

Jornadas de Auditoria Interna

Septiembre 8, 2011

Plan de Continuidad del Negocio



Glosario

BCP - Business Continuity Planning (Plan de Continuidad del Negocio)

DRP - *Disaster Recovery Plan*

COOP - Continuity of Operations (Continuidad de las Operaciones)

BRP - Business Recovery Plan

COB - Continuity of Business (Continuidad del Negocio)

BIA - Business Impact Analysis (Análisis de Impacto en el Negocio)

RTO - Recovery Time Objective (Tiempo Objetivo de Recuperación)

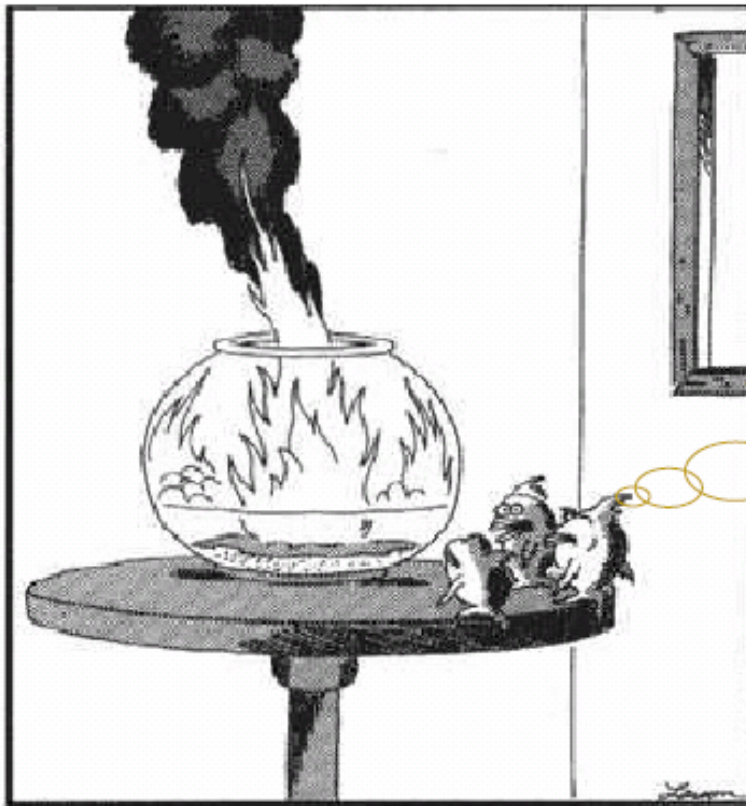
RPO - Recovery Point Objective (Punto Objetivo de Recuperación)

Que dicen los expertos?

- *“Dos de cinco empresas que han experimentado un desastre quedaron fuera del negocio en los siguientes cinco años. Los Planes de Continuidad y los servicios de recuperacion de desastres aseguran la viabilidad de la organización.”* Gartner (Roberta Witty, Donna Scott) - Disaster Recovery Plans and Systems Are Essential
- 72% de las organizaciones...
 - No cuentan con un Plan de Continuidad del Negocio;
 - Nunca o raras veces han probado el plan;
 - El plan cuando lo han probado ha presentado fallas;
 - Solo el 18% de los datos de las organizaciones están seguros ante eventos. □
- Fuente: VERITAS Disaster Recovery Survey

Planificación?

Muchos piensan como estos peces ...



Pudimos salir
planificadamente
del desastre

Y ahora que hacemos
??



Que es una Contingencia?

Es **una interrupción no planificada**, de duración indeterminada, que no puede ser manejada por procedimientos normales y que fundamentalmente, no afecta a todos los competidores.

Consecuencias



Quién se ocupa del tema?

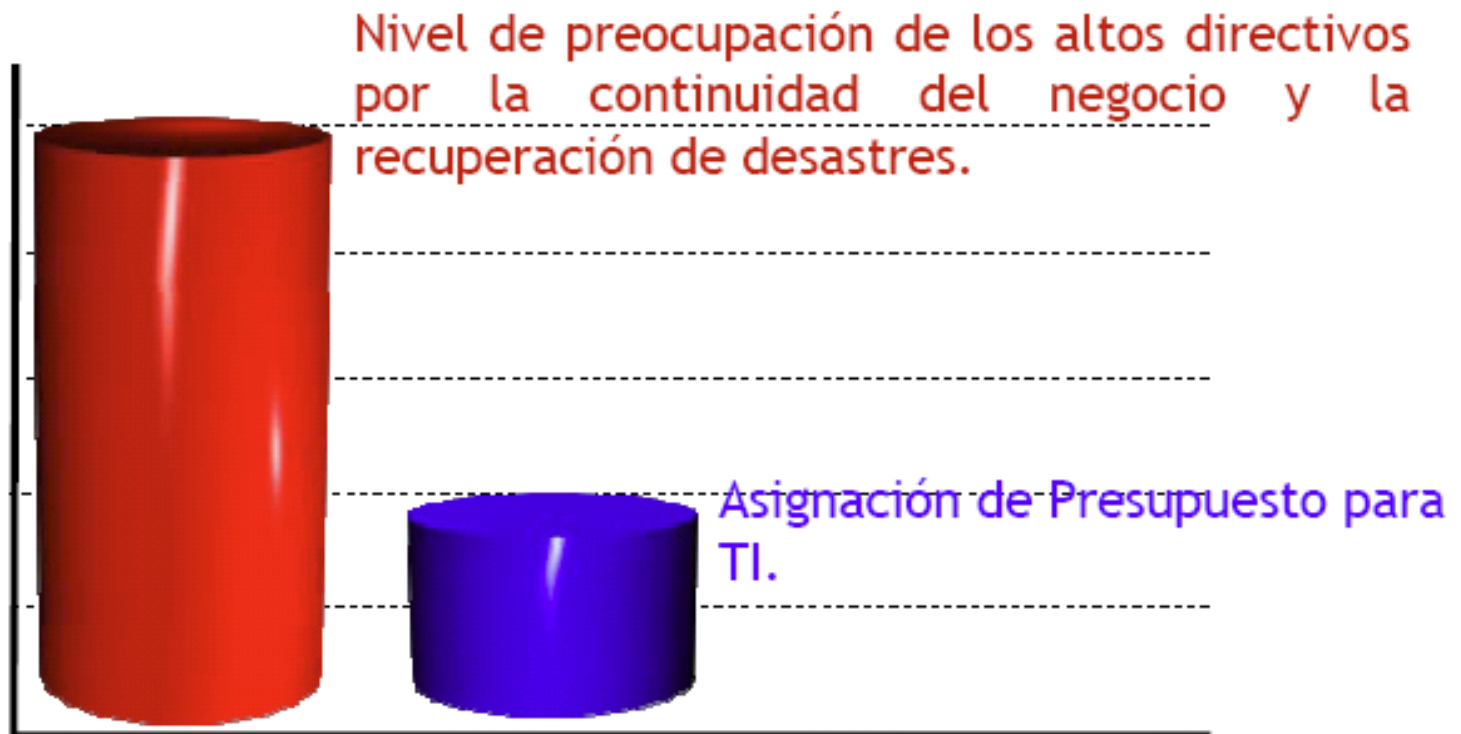
La continuidad del Negocio debe ser la **responsabilidad primaria de la Alta Dirección** para proteger los activos y la viabilidad de la organización, ante cualquier evento contingente que afecte a la misma.

DILBERT

By Scott Adams



Cual es el problema?



Fuente:
NOVELL

BCP-Continuidad del Negocio

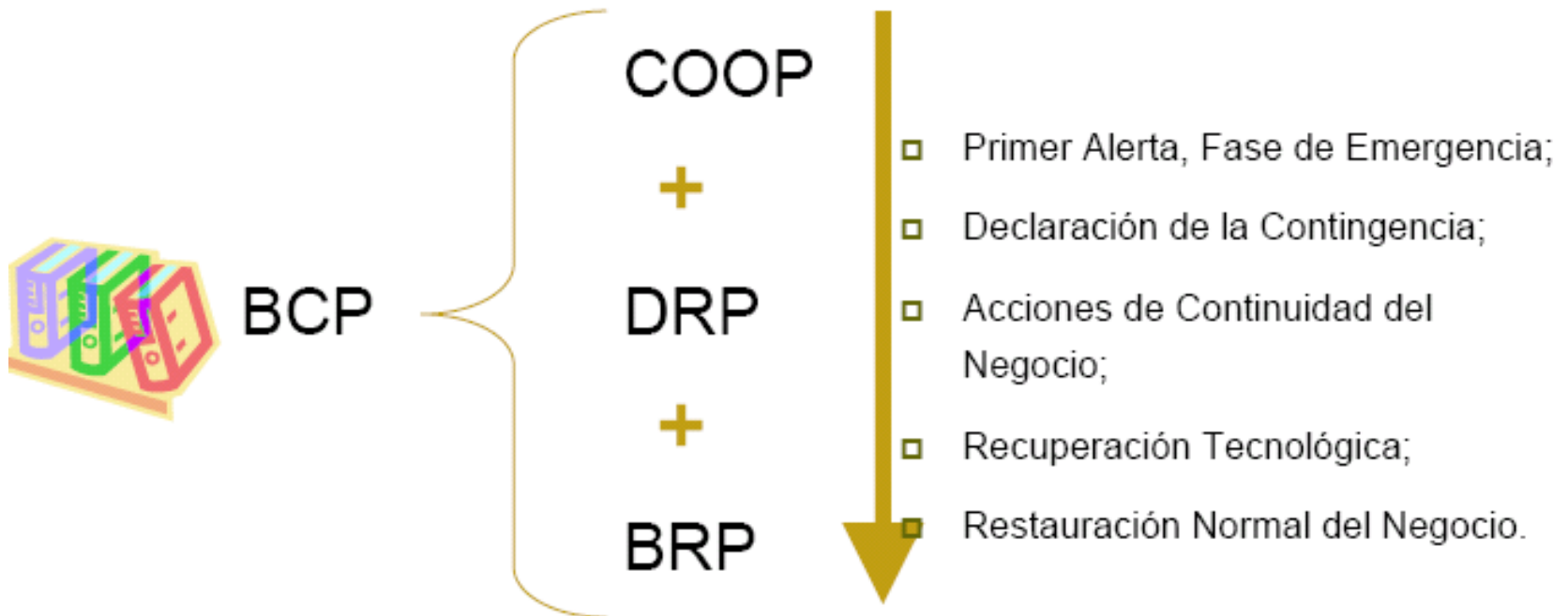
La planificación de la continuidad del negocio es un proceso diseñado para reducir el riesgo de la organización en una interrupción imprevista de sus funciones críticas, sean estas actividades manuales o automatizadas, y asegurar la continuidad de los servicios mínimos, además de:

Viabilidad de la
Organización

- La seguridad del personal;
- Minimizar la extensión de la interrupción;
- La rentabilidad y posicionamiento en el mercado;
- La Eficiencia en la atención de los clientes;
- La seguridad y confiabilidad de la información;
- Cumplir las responsabilidades contractuales;
- Cuidar la imagen y percepción pública;
- Atender el cumplimiento de regulaciones;
- Atenuar el impacto social;
- Minimizar el Riesgo Legal por litigios.



Como se compone la Continuidad?



- **Contingencia:** Para ser usada en circunstancias no anticipadas.
- **Continuidad:** Para continuar sin interrupción.

Plan de Continuidad

- Requisitos, planificación.
 - Estrategia de continuidad consistente con Objetivos de Negocio.
 - Proceso liderado por la Alta Gerencia.
 - Comprender los riesgos de la organización priorizando los procesos críticos.
 - Comprender y cuantificar el impacto de la interrupción.
 - Roles y responsabilidades claras.
 - Recursos suficientes aprobados.
 - Política de COB.



Plan de Continuidad

Objetivo del plan de continuidad

Su objetivo es **mantener operativas cada una de las funciones y áreas críticas** que han sido afectadas por los distintos **eventos que se hayan considerado de riesgo**. El Plan debe **considerar a la organización entera**, y no solamente al servicio de procesamientos electrónico de datos.

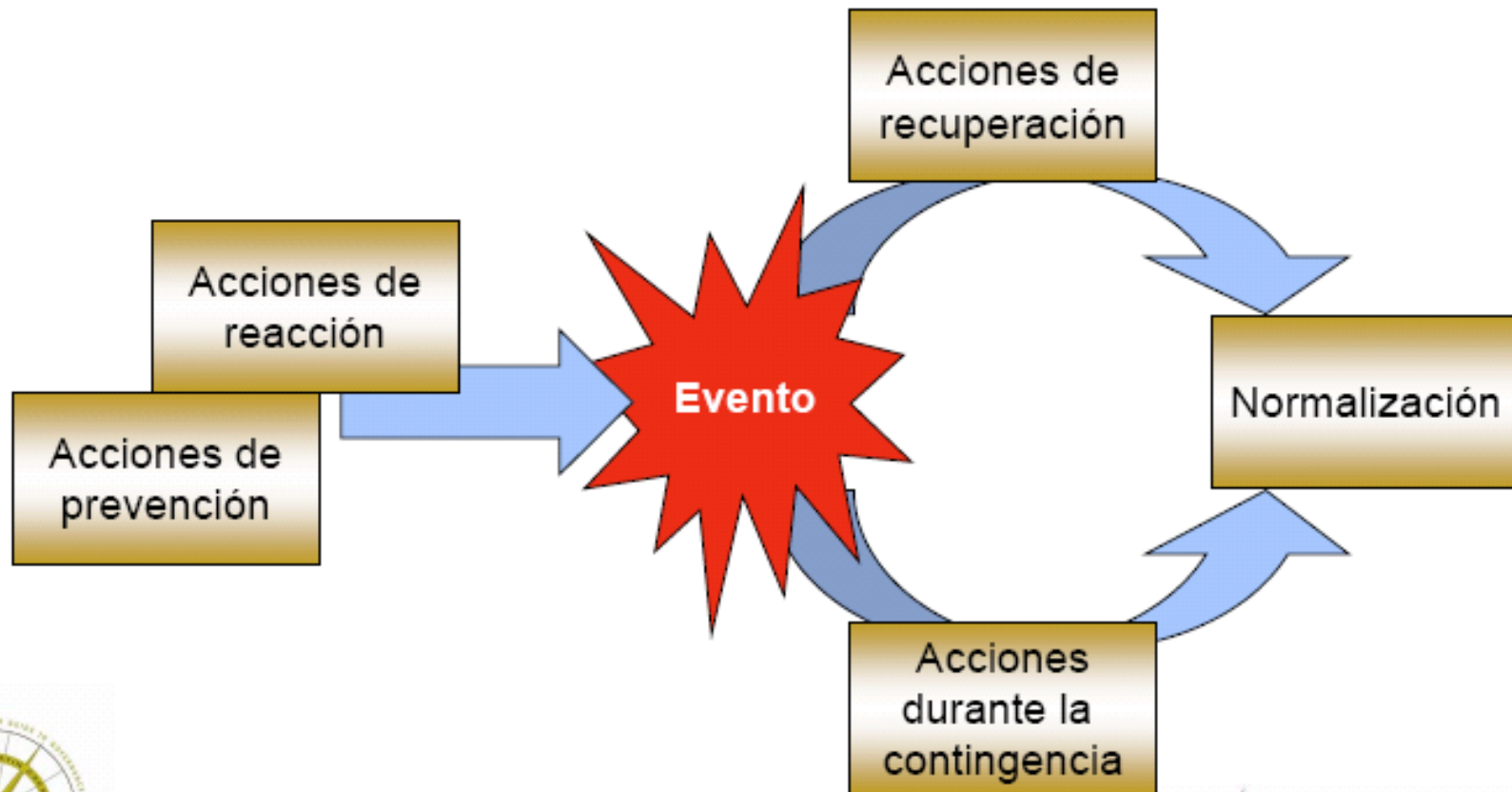


- ❑ Definir el objetivo primario del plan;
- ❑ Identificar riesgos, amenazas y escenarios;
- ❑ Determinar funciones críticas de negocio;
- ❑ Determinar aplicaciones críticas;
- ❑ Establecer prioridades de recuperación;
- ❑ Determinar estrategias de recuperación;
- ❑ Documentar los procedimientos alternativos;
- ❑ Evaluar recursos indispensables;
- ❑ Establecer criterios de prueba y mantenimiento;
- ❑ Definir el entrenamiento del personal involucrado;
- ❑ Documentar todo, no basarse en la mente.



¿ Qué planificar ?

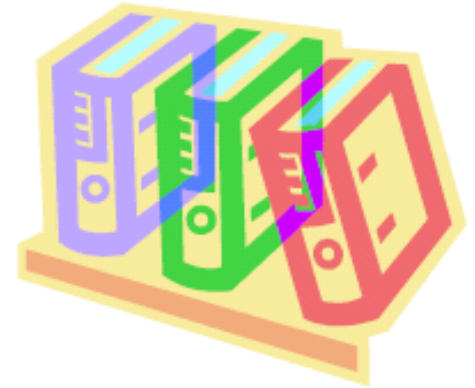
¿Qué hacer ante la ocurrencia de un evento?



Políticas y Documentos

- Políticas de Apoyo

- Política de Seguridad Física y responsable.
- Política de Respaldo. Custodia y acceso.
- Política de COB.
 - Estrategias de continuidad en un desastre (off site, remoto).
 - Duración de los escenarios short, medium, long.
 - Valores de priorización: crítico, necesario, importante.
 - Roles y responsabilidades.
 - Documentación, revisión y pruebas del plan.
 - Tipos de prueba. Control de Cambios.
 - Entrenamiento y comunicación.



- Roles

- Equipo de manejo de crisis (CMT-Crisis Management Team). Comunicaciones Públicas.
- Responsables de seguridad física, oficial bombero, resp
- Oficial de Continuidad.
- Coordinadores en cada sector. Gerencia Ejecutiva.
- Soporte infraestructura, comunicaciones.
- Soporte de proveedores.



Orientación al Negocio

- Plan de Manejo de Crisis – Definiciones estratégicas
 - Definición del equipo de Manejo de Crisis
 - Arbol de llamadas (Call Tree) y Command Center.
 - Contención. ***Plan de Evacuación.***
 - Estrategia de Continuidad. Procesos Críticos.
 - Niveles de Servicio y su tiempo.
 - Recursos mínimos.
 - Finalización de la contingencia y vuelta atrás.
 - Gestión del impacto residual.



Riesgos e Impactos

- Impacto en el Negocio (BIA)
 - Potenciales riesgos y su probabilidad de ocurrencia.
 - Distintos escenarios. Short, medium y long term.
 - Impacto de los riesgos, severidad.
 - Tipos de impacto. Cuantitativo y cualitativo.
 - Recovery Time Objective, Point Objective.
 - SLA Tecnología.
 - Gap Análisis. Estrategia.



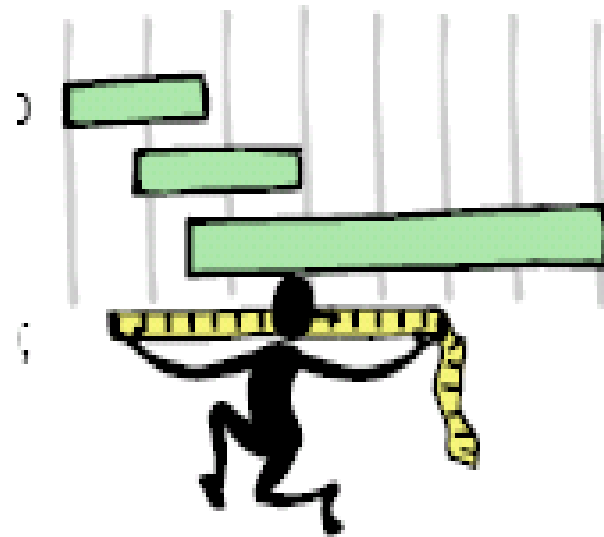
Tiempos?

Recovery Time Objective: el tiempo que el Negocio define deben estar recuperados los procesos para no incurrir en pérdidas.

¿Cuál es la tolerancia sin servicio?

Recovery Point Objective: momento anterior a la contingencia hasta el cual se pueden recuperar los datos y procesos.

¿Qué tan recientes deben ser los datos?



En función de estos tiempos, la priorización de recursos del BIA y la priorización de procesos por el Negocio, se define el orden de recuperación.

Impactos

Consideraciones sobre el impacto

Tangibles

- La pérdida de rédito;
- Los incumplimiento de contratos;
- Las multas impuestas;
- Los pagos extras;
- La compensación por cese;
- La degradación del valor de mercado; ...



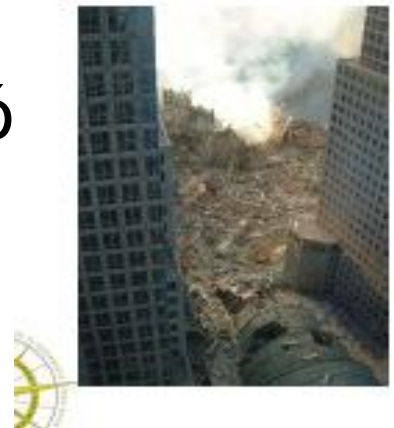
Intangibles

- La reputación;
- La imagen y permanencia ;
- La cuota del mercado;
- La confianza de los clientes;
- La retención de los empleados;



Planes de Continuidad

- Contenido del Plan - PDCA
 - Declaración, alcance (COOP).
 - Comunicación y responsables.
 - Contención.
 - Traslado y ubicación en el off site.
 - Implementación de las estrategias.
 - Recuperación del sitio primario (BRP).
 - Mitigación del Riesgo (DRP).
 - Mantenimiento y monitoreo de la contingencia.
 - Fin de la contingencia. Comunicació inversa.
 - Lecciones aprendidas.
 - Mejoras del Plan.



Sobrecarga, Controles y Costos

En caso de tener que activar procedimientos manuales de continuidad, se deberá tener en cuenta la ventana de tiempo en la cual se podrán realizar las tareas sin causar inconvenientes por sobre carga de tareas y su posterior re-ingreso cuando la tecnología se normalice.



Día 1



Día 2



Día 3



Día 4



Comunicación del Plan

Self Explanatory

Para conocer qué se debe hacer en el momento de la contingencia, el plan de continuidad del negocio debe ser conocido por todo el personal clave y responsable de accionar ante los distintos eventos que ameriten su utilización.



ISO IEC 27000 Family

- Antecedentes – British Standard (BS) 25999, parte 1 y 2
- 27001 Requisitos – Anexo A (Normativo)
- A.14 Gestión de la Continuidad del Negocio
- 27002 Buenas Prácticas
- 14 Gestión de la Continuidad del Negocio
- 14.1 Aspectos de SI en la gestión de la continuidad.



Otras normas ISO



ISO/IEC JTC 1/SC27 **N5726**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Text for NP Ballot

TITLE: New Work Item Proposal on ICT readiness for business continuity (27031)

SOURCE: Secretariat JTC 1/SC27

DATE: 2007-06-19

PROJECT:

STATUS: In accordance with resolution 32 (contained in SC27 N5939) of the 19th SC27 Plenary meeting held in St. Petersburg, 2007-05-11/12, this document is circulated to the SC27 National Bodies for a 3-month NWI letter ballot and to JTC 1 for a concurrent review.

P-Members of SC27 are requested to submit their votes on this document via the ISO e-balloting application by **2007-09-19**.

- ISO 27031 – Readiness for Business Continuity, comité SC 27
 - Orientada a prácticas de IT, publicada.
- ISO 22301 – Seguridad de la Sociedad – Continuidad de Negocio, comité Social Security
 - Deriva de la BS 25999, aún en inglés.

Estamos preparados?

Finalmente no nos encontremos así

...



Referencias

- A Primer for Disaster Recovery Planning in an IT Environment. Charlotte J. Hiatt.
- Building a Comprehensive Disaster Recovery Plan. Info-Tech Research Group.
- Business Continuity & Disaster Recovery for Dummies - Gregory A. Gilbert.
- Business Continuity Planning Methodology. Akhtar Syed, Afsar Syed.
- Business Continuity Planning: A Step-by-Step Guide. Third Edition. Kenneth L. Fulmer, Philip Jan Rothstein.
- Business Continuity: Best Practices - World-Class Business Continuity Management, Second Edition. Andrew Hiles.
- Control Objectives for Information and related Technology - ISACA.
- Contingency Planning and Disaster Recovery: Protecting Your Organization's Resources. Janet G. Butler, Poul Badura.
- Disaster Recovery Handbook. Michael Wallace, Lawrence Webber.
- Disaster Recovery Planning: Strategies for Protecting Critical Information
- ISO IEC 27001 y 27002
- FDIS ISO/IEC 24762 Guidelines for ICT Disaster Recovery Services
ISO/IEC JTC 1/SC 27New Work Item Proposal

Preguntas?

- Muchas Gracias

Ing. Cristina Ledesma, CISA, CISM,

- CRISC, ISO 27001

- Maria.cristina.ledesma
- @gmail.com



Reflexión vigente...

“Sabíamos de algunas debilidades que habíamos superado.

Adicionalmente, teníamos un buen entendimiento de algunas debilidades que habíamos determinado.

Lo que realmente nos ha perjudicado, son las debilidades que no sabíamos que teníamos.”

Declaraciones de Donald Rumsfeld, Secretario de Defensa de los Estados Unidos a CNN, Jueves 13 de septiembre de 2001.