

**TEMAS QUE SE INCLUYEN EN EL EXAMEN GENERAL DE CONOCIMIENTOS ESCRITO Y ORAL
PARA LA OBTENCIÓN DEL GRADO DE LA MAESTRÍA EN TECNOLOGÍAS DE LA
INFORMACIÓN EN LA DIRECCIÓN DE NEGOCIOS**

ADMINISTRACIÓN DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

I. PERFIL DEL PERSONAL QUE ADMINISTRA LOS SERVICIOS DE TI.

1. Conocimientos, habilidades y actitudes.
2. Enfoque para administrar el portafolio de habilidades de TI.
3. Optimización de las habilidades del personal de TI.
4. Cadenas de suministro de *outsourcing* de TI.

II. SISTEMAS DE INFORMACIÓN.

1. Sistemas de información basados en computadoras: contable; administrativa; de soporte para la toma de decisiones.
2. Sistemas de información organizacionales: empresarial; ejecutivo; de recursos de información.

III. SERVICIOS DE TI.

1. Administración de sistemas de información *versus* administración de servicios de TI.
2. Administración de la infraestructura de TI: activos de *hardware* y *software*; recursos de datos; telecomunicaciones y redes; Internet; nueva infraestructura de TI.
3. Mejores prácticas internacionales: modelos de gobernabilidad; modelos de auditoría (*COSO [Committee Of Sponsoring Organizations of the Treadway Comision]*, *COBIT [Objetivos de Control para la información y Tecnologías Relacionadas]*, *SOX [Ley Sarbanes-Oxley]*).
4. Marcos de referencia de procesos: *COBIT*; *ITIL (Librería de Infraestructura de TI)*; *ISO 2000*; *Gartner*; *IBM*; *HP*; *Microsoft*; entre otros.
5. Sistemas de calidad: *ISO 900x*; *TQM (Total Quality Management)*; *EFQM (Fundación Europea para la Gestión de la Calidad)*; *Six Sigma*; *Deming*; entre otros.
6. Desarrollo de aplicaciones: *CMMI (Capability Maturity Model)*; *ASL (Application Software Library)*; *ITIL*.
7. Seguridad de TI: *ITIL*; *BS7799*; *ISO 17799/27001*.
8. Planeación de TI: *e TOM (enhanced Telecommunication Operations Map)*.
9. Fundamentos de administración de servicios de TI (*ITSM*) basado en la librería de infraestructura de TI (*ITIL*).
10. Procesos de soporte de servicios y procesos de entrega de servicios.

BASES DE DATOS

I. PROCESAMIENTO DE BASES DE DATOS.

1. Conceptos generales.
2. Evolución.
3. Arquitectura.
4. Sistemas.
5. *Frontend versus Backend.*
6. Lenguajes: de explotación; de 4ª generación.

II. DISEÑO DE BASES DE DATOS.

1. Modelado de datos.
2. Diseño de bases de datos en el modelo relacional: estructura, manipulación e integridad.
3. Normalización de bases de datos relacionales.
4. Métodos, técnicas y herramientas automatizadas del diseño de bases de datos.

III. MANIPULACIÓN DE BASES DE DATOS.

1. Fundamentos matemáticos: teoría de conjuntos y álgebra relacional.
2. Estructura.
3. Funciones
4. Agrupación y ordenamiento.
5. Consulta de tablas y múltiples tablas.
6. Consulta mediante expresiones regulares.
7. Consulta a través de operadores relacionales: básicos y avanzados.
8. Creación de funciones.

IV. PROGRAMACIÓN AVANZADA.

1. Programación básica en el *Backend*.
2. Lenguajes nativos de 4GL (cuarta generación).
3. Creación y manejo de: *stored procedures; functions; cursores; rules; defaults; trigger; cheks.*
4. Interfaz: con la *web*; con otros lenguajes de alto nivel.

V. ADMINISTRACIÓN DE BASES DE DATOS.

1. Estructura de la base de datos: física y lógica.
2. Estructura de la memoria.
3. Métodos: de integridad; consistencia; concurrencia; manejo de transacciones de datos.
4. Indización.
5. Administración de la seguridad de la base de datos.
6. Administración de objetos.
7. Sistemas Administradores de Bases de Datos Relacionales (*RDBMS*).
8. Utilerías del *RDBMS*.

INTELIGENCIA DE NEGOCIOS

I. **MODELOS DE BASES DE DATOS.**

1. Evolución de las tecnologías asociadas a los modelos de bases de datos.
2. Análisis transaccional *versus* analítico de los datos.
3. Bases de datos analíticas.
4. Bodega de datos, *data marts* y bases de datos multi-dimensionales.

II. **DATA WAREHOUSE.**

1. Definición y funciones de *Data Warehouse* y *Data Farming*.
2. Diferencias con los sistemas de información.
3. Características.
4. Estructura.
5. Arquitectura.
6. Operaciones.
7. Usos.
8. Ventajas y desventajas.

III. **CUBOS.**

1. Fundamentos: técnica *OLAP (On-Line Analytical Processing)*.
2. Diseño y configuración.
3. Dimensiones, medidas y celdas.
4. Diferencias existentes en cada una de las dimensiones.
5. Funciones básicas: modos de almacenamiento, metadatos.
6. Funciones avanzadas: establecimiento conexiones remotas; administración avanzada.

IV. **DATA MINING.**

1. Concepto y áreas relacionadas.
2. Diferencia entre *Data Mining* y *Text Mining*.
3. Descubrimiento de conocimientos en bases de datos.
4. Alcance y componentes del *Data Mining*.
5. Proceso de descubrimiento y formas de trabajar del *Data Mining*.
6. Técnicas utilizadas en el *Datamining*: redes neuronales artificiales; árboles de decisión; algoritmos genéticos; método del vecino más cercano; reglas de inducción.

V. **APLICACIONES DE MINERÍA DE DATOS.**

1. *Database Marketing*.
2. Predicción.
3. Reducción de riesgos.
4. Detección de fraude.
5. Control de calidad.
6. Procesos industriales.
7. Evaluación de solvencia.
8. *Web Mining*.

CALIDAD EN EL DESARROLLO DE APLICACIONES

I. FUNDAMENTOS DE SOFTWARE.

1. Evolución.
2. Características.
3. Componentes.
4. Paradigmas de programación.
5. Ciclo de vida.

II. CONTROL DE CALIDAD DEL SOFTWARE.

1. Principales conceptos: calidad; control de calidad; garantía de calidad; costo de la calidad; aseguramiento de calidad.
2. Revisiones del software.
3. Plan de Aseguramiento de la Calidad del Software (SQA).

III. NORMAS Y ESTÁNDARES DE CALIDAD APLICABLES AL DESARROLLO DEL SOFTWARE.

1. ISO 9000.
2. Capability Maturity Model (CMM).
3. Capability Maturity Model Integration (CMMI).
4. Mo Prosoft.

IV. INGENIERÍA DE SOFTWARE.

1. Visión general de la ingeniería de software.
2. Procesos, métodos y herramientas.
3. Modelos de proceso de software.
4. Técnicas de 4ª generación.
5. Evolución de la tecnología.

V. MÉTODOS DE DISEÑO DE SOFTWARE.

1. Proceso de diseño: principios y conceptos.
2. Diseño modular efectivo.
3. Métodos de diseño: de datos; arquitectónico; de interfaz; procedimental.

VI. MÉTODOS Y ESTRATEGIAS DE PRUEBA DE SOFTWARE.

1. Diseño de casos de prueba.
2. Tipos de prueba: caja blanca; camino básico; estructura de control; caja negra; entornos y aplicaciones especializadas.
3. Tipos de estrategia de prueba de: unidad; integración; validación; del sistema.
4. Proceso de depuración.

SISTEMAS EMPRESARIALES Y TENDENCIAS WEB

I. SISTEMAS DE INFORMACIÓN.

1. La información como un recurso de las organizaciones.
2. Análisis y diseño estructurado de sistemas.
3. Ciclo de vida del desarrollo de sistemas.
4. Ingeniería del producto.
5. Enfoque de flujo de datos para la determinación de requerimientos.
6. Diseño de datos, arquitectónico, de interfaz y procedimental.
7. Diccionario de datos.
8. Prueba, mantenimiento, auditoría e implementación.

II. ESTILOS ORGANIZACIONALES Y SU IMPACTO EN LOS SISTEMAS DE INFORMACIÓN.

1. Las organizaciones desde el punto de vista de sistemas.
2. Arquitectura empresarial.
3. Estrategia de sistemas y niveles de administración.
4. Fundamentos de un proyecto de sistemas: determinación de factibilidad; administración de las actividades de análisis e implantación.
5. Sistemas de apoyo a decisiones.

III. SISTEMAS DE INFORMACIÓN VERSUS PLATAFORMAS WEB.

1. Sistemas de información en red y cliente – servidor.
2. Sistemas de información con plataforma *Web*.
3. Diferencias entre sistemas *legacy* y sistemas con tecnología *Web*.
4. Lenguajes de programación para Internet.
5. Intercambio de información mediante tecnología *Web*.
6. Nuevas tendencias en tecnología *Web*.

IV. PLANIFICACIÓN DE RECURSOS EMPRESARIALES (ERP).

1. Antecedentes.
2. Características principales.
3. Finalidad de un *ERP*.
4. Ventajas y desventajas.
5. Principales proveedores.
6. Impacto en la industria.
7. Riesgos de negocio.
8. Implantación de *ERP*'s.
9. *Software* gratuito relacionado.

V. SISTEMAS EMPRESARIALES Y SU RELACIÓN CON LAS TENDENCIAS WEB .

1. Sistemas, Aplicaciones y Productos (*SAP*) *R/3*.
2. *Oracle - Peoplesoft*.
3. *Business Intelligence*.
4. *E-Business*.

5. *Customer Relationship Management (CRM).*
6. *Selling-Supply Chain Management.*
7. *E-Procurement.*

TECNOLOGÍAS APLICADAS AL TRATAMIENTO DE DATOS

I. INTRODUCCIÓN A LAS TECNOLOGÍAS DE TRATAMIENTO DE DATOS.

1. Panorama general de las TI aplicadas al tratamiento de datos.
2. Características de los datos en los sistemas de información.
3. Calidad de los datos.
4. Administración de la información empresarial.

II. HARDWARE Y ARQUITECTURA DE INFRAESTRUCTURA.

1. Microprocesadores.
2. Arquitectura de sistemas.
3. Servidores.
4. Configuraciones especiales para el procesamiento de datos.
5. Centros de datos.

III. REDES Y CÓMPUTO DISTRIBUIDO.

1. Conceptos y fundamentos de redes.
2. Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP).
3. Internet y la web.
4. Sistemas, bases de datos y aplicaciones distribuidas.
5. Metadatos e intercambio electrónico de datos.
6. Arquitectura orientada a servicios.
7. Cómputo e inteligencia colaborativa.

IV. SOFTWARE DE BASE PARA EL TRATAMIENTO DE DATOS.

1. Sistemas operativos: de red; distribuidos; middleware.
2. Sistemas manejadores de bases de datos: relacionales; orientados a objetos; distribuidos; de sincronización-replicación; de indexación-búsqueda; desconectados; móviles.
3. Sistemas de soporte a las transacciones de negocio: monitores de transacciones, colas de mensajes de negocio, sistemas de administración de procesos (Business Process Management).
4. Tecnologías para el descubrimiento del conocimiento a partir de los datos.
5. Tecnologías aplicadas a la inteligencia de negocios.

V. ALMACENAMIENTO.

1. Tecnologías de almacenamiento de datos empresariales.

2. Tecnologías de almacenamiento en tiempo real.
3. Red de área de almacenamiento (SAN).
4. Configuraciones de almacenamiento para aplicaciones.
5. Respaldo y recuperación.
6. Administración y automatización.

VI. TECNOLOGÍAS APLICADAS A LOS SERVICIOS DE ADMINISTRACIÓN.

1. Fundamentos de administración de sistemas.
2. Calidad de servicio (QoS).
3. Directorios.
4. Metodologías.

VII. TENDENCIAS EN EL TRATAMIENTO DE DATOS.

1. Transformación de la operación de tecnologías de la información a la administración de servicios.
2. Mejores prácticas en el tratamiento de datos.
3. Integración de datos en tiempo real.
4. Tendencias actuales en el procesamiento de datos.

APLICACIONES MÓVILES

I. SELECCIÓN E IMPLANTACIÓN DE APLICACIONES MÓVILES.

1. Estrategias para la detección de oportunidades que permitan aprovechar las aplicaciones móviles.
2. Mecanismos y metodologías de implantación de las aplicaciones móviles.
3. Beneficios del desarrollo de aplicaciones inalámbricas.

II. EL TRABAJADOR NÓMADA.

1. Definición y características.
2. Posibilidades de integración en la organización y legalidad del uso de aplicaciones móviles.
3. El compromiso del trabajador nómada y su relación con el proyecto de la organización.
4. Proceso operativo y plan de entrenamiento: uso y mejora continua del proceso.
5. Infraestructura y red con aplicaciones móviles.
6. Aspectos del contexto real en el que se desarrollan de actividades del trabajador nómada: participación gubernamental (regulación nacional e internacional); participación de la iniciativa privada (regulación nacional e internacional); servicios de conectividad a la ciudadanía; análisis del ciudadano "ubicuo".

III. TENDENCIAS EN EL DESARROLLO DE APLICACIONES MÓVILES.

1. Innovación y mejora continua de procesos.
2. Selección de procesos de soporte.

3. Expansión de aplicaciones ligeras.
4. Conectividad.
5. Tendencias de mejora del rendimiento y vigencia de las aplicaciones móviles.

IV. ELEMENTOS TECNOLÓGICOS.

1. Dispositivos móviles.
2. Pantallas.
3. Limitaciones de enlace de datos.
4. Batería.
5. Portabilidad.
6. Conectividad inalámbrica.
7. Cobertura.
8. Velocidad y ancho de banda.
9. Confiabilidad en el proveedor.
10. Seguridad.
11. Protección de los datos y de la infraestructura.
12. Cifrado, autenticación y limpieza de datos.
13. *Software*.
14. Sincronía.
15. *Browser* y/o *software* del cliente.
16. Aplicaciones adicionales.

V. INVERSIÓN EN APLICACIONES MÓVILES.

1. Beneficios.
2. Costos.
3. Tangibles e intangibles.

VI. SELECCIÓN DEL AMBIENTE DE DESARROLLO.

1. *Java.net*, entre otros.
2. Selección de la arquitectura móvil.
3. Selección de la arquitectura del servidor.
4. Herramientas para el desarrollo móvil y plataformas.
5. Evaluación y elección de los diferentes ambientes.

ALINEACIÓN ESTRATÉGICA Y ADMINISTRACIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN

I. ELEMENTOS DE ALINEACIÓN ESTRATÉGICA.

1. Requerimientos tecnológicos para la alineación con los objetivos de la organización.
2. Requerimientos para la integración de proyectos de TI alineados a los objetivos organizacionales: alcance; manejo; costos y retorno de inversión; calidad; recursos humanos; comunicación; riesgos; adquisiciones.

3. Estrategia tecnológica para habilitar los procesos clave del negocio.

II. FACTORES A CONSIDERAR EN LA ADMINISTRACIÓN DE PROYECTOS DE TI.

1. Marco de referencia de la administración de proyectos.
2. Estándares que se aplican en la administración de proyectos.
3. Perfil del administrador de proyectos de TI.
4. Factores críticos de éxito para la administración de proyectos: definición; criterios de satisfacción y cumplimiento; generalización de los factores de éxito en TI; administración para obtener éxito.

III. MODELOS DE ADMINISTRACIÓN DE PROYECTOS DE TI.

1. Organizaciones de administración de proyectos.
2. *Project Management Institute (PMI)* y *Project Management Body of Knowledge (PMBOK)*.
3. *Prince 2*.
4. *MSF Project management discipline*.
5. *Software engineering vs. Project management*.
6. *PMI y Work Breakdown Structure (WBS)*.

LEGISLACIÓN INFORMÁTICA, NORMATIVIDAD Y AUDITORÍA EN TECNOLOGÍAS DE INFORMACIÓN

I. ELEMENTOS DE DERECHO Y DE AUDITORÍA.

1. Concepto y propósitos del derecho.
2. Principales conceptos jurídicos.
3. Ramas del derecho.
4. Derecho informático: primicias y problemas.
5. Concepto y propósito de la auditoría.
6. Divisiones de la auditoría.
7. Auditoría informática: primicias y problemas.
8. Aspectos legales de la auditoría.

II. LEGISLACIÓN Y NORMATIVIDAD NACIONALES E INTERNACIONALES RELATIVAS AL USUARIO.

1. Derechos del usuario: derecho de información; libertad de expresión; derecho a la privacidad; entre otras.
2. Debilidades de la normatividad: la firma electrónica y/o digital; la criptografía y sus respectivas legislaciones.
3. Políticas de seguridad al usuario que cubren la insuficiencia en la normatividad.
4. Auditoría de las actividades del usuario (contratos, perfiles, entre otros).
5. Herramientas enfocadas a la auditoría del usuario.

III. LEGISLACIÓN Y NORMATIVIDAD NACIONALES E INTERNACIONALES RELATIVAS A LA INFORMACIÓN.

1. Daño; robo; acceso no autorizado; alteración de datos.
2. Debilidades de la normatividad: *hackers* y *crackers*; código malicioso.
3. Derecho de la sociedad de información.
4. Políticas de seguridad de la información que cubren la insuficiencia en la normatividad.
5. Auditoría de la información: metodología.
6. Herramientas enfocadas a la auditoría de la información.

IV. LEGISLACIÓN Y NORMATIVIDAD NACIONALES E INTERNACIONALES RELATIVAS AL SOFTWARE Y AL HARDWARE.

1. *Software*: piratería y falsificación del *software*; acceso no autorizado a sistemas informáticos.
2. *Hardware*: acceso no autorizado al equipo de cómputo y de telecomunicaciones; robo de equipo.
3. Debilidades de la normatividad: *hackers* y *crackers*; código malicioso; lo público y lo privado.
4. Políticas de seguridad del *software* y del *hardware* que cubren la insuficiencia en la normatividad.
5. Auditoría: del *software* (creación; contratos y licencias); del *hardware* (contratos).
6. Herramientas de apoyo a la auditoría del *software*.

V. LEGISLACIÓN Y NORMATIVIDAD NACIONALES E INTERNACIONALES RELATIVAS A LA FUNCIÓN INFORMÁTICA.

1. Área de TI: normatividad (fiscal; económica; mercantil; penal; laboral; entre otras).
2. Debilidades de la normatividad.
3. Auditoría del área de TI: contratos (laborales, *outsourcing*, entre otros).
4. Herramientas de apoyo a la auditoría del área de TI.

AMBIENTES SEGUROS DE INFORMACIÓN

I. SEGURIDAD DE LA INFORMACIÓN.

1. Conceptos fundamentales.
2. Antecedentes y datos históricos.
3. Prejuicios de la seguridad informática.
4. La seguridad en la sociedad de la información.

II. ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA.

1. Planeación y administración de la seguridad: integración de seguridad a los procesos de tecnologías de información (TI); políticas corporativas de seguridad; compromisos de la seguridad; opciones sobre el análisis de riesgo oficial de seguridad de TI.
2. Cultura de la seguridad informática.

3. Mejoramiento de la seguridad.

III. ESQUEMAS DE SEGURIDAD.

1. Seguridad perimetral.
2. Seguridad interior.

IV. PLANES DE CONTINGENCIA Y DE RECUPERACIÓN DE DESASTRES.

1. Clasificación de la información.
2. Planes de contingencia: *BCP (Process Control Block)*, *DRP (Disaster Recovery Plan)*, entre otros.
3. Identificación de controles preventivos.
4. Plan de recuperación de desastres: servidores; sitios *web*; *LAN*; sistemas de escritorio y móviles; requerimientos del personal; recursos necesarios.
5. Pruebas de los planes de contingencia.

V. MODELO DE MADURACIÓN DE LA SEGURIDAD INFORMÁTICA.

1. Arquitectura del modelo.
2. Mejoramiento del modelo.
3. Niveles de capacidad: seguridad informal; planeación y seguimiento; controles de calidad; mejoramiento continuo.
4. Mejores prácticas en la organización para la seguridad de los datos.

VI. GRUPOS DE RESPUESTA A INCIDENTES.

1. Definición, misión, visión.
2. Capacidades de los grupos: servicios y actividades, entre otras.
3. Factores operacionales: estructura organizacional; autoridad.
4. Alcances de los grupos: recursos; campos de acción.
5. Modelos de grupos: centralizado; distribuido; combinado; coordinador.
6. Manejo de incidentes: conceptos y procesos; mapeo de procesos; flujo de información y descripciones; tipos de incidentes; ciclo de vida de un incidente.
7. Cómputo forense: concepto; ciberleyes; recolección de evidencia (volátil y persistente); análisis de evidencia.

VII. PRUEBAS DE PENETRACIÓN.

1. Metodologías existentes.
2. Acuerdos y contratos para la aplicación de pruebas.
3. Planeación de pruebas.
4. Análisis de vulnerabilidades.
5. Pruebas internas y externas de penetración.
6. Penetración de aplicaciones.
7. Reportes y seguimiento.

VIII. TÓPICOS AVANZADOS DE SEGURIDAD INFORMÁTICA.

1. Seguridad en *VoIP* (Voz sobre Protocolo de Internet).
2. Robo de identidad y engaños por correo.
3. Seguridad en dispositivos móviles.
4. Herramientas de apoyo a la seguridad informática.