

CELAES 2015

XXX Congreso Latinoamericano de Seguridad Bancaria
Latin American Bank Security Conference

PANAMA • Octubre 15-16, 2015



Cómo gestionar y automatizar DRP&BCP

(Recuperación en casos de Desastres y Continuidad del Negocio)

16/10/2015



SAYQA

SOLUTION PARTNER

ORADOR

Liliana R. Mira

Ingeniera en Sistemas Informáticos



Con mas de 15 años de experiencia como Profesional en empresas correspondientes al Mercado Financiero/Bancario, Producción, Alimentos, Consultoras de Servicios y Laboratorios, ubicadas en la Región de Latinoamérica.

- Auditor Líder ISO9001 Gestión de Calidad certificada por el IRAM y IMQ de Italia.
- Risk Manager Certification ALARYS
- Experto DGQ en Seguridad Informática ISO-IEC 27001.
- Auditor de Sistemas según CISA/COBIT
- Team Member para análisis SCAMPI – CMMi (reconocido por SEI)
- ITIL V3, fundamentos y aplicación
- ***Mentora de la Metodología ePDM para la Automatización de BCP&DRP***

INICIO

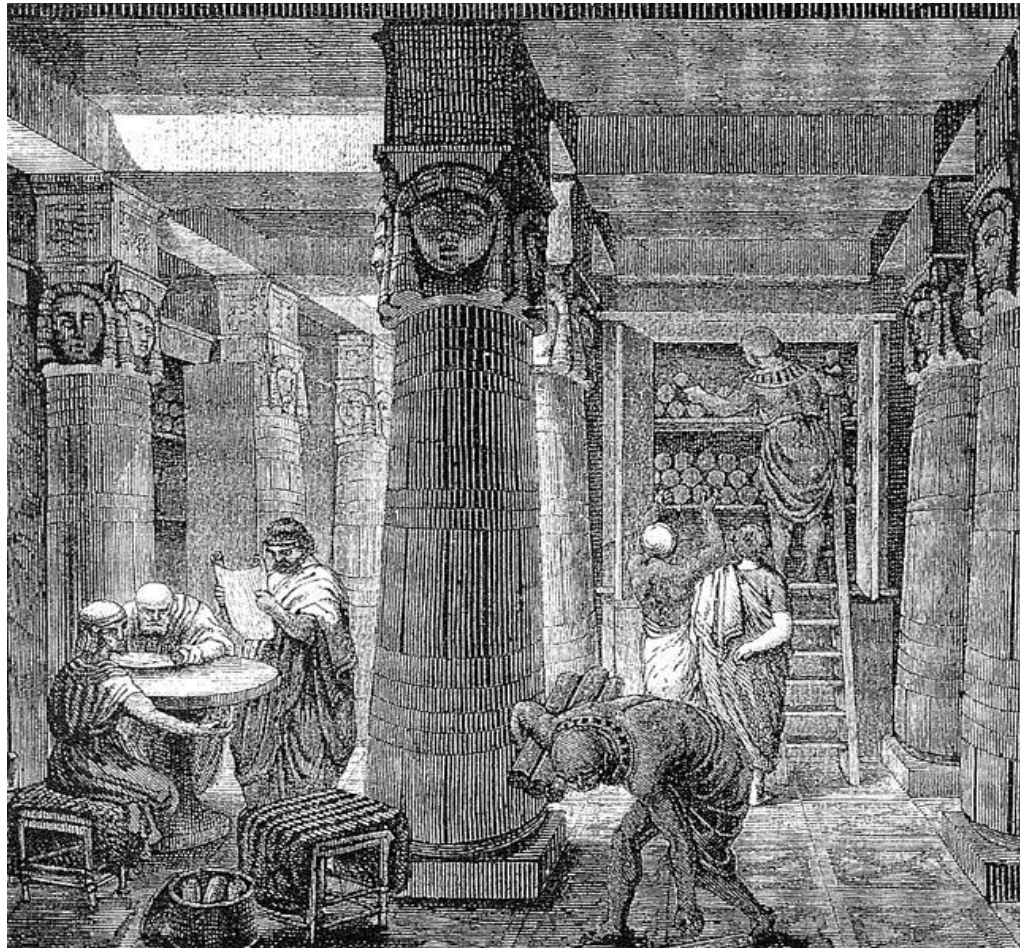
Tips → compartiré con Uds un resumen de los focos que sugerimos, desde experiencia en campo, a la hora de Gestionar y Automatizar un Proyecto de BCP&DRP.

La siguiente información tiene los derechos reservados de Software de Calidad SRL, No se puede distribuir y/o duplicar parte o total de la misma sin la autorización de Software de Calidad SRL.

BIBLIOTECA DE ALEJANDRIA

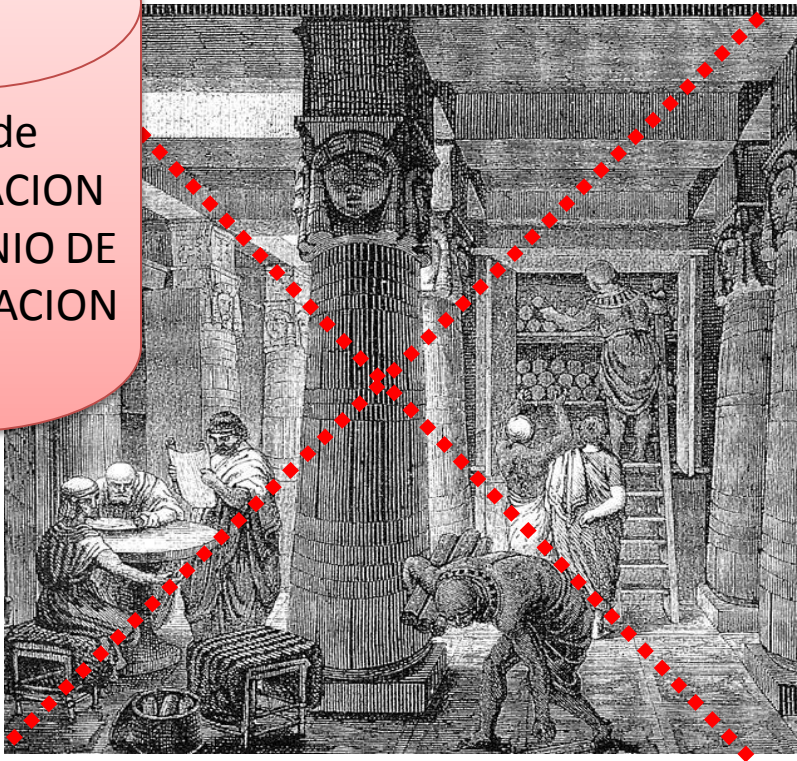
Hace 2000 años

- Trabajaron las mentes mas privilegiadas del mundo.
- Cerebro y la gloria de la sabiduría del Planeta.
- Toda la ciencia del Mundo antiguo.
- 1er instituto de Investigación que estudiaba el Cosmos. (1er Mapa de Constelaciones)
- Inicios de las Geometría, Literatura, Matemáticas, Astronomía, Medicina.
- Tenian Libros de Todas las culturas y lenguas.
- Llego a tener cerca de 1.000.000.- de Pergaminos.



Unas de las 1eras Bases en Contingencia

BASE de
INFORMACION
PATRIMONIO DE
LA CIVILIZACION



- Aristarco de Samos escribió el 1er libro con la teoría de que la tierra era un planeta mas que giraba alrededor del Sol y se tuvo que esperar mas de 2000 años para su redescubrimiento.

Si multiplicamos por 100.000 nuestro sentido de la perdidas podremos apreciar la Grandeza del logro de la civilización Clásica y la Magnitud de la tragedia de esta pérdida.

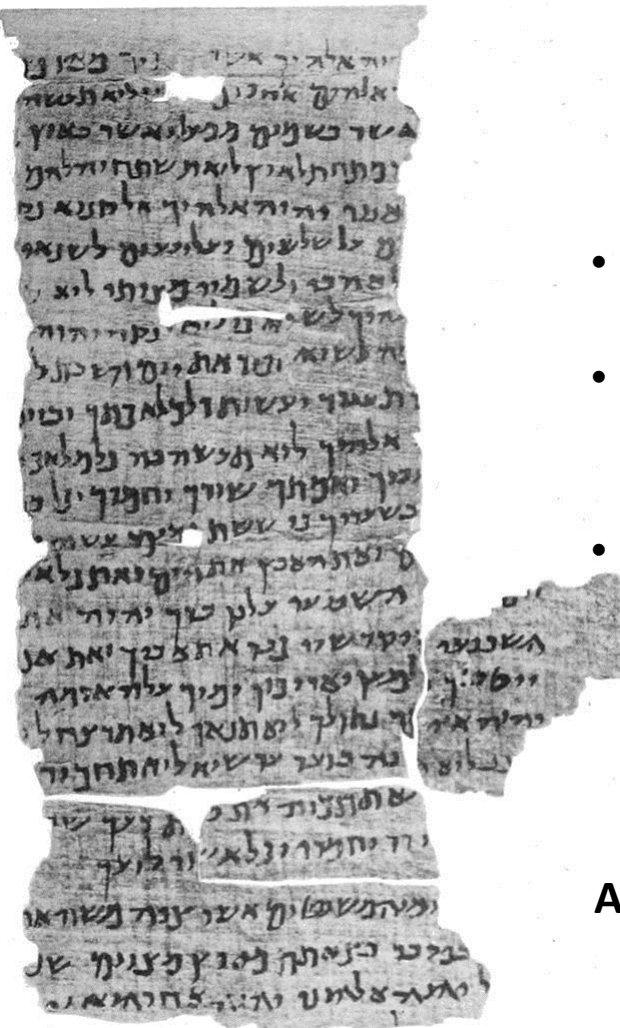
Existió una obra en 3 volúmenes del mundo, desde la creación hasta escrita por un Sacerdote **Beroso** de Babilonia.

Recién en el siglo XV Europa tuvo la Madurez para poder leer los escasos papiros que sobrevivieron a la destrucción de la Biblioteca.

RECONSTRUCCIÓN

- La primer base de información destruida
La biblioteca de Alejandría
- ¿Que hubiese pasado si la humanidad
no hubiese tenido que **redescubrir** parte
de la información ?
- Donde estaría hoy el punto de
evolución?

**Aun existen Lagunas Irreparables sobre el
conocimiento perdido**



Como vemos, los BCP y DRP, **no son un tema nuevo** pero así y todo en las empresas no se toma conciencia



- **Banco Mundial de Semillas de Svalbard** : "Bóveda del fin del mundo" La red de mas de 20 millones de semillas que están resguardadas esta diseñado para la mayor catástrofe de la tierra. La bóveda es impermeable a la actividad **volcánica**, **los terremotos, la radiación y la crecida del nivel del mar**, y en caso de fallo eléctrico, el [permafrost](#) (capa de hielo permanentemente congelada) del exterior actuará como refrigerante natural.

✓ **Madurez, la civilización aprendió de eventos.**

La tierra continua mas allá del humano.
La existencia del humano ocupa 1% del estimado total de la tierra

*Compartiendo Experiencias → camino a la
Automatización*

¿Cómo estaban las empresas ante los temas
de Contingencia?



Compartiendo Experiencias

1) Encontrar La Puerta



Encontrar al Referente



Compartiendo Experiencias

2) Arquitectura de procesos preparados para sostener la escalabilidad

Dpto 1

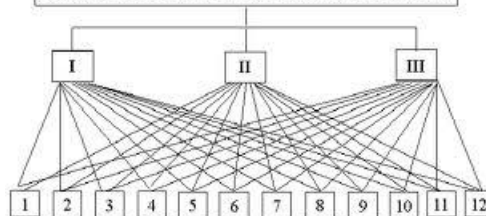
colaboradores

Dpto 2

Colaboradores

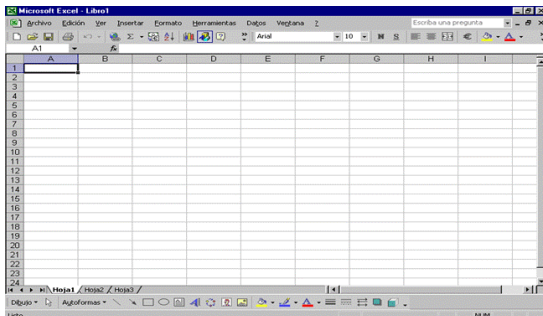
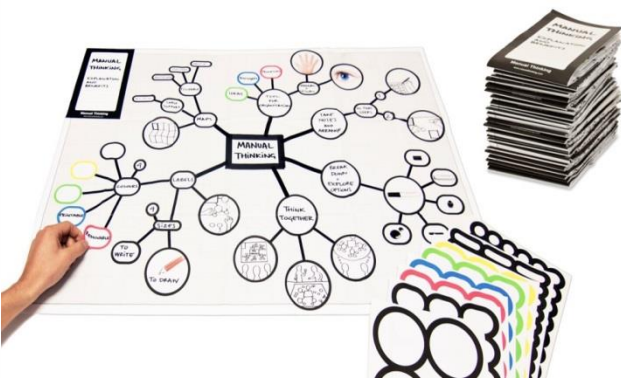


Establecer un orden secuencial para la mejora de procesos



Compartiendo Experiencias

3) Información Vs. Documentación



Compartiendo Experiencias

4) Exigencias Normativas + Escenarios cambiantes **VS** Adaptabilidad y cultura Interna.

¿Dónde ESTA UBICADO EL GESTOR/ES DE DRP,BCP?

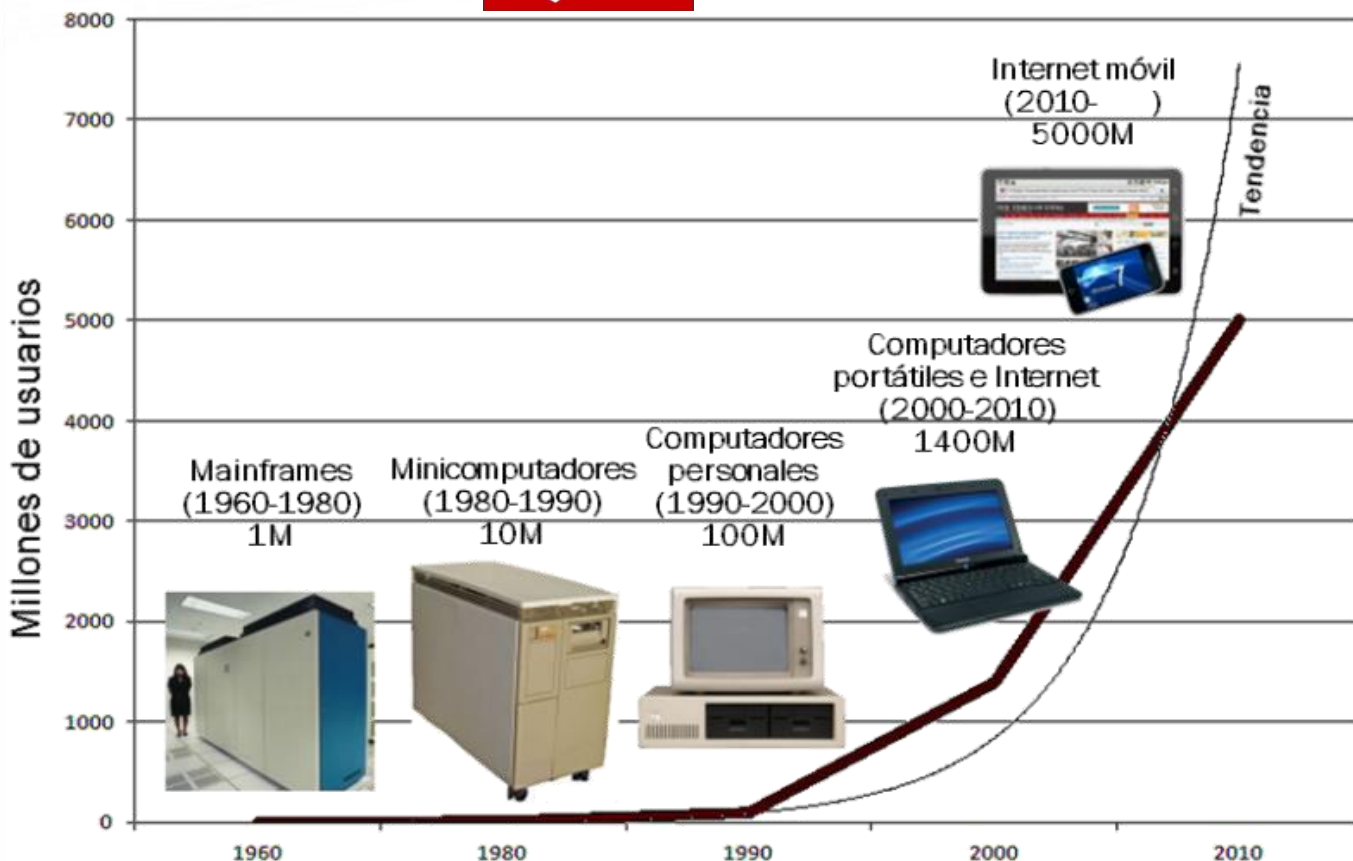


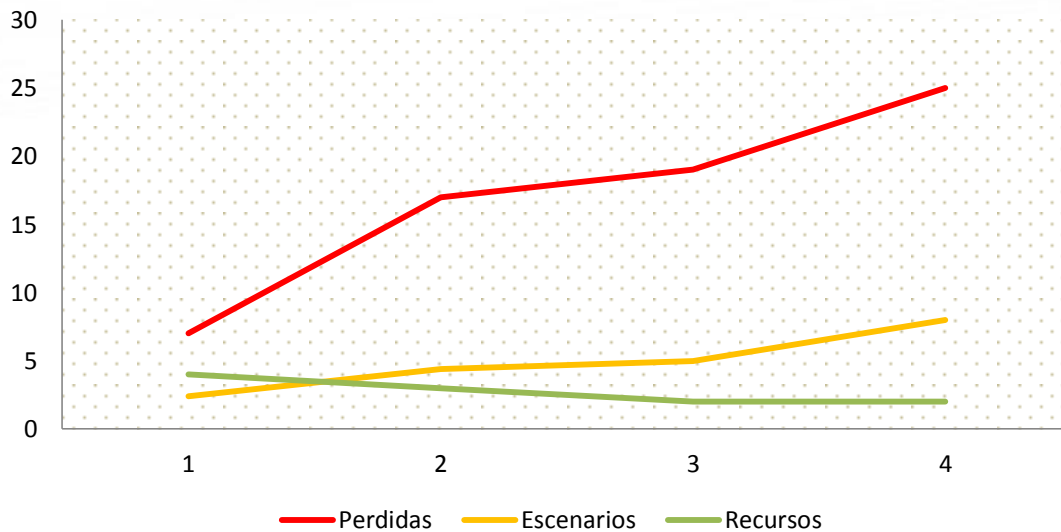
Compartiendo Experiencias

5) Evolución TI



Evolución de DRP, BCP ...BCM?



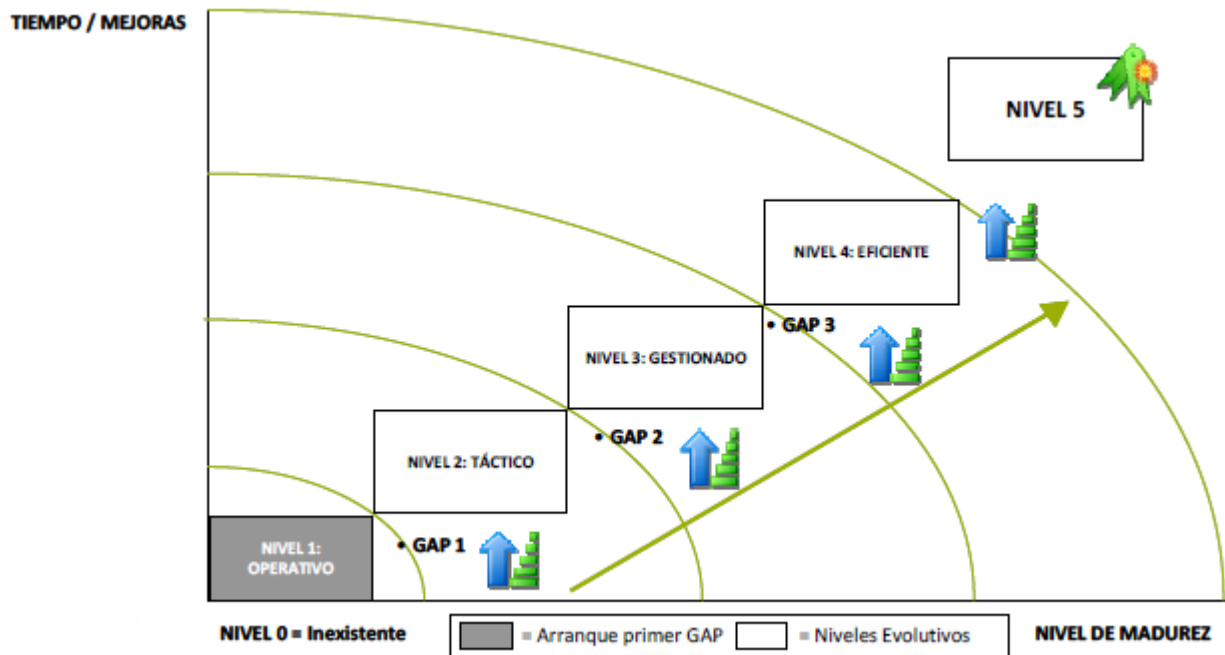


Escenarios variables con poco tiempo físico para reunir información → posibles incremento de Perdas

Con lo Observado , la pregunta fue:
¿ Como iniciamos la Gestión de los Planes BCP&DRP?



¿Cual es el nivel de sus planes?



| Nivel 1 - Analisis del Negocio | | |
|---|---------------------------------|---------------------------|
| Estrategia (obj. Operativos con el Negocio) | Factores Criticos del Negocio | |
| Nivel 2- Estrategia BCM | | |
| Estrategia BCM (Organizacional) | Estrategia BCM (Procesos) | Estrategia BCM (Recursos) |
| Nivel 3 - Diseño e Implementacion | | |
| Planes de Continuidad | Soluciones para la Recuperacion | Gestion de Crisis... |
| Nivel 4- construccion y elevar Cultura BCM | | |
| Programa de Difusion para aumentar la Cultura sobre BCM | Construccion | Entrenamiento de BCM |
| Nivel 5- Pruebas, matenimiento y Auditoria | | |
| Plan de Pruebas | Mantenimiento del BCM | Auditoria de Planes |
| Nivel 6- Program Management | | |
| Programa de Gestion (PM) | | |

TIPS 4x4 : ¿Cómo COMENZAR TUS BCP&DRP?

Extrínseco

1. Objetivos de los Planes
2. Apoyo Interno
3. Cultura Interna
4. Reglamentaciones

Intrínseco

1. ¿Qué tengo que proteger?
2. Amenazas
3. Herramientas
4. Hacer el Plan



TIPS : ¿Cómo COMENZAR TUS BCP&DRP?

Extrínseco

1. Objetivos de los Planes
2. Apoyo Interno
3. Cultura Interna
4. Reglamentaciones

Intrínseco

1. ¿Qué tengo que proteger?
2. Amenazas
3. Herramientas
4. Hacer el Plan



1-EXTRINSECO → Objetivos de los Planes



- Identificar cuales son los Objetivos:
 - ¿Son planes exigidos por Auditorias?
 - ¿Se necesitan porque hubo incidentes?
 - ¿La inestabilidad de los escenarios originó la necesidad de planes?
 - ¿Porque la empresa pertenece a un Grupo Internacional?
 -?

El éxito de un plan es la materialización gradual de sus objetivos

Entregable sugerido →

- Alcance de los planes
- Planificación del Proyecto
- Diseño e Implementación del Proceso de Gestión de Continuidad de Servicios de IT y del Negocio.

2-EXTRINSECO → Apoyo Interno



TIP 2 – APOYO INTERNO

Podemos tener la mejor idea, pero sin el respaldo Interno, iremos por un camino de desgaste.

La Empresa es un Organismo integrado que solo logra el Éxito con la Sincronización bajo un mismo Objetivo de cada uno de sus miembros Colaboradores.

Cláusula 5 - Liderazgo

La ISO 22301 hace especial hincapié en la necesidad de un liderazgo adecuado.

Entregable sugerido →

- Sponsor Principal de Alta dirección
- Id de Focal Point claves y
- Distribución de Roles y Funciones

3- EXTRINSECO → Cultura Interna



A veces decimos lo mismo de diferentes “maneras”

- Niveles de madures
 - ¿la Organización tiene cierta conciencia de los riesgos posibles?
 - ¿Se capacitó a los referentes claves con terminologías ?

Cuadro Componentes del Nivel 1 del Modelo de Kerzner
Nivel 1: Lenguaje Común

| Características | Obstáculos | Riesgos | Criterios de avance |
|--|---|---|---|
| <ul style="list-style-type: none"> • No existe apoyo de la alta gerencia • Existen pequeños grupos de interés en administración de proyectos; provenientes principalmente del área que manejan los proyectos de la organización • No se intenta reconocer los beneficios del administración de proyectos • El interés propio se antepone a los intereses de la organización • No existe inversión en capacitación y entrenamiento en el área de administración de proyectos | <ul style="list-style-type: none"> • Resistencia al cambio • Aparecen excusas tales como: <ul style="list-style-type: none"> ○ Lo hacemos mejor solos ○ No aplica para nosotros ○ No lo necesitamos | <ul style="list-style-type: none"> • Temor a una reestructuración organizacional • Temor a los cambios en los errores y responsabilidades • Temor a los cambios en las prioridades | <ul style="list-style-type: none"> • Iniciar entrenamiento y educación en administración de proyectos • Alentar el entrenamiento de profesionales certificados en administración de proyectos • Alentar a los empleados para que inicien a comunicarse en un lenguaje común de administración de proyectos • Reconocer las herramientas disponibles de administración de proyectos • Desarrollar un entendimiento de los principios de administración de proyectos |

3- Extrínseco → Cultura Interna

TIP 3 - CULTURA INTERNA

El siguiente cuadro es un resumen del modelo de evaluación de madurez con respecto a la Gestión del Riesgo.

| | Nivel 1 | Nivel 2 | Nivel 3 | Nivel 4 | Nivel 5 |
|---------------------------|---|---|---|--|---|
| | Proceso Inicial | Proceso Estructurado y Estándares | Proceso Institucionalizado y Estándares Organizacionales | Proceso Administrado | Proceso Optimizado |
| Gestión del Riesgo | No hay prácticas y estándares establecidos. La documentación es mínima y los resultados no son compartidos. La respuesta al riesgo es reactiva. | Los procesos están documentados se utilizan en proyectos grandes. La Administración se involucra consistentemente en los riesgos de los proyectos grandes y visibles. | Los procesos de gestión del riesgo son usados en la mayoría de los proyectos. Las métricas se utilizan para dar apoyo a las decisiones de riesgo al nivel de proyectos y programas. | La Administración está activamente involucrada en la gestión de riesgos de los proyectos al nivel organizacional. Los sistemas de riesgo están totalmente integrados con tiempos, costos y sistemas de recursos. | Los procesos de mejoramiento son utilizados para asegurar que los proyectos continuamente son medidos y manejados contra las métricas de rendimiento. |

Entregable sugerido →

- Evaluación de Cultura-Madurez con respecto al Proyecto BCP&DRP
- Plan de Acción según el nivel alcanzado vs. El requerido.

4- EXTRINSECO → Reglamentaciones



TIP 4 - Reglamentaciones

La normas y reglamentaciones son herramientas importantes de guía y apoyo, pero no indican el “como” llevar a la practica

Mejores Practicas de la industria para **Procesos de desarrollo BCP&DRP**
Exigencias Reglamentaria del **Negocio de su Empresa**

- Bancos, Financieras → Regulaciones de los Banco Centrales de su país, Basilea, CAMEL (Capital, Asset, Management, Earning and Liquidity)
- Objetivos de Certificaciones → ISO27001, ISO9001, Etc.
- Objetivos de Negocios → Certificaciones PCI (Security Standards Council)
- Etc.

Entregable sugerido →

- Alinear objetivos del desarrollo de los planes BCP&DRP con los Objetivos reglamentarios de su Empresa.

TIPS : ¿Cómo COMENZAR TUS BCP&DRP?

Extrínseco

1. Objetivos de los Planes
2. Apoyo Interno
3. Cultura Interna
4. Reglamentaciones

Intrínseco

1. ¿Qué tengo que proteger?
2. Amenazas
3. Herramientas
4. Hacer el Plan



1- INTRINSICO → ¿Qué tengo que Proteger?

TIP 1 – Activos

Identificar → activos de información de su Empresa, para ello se debe establecer qué es y qué no es un activo de información.



Entregable sugerido →

- Listado de Activos de la Información Clasificados.

2- INTRINSECO → Amenazas

Amenazas concretas o potenciales y no en un listado de Amenaza teóricas.

Una vez clasificados los activos de información permite conocer la sensibilidad al riesgo de cada uno e identificar los mas críticos y sobre ellos el mapa de posibles Amenazas.

Algunos pilares para la realización de la lista de Amenazas **no** teóricas:

- **Historia:** Gestión de incidentes, tipo de resolución del incidentes → se atendió la causa y/o el efecto?
- **Bajos presupuestos** → posible falla de mantenimientos → bajo **Calidad** → posibles incidentes.
- **Conocimiento experto**

Entregable sugerido →

- Listado de Amenazas posibles.



SAYQA

SOLUTION PARTNER



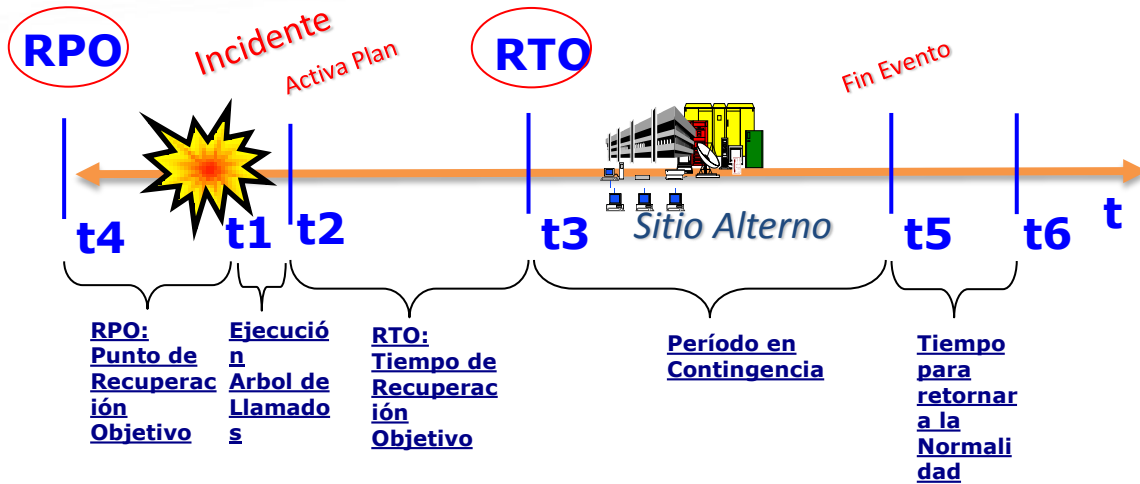
Unidades de Negocio

Unidades Operativas



Comité Administración de Crisis

Comité Continuidad de Negocio



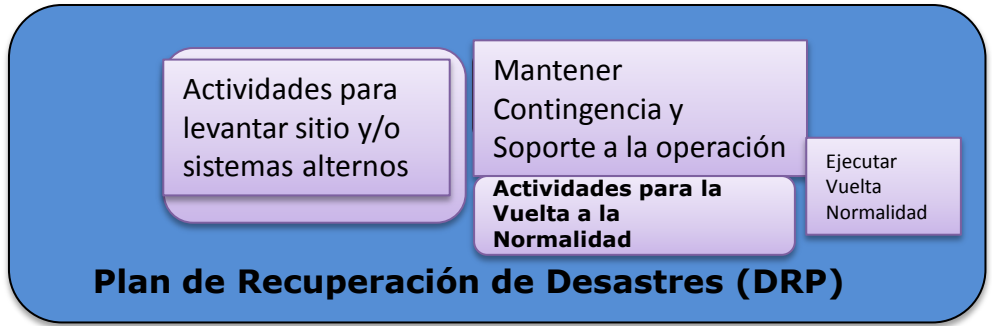
Tecnología

Administración

Auditoria

Comunicaciones

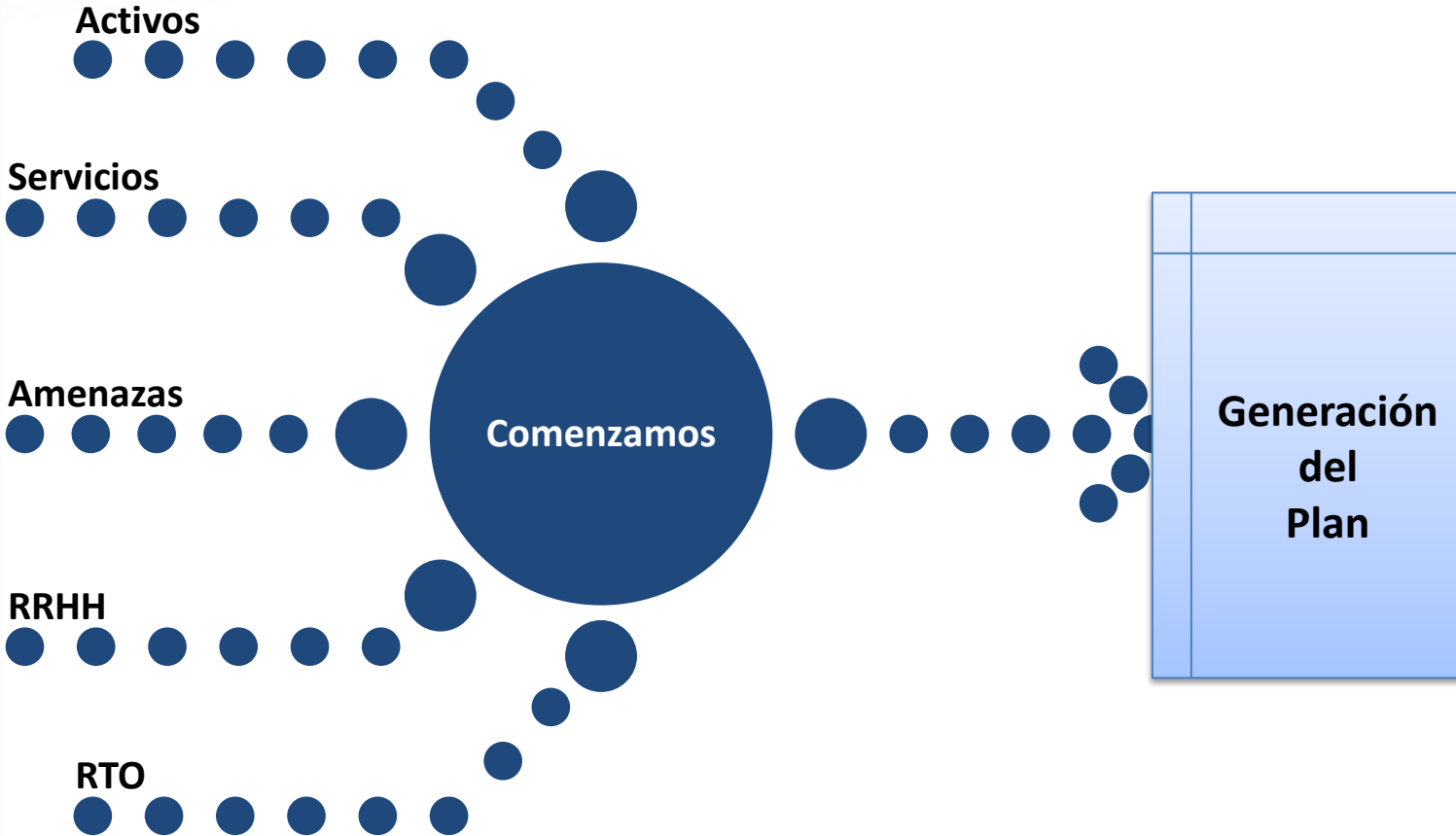
RRHH





Intrínseco → ¿Qué tengo que Proteger?

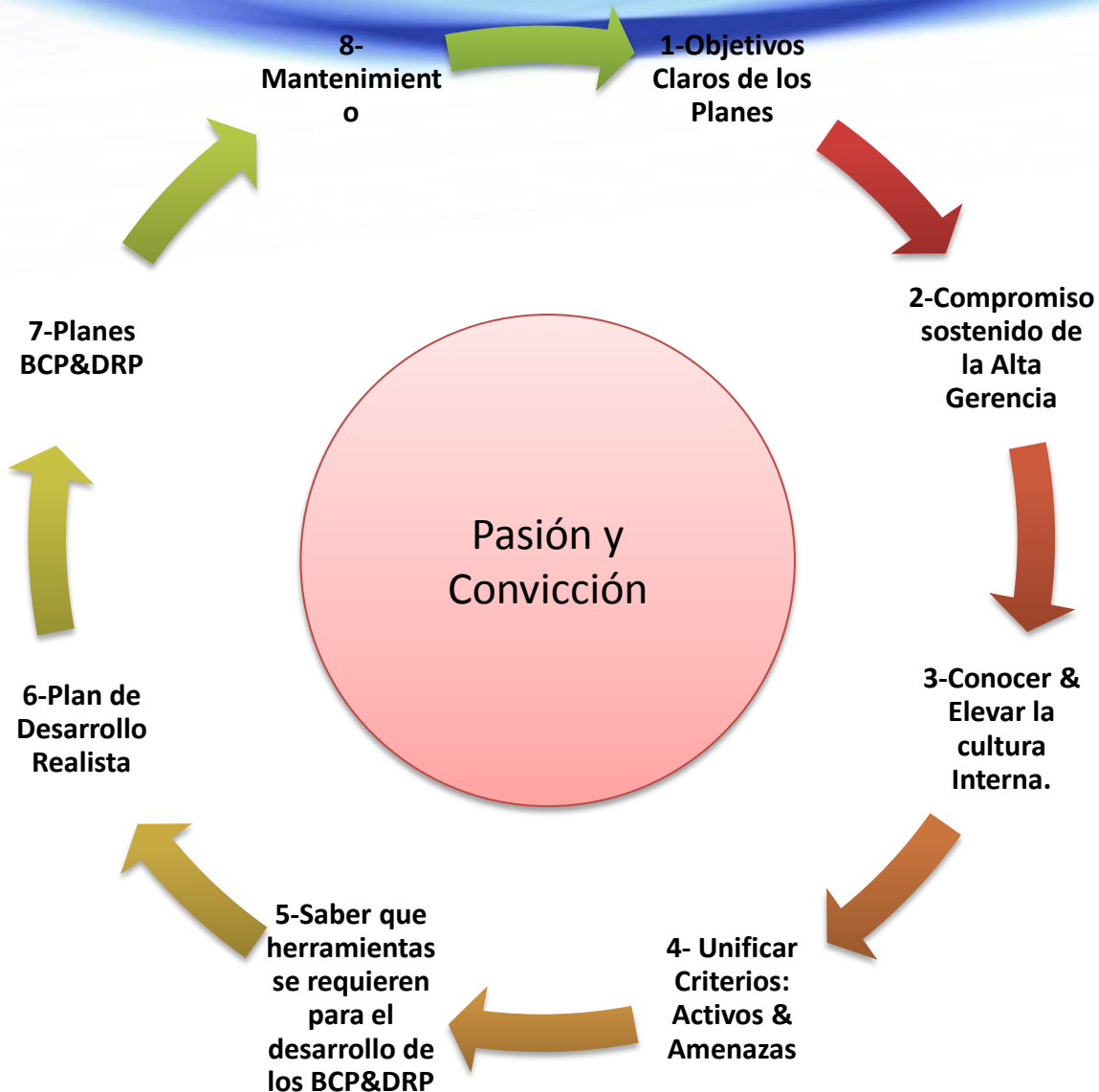
TIP 4 – Hacer el Plan



Intrínseco → ¿Qué tengo que Proteger?

TIP 4 – Hacer el Plan

- 1) Tiempo para la realización del plan
- 2) Tipos de Planes y su sincronización
- 2) Activos y amenazas
- 3) Tiempo de RTO y de Trabajo
- 4) Actividades por roles
- 5) Rollback
- 6) Lecciones Aprendidas
- 7) Plan de pruebas
- 8) Mantenimiento





¿Preguntas, Comentarios, Sugerencias?

2015

INVITACION A VER UN PLAN AUTOMATIZADO





MUCHAS GRACIAS POR SU PARTICIPACION

COMENTARIOS, DUDAS, CONSULTAS Y SUGERENCIAS A

soluciones@sayqa.com

info@sayqa.com



SAYQA

SOLUTION PARTNER