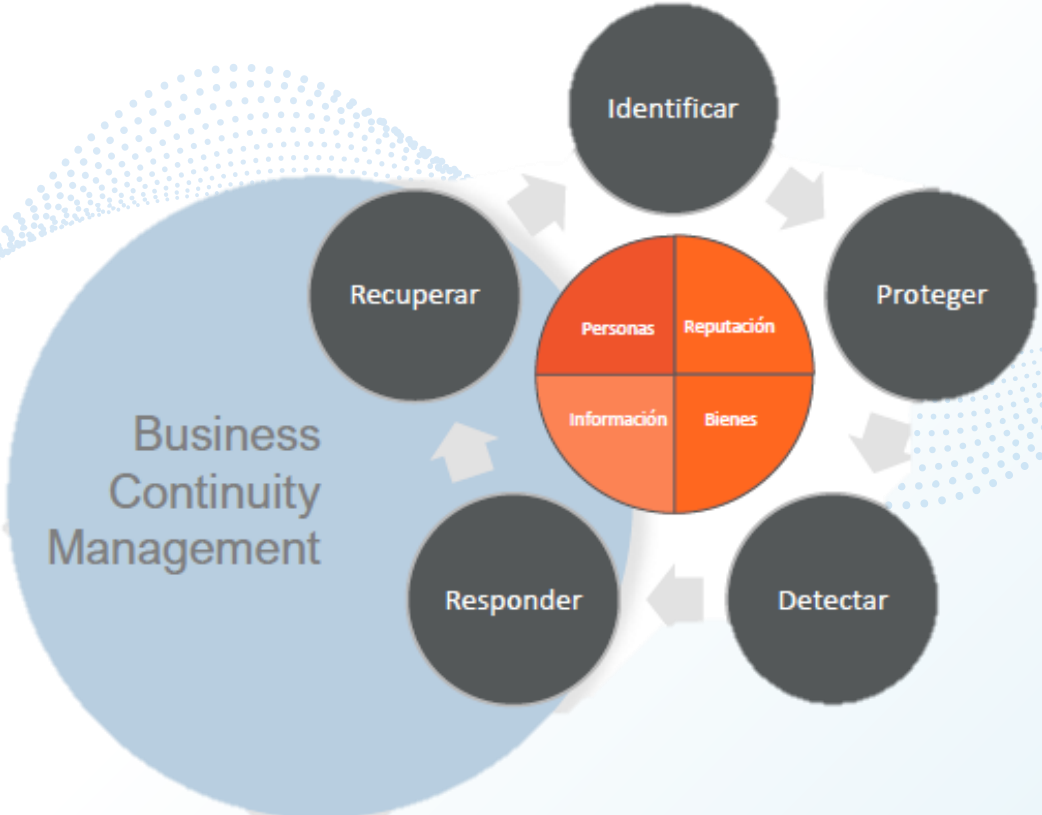
La CIA de la Seguridad Información

https://cio.com.mx/triada-cia-importante-nunca-la-seguridad-ti/



https://www.soluinnova.com/la-transformacion-digital-esta-redefiniendo-las-reglas-y-no-hay-duda-de-ello/

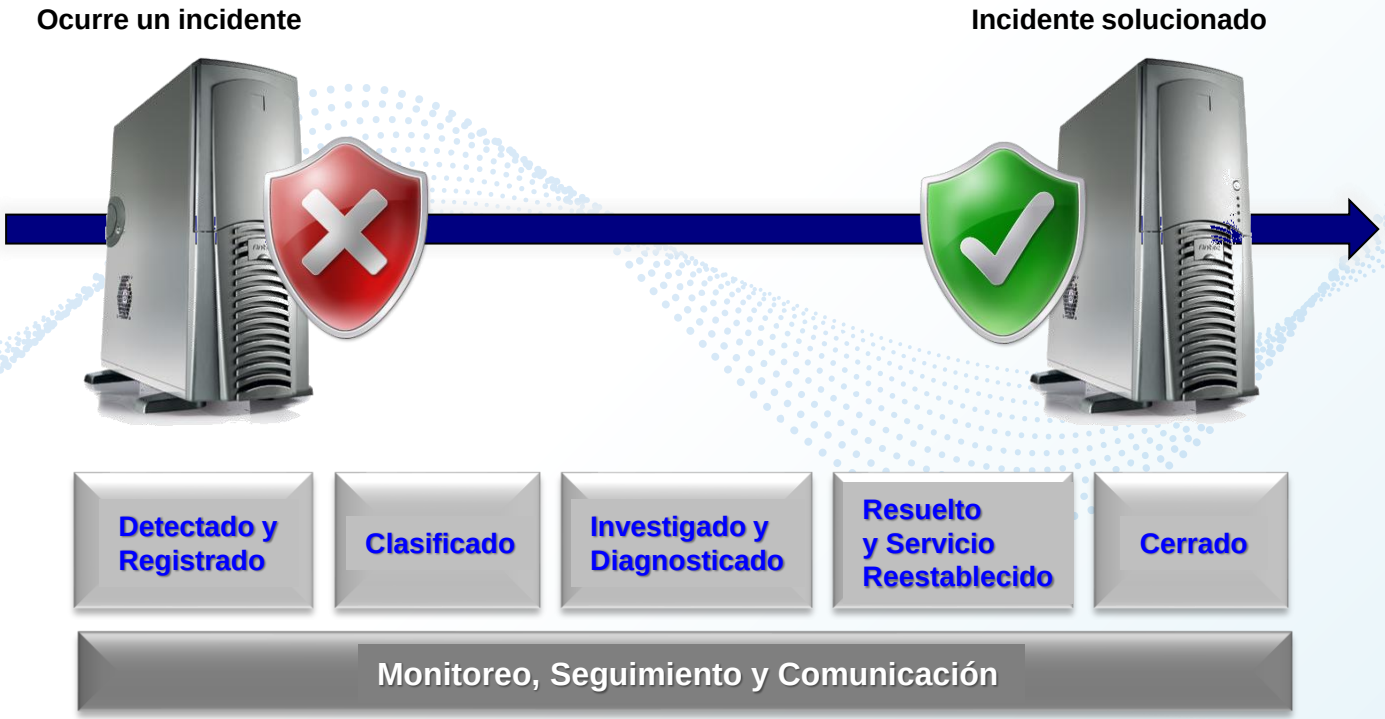
¿Donde queda la continuidad del negocio?



A tomar en cuenta

- **Seguridad vs Operaciones**

Ciclo vida incidente

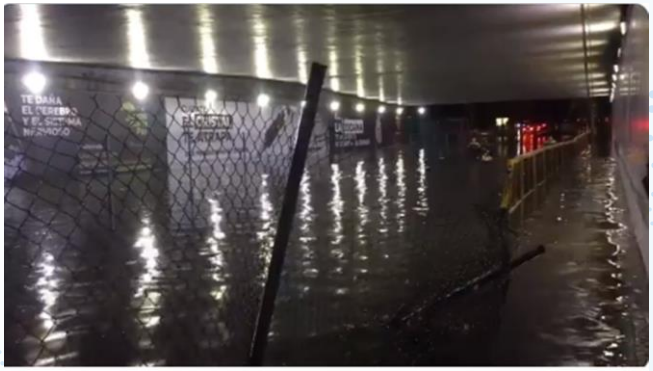


Ejemplos de incidentes

- Un servicio que no está disponible
- Corrupción de Software
- Una falla de Hardware
- La detección de un virus
- La “Caída de un sistema”
- El uso no autorizado de la cuenta de un usuario
- El uso no autorizado de Privilegios de acceso al Sistema
- La ejecución de código malicioso que destruye datos

También son incidentes

- Una Interrupción en el suministro de Energía Eléctrica
- Un Calentamiento excesivo que provoca que falle el Sistema
- La Inundación del Site de Cómputo
- Un Incendio en el Site de Cómputo
- Un Desastre Natural



¿Y en el ambiente informático?

“Incidente” =

Cualquier evento que no es parte de la operación normal de un servicio el cual causa, o puede causar una interrupción o una reducción en la calidad de ese servicio.

¿Qué es un desastre?

- Cualquier evento accidental, natural o malicioso que amenaza o interrumpe las operaciones o servicios normales por un período de tiempo que afecta significativamente a una organización
- Punto vista *informática*
  Interrupción no planeada, prolongada y no tolerable del servicio informático
- Punto vista *negocio*
  Interrupción no planeada, prolongada y no tolerable de las operaciones críticas de la empresa

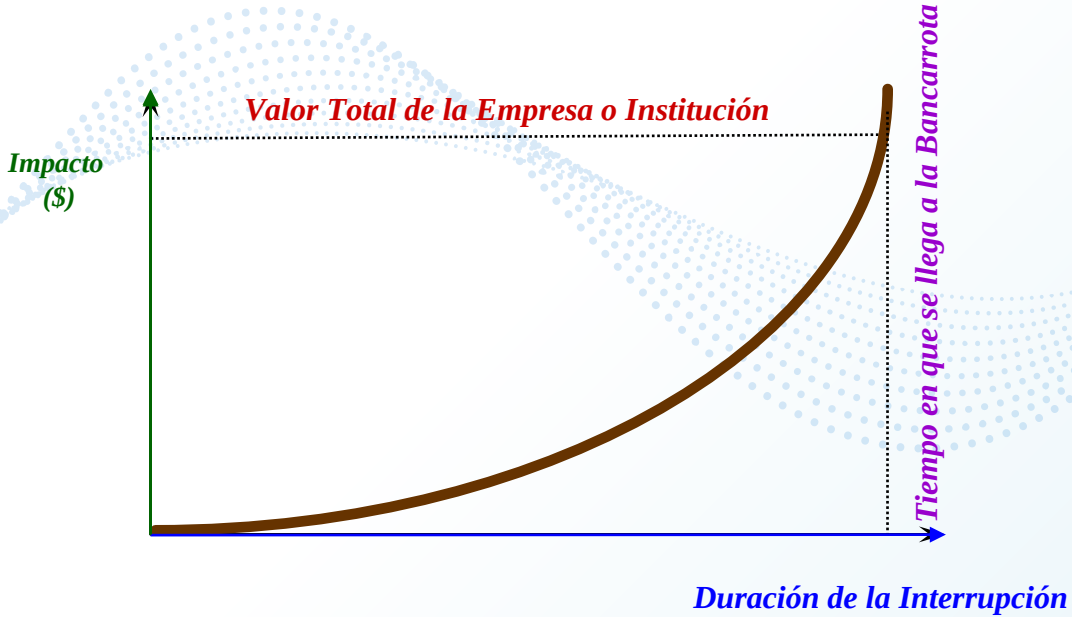
Los 10 desastres de mayor magnitud en México

Los 10 desastres desencadenados por amenazas naturales y socio naturales de mayor magnitud en México con base en el número total de víctimas fatales, el número total de personas afectadas y el daño económico total durante el periodo 1900-2018.

Tipo	Fecha	Víctimas fatales	Tipo	Fecha	Personas afectadas	Tipo	Fecha	Daño total (millones de dólares)
Sismo	19/09/1985	9 500	Sequía	Septiembre de 2011	2 500 000	Sismo	19/09/2017	6 000 000
Inundación	1959	2 000	Sismo	19/09/1985	2 130 204	Tormenta	19/10/2005	5 000 000
Actividad volcánica	1949	1 000	Tormenta	01/10/2005	1 954 571	Tormenta	13/09/2013	4 200 000
Tormenta	27/10/1959	960	Inundación	28/10/2007	1 600 000	Sismo	19/09/1985	4 104 000
Inundación	12/09/1999	636	Sismo	08/09/2017	1 200 250	Tormenta	15/09/2010	3 900 000
Tormenta	01/10/1976	600	Tormenta	19/10/2005	1 000 000	Inundación	28/10/2007	3 000 000
Sismo	28/08/1973	500	Inundación	20/09/2010	1 000 000	Tormenta	01/10/2005	2 500 000
Tormenta	28/09/1955	500	Tormenta	07/10/1997	800 200	Tormenta	10/09/2014	2 500 000
Tormenta	12/11/1961	436	Inundación	12/09/1999	616 060	Sismo	08/09/2017	2 300 000
Temperatura extrema	30/04/1990	380	Tormenta	20/09/2002	500 030	Tormenta	30/06/2010	2 000 000

Referencia:
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-46112019000300013&lng=es&nrm=iso
Université catholique de Louvain (UCLouvain) - CRED, D. Guha-Sapir – https://www.emdat.be/emdat_db/, Brussels, Belgium [Links]

Impacto y Duración del Incidente



Impacto de un desastre

GENAP Tecnología

FACT:

A company denied access to mission-critical data for more than 48 hours will likely be out of business within one year

Fuente: Jon W. Toigo. www.drplanning.org

Causas de un Desastre

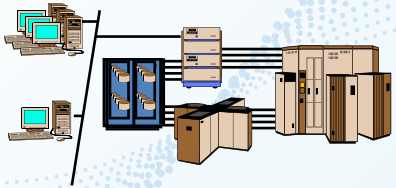
Causas Naturales	Causas Humanas	Causas Técnicas
• Incendios • Terremotos • Exhalaciones volcánicas • Hundimientos • Inundaciones • Tornados • Huracanes	• Amenazas de bomba • Huelgas • Plantones • Empleados inconformes • Empleados mal capacitados • Disturbios sociales	• Fallas en el equipo de cómputo o periféricos • Falla en el suministro de energía • Fallas en redes o Telecomunicaciones • Fallas en el Enlace • “Infección” por Virus Informático

Escenarios de Desastre

1. Destrucción de las Instalaciones

2. No Acceso a las Instalaciones

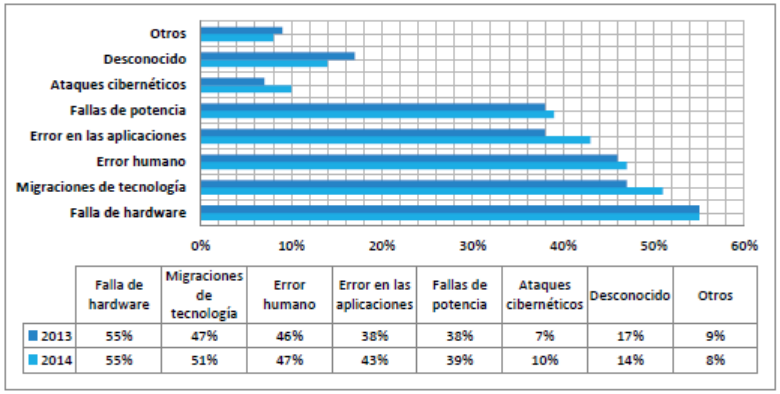
3. Sistemas o Equipos Inutilizables



4. Falta de Insumos o Suministros

5. Colapso Financiero

Causa más frecuente de Interrupciones



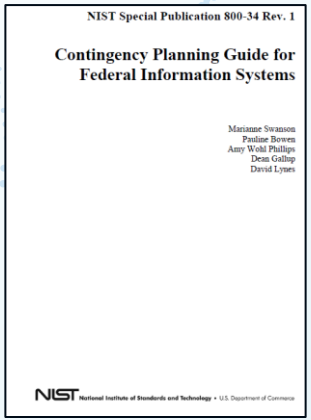
	Falla de hardware	Migraciones de tecnología	Error humano	Error en las aplicaciones	Fallas de potencia	Ataques cibernéticos	Desconocido	Otros
2013	55%	47%	46%	38%	38%	7%	17%	9%
2014	55%	51%	47%	43%	39%	10%	14%	8%

La Causa más frecuente de Interrupciones
No Planeadas, Prolongadas y No Tolerables del Servicio Informático en México
es:

!!!! Fallas de Hardware !!!

Estándares relacionados

- **BS 25999**
  Norma británica emitida en 2007. para la gestión de la continuidad del negocio: fue reemplazada por ISO 22301 en 2012.
- **ISO 27031**
  Guía para la “Gestión de la Tecnología de Información y Comunicación y obtención de Continuidad de Negocio”.
- **ISO 22301**
  Identifica los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.
- **NIST SP 800-34**
  Proporciona instrucciones, recomendaciones y consideraciones para los planes de contingencia para sistemas de información federales en USA-



Buenas prácticas y certificaciones

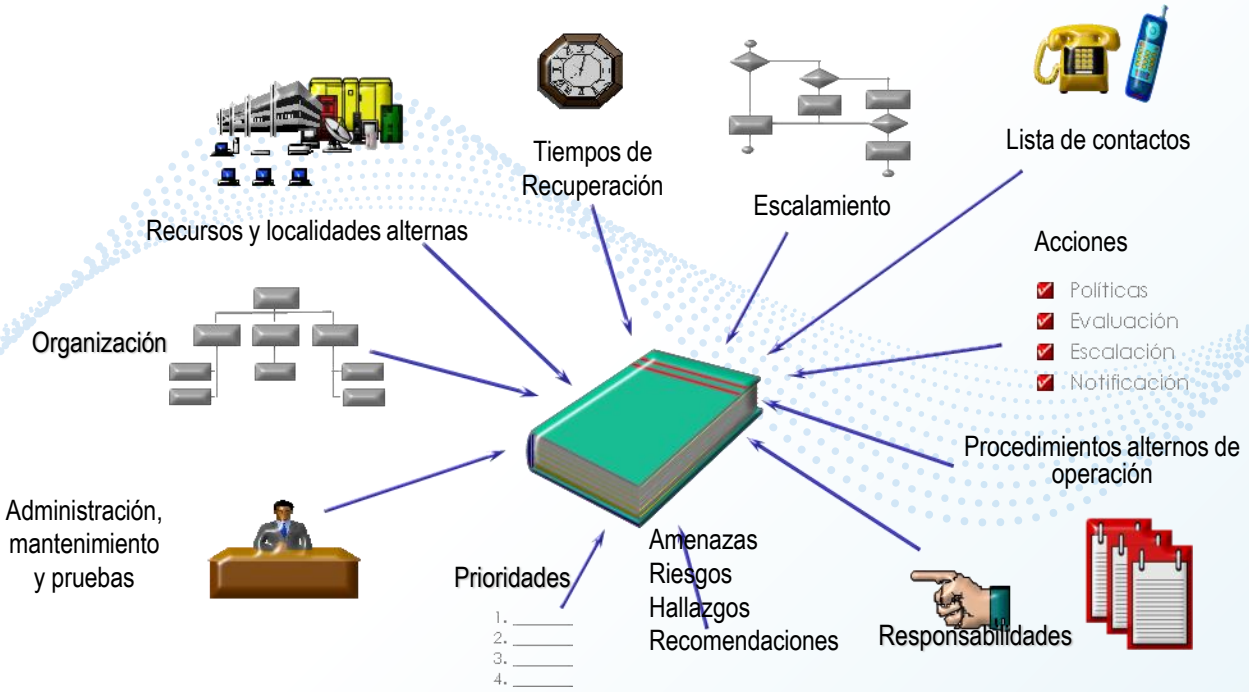
- The BCI Good Practice Guidelines (GPG)
  Producidos por el Business Continuity Institute (BCI) y son la guía definitiva para los profesionales de la continuidad empresarial y la resiliencia. Estos se actualizan periódicamente, más recientemente en 2018.

- DRI International Institute's Professional Practices for Business Continuity Planners

  Organismo mundial de educación y certificación en Continuidad de Negocio (BCM, Business Continuity Management) y Recuperación ante Desastres (DRP, Disaster Recovery Planning).

  Establece el estándar para los profesionales de planificación de continuidad de negocio.

Entregables del Proyecto BCP



¿BCP o DRP?

El concepto de “Desastre” en DRP - BCP

Desastre

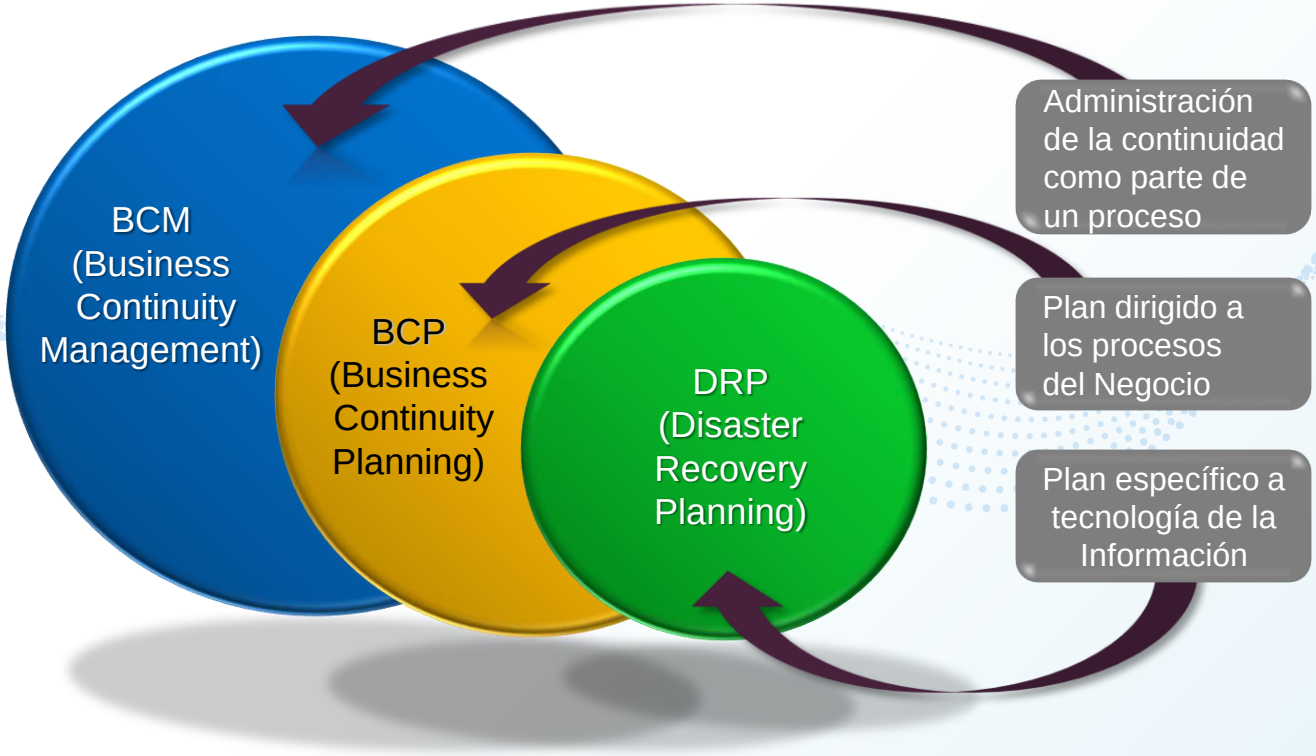
Desde el punto de vista **Informática**

INTERRUPCIÓN NO PLANEADA, PROLONGADA Y NO TOLERABLE DEL SERVICIO INFORMÁTICO

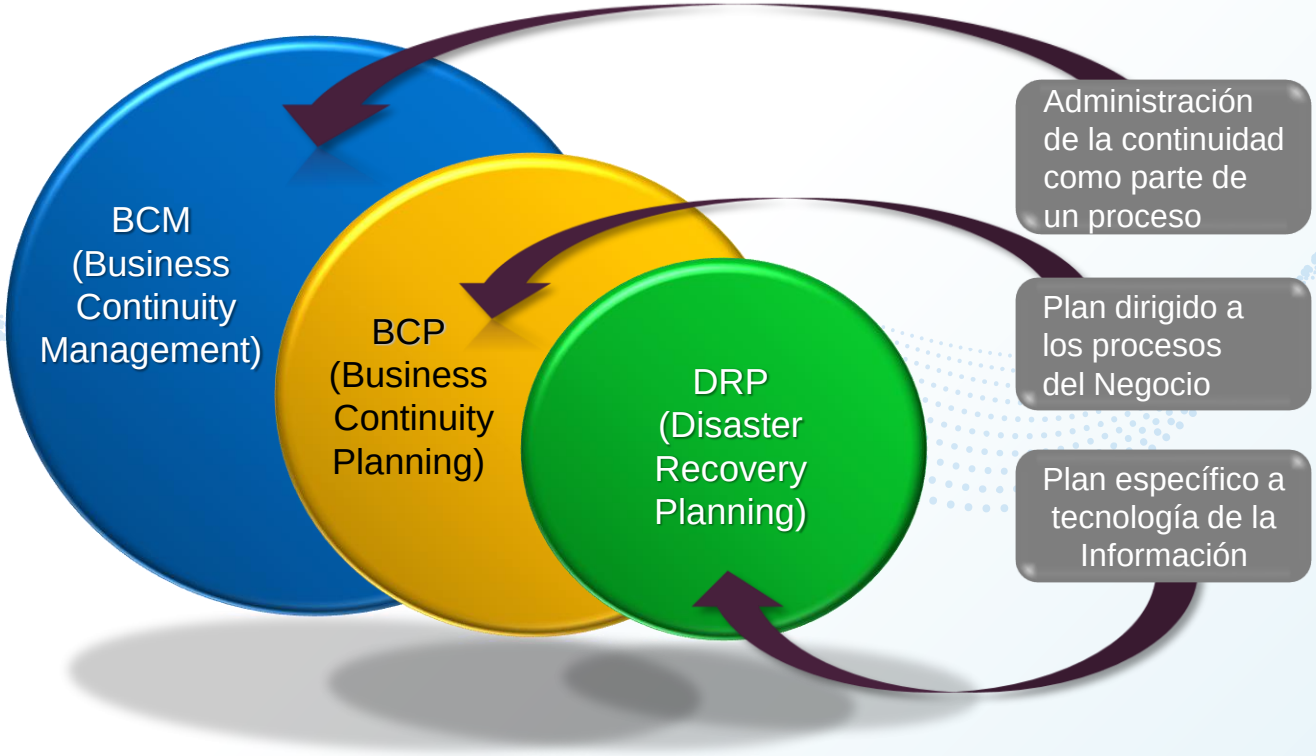
Desde el punto de vista del **Negocio**

INTERRUPCIÓN NO PLANEADA, PROLONGADA Y NO TOLERABLE DE LAS OPERACIONES CRÍTICAS DE LA EMPRESA

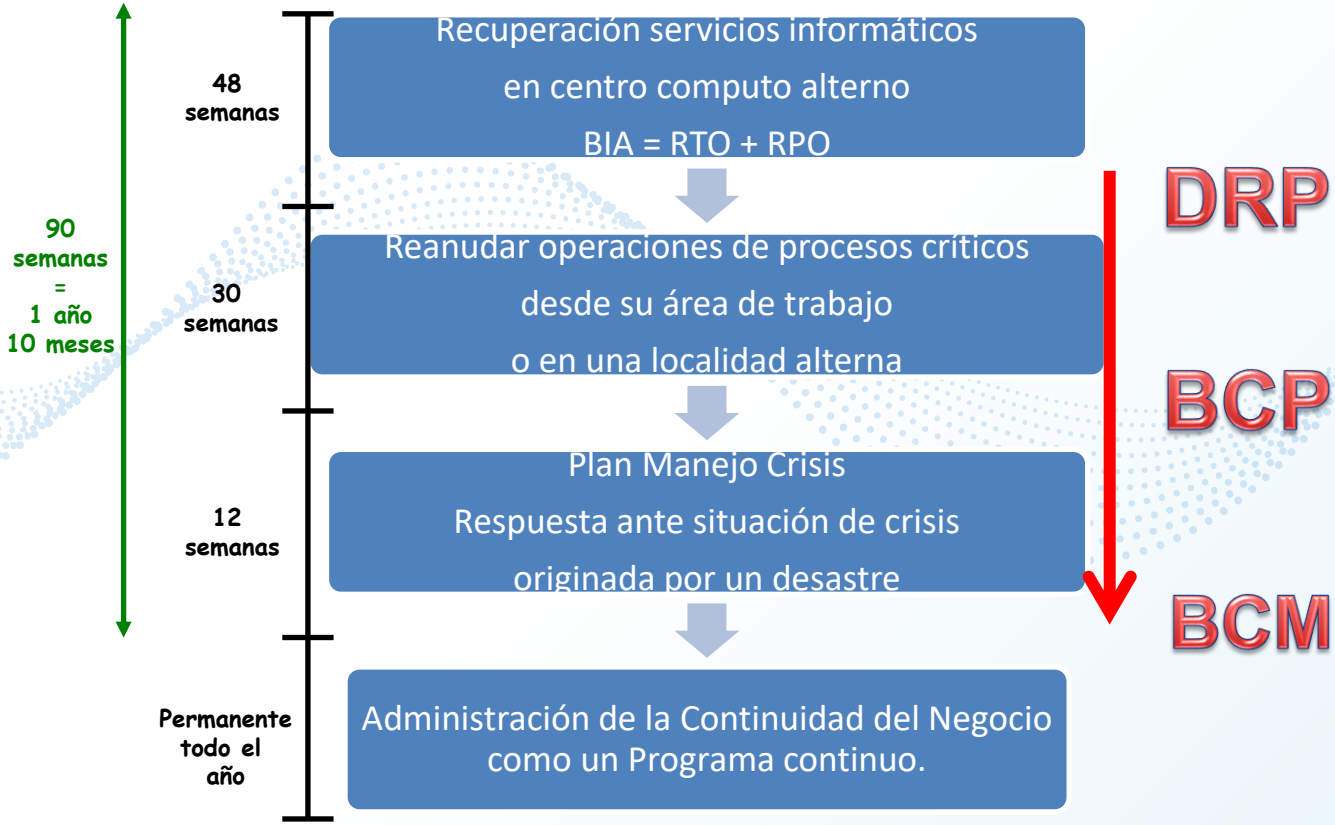
BCM vs BCP vs DRP



BCM vs BCP vs DRP



Tiempos: BCM vs BCP vs DRP



Metodología del DRII* para desarrollar un BCP

(*) DRII = Disaster Recovery Institute International

Un poco más de detalle

GENAP Tecnología

1. Planeación y Organización del Proyecto
2. **Evaluación y control del riesgo**
3. Análisis de Impacto al Negocio (BIA)
4. **Estrategias para la recuperación**
5. Desarrollo del Plan para el Restablecimiento del Servicio Informático (Cómputo y Comunicaciones) (DRP).
6. **Prueba del Plan de DRP**

- Establecer la necesidad de desarrollar e implementar un Plan de Continuidad del Negocio
- Obtener el soporte directivo
- Organizar y administrar el proyecto hasta su completa realización y acorde con los límites de tiempo y presupuesto

- Determinar los eventos y circunstancias del ambiente (interrupciones y desastres) que pueden afectar adversamente a la Organización y sus instalaciones y facilidades.
- Determinar el daño que tales eventos pueden causar
- Determinar los controles necesarios para prevenir o minimizar los efectos de pérdidas potenciales.
- Proveer el análisis costo-beneficio para justificar la inversión en controles para mitigar los riesgos

- Identificar los Impactos que resultan de las interrupciones y escenarios de desastre que pueden afectar a la organización
- Identificar las técnicas que pueden ser usadas para cuantificar y calificar tales Impactos

- Determinar y guiar la selección de estrategias funcionales alternativas para recuperar el negocio y el servicio informático dentro del Tiempo Objetivo de Recuperación (RTO), al tiempo que se mantienen las funciones críticas de la organización.

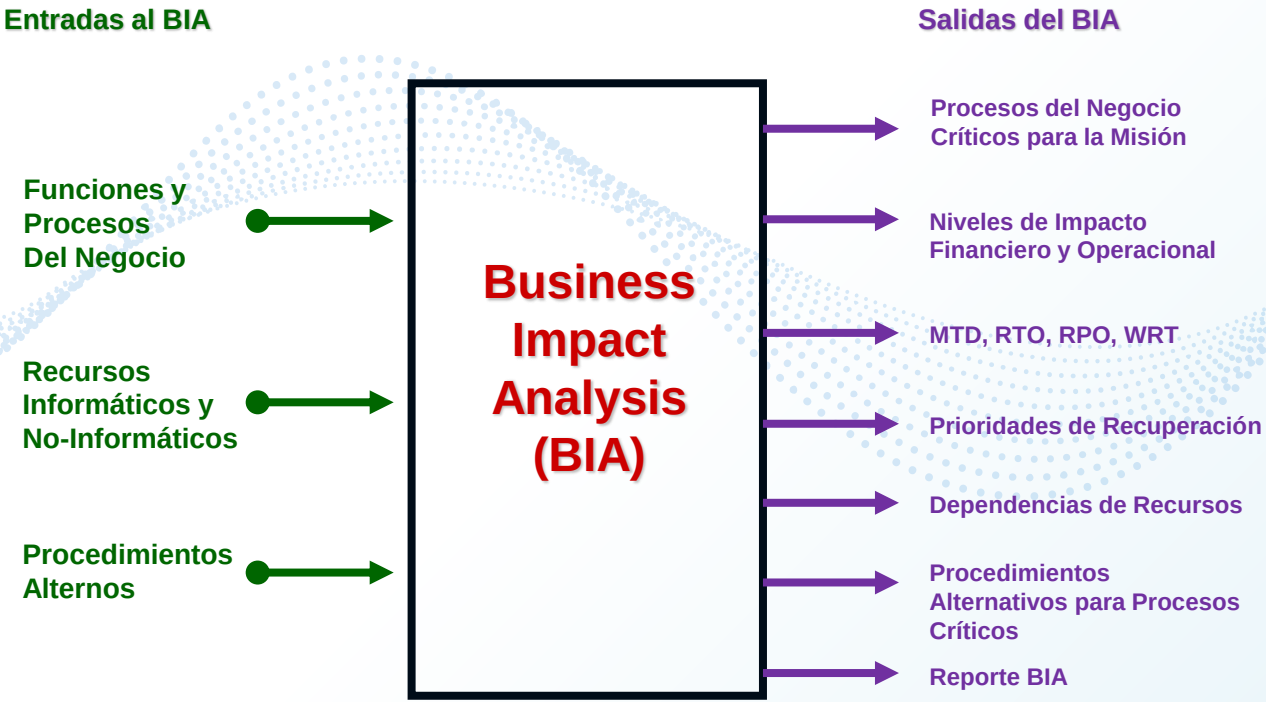
- Desarrollar e implementar Procedimientos para Responder y Estabilizar la situación inmediata siguiente a un incidente o evento.

- Planear y coordinar las Pruebas del BCP
- Evaluar y documentar los resultados de las pruebas.

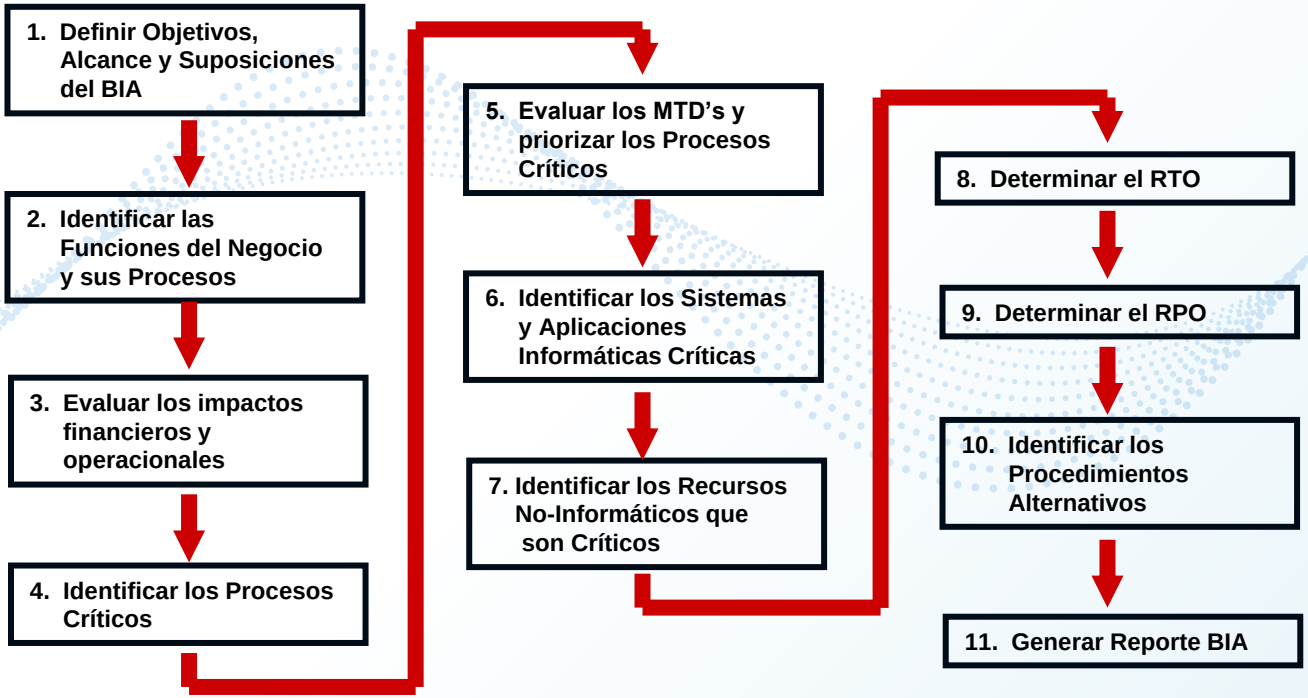
Análisis del Impacto al Negocio (BIA)

- Identificar los Impactos que resultan de las interrupciones y escenarios de desastre que pueden afectar a la organización
- Determinar el impacto de una interrupción significativa del servicio (desastre) en las *unidades funcionales*.
- Estos impactos pueden ser financieros en términos de pérdida de dinero, o pueden ser de naturaleza operacional, tal como perder la capacidad para atender a los clientes y/o usuarios y no poder proporcionar un servicio de calidad.
- Identificar las técnicas que pueden ser usadas para cuantificar y calificar tales Impactos

Vista funcional del BIA



Procesos desarrollo del BIA



1. Objetivos, alcance suposiciones

- Alcance
  - Toda la empresa
  - Localidades especificas de la empresa
- Suposiciones (escenarios)
  - La interrupción ocurre durante las horas pico de operación
    - Peor momento y peores circunstancias
  - No existe un centro de cómputo de respaldo
  - No hay áreas de trabajo alternas para usuarios
  - La localidad afectada está inaccesible

2. Identificar funciones negocio y procesos

Funciones del Negocio	Procesos del Negocio
Ventas	Generar Pedidos
	Reportar Datos de Ventas
Marketing	Promover Productos
	Mantener Catálogo
Servicio a Clientes	Manejar Reclamos de Clientes
	Procesar Pedidos
Logística	Empacar Producto
	Embarcar Producto

3. Evaluar impactos financieros y operacionales

- **Impacto Financiero:**
  - **Mide la amplitud y severidad de la pérdida financiera para la empresa**

Funciones del Negocio	Procesos del Negocio	Pérdida Financiera (USD por día)
Ventas	Generar Pedidos	$ 700,000
	Reportar Datos de Ventas	$ 0
Marketing	Promover Productos	$ 10,000
	Mantener Catálogo	$ 5,000
Servicio a Clientes	Manejar Reclamos de Cltes	$ 5,000
	Procesar Pedidos	$ 500,000
Logística	Empacar Producto	$ 15,000
	Embarcar Producto	$ 20,000

Niveles severidad

- Nivel de Severidad “0” (No impacto)
- Nivel de Severidad “1” (Impacto Menor)
- Nivel de Severidad “2” (Impacto Medio)
- Nivel de Severidad “3” (Impacto Mayor)

Funciones del Negocio	Procesos del Negocio	Pérdida Financiera (USD por día)	Nivel de Severidad
Ventas	Generar Pedidos	$ 700,000	3
	Reportar Datos de Ventas	$ 0	0
Marketing	Promover Productos	$ 10,000	1
	Mantener Catálogo	$ 5,000	1
Servicio a Clientes	Manejar Reclamos de Cltes	$ 5,000	1
	Procesar Pedidos	$ 500,000	3
Logística	Empacar Producto	$ 15,000	2
	Embarcar Producto	$ 20,000	2

3. Evaluar impactos operacionales

- Impacto operacional
  - Mide el impacto negativo de la interrupción sobre varios aspectos de las operaciones del negocio.
  - Ejemplos de Impactos operacionales:
    - Inadecuado Flujo de Efectivo
    - Pérdida de la confianza de los inversionistas

Función del Negocio	Proceso del Negocio	Impactos Operacionales				
		Flujo de Efectivo	Confianza del inversionista	Participación de Mercado	Ventaja Competitiva	Satisfacción de Clientes
Ventas	Generar Pedidos	Alto	Alto	Muy Alto	Alto	Nada
	Reportar datos de Ventas	Nada	Muy Alto	Bajo	Nada	Nada
Marketing	Promover Productos	Bajo	Alto	Alto	Muy Alto	Bajo
	Mantener Catálogo	Bajo	Medio	Alto	Muy Alto	Alto
Servicio a Clientes	Manejar Reclamos de Clientes	Medio	Bajo	Bajo	Medio	Alto
	Procesar Pedidos	Muy Alto	Medio	Bajo	Medio	Muy Alto
Logística	Empacar Producto	Alto	Medio	Bajo	Alto	Alto
	Embarcar Producto	Alto	Medio	Bajo	Alto	Alto

4. Identificar los procesos críticos

- **Un Proceso es considerado Crítico si cumple alguno de los siguientes Criterios**
  - Impacto Financiero con Severidad de Nivel 2 o 3
  - Al menos 3 de sus Impactos Operacionales son evaluados como “Alto”
  - Al menos 2 de sus Impactos Operacionales son evaluados como “Alto” y al menos 1 como “Muy Alto”
  - Al menos 2 de sus Impactos Operacionales son evaluados como “Muy Alto”

Funciones del Negocio	Procesos del Negocio
Ventas	Generar Pedidos
	Reportar Datos de Ventas
Marketing	Promover Productos
	Mantener Catálogo
Servicio a Clientes	Manejar Reclamos de Clientes
	Procesar Pedidos
Logística	Empacar Producto
	Embarcar Producto

5. Evaluar MTDs

- **Maximum Tolerable Downtime**
- **Cantidad de tiempo que un proceso puede permanecer no-disponible antes que los impactos financiero y operacionales alcancen un nivel inaceptable**

Funciones Críticas del Negocio	Procesos Críticos del Negocio	MTD	Prioridad de Recuperación
Ventas	Generar Pedidos	3 días	1
	Reportar Datos de Ventas	5 días	3
Marketing	Promover Productos	7 días	4
	Mantener Catálogo	5 días	3
Servicio a Clientes	Manejar Reclamos de Cltes	10 días	5
	Procesar Pedidos	3 días	1
Logística	Empacar Producto	4 días	2
	Embarcar Producto	4 días	2

6. Identificar los sistemas y aplicaciones informáticas críticas

- Una aplicación o sistema informático se considera “critico” si soporta a un proceso de negocio que es crítico

Función Crítica del Negocio	Proceso Crítico del Negocio	Aplicaciones y Sistemas Informáticos Críticos
Ventas	Generar Pedidos	Sistema de Información de Clientes
		Sistema de Pedidos
		E-mail
		Aplicación EDI
		Sistema de Rastreo y Consulta de Ventas
Marketing	Promover Productos	Sistema de Información de Clientes
		E-mail
	Mantener Catálogo	Catálogo en Línea
Servicio a Clientes	Procesar Pedidos	Sistema de Pedidos
		Sistema de Inventarios
		Sistema de Facturación
Logística	Empacar Producto	Sistema de Pedidos
		Sistema de Administración de Embarques
	Embarcar Producto	Sistema de Administración de Embarques
		Sistema de Inventarios
		Sistema de Pedidos

7. Identificar los recursos no-informáticos que son críticos

- Se identifican los recursos no-informáticos que son críticos y que son requeridos por los procesos críticos del negocio.
- Ejemplos
  - Planta de Manufactura y Producción
  - Área de Oficina
  - Equipo de Manufactura y Producción
  - Materia Prima
  - Mobiliario de Oficina
  - Equipo de Seguridad

8. Determinar el RTO

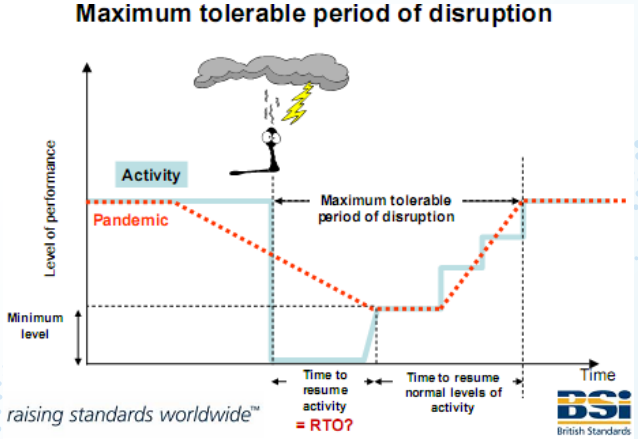
- Define el límite de tiempo máximo tolerable dentro del cual se recuperan los datos. Si se produce un desastre y los sistemas deben estar disponibles inmediatamente, pero se permite que haya alguna pérdida de datos, el RTO es cero.
- Sin embargo, si se tolera una hora de recuperación de datos, el RTO es una hora

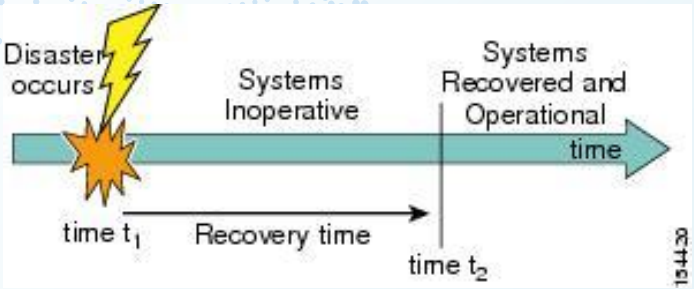
Función Crítica del Negocio	Proceso Crítico del Negocio	Aplicaciones y Sistemas Informáticos Críticos	RTO	MTD	WRT
Ventas	Generar Pedidos	Sistema de Información de Clientes	2.5 días	3 días	0.5 días
		Sistema de Pedidos	1 día	5 días	2 días
		E-mail	2.5 días	7 días	0.5 días
		Aplicación EDI	2 días	5 días	1 día
		Sistema de Rastreo y Consulta de Ventas	2.8 días	10 días	0.2 día

WRT: Work Recovery Time

8. Determinar el RTO

- Si el RTO es de dos hora, es necesario investir bastante recursos ($) en un centro de recuperación de desastres, telecomunicaciones, sistemas automatizados y redundantes, etc.
- Si el RTO es de dos semanas, entonces la inversión requerida será mucho menor ya que se tendrá el tiempo necesario de conseguir recursos después de que el incidente ocurrió.





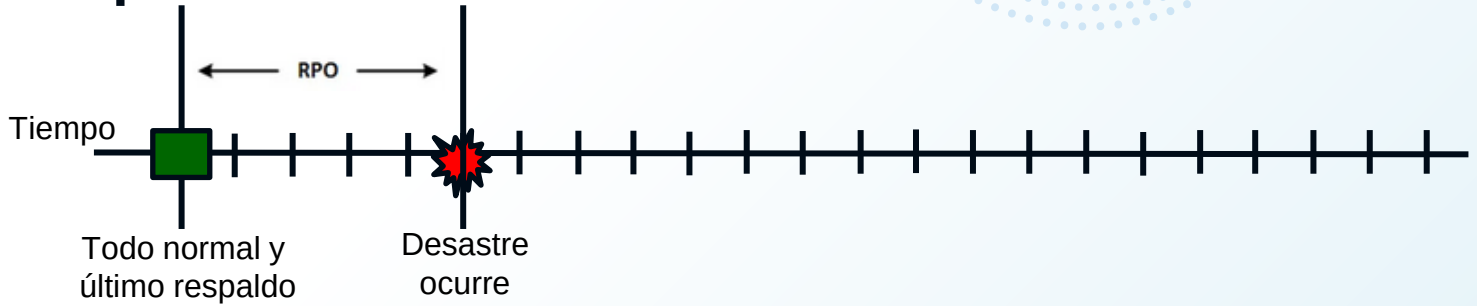
9. Determinar el RPO

- RPO = Recovery Point Objective
- Periodo de tiempo máximo en el cual los datos de un servicio TI pueden perderse debido a un incidente.
- Comúnmente se mide como el tiempo entre el último respaldo (backup) de los datos y el momento del desastre.

RPO (Recovery Time Objective)

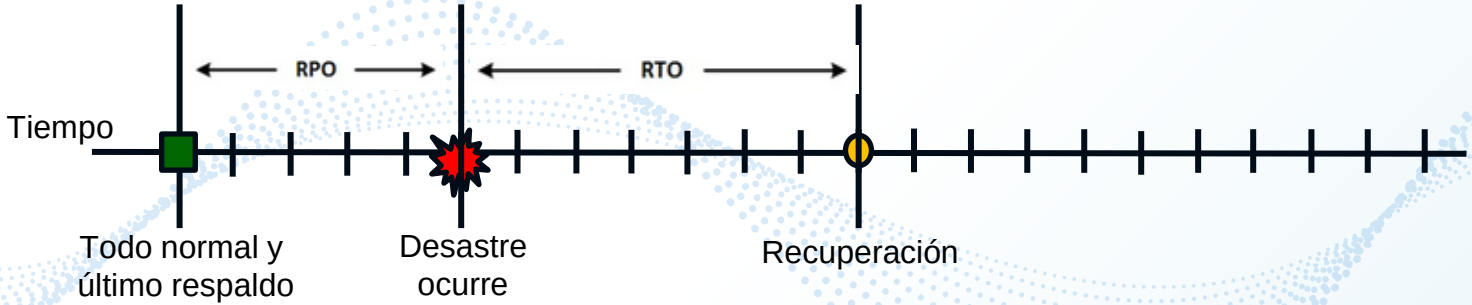
- **Etapa 1: Proceso ejecutándose de forma normal**

- **Etapa 2: El desastre ocurre**

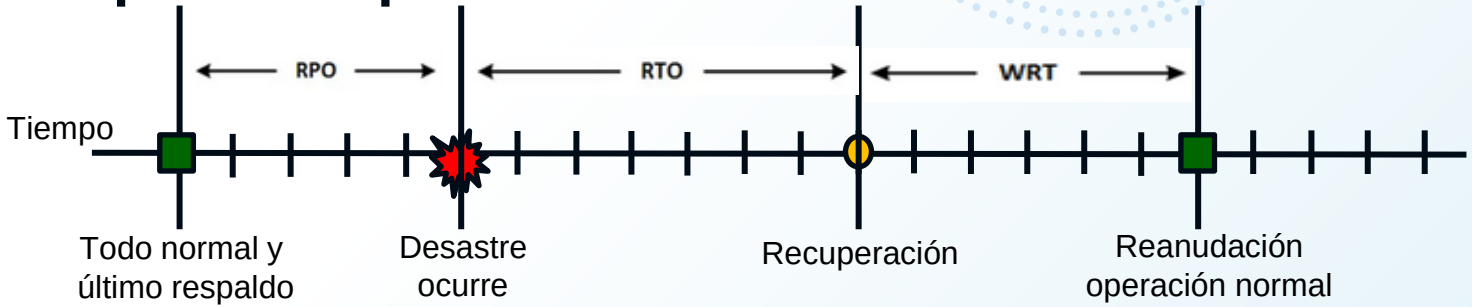


RPO, RTO (Recovery Time Objective), WRT (Work Recovery Time)

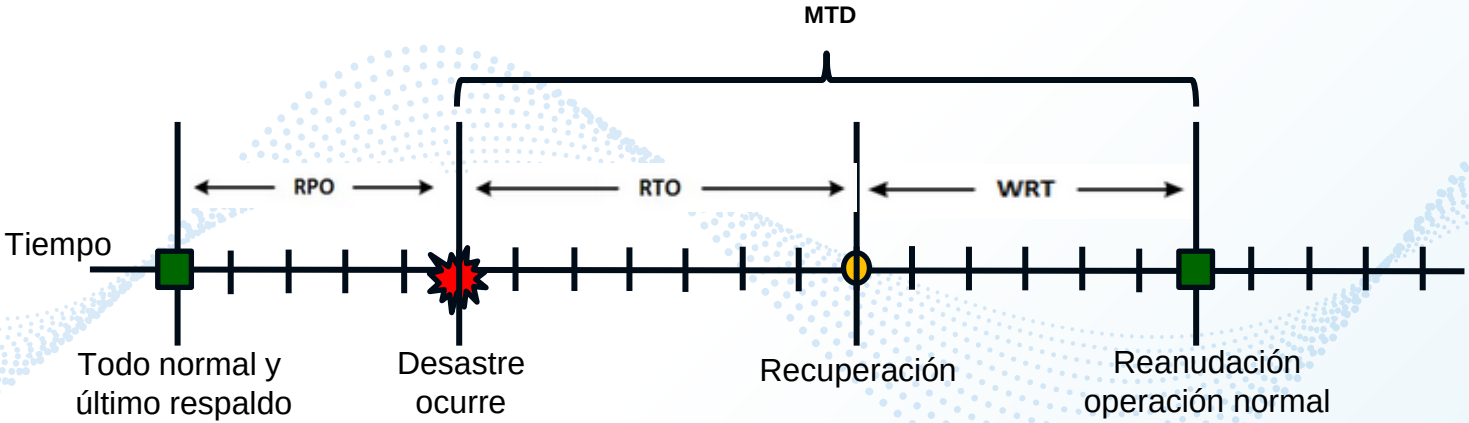
- **Etapa 3: Recuperación**



- **Etapa 4: de producción**

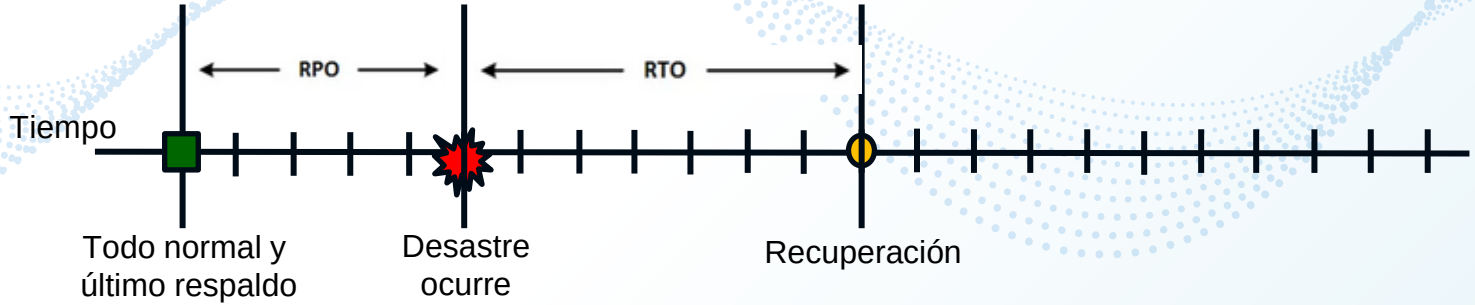


RPO, RTO, WRT. MTD (Maximum Tolerable Downtime)



RPO, RTO, WRT, MTD

- **MTD: Maximum Tolerable Downtime**



10. Identificar los procedimientos alternativos

- Permiten que los Procesos del Negocio continúen, en el caso de que los recursos informáticos y no-informáticos no estén disponibles, a través de métodos alternativos.
- Estos métodos alternativos, los cuales con frecuencia involucran operaciones manuales, tienden a ser temporales, poco eficientes, o más costosos en comparación con los procedimientos normales.
- Se identifican preguntando:
  - ¿Hay algún(os) procedimientos alternativos documentados que existan para este Proceso?
  - ¿Identifica alguna tarea o actividad del proceso que no esté cubierta por estos procedimientos alternativos?

10. Identificar los procedimientos alternativos

Función Crítica del Negocio	Proceso Crítico del Negocio	Aplicaciones y Sistemas Informáticos Críticos	Procedimientos Alternativos
Ventas	Generar Pedidos	Sistema de Pedidos	Rastrear manualmente los pedidos de los Clientes usando la información de Clientes contenida en las microfichas. Manualmente procesar los pedidos con excepción de la aprobación de crédito. Procesar la aprobación del crédito una vez que el sistema haya sido recuperado y se haya establecido el enlace para verificar externamente el crédito.
Logística	Empacar Producto	Maquinaria Equipo: Empacadora horizontal de cajas	Empacar manualmente sólo los productos para cajas pequeñas y medianas. Empacar las cajas grandes una vez que el equipo de empaquetamiento esté operacional

11. Generar reporte BIA

- Los resultados de todos los pasos anteriores se resumen en este paso para proporcionar una visión interna dentro de todos los hallazgos del BIA.
- El reporte deberá incluir entre otras cosas:
  - La proporción entre el número de procesos del negocio y el número de procesos críticos por unidad funcional o función de Negocios
  - El valor promedio de RTO para todos los procesos críticos
  - Los valores promedio de MTD para todos los procesos críticos
  - Los valores de RPO de cada proceso crítico
  - La pérdida financiera esperada por día de interrupción

Certificaciones Data Center

- Certificación enfocada en evaluar y certificar el cumplimiento de requisitos de diseño, construcción y operación, para la obtención final de un concepto: Disponibilidad.
- Todas requieren un proceso inicial de certificación, que luego es avalado por una auditoría anual para mantenerla vigente.
- Cada una es ejecutada por empresas asociadas al certificador, que realizan una labor autónoma a través de ingenieros especialistas.
- Los Data Center Certificados, tienen unos parámetros que les brinda una alta seguridad y disponibilidad a los datos.
- No es rentable construir un Data Center Certificado para una empresa no especializada, porque la inversión es millonaria, y el costo unitario sería altísimo.

Tiempos de recuperación sites

Nivel de disponibilidad / Coste				
Nivel	**Tiempo parada / año**	**Tiempo en minutos**	**Coste/Hora**	**Coste anual**
90%	36,5 días	52560	10.000 €	8.760.000 €
95%	18,25 días	26280	10.000 €	4.380.000 €
99%	3,65 días	5256	10.000 €	876.000 €
99,50%	44 horas	2640	10.000 €	440.000 €
99,90%	8,76 horas	525,6	10.000 €	87.600 €
99,95%	4,38 horas	262,8	10.000 €	43.800 €
99,99%	52,5 minutos	52,5	10.000 €	8.750 €
99,999%	5,3 minutos	5,3	10.000 €	883 €

https://www.altadisponibilidadlogitek.com/los-nueves-de-disponibilidad-que-son/

Estándares

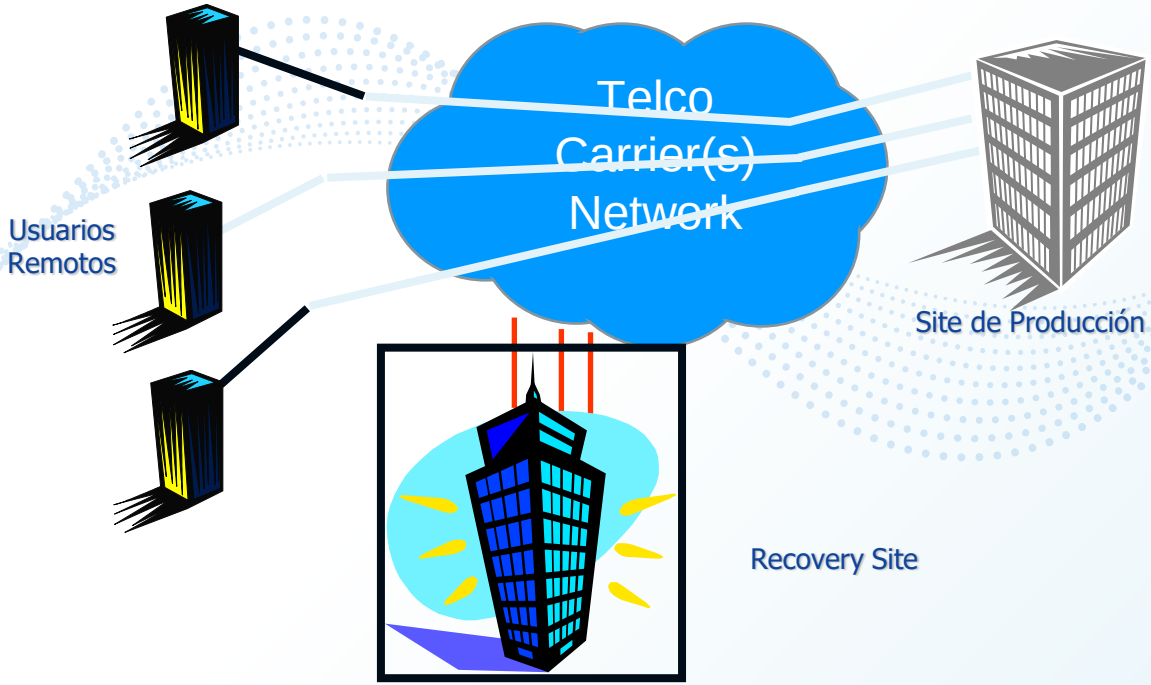
ICREA	Nivel I	Nivel II	Nivel III	Nivel IV	Nivel V
Disponibilidad	95%	99%	99.9%	99.99%	99.999%
Horas en el año	8,760	8,760	8,760	8,760	8,760
Minutos en al año	525,600	525,600	525,600	525,600	525,600
Δ Tiempo	499,320	8,672.4	8,751.2	8,759.1	8,759.9
Horas x Año Indisponibilidad	438	87.6	8.76	0.876	0.0876
Días x Año Indisponibilidad	18.3	3.7	0.4	0.04	0.004
Min x Año Indisponibilidad	26,280	5,256	525.6	52.56	5.256

Uptime Institute	TIER I	TIER II	TIER III	TIER IV
Disponibilidad	99.671%	99.95%	99.982%	99.99%
Horas en el año	8,760	8,760	8,760	8,760
Minutos en al año	525,600	525,600	525,600	525,600
Δ Tiempo	523,871	525,337	525,505	525,547
Horas x Año Indisponibilidad	28.8204	4.38	1.5768	0.876
Días x Año Indisponibilidad	1.2	0.2	0.1	0.04
Min x Año Indisponibilidad	1,729	263	94.6	52.6

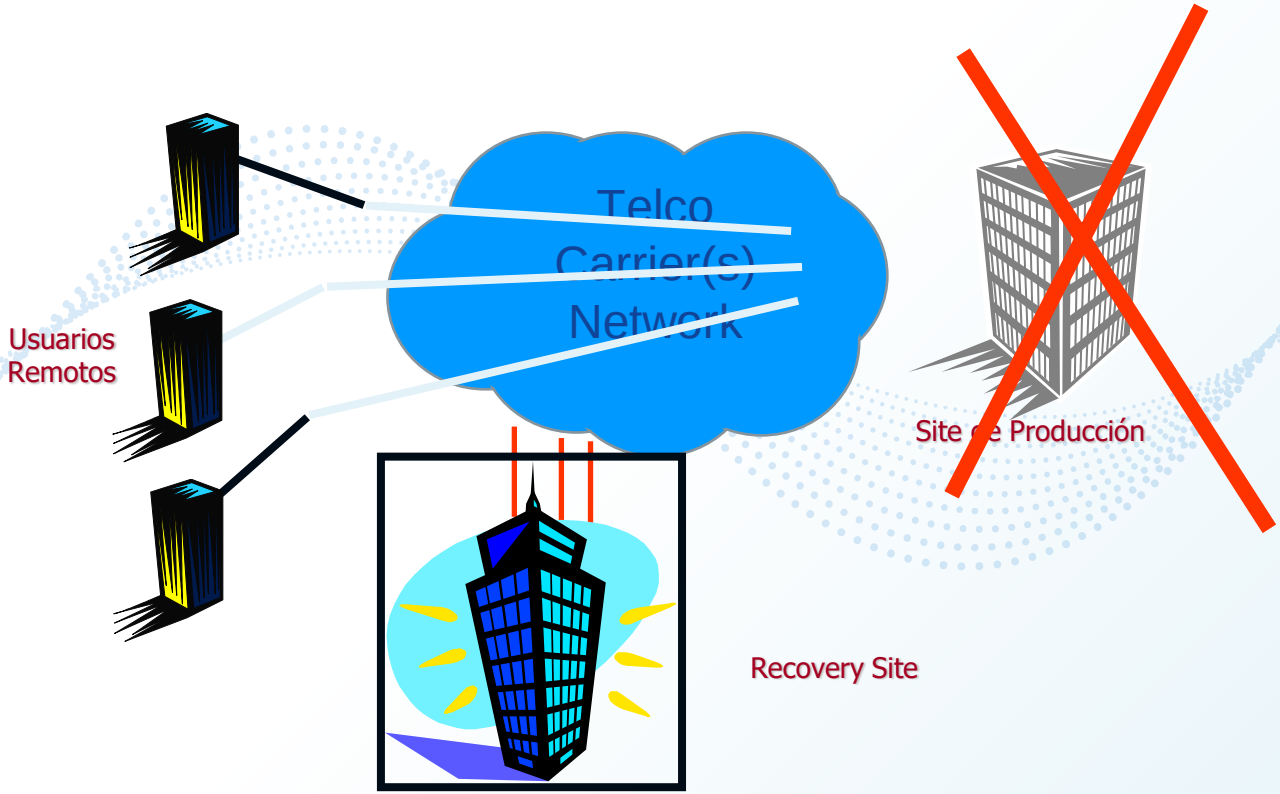
Requerimientos de recuperación de TI y áreas usuarios

- Recuperación red y telecomunicaciones.
- Configuración de recuperación mínima aceptable.
- El centro alterno de recuperación.

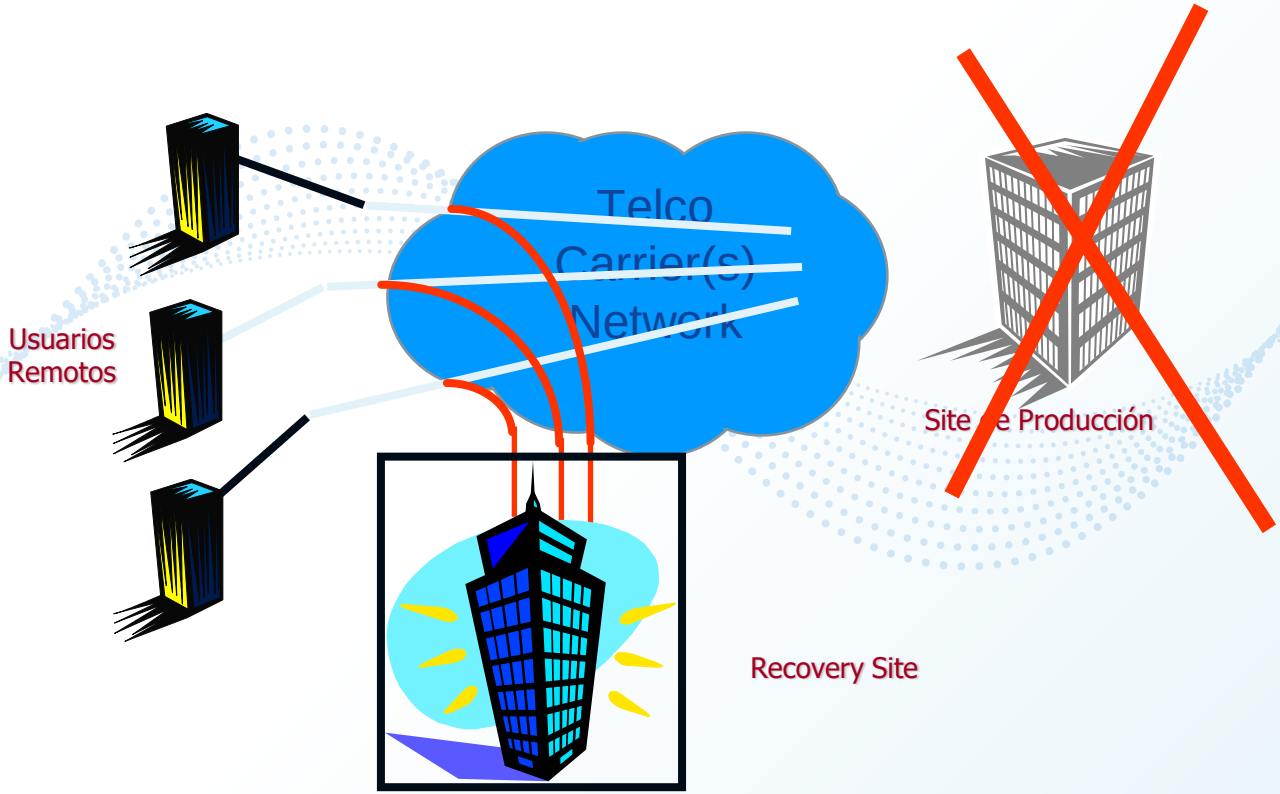
Recuperación de la red



Recuperación de la red



Recuperación de la red

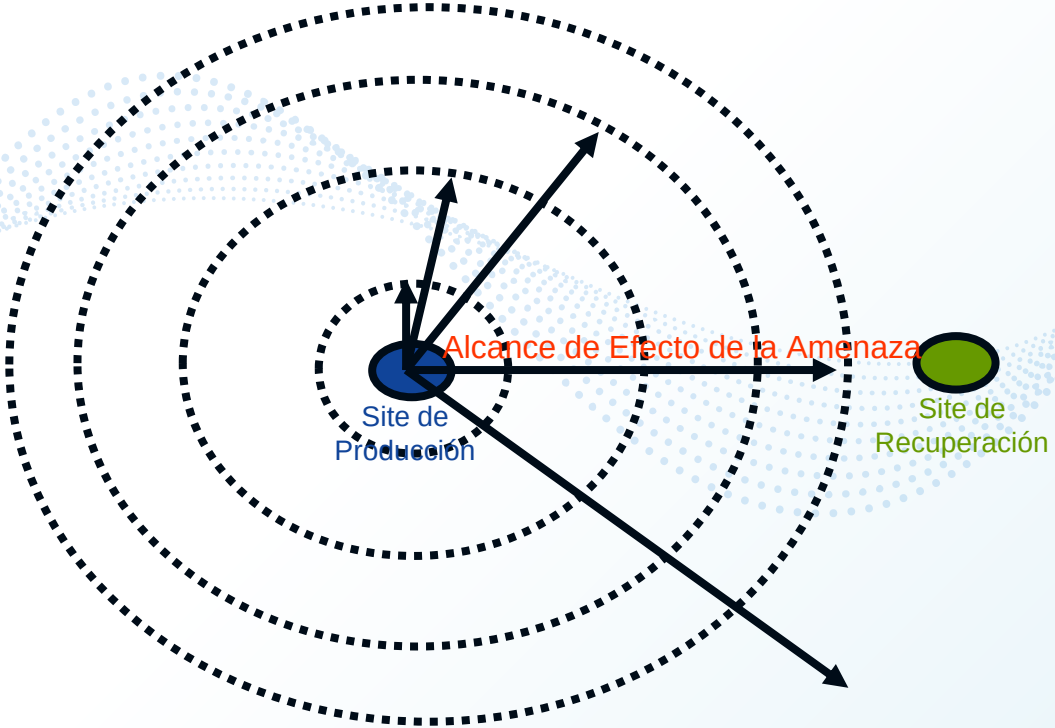


Recuperación de la red

Centro alterno de recuperación

- Distancia y alcance del efecto de desastre
  - El Alcance de Efecto del desastre puede ser tal que un área completa o aún varias ciudades sean afectadas
  - Por lo tanto se puede asumir que una gran distancia entre los “Sites” genera una mayor seguridad contra cualquier desastre de amplio alcance
  - Sin embargo, una gran distancia tiene su precio; esto es, el costo de interconexión, el esfuerzo y el costo de reubicación de la empresa, etc.

Determinar distancia entre Site de Producción y Site Recuperación



Alcance de efecto del riesgo

- El Alcance de Efecto del Riesgo significa:
  - La distancia a la cual, el Efecto del Riesgo puede generar cualquiera de los siguientes escenarios de desastre:
    - Destrucción
    - No acceso
    - Inutilización del sistema y/o oficinas
    - Falta de suministros o materias primas

Distancia correcta

- La distancia correcta pretende:
  - En primer termino (70% – 90% de importancia)
    - Hacer que se cumpla el propósito del site alterno que es que esté a salvo de los riesgos del site de producción
  - En segundo termino (10% – 30% de importancia)
    - Minimizar la logística de traslado de la capacidad de operación del site de producción al site de respaldo

Distancia correcta

- La distancia recomendable entre el site de producción y el site de recuperación puede ser expresada como:
  - Fuera del edificio
  - Fuera de la zona
  - +10 Kms
  - +50 Kms
  - +100 Kms
  - Fuera de la ciudad
  - Fuera del país
- Además, considerar:
  - Que el site de recuperación dependa de otra subestación eléctrica y
  - Que el site de Recuperación dependa de otro PoP (Point of Presence) del carrier de comunicaciones

Off-Site Storage

- Cualquier lugar físicamente convenientemente separada del site primario, donde se pueden almacenar registros vitales o duplicados (en forma impresa o en forma electrónica y/o equipo) para ser usados durante el proceso de recuperación.

- Convenientemente separada significa que las instalaciones de la bóveda externa deben estar a una distancia tal que evite ser afectada por el mismo desastre, local o regional, que afecta a las instalaciones donde se producen los registros.

Opciones para un Off-Site Storage

- Una oficina regional de la propia empresa u organización
- En alguna instalación, agencia o sucursal de la empresa
- En alguna oficina de otra organización o empresa
- En algún área comercial dedicada al almacenaje
- En un hot site
- En un cold site
- En una empresa especializada en Servicios de Almacenamiento Externo de Registros (Off-Site Storage Services)

Hot Site

- Uso inmediato y exclusivo de las Instalaciones
- No hay preferencias de acceso y/o uso
- Sistemas de cómputo totalmente operacionales
- Múltiples niveles de redundancia en redes
- Instalaciones robustas y seguras
- Soporte técnico especializado a la medida

Warm Site

Una sala o instalación de cómputo alterna con acondicionamiento eléctrico y ambiental la cual tiene preinstalado algún equipo periférico e interfaces de comunicaciones mas no el procesador central o servidores, los cuales, normalmente son los equipos más caros y que son indispensables para poder realizar la recuperación de los sistemas, aplicaciones y servicios que soportan los procesos de la organización

Cold Site

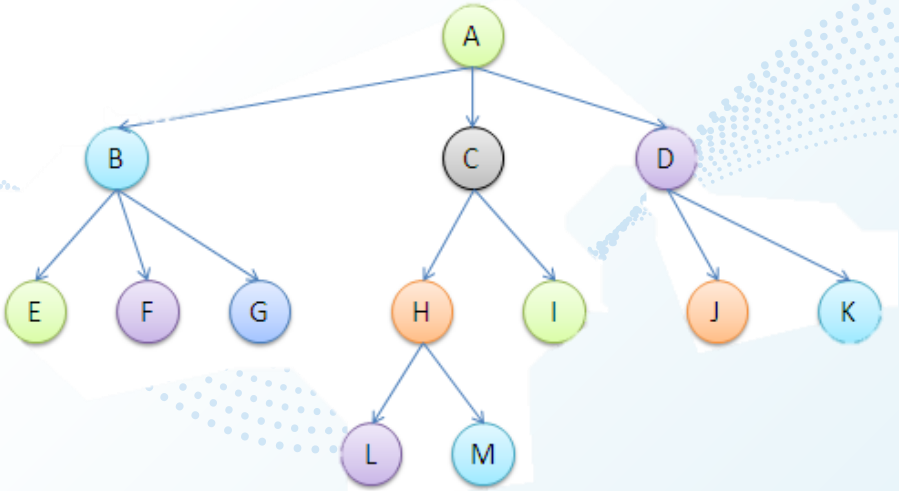
Una sala o instalación de cómputo alterna que cuenta con la infraestructura ambiental requerida para recuperar los sistemas, aplicaciones y servicios que soportan los procesos de la organización, pero que no tiene preinstalado ningún equipo de cómputo, equipo de telecomunicaciones ni Red, los cuales deberán ser proporcionados e instalados en la etapa del desastre.

Personal

- Se requiere personal capacitado para llevar a cabo el proceso de recuperación.
- Alternativas
  - Crisis Management Team
  - IT Recovery teams
  - Business recovery teams
  - Proveedores críticos
  - Otros (auditores, asesores, etc).

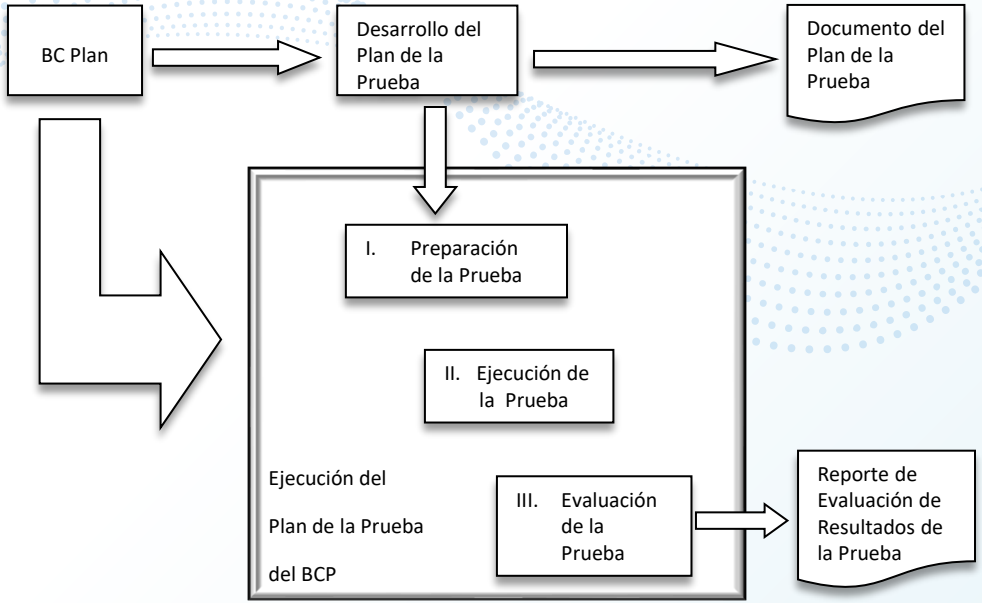
Directorio de notificaciones

Desarrollar un “Directorio” con nombres, números telefónicos y datos para su localización, de las personas a ser notificadas en el evento de un desastre, así como el “Árbol de Notificaciones” que indique quién es responsable de contactar a quién.



Pruebas

- **Sirven para estar seguros de que el Plan de Recuperación funciona cuando se necesita.**



Algunos tipos de pruebas

	Pruebas de Escritorio (check list)
	Walk Through
	Pruebas por fases (S.O., Comm, Aplicaciones DB´s Usuarios)
	Paralelo
	Simulación (transacciones)
	Full Interruption Test
	Prueba Sorpresa

Conclusiones

GENAP Tecnología

¡Gracias!

¿Alguna pregunta?

Favor de contactarnos

- Roberto.Gomez@genap.com.mx
- Ventas@genap.com.mx

ORACLE®

72