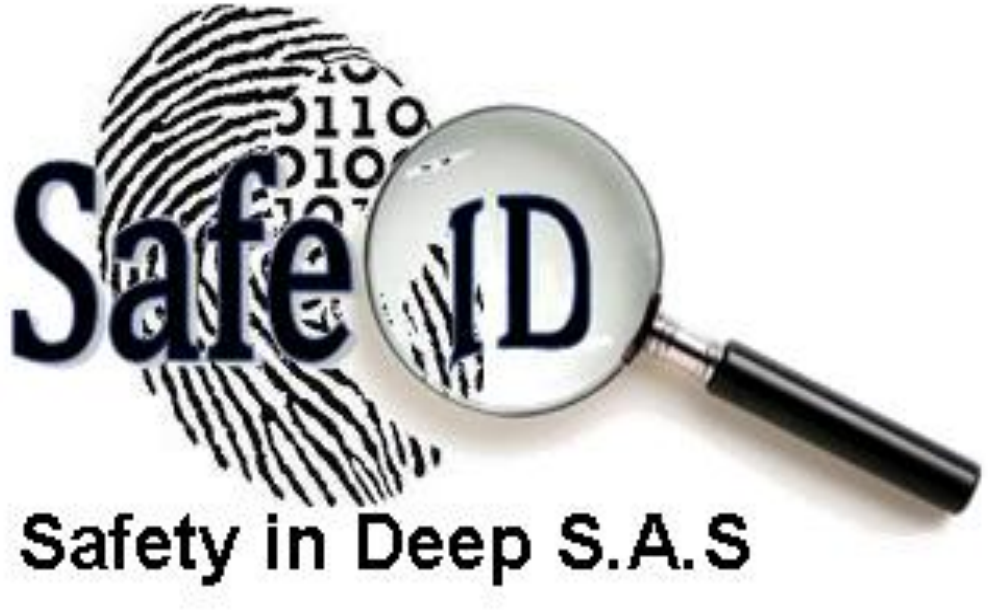


ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS

TENDENCIAS EN CONTINUIDAD DEL NEGOCIO

HOJA DE VIDA CONFERENCISTA

RAMIRO MERCHAN PATARROYO
Ingeniero de Seguridad - SAFEID

•Formación profesional

•Certified Information Security Manager (CISM), ISACA, 2016
•Especialista en Seguridad Informática, Universidad Piloto de Colombia, 2016
•ISO 27001 LA – SGS, Bogotá, Julio de 2015
•ISO 22301 IA – SGS, Bogotá, Junio de 2014
•Certified Business Continuity Planning (CBCP) – Disaster Recovery Institute, 2004
•Certified Information Systems Auditor (CISA), ISACA, 2000.
•Especialista en Desarrollo de software de redes, Universidad de los Andes (1997).
•Ingeniero de Sistemas, Universidad Distrital Francisco José de Caldas (1995)

•Experiencia profesional

• + 20 años de experiencia profesional continua en proyectos de seguridad, control y auditoria de sistemas
•Consultor especialista en continuidad del negocio y seguridad de la información

Agenda

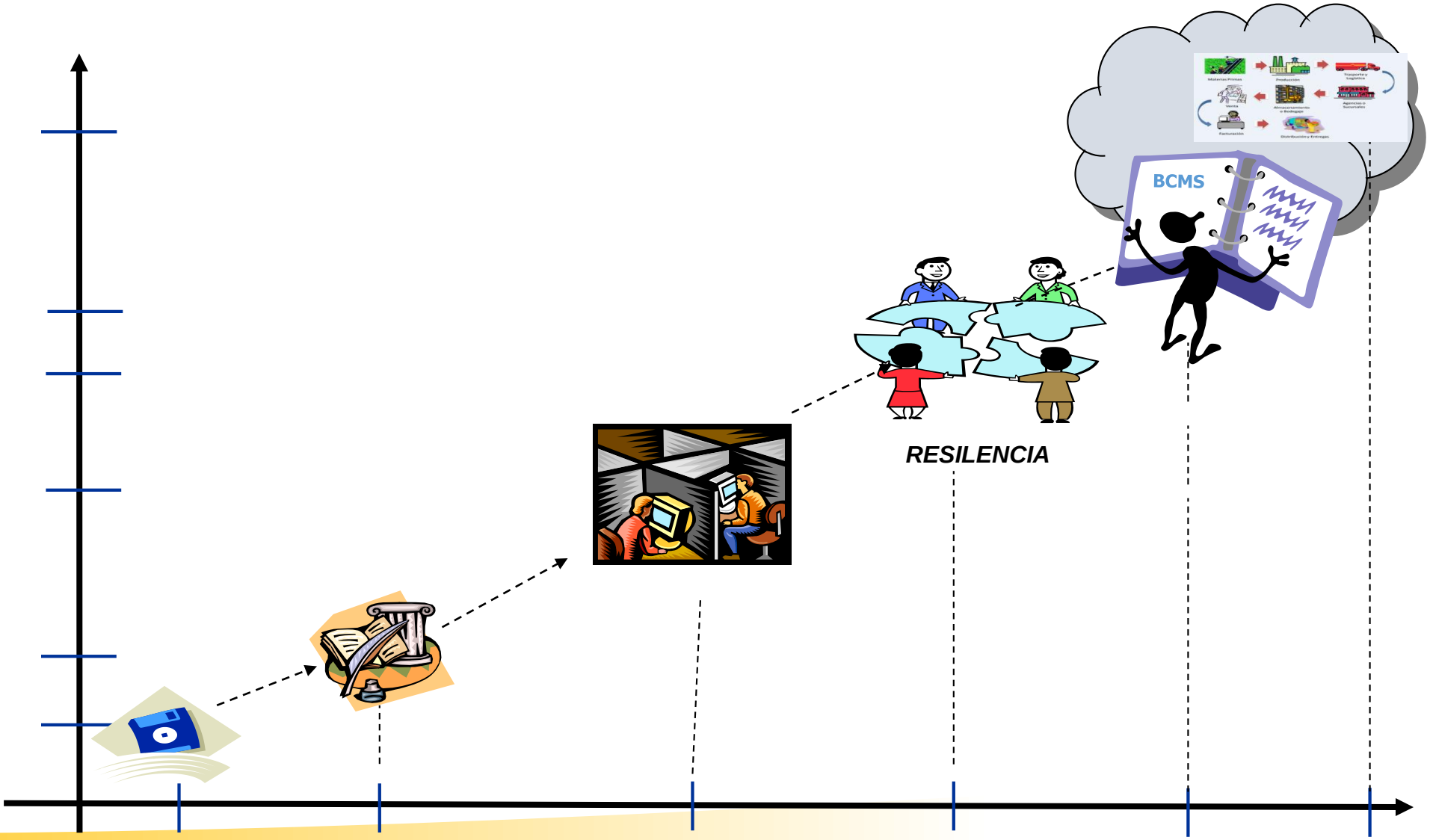
- Predicciones DRI para 2017
- Evolución de conceptos en BCP
- Tecnologías emergentes y su impacto en el BCP
- Una aproximación a un nivel de madurez promedio
- Camino a seguir
- Retos

Safe ID
Safety in Deep S.A.S

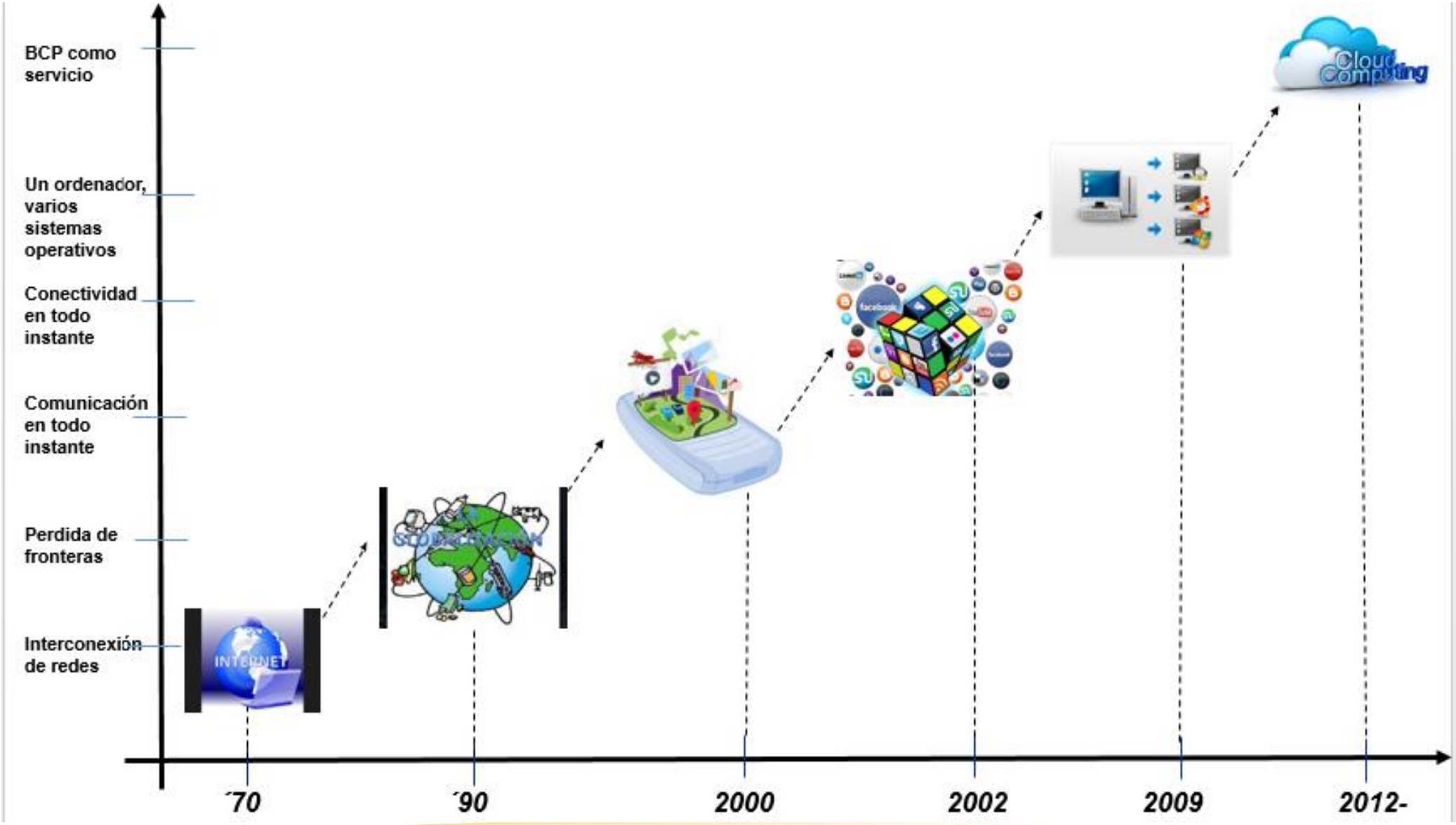
DRI 2017 Global Risk and Resilience Survey

1. Incremento de la colaboracion entre sector público y privado para compartir información de manera segura (6/10)
2. Al menos una compañía internacional colapsará o sera rescatada de la bancarota debido a fallas de la cadena de suministro (6/10)
3. Se presentará un ataque en sectores populares de una capital de occidente (10/10)
4. Las inundaciones seran el sintoma más evidente del cambio climático, incluso en zonas donde nunca se han presentado (10/10)
5. Mayor proactividad de las empresas privadas en fortalecer sus defensas frente a ciberataques y el terrorismo (7/10)
6. La Eurozona no collapsara pero su moneda perdera valor frente al dólar (5/10)
7. Se presentará un desastre natural grave en ASIA (8/10)
8. Se presentará una falla en servicios prestados por el gobierno , tales como asistencia social o infraestructura crítica, lo cual derivara en disturbios civiles graves. (8/10)
9. Decisiones sobre la cadena de suministro hara que grandes empresas incremente las adquisiciones y fusiones (5/10)
10. La gestión de riesgos se consolidará y agrupara otras áreas donde la “resiliencia” es fundamental (5/10)

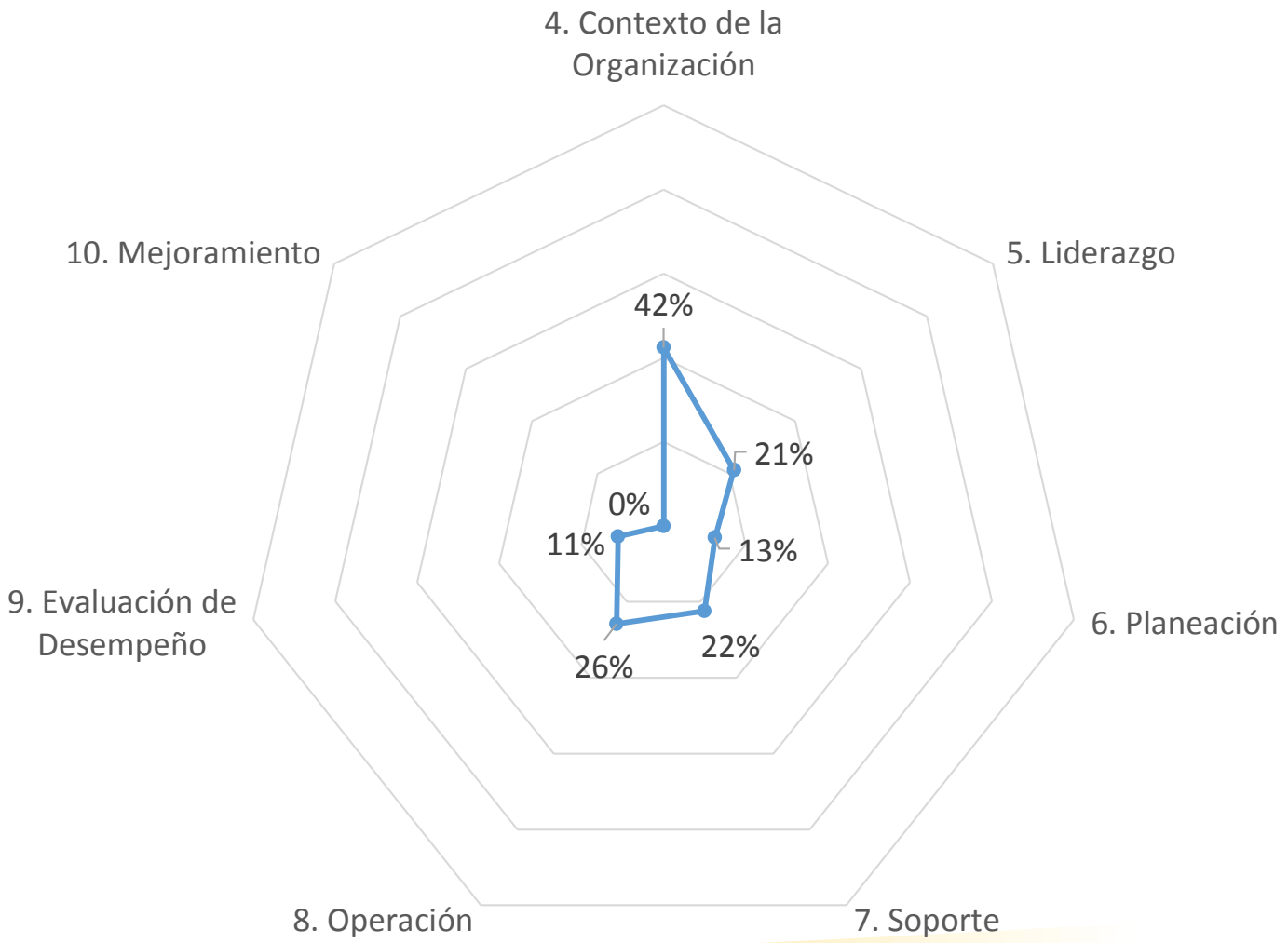
EVOLUCION DE LOS CONCEPTOS DE CONTINUIDAD DEL NEGOCIO



TECNOLOGIAS EMERGENTES



Un ejemplo de madurez en en SGCN - ISO 22301:2012



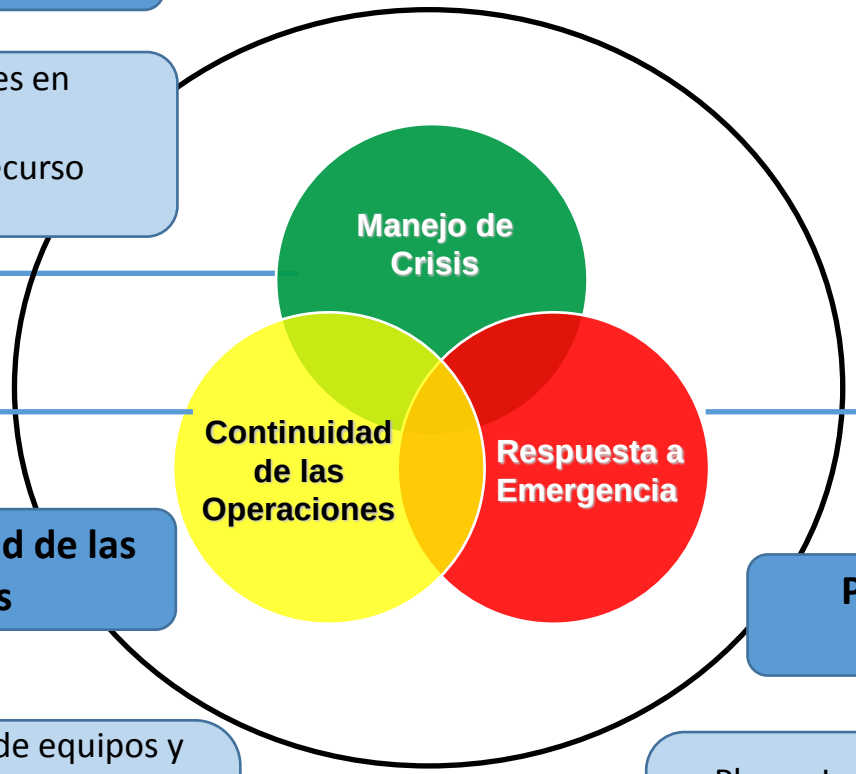
Camino a Seguir

- Comprender que es continuidad del negocio
- Definir un marco de trabajo
- Entender que nos puede pasar durante una interrupción
- Organizar los equipos de trabajo
- Comprender el alcance de las estrategias
- Prepare la gestión de crisis
- Simulacros y ejercicios

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Plan General de Manejo de Crisis

- Plan de Comunicaciones en Crisis
- Plan de Asistencia al recurso humano



Plan de Continuidad de las Operaciones

- Planes de Contingencia de equipos y obras civiles de sedes.
- Planes de continuidad de procesos de la organización
- Plan de Recuperación de Desastres (TIC)

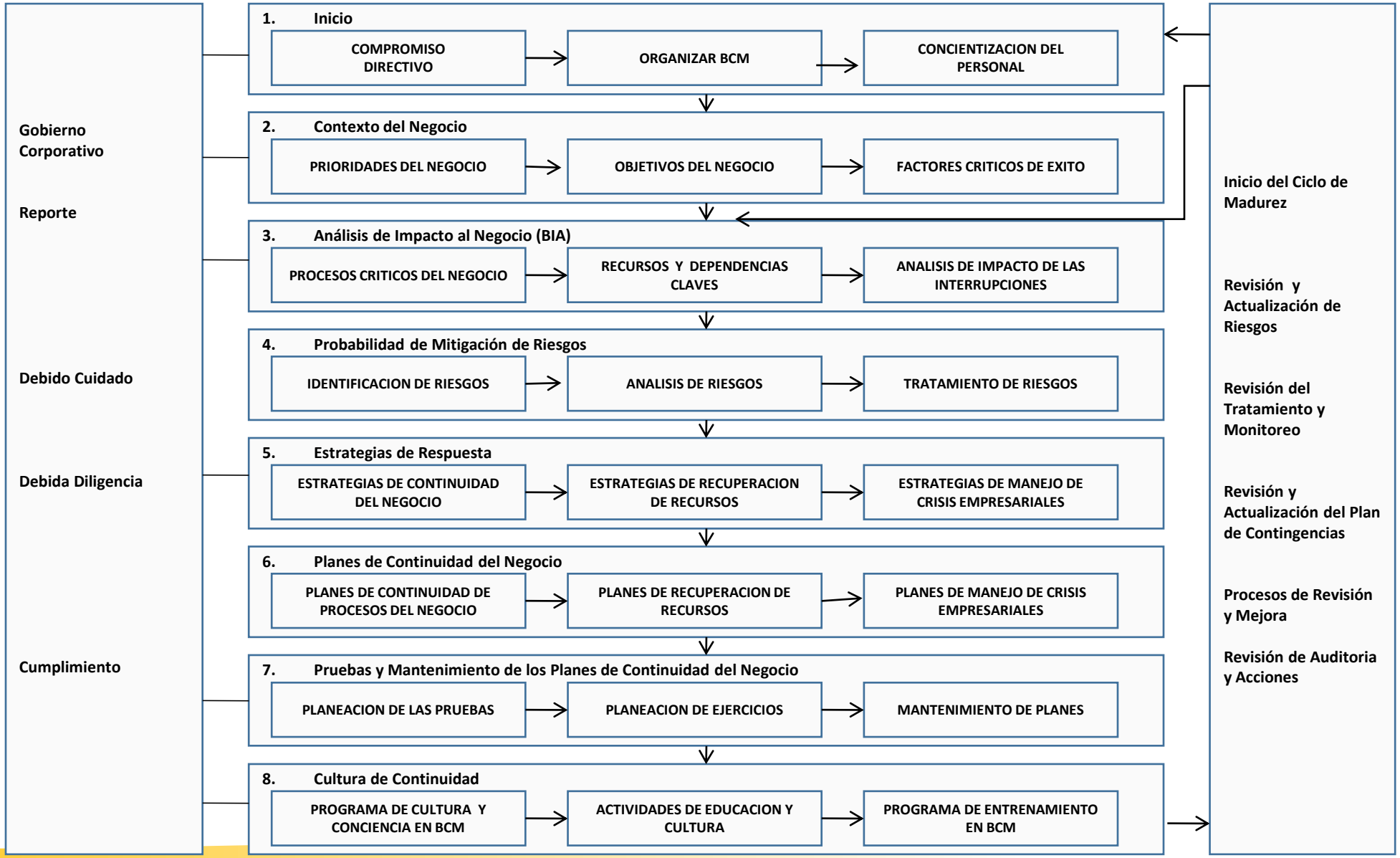
Plan Maestro de Emergencias

- Planes Locales de Emergencias
  - Sedes
  - Oficinas Principales
  - Otras instalaciones

COMPONENTES DE LOS PLANES DE CONTINUIDAD

Plan	Propósito
Plan de Continuidad del Negocio – BCP	Proporcionar procedimientos para sostener operaciones críticas del negocio mientras se recupera de una interrupción significativa.
Plan de Continuidad de Operaciones (COOP)	Proporciona procedimientos y guías para sostener funciones esenciales de la organización en un sitio alterno, durante un máximo de 30 días.
Plan de Comunicaciones en Crisis	Proporciona procedimientos para difundir las comunicaciones internas y externas, así como brindar información de la situación y controlar rumores.
Plan de Protección de Infraestructura Crítica (CIP)	Proporciona las políticas y procedimientos para la protección de los componentes nacionales de infraestructura crítica. Actualmente en definición en nuestro país.
Plan de Respuesta a Ciber-Incidentes	Proporciona procedimientos para la mitigación y corrección de un ataque cibernético, como: virus, gusanos informáticos y hoy día APT´s (Amenazas Persistentes Avanzadas).
Plan de Recuperación de Desastres (DRP)	Proporciona procedimientos para la recuperación de los sistemas de información y servicios tecnológicos críticos, en una locación alterna (Centro de cómputo alterno).
Plan de Contingencias de Sistemas de Información (ISCP)	Proporciona procedimientos y capacidades para la recuperación de un sistema de información en particular.
Plan de Respuesta a Emergencias (OEP)	Proporciona procedimientos coordinados para reducir al mínimo la pérdida de vidas, lesiones y proteger daños materiales en respuesta a una amenaza física.

PROGRAMA DE CONTINUIDAD DEL NEGOCIO

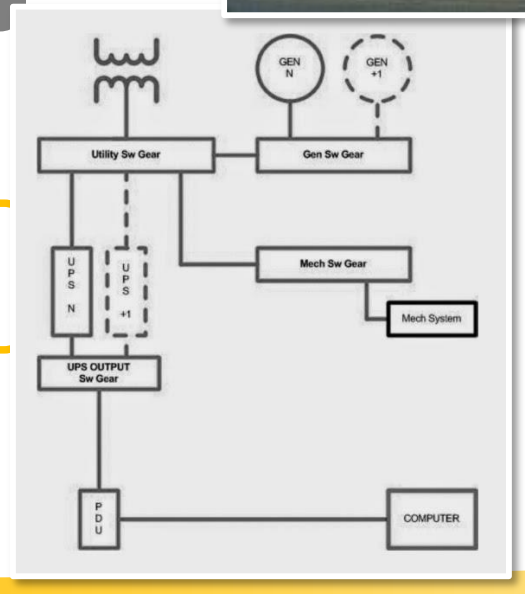


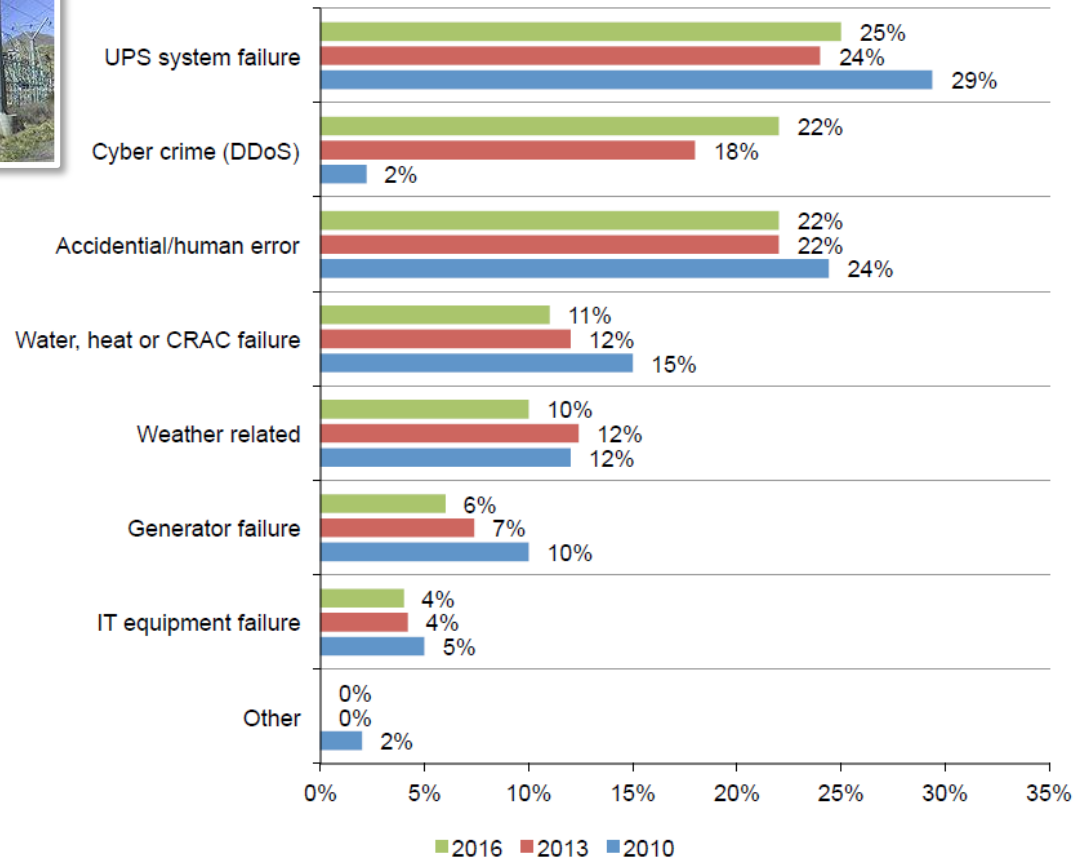
¿QUE PASA EN UN DESASTRE?

1. **Protecciones físicas** pueden estar comprometidas
2. **El procesamiento** de datos es reubicado
3. **Los empleados y colaboradores** trabajan en las centro alternos de operación
4. **Si es un impacto regional,** las familias pueden estar impactadas
5. **Las directivas y la gerencia** pueden estar heridos o ausentes
6. **Los procesos de abastecimiento** normal se quedan sin efecto
7. **Incomunicados**

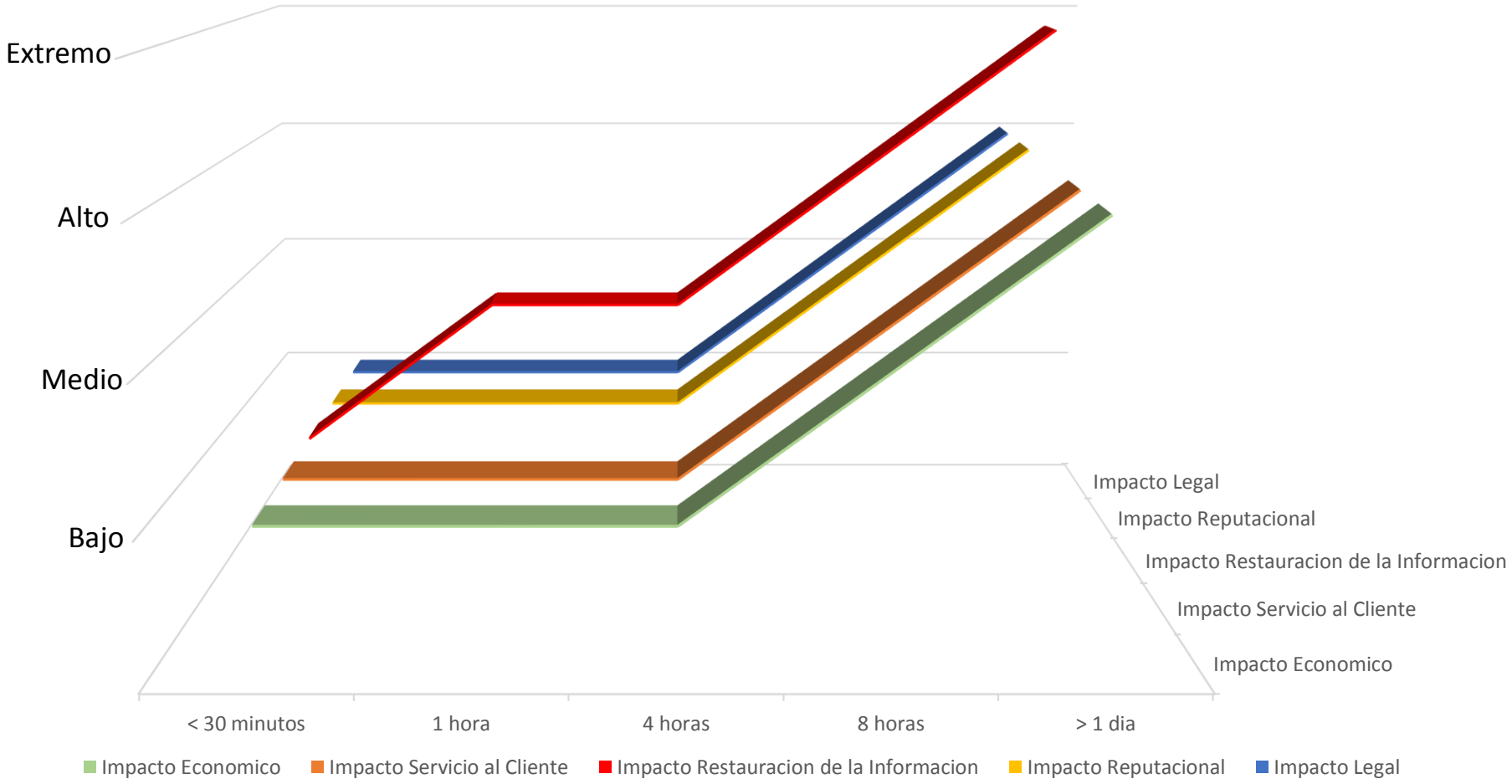
DURMIENDO CON EL ENEMIGO

Análisis de Impacto + Evaluación de Riesgos

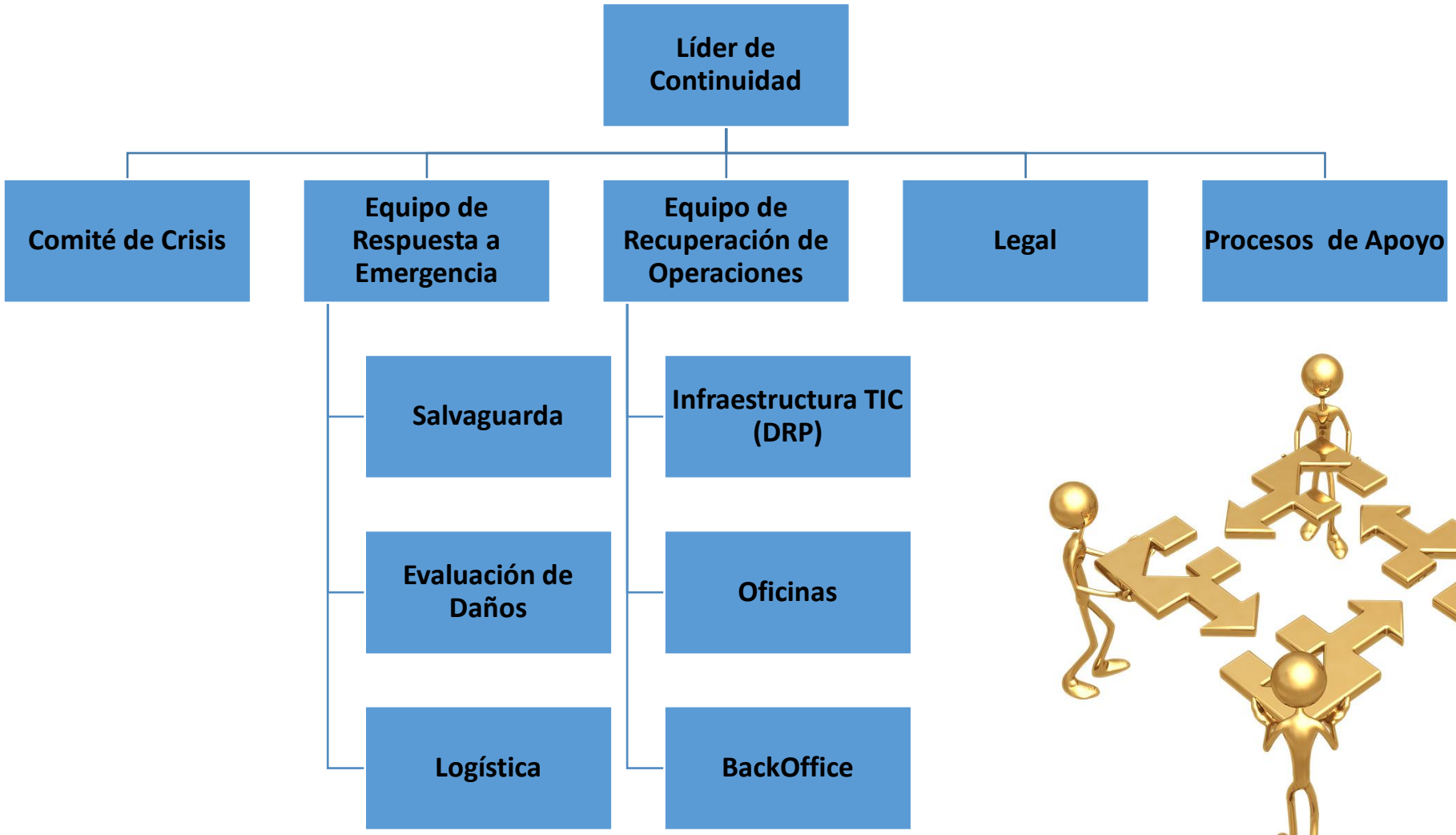




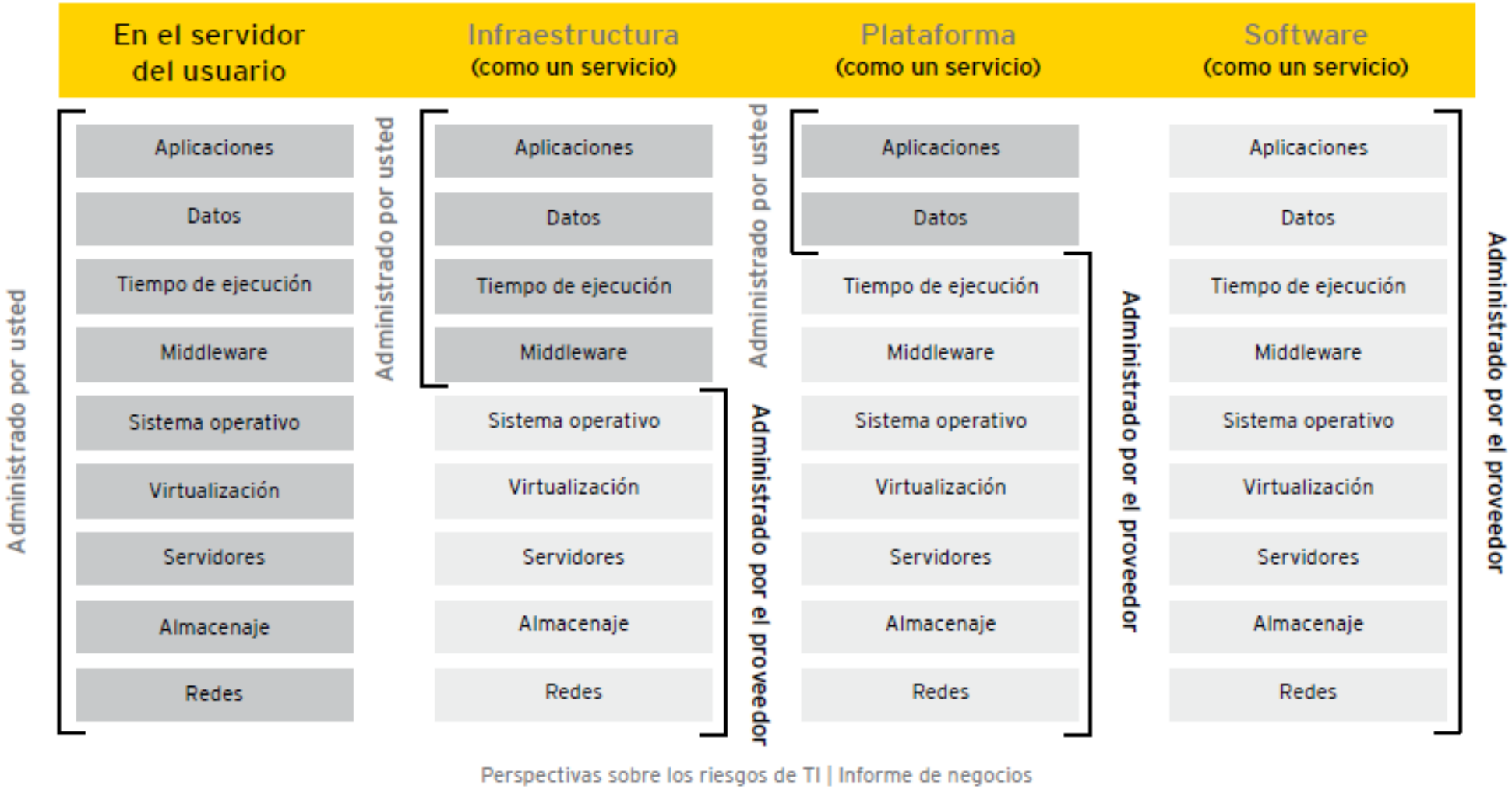
BIA – Efectos de una Interrupción



EQUIPOS DE TRABAJO

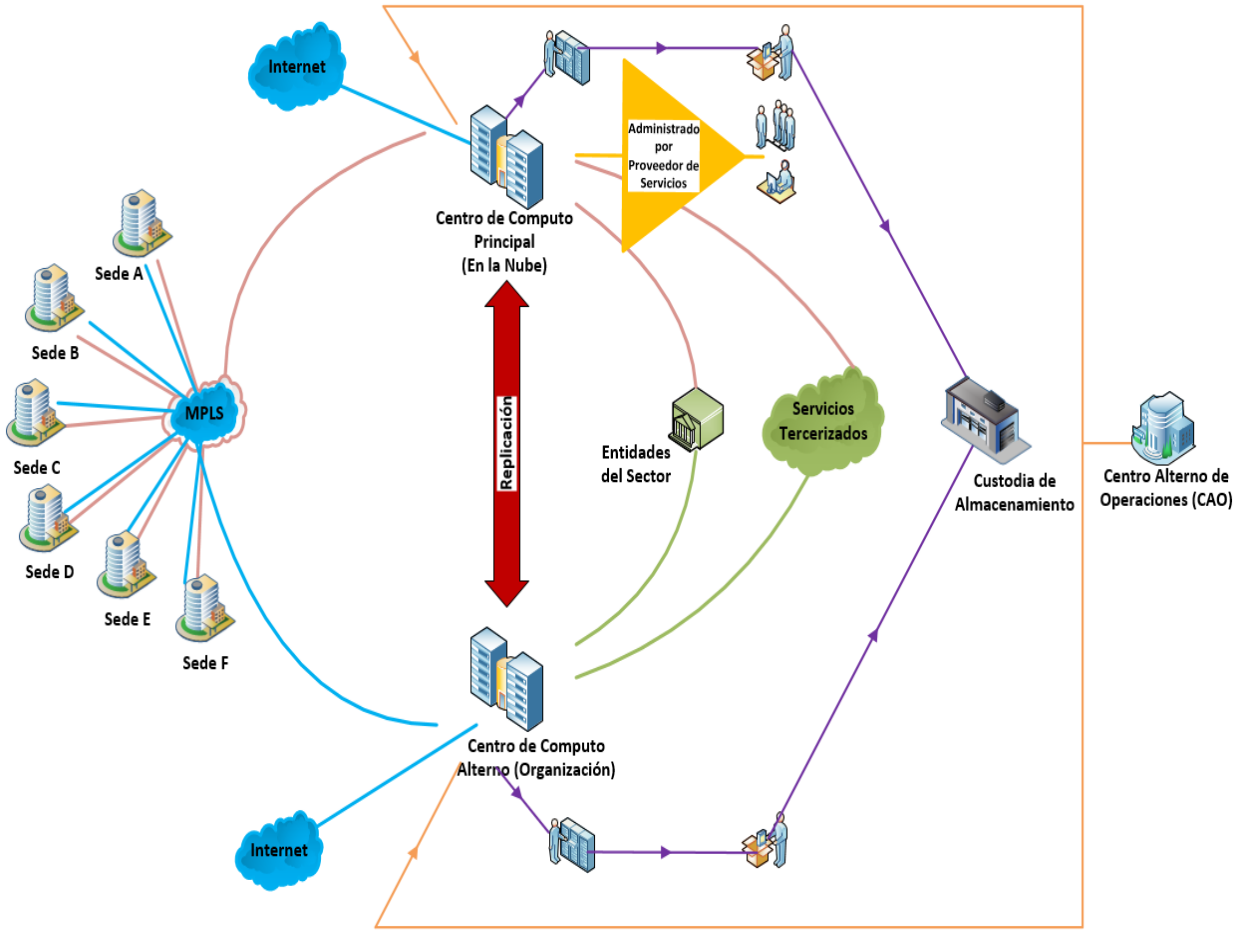


SERVICIOS DE CENTROS DE DATOS



Perspectivas sobre los riesgos de TI | Informe de negocios

VENTAJAS E IMPLICACIONES DE LA NUBE



Ventajas

- Se pacta con el proveedor los ANS.
- Se pueden aprovisionar servicios adicionales a los contratados inicialmente.
- Cumplimiento de RPO y RTO.
- Fortalece el esquema de Backups.
- Mitiga todos los escenarios.
- Se elimina la gestión de activos de tecnología.
- Se concentra en el gobierno del servicio.
- Crecimiento se da por demanda.
- Obsolescencia, fallas, licenciamiento quedan en manos del proveedor.
- Operación por personal capacitado.
- Implementación rápida.
- **Sistemas de información y servicios tecnológicos no críticos respaldados mediante ANS con el proveedor.**
- **Los costos en comparación con el CCA en la nube son mínimos.**
- **El CCA es un backup completo de todos los sistemas de información y servicios tecnológicos de la organización.**

Implicaciones

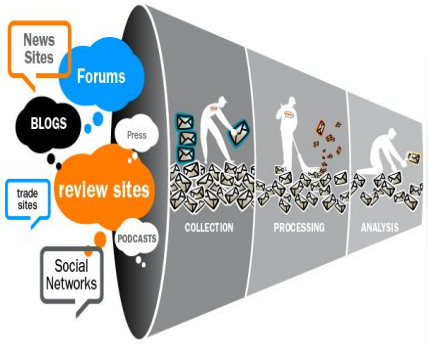
- Gestionar el tipo de contratación.
- Problemas relacionados con confidencialidad de la información propia de la organización.

GESTION DE COMUNICACIONES EN CRISIS

Saber quién, cuándo, a quién, cómo, qué comunicar a nivel interno y externo

10 PASOS EN GESTION DE COMUNICACIONES EN CRISIS

1. Anticipar las crisis
2. Mantener un equipo de manejo de crisis entrenado
3. Contar con un plan de manejo de crisis documentado
4. Definir y entrenar el vocero autorizado
5. Establecer el sistema de notificación
6. Monitorear los medios de comunicación convencionales y las redes sociales
7. Identificar y conocer las partes interesadas
8. Desarrolle comunicados preliminares
9. Finalice y adapte mensajes claves
10. Realice un análisis post-crisis



RETOS

- ✓ La gestión de riesgos de las empresas deben contemplar los riesgos de las tecnologías emergentes.
- ✓ Las estrategias de gestión de incidentes se deben ampliar a cyberataques. No se debe trabajar aisladamente.
- ✓ Independiente de las estrategias de recuperación de desastres y de continuidad del negocio, la gestión de cambios es fundamental.
- ✓ Las estrategias de DRP y el BCP se pueden llevar a la nube, pero el gobierno de las mismas debe permanecer en la organización.
- ✓ ¿Nuestros planes de continuidad hacen uso de las ventajas de las tecnologías emergentes? ¿Cuanto cuesta mantener nuestros planes actuales?

GESTIÓN DE RIESGOS

Enfoque Estratégico → Manejo de Crisis

Amenazas →

- Clientes y otros
- Ambiente Competitivo
- Ciclos Económicos
- Información
- Desastres Naturales
- Personal
- Políticas / Metodologías
- Políticas Regulatorias
- Reputación de Marca
- Proveedores
- Tecnología

Riesgos →

- Unidad de Negocios
- Unidad de Negocios
- Unidad de Negocios
- Unidad de Negocios

- INCUMPLIMIENTO REGULATORIO
- INTERRUPCIÓN DEL NEGOCIO
- PERDIDA DE CONFIDENCIALIDAD
- COSTOS ADICIONALES
- INTERRUPCION DE TI
- PERDIDA REPUTACIONAL

Mitigación de Riesgos →

- OPCIONES DE TRATAMIENTO DE RIESGOS (Considerar cambios)
- RESPUESTA A RIESGOS (SGSI y SGCN)
- MEJORA CONTINUA (Monitoreo y Mantenimiento)

FUENTES CONSULTADAS

- ✓ DRII, Disaster Recovery Institute International, DRI 2017 Global Risk and Resilience Survey
- ✓ INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO - IEC 22301:2012 Societal Security – Business Continuity Management Systems Requirements
- ✓ ISACA, Business Continuity Management: Emerging Trends, 2012
- ✓ NIST 800-34, Contingency Planning Guide For Federal Information Systems.
- ✓ NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special publication 800-39, Managing information security risk, organization, mission and information systems, EEUU. 2011.
- ✓ SAFEID - Conozco los riesgos de mi cadena de suministro. 2015
- ✓ SAFEID - Impactos de las tecnologías emergentes en el BCP. 2015
- ✓ http://www.drii.org
- ✓ http://www.gartner.com/technology/
- ✓ www.sans.org.
- ✓ www.safeid-sas.com

Sandra Suarez

Gerente General

milena.suarez@safeid-sas.com

Ramiro Merchán

Consultor

ramiro.merchan@safeid-sas.com

Milena Gutiérrez

Ejecutiva Comercial

Milena.gutierrez@safeid-sas.com

Gracias ...