UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA Y CONTROL DE SISTEMAS

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

AUDITORÍAS A LA CONTINUIDAD DE NEGOCIOS

Buscar en Internet los siguientes términos:

- DESASTRE
- PLAN DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRE
- LUGAR ALTERNATIVO: HOT SITE, WARM SITE, COLD SITE
- RPO Y RTO

AGENDA

- Conceptos generales
- Alternativas de recuperación
- Ejecución de auditoría de continuidad de negocios
- Referencias

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

CONCEPTOS GENERALES

Desastre e interrupción

- ✓ Toda interrupción que ocasiona que los recursos críticos de información y TI queden inoperantes por un período considerable de tiempo impactando negativamente en la organización, es considerado **un desastre. Pueden agruparse en diferentes tipos tales como**:
  - ❑ Naturales
  - ❑ Fallas en los activos (de TI o en la información)
  - ❑ Provocadas o accidentales

Gestión de la continuidad

- **Definición**
  - Procedimientos que permiten dar **soporte a la continuidad del negocio**, garantizando que **instalaciones, activos y servicios de TI** pueden volver a funcionar en plazos de tiempos requeridos y razonables, ante la ocurrencia de eventos que los afecten.

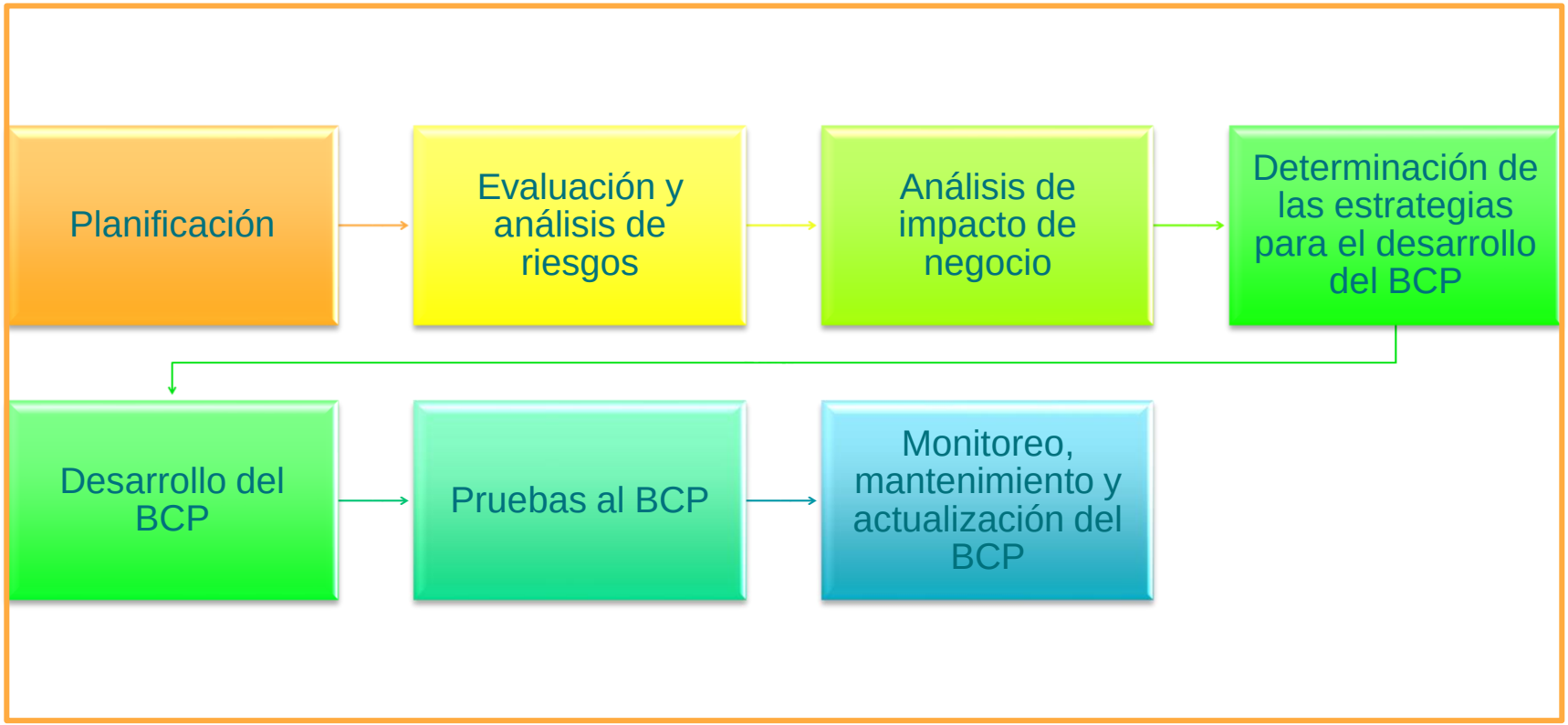
Plan de continuidad de negocios (BCP)

- Estrategia, documento y a la vez proceso
- Lista de acciones, funciones de TI y activos de información requeridos para continuar y mantener la viabilidad del negocio de la organización que lo enuncia, caso suceda algún tipo de interrupción a dicha continuidad.

Plan de continuidad de negocios (BCP)

- Componentes
  - ✓ El plan de recuperación de desastres (o DRP por las siglas en inglés de Disaster Recovery Plan)
  - ✓ El plan de restauración.
  - ✓ Los planes de emergencia.
  - ✓ Los planes de contingencia por área

Plan de continuidad de negocios (BCP)

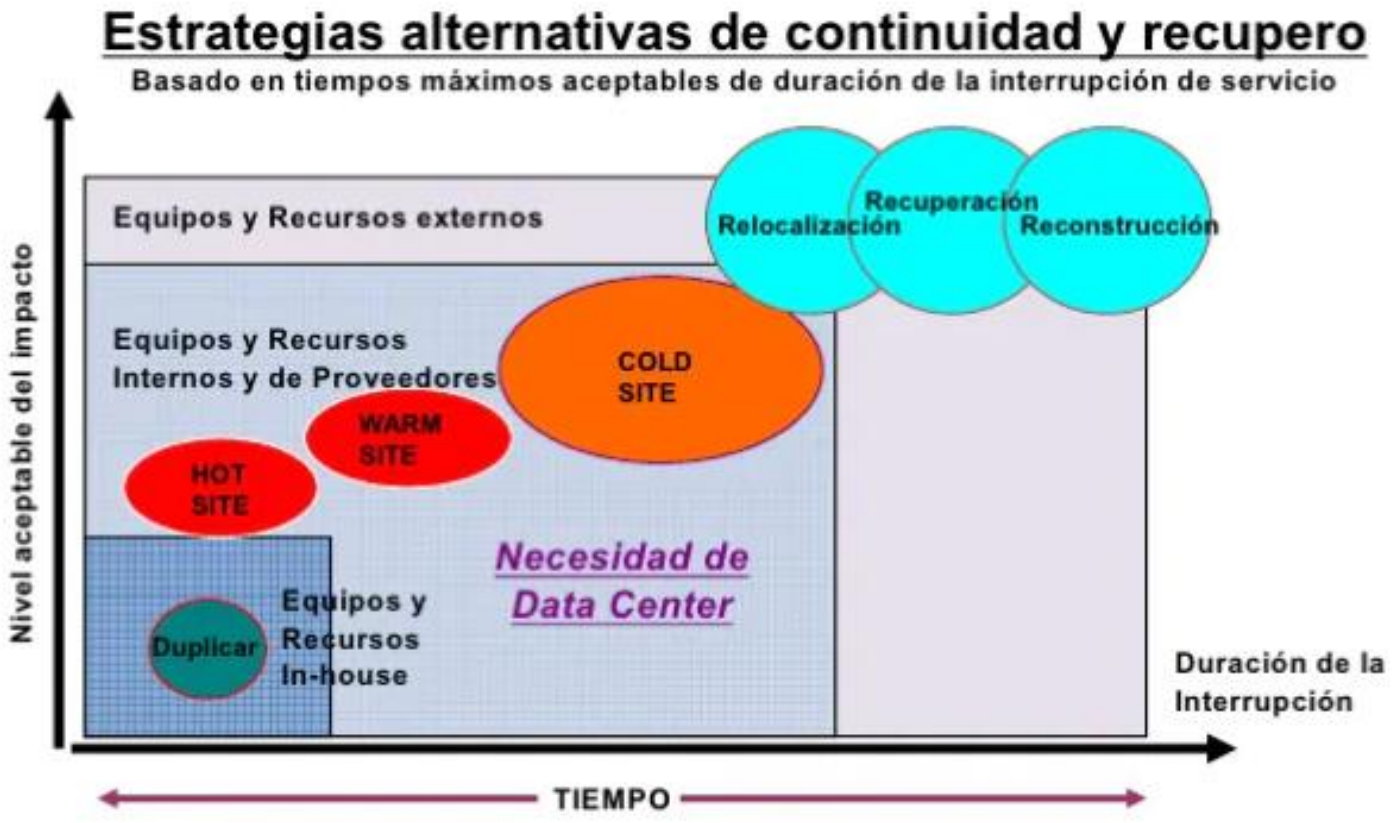


UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

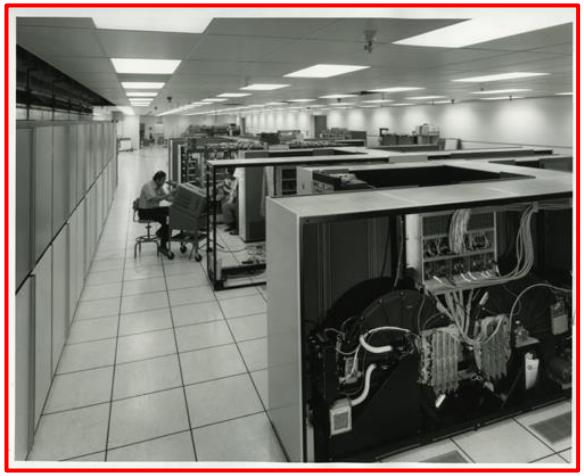
ALTERNATIVAS DE RECUPERACIÓN

Alternativas de recuperación



Hot sites

- Recuperación (total) de las operaciones en un sitio de procesamiento absolutamente idéntico a la instalación de procesamiento primaria (original y supuestamente siniestrada)
- Son iguales en equipamiento, arquitectura y topología de red, software.



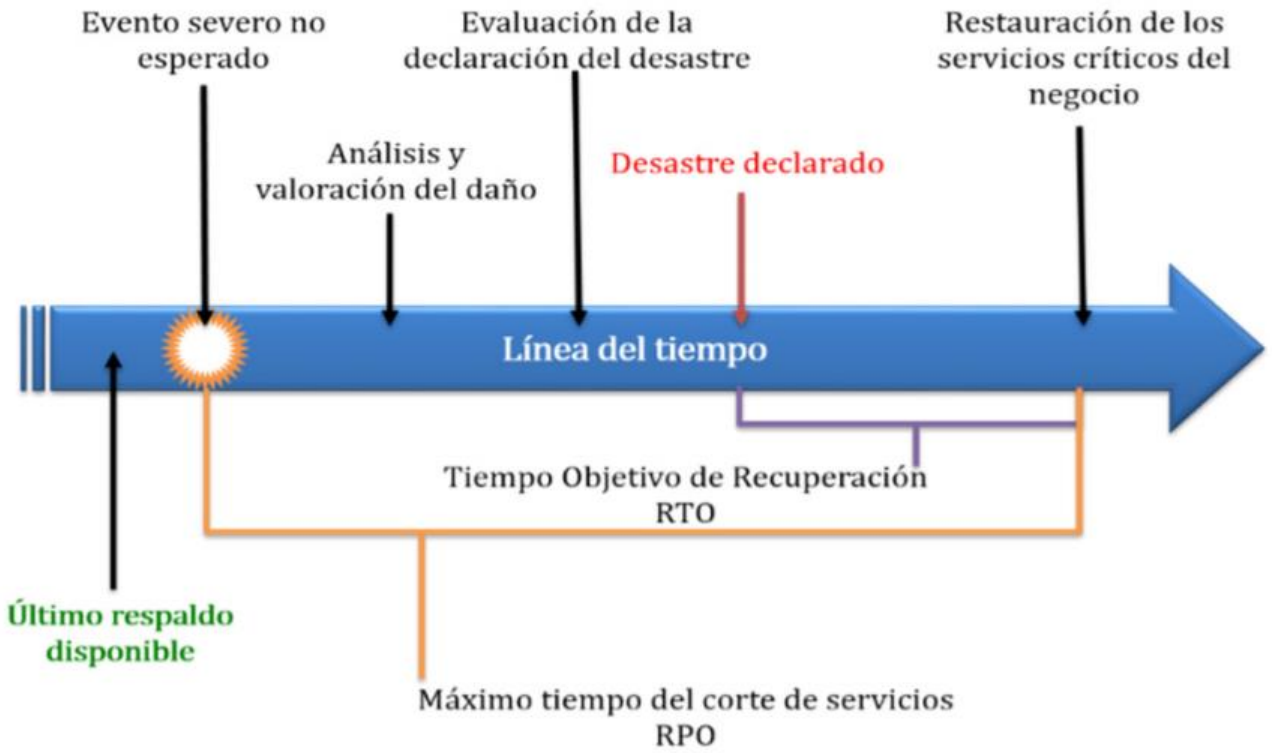
Warm sites

- Recuperación de operaciones en un sitio parcialmente configurado como la instalación primaria.
- Tiene la misma arquitectura y topología de red, algún hardware periférico pero sin los equipos completos o en su defecto con equipamiento que no tiene la misma configuración que la instalación siniestrada.

Cold sites

- Está constituido por un ambiente físico básico acondicionado para que opere en él, una instalación de procesamiento. Carece de todo tipo de software o hardware particular

Alternativas de recuperación



Alternativas de recuperación

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

EJECUCIÓN DE AUDITORÍA DE CONTINUIDAD DE NEGOCIOS

AUDITORÍA Y CONTROL DE SISTEMAS

Prácticas comunes

- Verificar la existencia y entender la estrategia de la continuidad de negocio y su alineamiento a los objetivos de negocio.
- Evaluar el BCP y su adecuación a los estándares internacionales, regulaciones legales a las que está sujeta la organización junto con su mecánica de actualización ante cambios en los entornos organizacionales, de mercado y de la tecnología.

Prácticas comunes

- Verificar la efectividad del BCP por medio de la conducción de pruebas.
- Evaluar las condiciones del sitio de almacenamiento y procesamiento alternativo por medio de inspecciones y auditorías ambientales.
- Evaluar las capacidades del personal de SI para responder con eficiencia en los diversos equipos que se forman para atención de contingencias.

Análisis de evidencias

- Copia vigente del BCP.
- Copias distribuidas del BCP.
- Memorias de las charlas / talleres de capacitación al personal sobre la ejecución o pruebas al BCP.
- Copia de los contratos con proveedores para la prestación del servicio de almacenamiento y procesamiento alterno, si los hubiere.
- Lista de los involucrados en el proceso de continuidad y responsables (árbol de llamadas).
- Resultados de anteriores pruebas y revisiones al plan, caso existan.
- Entrevistas con el personal clave.

Referencias bibliográficas

- [García, 2017] J. García. Metodología para la auditoría de sistemas Big Data (Máster En Ingeniería Informática). Universidad De Castilla-la Mancha, España (2017).
- [ISACA, 2018] ISACA International. Certified Information Systems Auditor (CISA) Exam Preparation Guide. ISACA Publishing, USA (2018).
- [ISACA, 2019] ISACA International. COBIT 2019 Framework. ISACA Publishing, USA (2019).
- [ISO, 2019] ISO International. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. ISO Publishing, Suiza (2019)

¿Consultas?

UNIVERSIDAD DE LIMA | 60 años

AUDITORÍAS A LA CONTINUIDAD DE NEGOCIOS