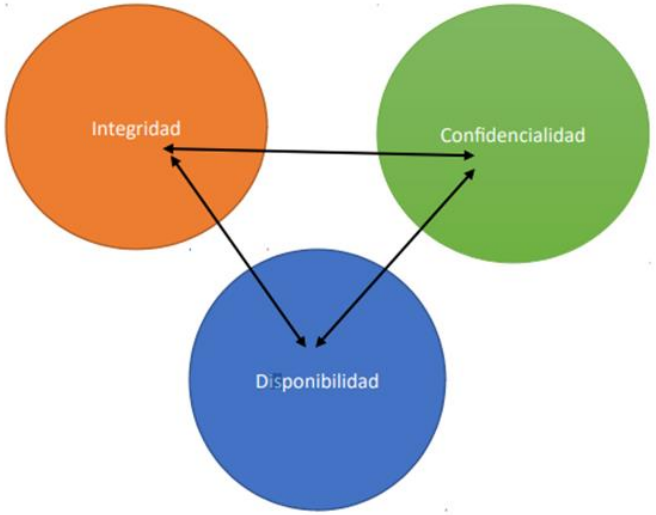
FIDE VIRTUAL

Principios de Ciberseguridad

Estándares y regulaciones sobre seguridad en TI

Introducción al módulo

- Módulo anterior: Conceptos sobre Ciberseguridad
  - Generalidades de la seguridad informática
  - El valor de la información
  - Definición y tipos de seguridad informática
  - Objetivos de la seguridad informática
  - Gestion y evaluación del riesgo



FIDE VIRTUAL

Introducción al módulo

- Estándares y regulaciones sobre seguridad en TI
  - ISO27000
  - COBIT
  - ITIL
  - Entes éticos reguladores
  - Ley en CR

COBIT®

ITIL®

FIDE VIRTUAL

Estándares y regulaciones sobre seguridad en TI

- Estándar: se indica que hace referencia a que sirve como modelo, patrón o referencia. (RAE)

- Regulación: acción y efecto de regular. (RAE)
  - Regular: Determinar las reglas o normas a que debe ajustarse alguien o algo. (RAE)

- Por tanto, en relación a la seguridad informática se analizarán los siguientes estándares: ISO2700, COBIT e ITIL

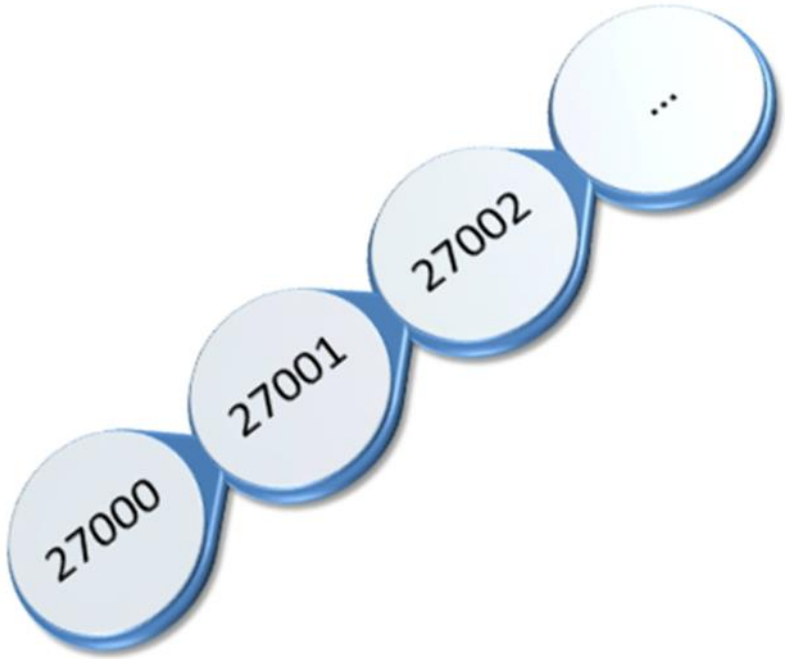
FIDE VIRTUAL

COBIT®

ITIL®

ISO27000

- ISO/IEC 27000: son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). **Es un vocabulario estándar para el SGSI (tercera versión Enero 2014)**.
- La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).



FIDE VIRTUAL

ISO27001

- ISO/IEC 27001: es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). **Es la certificación que deben obtener las organizaciones.**
- Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

DOMINIOS DE LA NORMA ISO 27001

FIDE VIRTUAL

ISO27002 / BS17799

- BS 17799: **es un código** de prácticas o de orientación o documento de referencia se basa en las **mejores prácticas de seguridad de la información**, esto define un proceso para evaluar, implementar, mantener y administrar la seguridad de la información.

- BS 17799 se basa en BS 7799-1 de control consta de 11 secciones, 39 objetivos de control y 133 prácticas; hoy en día no se utiliza para la evaluación y la actualización de este norma fue rebautizado con la norma ISO 27002, última versión setiembre 2013.

FIDE VIRTUAL

BS: British Standard del British Standard Institute

ISO27002 / BS17799

- ISO 27002: se base en 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

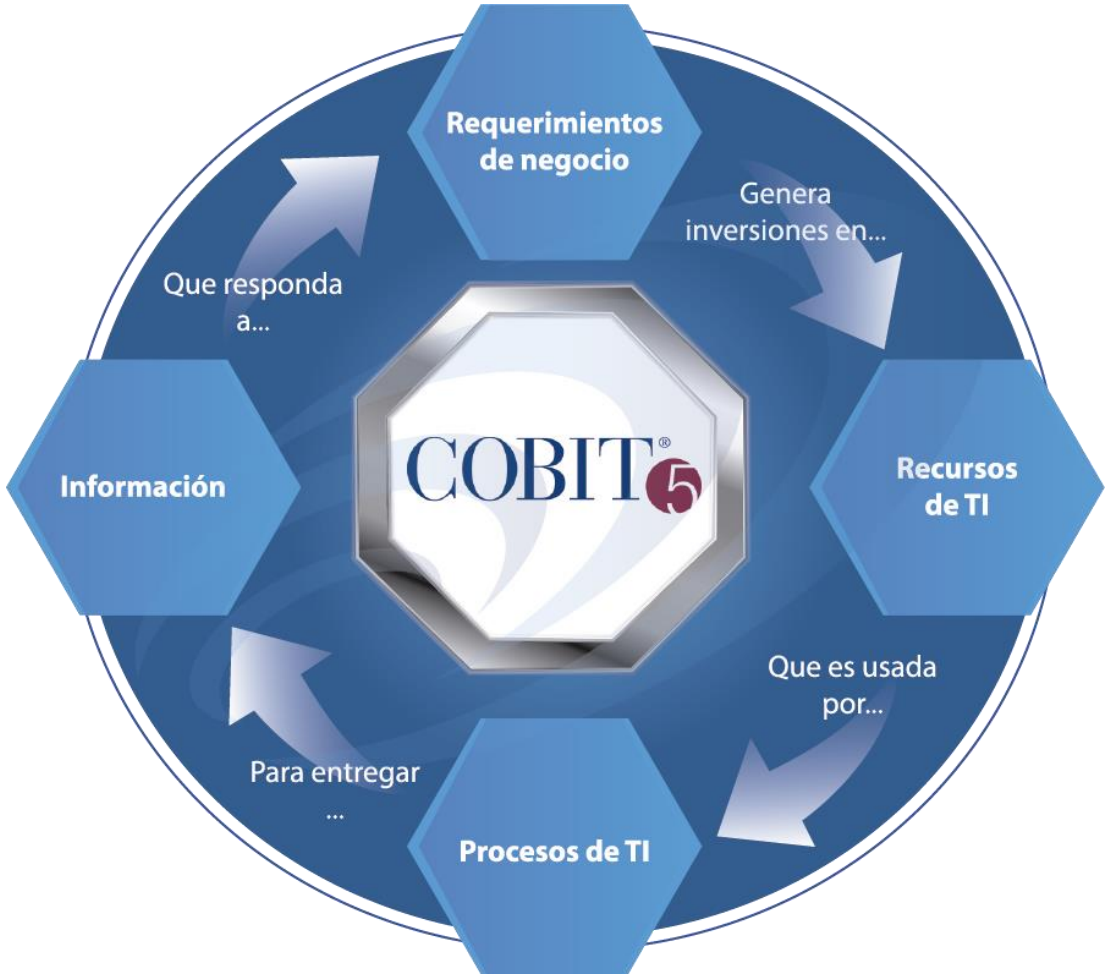
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

https://www.iso27000.es/iso27000.html

COBIT

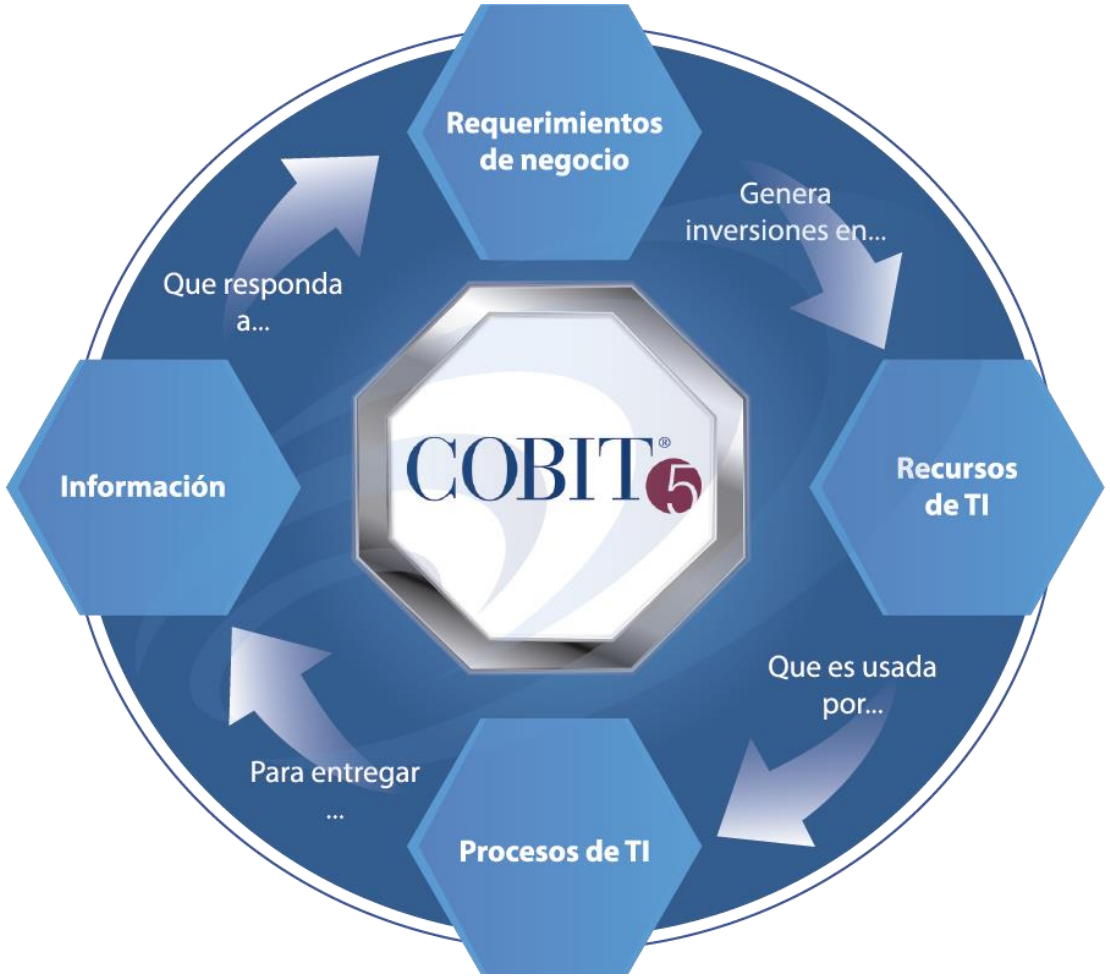
- Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información (TI).
- Mantenido por ISACA (en inglés: Information Systems Audit and Control Association) y el IT GI (en inglés: IT Governance Institute), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.



FIDE VIRTUAL

COBIT

- La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 (la edición en línea estuvo disponible en 2003); la cuarta edición en diciembre de 2005, y la versión 4.1 está disponible desde mayo de 2007.



FIDE VIRTUAL

COBIT

- COBIT 4.1.4: tiene 34 procesos que cubren 210 objetivos de control (específicos o detallados) clasificados en cuatro dominios:
    1. Planificación y Organización (Plan and Organize))
    2. Adquisición e Implantación (Acquire and Implement)
    3. Entrega y Soporte (Deliver and Support)
    4. Supervisión y Evaluación (Monitor and Evaluate)

FIDE VIRTUAL

COBIT

- COBIT 5: es la edición del framework aceptado en abril de 2012, se basa en COBIT 4.1, y a su vez lo amplía mediante la integración de otros importantes marcos y normas como Val IT y Risk IT, ITIL y las normas ISO relacionadas en esta norma.
- COBIT 5 ayuda a empresas de todos los tamaños a:
    1. Optimizar los servicios el coste de las TI y la tecnología
    2. Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas
    3. Gestión de nuevas tecnologías de información

- En junio de 2012, ISACA lanzó **"COBIT 5 para la seguridad de la información",** actualizando la última versión de su marco a fin de proporcionar una guía práctica en la seguridad de la empresa, en todos sus niveles prácticos.

- COBIT 5 para seguridad de la información puede ayudar a las empresas a reducir sus perfiles de riesgo a través de la adecuada administración de la seguridad.

FIDE VIRTUAL

COBIT® 5

COBIT

- COBIT 2019: Este marco de gobernanza revisado contiene todo lo que valora sobre COBIT 5, además de nuevas funciones y áreas de enfoque interesantes.
- Contiene una descripción detallada del Modelo Básico de COBIT y sus 40 objetivos de gobernanza / gestión.
- Cada objetivo de gobernanza / gestión y su propósito se definen y luego se combinan con el proceso relacionado, los objetivos de alineación y los objetivos empresariales.
- Describe prácticas probadas para anticipar, comprender y optimizar el riesgo de IT mediante la implementación del Marco del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. para mejorar la ciberseguridad de infraestructura crítica

FIDE VIRTUAL

COBIT 2019

ITIL

- Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un conjunto de conceptos y prácticas para la **gestión de servicios de tecnologías de la información**, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.
- ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a **lograr calidad y eficiencia en las operaciones de TI**. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

FIDE VIRTUAL

ITIL

- Se desarrolló durante los años 1980.
- Fue ampliamente adoptada hasta mediados de los años 1990.
- Las recomendaciones de ITIL fueron desarrolladas por la Central Computer and Telecommunications Agency (CCTA) del gobierno británico.
- ITIL fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la Gestión de TI.
- ITIL versión 1: terminó expandiéndose hasta unos 31 libros
- ITIL versión 2: agrupa los libros de manera lógica a tratar los procesos de administración que cada uno cubre: diversos aspectos de los sistemas de TIC, de las aplicaciones y del servicio.
- Actualmente existe la nueva versión ITIL v3 que fue publicada en mayo de 2007.

FIDE VIRTUAL

ITIL

Los ocho libros de ITIL y sus temas son:

Gestión de Servicios de TI,

1. Mejores prácticas para la Provisión de Servicio
2. Mejores prácticas para el Soporte de Servicio
3. Gestión de la infraestructura de TI
4. Gestión de la seguridad
5. Perspectiva de negocio
6. Gestión de aplicaciones
7. Gestión de activos de software
8. Planeando implementar la Gestión de Servicios

- Más recientemente se añadió una guía con recomendaciones para departamentos de TIC más pequeños:
  - 9. Implementación de ITIL a pequeña escala

FIDE VIRTUAL

ITIL

ITIL v3 reestructura el manejo de los temas para consolidar el modelo de "Ciclo de Vida del Servicio" separando y ampliando algunos subprocesos hasta convertirlos en procesos especializados.
Esta modificación responde a un enfoque empresarial para grandes corporaciones

El Ciclo de Vida del Servicio consta de cinco fases también llamadas disciplinas, correspondientes a los nuevos libros de ITIL®:

1. Estrategia del Servicio
2. Diseño del Servicio
3. Transición del Servicio
4. Operación del Servicio
5. Mejora Continua del Servicio

FIDE VIRTUAL

ITIL

FIDE VIRTUAL

Entes éticos reguladores

FIDE VIRTUAL

Entes éticos reguladores

acm.org

Libreria digital | MCCA | Cola | TechNews | Centro de carreras

Association for Computing Machinery

Promoción de la informática como ciencia y profesión

Unirse | Voluntario | myACM | Buscar

SOBRE ACM | AFILIACIÓN | PUBLICACIONES | SIG | CONFERENCIAS | CAPÍTULOS | PREMIOS | EDUCACIÓN | CENTRO DE APRENDIZAJE | POLÍTICA PÚBLICA

DIVERSIDAD E INCLUSIÓN

Asociación para Maquinaria de Computación

Promoción de la informática como ciencia y profesión

Vemos un mundo donde la informática ayuda a resolver los problemas del mañana, donde usamos nuestros conocimientos y habilidades para hacer avanzar la profesión y generar un impacto positivo.

ACM actualiza el código de ética

ACM actualizó recientemente su Código de Ética y Conducta Profesional . El Código de Ética revisado aborda los avances significativos en la tecnología informática desde la versión de 1992, así como la creciente omnipresencia de la informática en todos los aspectos de la sociedad. Para promover el Código en la comunidad informática, ACM creó un folleto, que incluye el Código, estudios de casos que ilustran cómo se puede aplicar el Código a situaciones que surgen en la práctica diaria y sugerencias sobre cómo se puede utilizar el Código en entornos educativos y en empresas y organizaciones. Descargue un PDF del folleto del Código ACM .

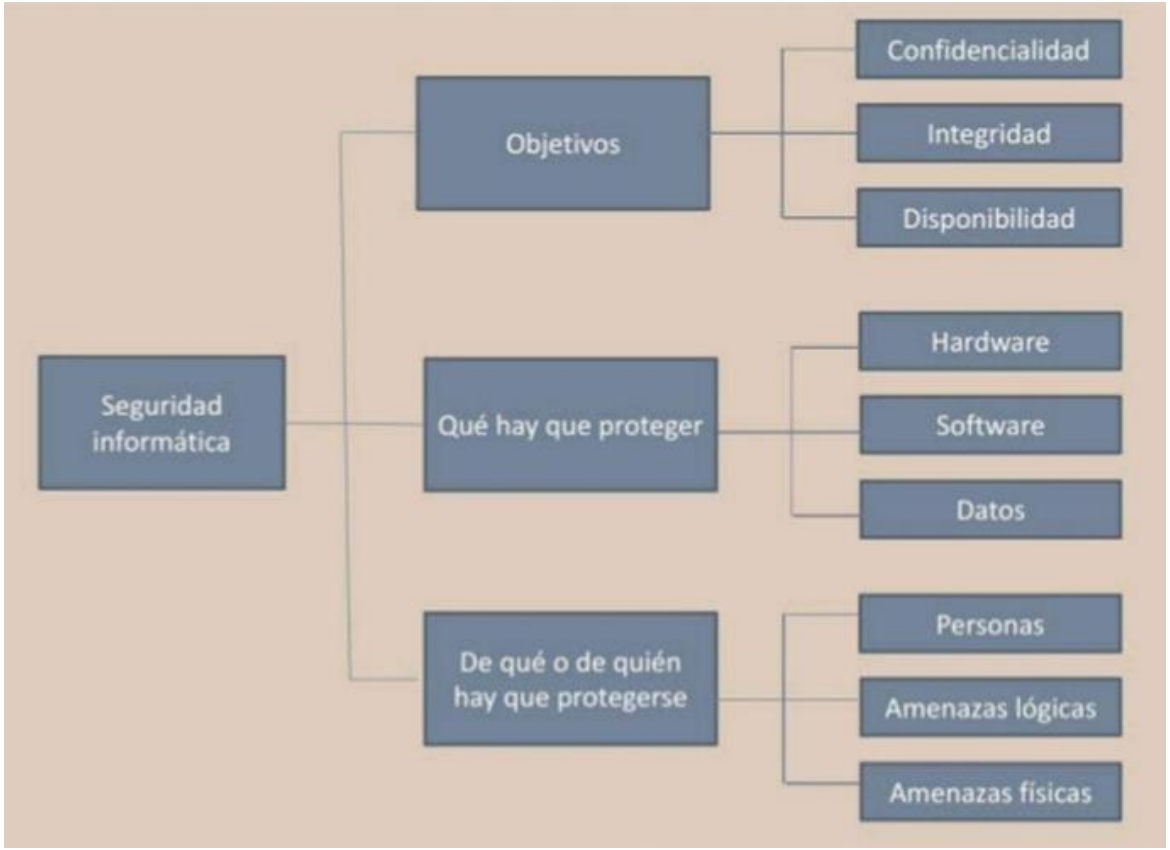
FIDE VIRTUAL

Entes éticos reguladores

FIDE VIRTUAL

Ley en Costa Rica

- Ley 9048: Delitos informáticos y conexos.
  - Corrupción
  - Violación de comunicaciones o correspondencias
  - Violación de datos personales
  - Extorsión
  - Estafa informática
  - Daño Informático
  - Espionaje
  - Entre otros…
- Los castigos son de 6 meses a 6 años de cárcel según el delito



FIDE VIRTUAL

Culminación del módulo

- Estándares y regulaciones sobre seguridad en TI
  - ISO27000/1/2
  - COBIT
  - ITIL
  - Entes éticos reguladores
  - Ley en CR

Ley 9048 Delitos informáticos Costa Rica

Gracias