Universidad de Buenos Aires
Facultad de Ciencias Económicas

Las Configuraciones Técnicas para la Gestión de Tecnologías

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

Las **configuraciones técnicas de las tecnologías** constituyen el conjunto de decisiones y ajustes relacionados con infraestructura, redes, seguridad, servidores, bases de datos y comunicaciones que permiten que un sistema funcione de manera estable, segura y eficiente. En proyectos de Tecnologías de la Información (TI), estas configuraciones son tan relevantes como la configuración funcional o la parametrización, ya que determinan el entorno operativo real del sistema.

Desde la perspectiva de la administración, las configuraciones técnicas no deben considerarse asuntos exclusivamente del área de sistemas. Impactan directamente en:

- Continuidad operativa.
- Seguridad de la información.
- Cumplimiento normativo.
- Costos de infraestructura.
- Escalabilidad del negocio.

- Gestión del riesgo tecnológico.

En implementaciones de ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales), sistemas financieros, plataformas de comercio electrónico o soluciones en Cloud Computing (Computación en la Nube), la arquitectura técnica define la capacidad del sistema para sostener la operación en el tiempo.

Entre los componentes técnicos más relevantes se encuentran:

- Redes y conectividad.
- VPN (Virtual Private Network – Red Privada Virtual).
- Servidores.
- Bases de datos.
- Firewalls.
- Balanceadores de carga.
- Sistemas de autenticación.
- Configuraciones de seguridad y cifrado.
- Infraestructura en la nube.
- Monitoreo y respaldo.

Desarrollo

1. Infraestructura y arquitectura técnica

La infraestructura tecnológica constituye la base física o virtual sobre la cual operan los sistemas.

Puede clasificarse en:

- On-Premise (infraestructura local).
- Cloud (infraestructura en la nube).
- Híbrida (combinación de ambas).

Desde la administración, la elección impacta en:

- CAPEX (Capital Expenditure – Inversión de Capital).
- OPEX (Operational Expenditure – Gasto Operativo).
- Escalabilidad.
- Seguridad.
- Dependencia del proveedor.

Una configuración incorrecta puede generar sobrecostos o limitaciones futuras.

---

2. Redes y conectividad

Las redes permiten la comunicación entre usuarios, servidores y aplicaciones.

Elementos técnicos relevantes:

- LAN (Local Area Network – Red de Área Local).
- WAN (Wide Area Network – Red de Área Amplia).
- DNS (Domain Name System – Sistema de Nombres de Dominio).
- Direccionamiento IP.

Desde la administración, la calidad de la conectividad afecta:

- Productividad.
- Disponibilidad del sistema.
- Experiencia del cliente.
- Operación remota.

---

3. VPN (Virtual Private Network – Red Privada Virtual)

Una VPN es un mecanismo que permite establecer una conexión segura entre dispositivos a través de una red pública como Internet.

Funciona mediante:

- Cifrado de datos.
- Túneles virtuales.
- Autenticación segura.

Objetivo:

- Proteger información sensible.
- Permitir acceso remoto seguro.
- Conectar sucursales geográficamente dispersas.

Ejemplo:

Un empleado que trabaja desde su hogar se conecta al sistema contable de la empresa mediante una VPN, garantizando que los datos no puedan ser interceptados.

Desde la perspectiva administrativa, la VPN:

- Reduce riesgos de seguridad.
- Permite trabajo remoto.
- Mantiene continuidad operativa.

---

4. Firewalls y seguridad perimetral

El Firewall (Cortafuegos) es un sistema que controla el tráfico entrante y saliente según reglas de seguridad.

Funciones:

- Bloqueo de accesos no autorizados.
- Filtrado de puertos.
- Control de protocolos.

Desde la administración, protege:

- Información confidencial.
- Datos financieros.
- Activos digitales críticos.

Una configuración incorrecta puede dejar vulnerabilidades abiertas.

---

5. Servidores y virtualización

Los servidores alojan aplicaciones y bases de datos.

Tipos:

- Servidores físicos.
- Servidores virtuales.
- Contenedores (Containers – Contenedores).
- Máquinas virtuales (VM – Virtual Machine – Máquina Virtual).

La virtualización permite ejecutar múltiples sistemas en un mismo hardware, optimizando recursos.

Desde la administración:

- Reduce costos.
- Mejora escalabilidad.
- Facilita recuperación ante fallas.

---

6. Bases de datos

La base de datos es el repositorio estructurado de información.

Configuraciones técnicas incluyen:

- Motor de base de datos.
- Replicación.
- Índices.
- Backups automáticos.
- Seguridad de acceso.

Ejemplo:

Configurar replicación de base de datos para alta disponibilidad.

Desde la administración, una mala configuración puede afectar:

- Integridad contable.
- Reportes gerenciales.
- Cumplimiento fiscal.

---

7. Balanceadores de carga (Load Balancer – Balanceador de Carga)

Distribuyen el tráfico entre múltiples servidores para:

- Evitar sobrecargas.
- Mejorar disponibilidad.
- Optimizar tiempos de respuesta.

Ejemplo:

En una plataforma de comercio electrónico durante una campaña masiva, el balanceador distribuye el tráfico entre varios servidores.

Impacto administrativo:

- Protección de ingresos.
- Reducción de interrupciones.
- Mejora en experiencia del cliente.

---

8. Configuración de autenticación y control de acceso

Incluye:

- Active Directory.
- LDAP (Lightweight Directory Access Protocol – Protocolo Ligero de Acceso a Directorios).
- MFA (Multi-Factor Authentication – Autenticación Multifactor).

Estas configuraciones determinan cómo se validan identidades.

Desde la administración:

- Reduce riesgo de fraude.
- Cumple requisitos regulatorios.
- Fortalece control interno.

---

9. Cifrado y certificados digitales

El cifrado protege la confidencialidad de la información.

Protocolos comunes:

- SSL/TLS (Secure Sockets Layer / Transport Layer Security – Seguridad de Capa de Transporte).

Ejemplo:

Un portal financiero utiliza cifrado para proteger transacciones.

Desde la administración, el cifrado es esencial para proteger datos personales y evitar sanciones legales.

---

10. Monitoreo y observabilidad

Incluye herramientas que permiten:

- Supervisar rendimiento.
- Detectar incidentes.
- Generar alertas.
- Analizar logs (registros).

Desde la perspectiva de gobernanza de TI, el monitoreo permite:

- Anticipar fallas.
- Reducir tiempo de inactividad.
- Tomar decisiones basadas en datos.

---

11. Respaldo y recuperación

Las configuraciones de backup (Respaldo) y recovery (Recuperación) aseguran continuidad ante fallas.

Incluyen:

- Copias automáticas.
- Replicación geográfica.
- Pruebas de restauración.

Desde la administración, protegen:

- Información crítica.

- Cumplimiento normativo.
- Continuidad del negocio.

---

12. Impacto financiero y estratégico

Las configuraciones técnicas influyen en:

- Costo total de propiedad.
- Nivel de riesgo.
- Capacidad de expansión.
- Velocidad de innovación.
- Protección de activos digitales.

Una mala configuración puede provocar:

- Caídas del sistema.
- Brechas de seguridad.
- Multas regulatorias.
- Pérdida de confianza.

Desde la administración, la infraestructura técnica es una inversión estratégica.

Conclusión

Las configuraciones técnicas de las tecnologías constituyen el fundamento operativo sobre el cual se sostienen los sistemas de información. Elementos como redes, VPN, firewalls, servidores, bases de datos, balanceadores de carga, autenticación y cifrado determinan la seguridad, disponibilidad y rendimiento del sistema.

Desde la perspectiva de las Tecnologías de la Información aplicadas a la administración, estas configuraciones impactan directamente en la continuidad operativa, el control interno y la sostenibilidad financiera del negocio. No se trata únicamente de decisiones técnicas, sino de decisiones estratégicas que protegen la inversión tecnológica y reducen riesgos organizacionales.

Comprender estos elementos permite a los futuros profesionales evaluar con criterio las implicancias técnicas y financieras de las decisiones de infraestructura.

Preguntas de autoevaluación

1. ¿Qué es una VPN y por qué es importante para la seguridad organizacional?
2. ¿Cómo impacta un firewall mal configurado en la operación del negocio?
3. ¿Qué diferencia existe entre infraestructura on-premise y cloud?
4. ¿Por qué el cifrado es esencial en sistemas financieros?
5. ¿Cómo influyen las configuraciones técnicas en el costo total de propiedad del sistema?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.