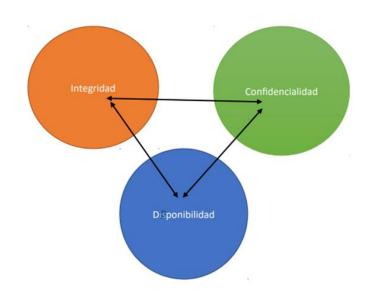


Introducción al módulo

- Módulo anterior: Conceptos sobre Ciberseguridad
 - o 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





Introducción al módulo

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









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



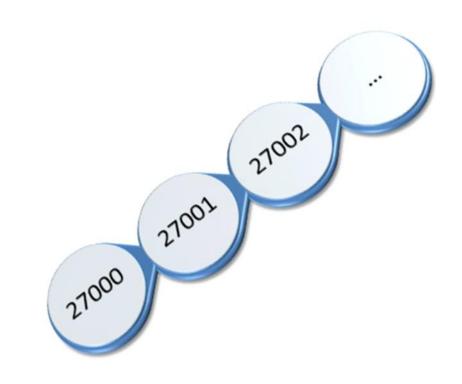






ISO27000

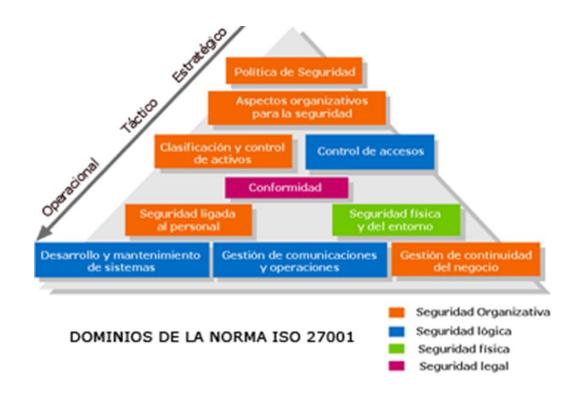
- ISO/IEC 27000: son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Es un vocabulario estándar para el SGSI (tercera versión Enero 2014).
- La serie contiene las mejores prácticas recomendadas en Seguridad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





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).





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.



BS: British Standard del British Standard Institute

ISO27002 / BS17799

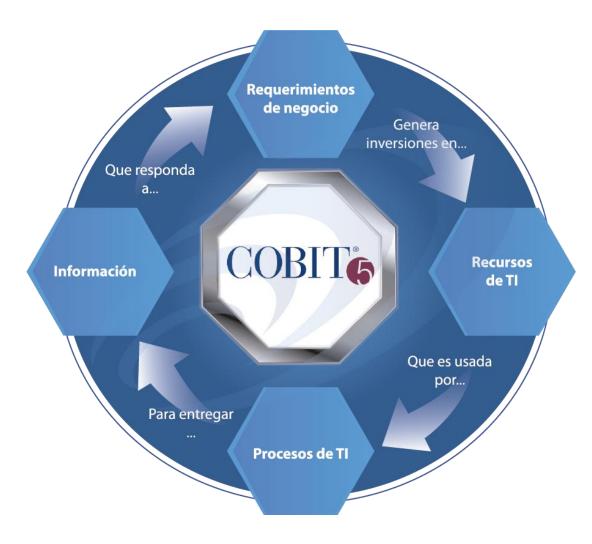
• ISO 27002: se base en 14 dominios, 35 objetivos de control y 114 controles de ISO/IEC 27002:2013



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

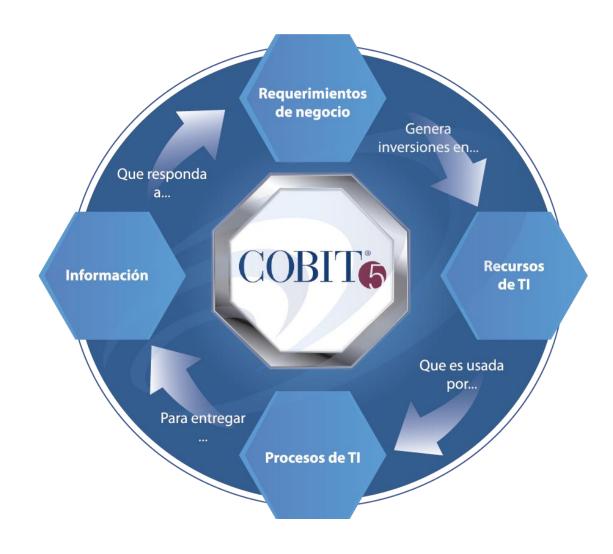
5.1.1 Corputade de pilitaces para la seguirada de la información. 5.1.2 Revisión de las políticas para la seguirada de la información. 5.1.1 Corputade de pilitaces para la seguirada de la información. 5.1.2 Revisión de las políticas para la seguirada de la información. 5.1.1 Corputado de pilitaces para la seguirada de la información. 6.1.1 Asparación de responsabilidades para la seguir de la información. 6.1.1 Asparación de responsabilidades para la seguir de la información. 6.1.2 Seguipación de responsabilidades para la seguir de la información. 6.1.3 Esguipación de responsabilidades para la seguir de la información. 6.1.4 Corputado de interior seguipación de proyectos. 6.1.5 Seguidad de la información en la gestión de proyectos. 6.1.6 Corputado de la información en la gestión de proyectos. 6.1.1 Asparación de responsabilidades para movilade y lebelarbaje. 6.1.1 Asparación de responsabilidades para la seguir de la información. 6.1.2 Disposibles para movilade y lebelarbaje. 6.1.3 Feducado de autocolomica de la información en la gestión de proyectos. 6.1.1 Asparación de responsabilidades para la seguir de de seguipos de la información en la gestión de proyectos. 6.1.1 Asparación de responsabilidades para la seguir de la información en la gestión de proyectos. 6.1.1 Asparación de responsabilidades de gestión de proyectos. 6.1.2 Politica de sua de de seguipos de la información en la gestión de proyectos. 7.1.1 Investigación de antecedentes. 7.1.2 Terminos y condiciones de contritación. 7.2.1 Persponsabilidades de gestión. 7.2.2 Proyecos despidinatos. 7.2.3 Proyecos despidinatos. 7.2.4 Responsabilidades de gestión. 7.2.5 Proyecos despidinatos. 7.2.6 Responsabilidades de gestión. 7.2.7 Responsabilidades de gestión. 7.2.8 Responsabilidades de gestión. 7.2.9 Responsabilidades de gestión. 7.2.1 Investigación de antecedentes. 8.2.1 Investigación de antecedentes. 8.2.2 Esperación de la información. 8.2.3 Esponsabilidades de la información. 8.2.4 Responsabilidades de la información. 8.2.5 Esponsabilidades de la informació			
10.1.1 Portural de politicos para la seguridad de la la información. 13.2 Revierdo de las politicas para la seguridad de la información. 14.3 Escurido de las politicas para la seguridad de la información. 15.12 Revierdo de las politicas para la seguridad de la información. 16.12 Seguridad de la información en la greativa de la información de la politica para la seguridad de la información de la politica para la seguridad de la información de seguridad de la información de la politica para la seguridad de la información de la politica para la seguridad de la información de la politica para la seguridad de la información de la politica para la seguridad de la información de la politica para la seguridad de la información de la politica para mortidad y lesiones para mortidad y electrica para mortidad para mortidad y electrica para mortidad y	. POLÍTICAS DE SEGURIDAD.	10. CIFRADO.	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS
1. SECURIDAD FISICA Y AMBIENTAL. 1. I Assignation de responsabilidades para la segur. de la información. 6. 1. F. Aspraction de responsabilidades para la segur. de la información. 6. 1. Contacto con supros de interés especial. 6. 1. Contacto con supros de interés especial. 6. 1. Contacto con supros de interés especial. 6. 1. Contacto con prupos de interés especial. 6. 1. Seguridad de la información en la gestión de proyedos. 6. 1. Portica de las de dispositivos para movilidad. 6. 2. Telerándo de la información. 7. 1. Portica de uso de dispositivos para movilidad. 6. 2. Telerándo de suprocedentes. 7. 1. 1. Terminos y condiciones de contratación. 7. 1. Terminos y condiciones de contratación. 7. 2. Dumarie la contratación de puesto de p	 5.1.1 Conjunto de políticas para la seguridad de la información. 	10.1.1 Política de uso de los controles criptográficos.	14.1 Requisitos de seguridad de los sistemas de información.
1.1 Aproximation de responsabilidades para la segur. de la información de la compración de responsabilidades para la segur. de la información de la compración de responsabilidades para la segur. de la información de la compración de responsabilidades para la segur. de la información de la compración de responsabilidades para la segur. de la información de la compración de responsabilidades para la segur. de la información de la compración de la reformación en la gestión de proyectos. 5. 1. Aproximación de mandra de la reformación en la gestión de proyectos. 5. 2. Escuritación de la compración de mandra de la reformación de la compración de mandra de la reformación de la compración de mandra de la reformación de la reformación de la compración de mandra de la reformación de la reformación de la compración de mandra de la reformación de la reform			14.1.2 Seguridad de las comunicaciones en servicios accesibles por rec
6.1.1 Segregación de transportabilidades para la segur. de la información. 6.1.2 Segregación e transportabilidades para la segur. de la información. 6.1.1 Portinetro de seguridad fisica. 6.1.2 Cortitato con grupos de interés especial. 6.1.3 Seguridad de la información en la gestión de proyectos. 6.2.1 Portinetro de seguridad de la información en la gestión de proyectos. 6.3.1 Portinetros para movitidad. 6.3.1 Portinetros para movitidad. 6.3.1 Portinetros para movitidad. 6.3.1 Portinetros para movitidad y leterbalogo. 7.3.1 Investigación de crisco para de la seguridad de la información de sequipos. 7.3.1 Investigación de crisco para de la contractión en la gestión de seguridad de la información de seguridad sobre los activos. 8.1 Marco participación de seguridad sobre los activos. 8.1 Marco participación de seguridad sobre los activos. 8.1 Marco participación de seguridad sobre los activos. 8.2 Marquicación de seguridad sobre los activos. 8.3 Marquicación de seguridad de la información de la informa			públicas:
7.2.2 Concioneriación, educación y capacitación en seguri. de la información. 7.2.3 Proceso disciplinario. 7.3 Ceseo combio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo. 7.3.1 Ceseo cambio de puesto de trabajo. 7.3.1 Ceseo o cambio de puesto de trabajo. 7.3.2 Ceseo de la uniformación de cambio de puesto de trabajo. 7.3.1 Ceseo o cambio de puesto de trabajo. 7.3.2 Ceseo de la uniformación de cambio de puesto de trabajo. 7.3.2 Ceseo de la uniformación de cambio de puesto de trabajo. 7.3.2 Ceseo de la uniformación de cambio de cambio de la información de cambio de cambio de la información de la cambio de cambio de la información de cambio de la información de la cambio de la información	6.1.1 Asignación de responsabilidades para la segur, de la información. 6.1.2 Segregación de larras. 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. 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Teminos y condiciones de contratación.	11.1.1 Perimetro de segunidad física. 11.1.2 Controles físicos de entrada. 11.1.3 Segunidad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas segunas. 11.1.6 Areas de acceso público, carga y descarga. 11.2 Segunidad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Segunidad 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 Segunidad de los equipos.	14.2 Segundad en los procesos de desarrollo y soporte. 14.2.1 Bellibra 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 Resificationes a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 14.2.6 Segundad 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.
1.2.2 Control de puesto de trabajo. 2.3 Cestos o disciplinario. 2.3 Cestos o disciplinario. 2.4 Esculpinado En La OPERATIVA. 2.1 Responsabilidades de puesto de trabajo. 2.1 Responsabilidades procedimientos, de operación. 2.1.1 Combre de carecto de la información para suministradores. 2.1.2 Projectad de los activos. 3.1.3 Los aceptable de los de carectos. 3.2 Projectad de los activos. 3.2 Eliminación de activos. 3.2.1 Directrices de clasificación. 3.2.2 Eliminación de activos. 3.2.3 Eliminación de activos. 3.3 Septentado y manipulación de activos. 3.4 Responsabilidades exprocedimientos, de operación. 2.4 Responsabilidades exprocedimientos, de operación. 2.5 Eliminación de activos. 3.6 Interpretado y manipulación de la información. 3.7 Protectivos de clasificación. 3.8 Manego de la superación de activos. 3.8 Manego de la superación de activos. 3.9 Eliminación de activos. 3.1 Política de seguridad de la información para subridad de la información y unique de peración. 2.2 Eliminación de activos. 3.2 Eliminación de activos. 3.3 Septentados y questos de vertiras de accidados y unique de peración. 2.4 Responsabilidades y procedimientos, de operación. 2.5 Protección de accidados de la información. 2.6 Responsabilidados de la información de la información y unique de la información de la info			15. RELACIONES CON SUMINISTRADORES.
7.3 Cese o cambio de puesto de trabajo. 7.3 Cese o cambio de puesto de trabajo. 8.1 Responsabilidades y procedimentos de operación. 9.2 In formación de la información de sucurior de la control de acceso a familio de puesto de trabajo. 9.2 Casardon de la información de la control de acceso a familio de la información			
7.3.1 Cese o cambin de puesto de trabajo. 1.4 Esponsabilidad sobre los activos. 1.5.1 Inventano de activos. 1.6.1.1 propiedad de los activos. 1.7.2 Propiedad de los activos. 1.8.1.2 Propiedad de los activos. 1.8.1.3 Use aceptable de los activos. 1.8.1.3 Use aceptable de los activos. 1.8.1.3 Use aceptable de los activos. 1.8.2 Classificación de la información. 1.8.2 Classificación de la información. 1.8.2.1 Directricos de classificación de la información. 1.8.2.3 Manejo de los sopries ficación de la información. 1.8.3.3 Soportes siscos en triariab. 1.8.3.3 Soportes siscos en triariab. 1.9.1 Política de control de acceso a fina redea y servicios asociados. 1.9.1 Política de control de acceso a las redea y servicios asociados. 1.9.2 Gestión de altrado e da attencación de superior de información. 1.9.2 Gestión de autorio de acceso a las redea y servicios asociados. 1.9.2 Recysialos de megodo para el control de acceso as las redea y servicios asociados. 1.9.2 Gestión de autorio de acceso a las redea y servicios asociados. 1.9.2 Gestión de altrado e de autorio confidencia de autoriorio de acceso a las redea y servicios asociados. 1.9.2 Gestión de información confidencia de autoriorio de acceso a las redea y servicios asociados. 1.9.2 Recysialos de neceso de usuario. 1.9.2 Recysialos de neceso de usuario. 1.9.2 Recysialos de la información. 1.9.2 Recysialos de la información de la información. 1.9.2 Recysialos de neceso de usuario. 1.9.2 Recysialos de la información de socialos. 1.9.2 Recysialos de neceso de usuario. 1.9.2 Recysialos de neceso de usuario. 1.9.2 Recysialos de la información de la inf		12. SEGURIDAD EN LA OPERATIVA.	
El Responsabilidad sobre los activos. 8.1.1 Inventance de activos. 8.1.2 Projectad de los activos. 8.1.2 Projectad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.3 Uso aceptable de los activos. 8.2.1 Develución de activos. 8.2.1 Develución de activos. 8.2.2 Eliquetado y manipulado de la información. 8.2.3 Manejo de los soprotes de almacenamiento. 8.2.3 Manejo de los soprotes de almacenamiento. 8.3.3 Soportes fisicos en trinistio. 8.3.4 Develución de activos. 8.3.5 Soportes fisicos en trinistio. 8.3.6 Soportes fisicos en trinistio. 9.1 Requisitate de regotio para el control de accesos. 9.1.1 Control de acceso de los susurios. 9.1.2 Control de acceso de las receptos para el control de acceso de los susurios. 9.2.2 Gestión de los derechos de acceso aceso acignados as usuarios. 9.2.3 Gestión de los derechos de acceso aceso acignados as usuarios. 9.2.4 Escrito de los derechos de acceso aceso acignados as usuarios. 9.2.5 Revisión de los derechos de acceso aceso acignados as usuarios. 9.2.6 Restrado a calapstación de los derechos de acceso aceso de los usuarios. 9.2.6 Restrado a calapstación de los derechos de acceso de los usuarios. 9.2.6 Restrado a calapstación de los derechos de acceso de los usuarios. 9.2.6 Restrado a calapstación de los derechos de acceso de los usuarios. 9.2.7 Procedimientos de la información. 9.2.8 Responsabilidades del susuarios. 9.2.9 Responsabilidades del susuarios. 9.2.1 Políticos de control de acceso de los usuarios. 9.2.2 Gestión de los derechos de acceso de los usuarios. 9.2.3 Estido de los derechos de acceso de los usuarios. 9.2.4 Servición de los derechos de acceso de los usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Restrado a calapstación de los derechos de acceso de los usuarios. 9.2.7 Procedimientos de los derechos de acceso de los usuarios. 9.2.8 Responsabilidades del substitución de los derechos de acceso de los usuarios. 9.2.9 Responsabilidades del substitución de los derechos de acceso de los usuarios. 9.2.1 Políticos de control de acceso de	7.3.1 Cese o cambio de puesto de trabajo.		
8.1.1 Propiedad de los activos. 8.1.2 Propiedad de los activos. 8.1.2 Propiedad de los activos. 8.1.3 Dos exeptables de los activos. 8.2 Propiedad de los activos. 8.2 Control de los activos. 8.2 Eliquetado y manipulado de la información. 8.2 Eliquetado y manipulado de la información. 8.2 Eliquetado y manipulado de la información. 8.3.1 Gestión de sopretes estrables. 8.3.2 Eliminación de sopretes estrables. 8.3.3 Sopretes fiscos en trificario. 9.1.2 Propiedad de control de acceso en trificario. 9.2 Recystiones de recipios estrables. 9.3.3 Eleminación de sopretes fiscos en trificario. 9.1.1 Política de control de acceso en trificario. 9.2.2 Gestión de sopretes de acceso de usuario. 9.3.3 Control de acceso a las redes y servicios asociados. 9.3.4 Control de acceso a de usuario. 9.4 Control de acceso a sistema y aplicaciones. 9.5 Recystion de los derechos de acceso de los usuarios. 9.6 Responsabilidades del usuario. 9.7 Recystion de los derechos de acceso de los usuarios. 9.8 Responsabilidades del usuario. 9.9 Recystion de los derechos de acceso de los usuarios. 9.1 Control de acceso a de sucuario. 9.2 Gestión de altra cambinación de software. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistema y aplicaciones. 9.5 Responsabilidades del usuario. 9.6 Responsabilidades del usuario. 9.7 Recystion de los derechos de acceso de los usuarios. 9.8 Responsabilidades del usuario. 9.9 Recystion de los derechos de acceso de los usuarios. 9.1 Recystion de los derechos de acceso de los usuarios. 9.2 Responsabilidades del usuario. 9.3 Le control de acceso a sistema y aplicaciones. 9.4 Control de acceso a sistema y aplicaciones. 9.5 Recystion de los derechos de acceso de los usuarios. 9.5 Recystion de los derechos de acceso de los usuarios. 9.6 Recystion de los derechos de acceso de los usuarios. 9.7 Recystion de los derechos de acceso de los usuarios. 9.8 Recystion de los derechos de acceso de los usuarios. 9.9 Recystion de los derechos de acceso de los usuarios. 9.1 Recystion de los derechos de acceso de los usuari	. GESTIÓN DE ACTIVOS.		
9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas. 18.2.1 Revisión independente de la seguridad de la información. 18.2.2 Cumplimiento de las políticas y normas de seguridad.	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. 8.1.4 Devolución de activos. 8.2 Clasificación de la información. 8.2.1 Directrices de clasificación. 8.2.2 Ediquetado y manipulado de la información. 8.2.3 Manipulación de activos. 8.3 Manipulación de activos. 8.3.1 Gestión de soportes estrabeles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito. 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 a las redes y servicios asociados. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Revisión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Revisión de los derechos de acceso de los usuarios. 9.2.7 Revisión de los derechos de acceso de los usuarios. 9.2.8 Revisión de los derechos de acceso de los usuarios. 9.2.9 Revisión de los derechos de acceso de los usuarios. 9.2.1 Uso de información confidencial para la autenticación de usuarios. 9.3 Responsabilidades del usuario. 9.4.1 Restincción del acceso a fa información.	12.1.2 Gestión de gampios. 12.1.4 Separación de enformos de desamollo, prueba y inoducción. 12.2 Protección centra código malidiose. 12.2 Corindes centra código malidiose. 12.3 Copins de segundad. 12.3 Copins de segundad. 12.3 Copins de segundad. 12.4 Registro de actividad y superissión. 12.4 Registro de actividad y superissión. 12.4.3 Registro de gestión de vermas de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registro de actividad del administrador y operador del sistema. 12.4.4 Sincronización de recipies. 12.5 Control del software en explotación. 12.6.1 Instalación del software en sistemas en producción. 12.6.1 Instalación del software en sistemas. 12.6.2 Restricciones en la retalidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorias de los sistemas de información. 12.7.1 Controles de auditoria de los sistemas de información. 13.1 Gestión de las guerradad en las redes. 13.1 Controles de red. 13.1.3 Segregación de redes. 13.1.1 Controles de red. 13.1.3 Segregación de redes. 13.2 Intercambio de información con parles externas. 13.2.1 Políticas y procedimientos de información de Información. 13.2.2 Acuerdos de información con parles externas.	15.22 Gestión de ciambios en los servicios prestados por terceros. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. 16. 10. Respinsabilidades y procedimientos. 16. 11. Responsabilidades y procedimientos. 16. 12. Notificación de los eventos de seguridad de la información. 16. 13. Notificación de puntos debiles de la seguridad. 16. 14. Valoración de eventos de seguridad de la información y toma de decisiones. 16. 15. Respuesta a los incidentes de seguridad de la información. 16. 16. Aprendizaje de los incidentes de seguridad de la información. 16. 17. Recoplización de evidencias. 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN E LA CONTINUIDAD DEL NEGOCIÓ. 17. 1. Continuidad de la seguridad de la información. 17. 1. Planificación de la continuidad de la seguridad de la información. 17. 1. Implantación de la continuidad de la seguridad de la información. 17. 1. Planificación de la continuidad de la seguridad de la información. 17. 2. Redundancias. 17. 2. Redundancias. 18. 1. 2. Disponibilidad de instalaciones para el procesamiento de la información. 18. 1. 1 Identificación de la optimidad de la información. 18. 1. 1 Derechos de propiedad intelectual (IDP). 18. 1. 2. Protección de las registros de la organización. 18. 14. Protección de datos y privacidad 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.

- 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.





 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.





- 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)





- 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.





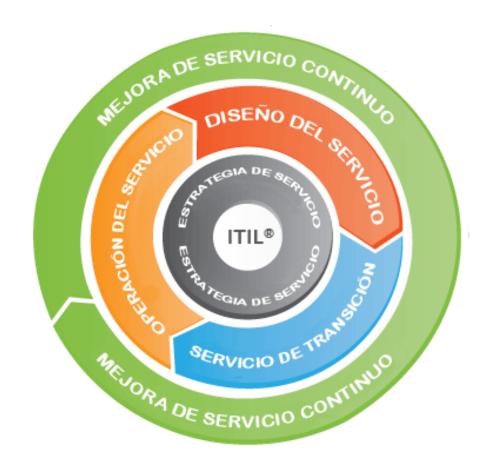
- COBIT 2019: Este marco de gobernanza revisado contiene todo lo que valora sobre COBIT 5, además de nuevas funciones y áreas de enfoque interesantes.
- Contiene una descripción detallada del Modelo Básico de COBIT y sus 40 objetivos de gobernanza / gestión.
- Cada objetivo de gobernanza / gestión y 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



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.





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.



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



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





Estrategia del servicio

- Gestión del portafolio de servicios
- Gestión financiera de TI
- Gestión de relaciones de negocio

Diseño del servicio

- Coordinación del Diseño
- Gestión de niveles del servicio
- Gestión del catálogo de servicios
- Gestión de proveedores
- Gestión de la seguridad de la información
- Gestión de la disponibilidad
- Gestión de la capacidad
- Gestión de la continuidad de servicios TI

Transición del servicio

- Planificación de la transición y soporte
- Gestión de la configuración y de activos del servicio
- Gestión de cambios
- Gestión de liberación e implementación
- · Gestión del conocimiento

Operación del Servicio

Procesos:

- Gestión de eventos
- Gestión de incidencias
- Gestión de solicitudes
- Gestión de problemas
- Gestión de accesos

Funciones:

- Servicie Desk
- Gestión técnica
- Gestión de aplicaciones Gestión de operaciones TI

Estrategia

Diseño

Transición

Operación

Mejora continua del servicio

Informes del servicio, Medición del servicio Retorno de inversión para la mejora y Preguntas al negocio para la mejora



Entes éticos reguladores

computerethicsinstitute.org/home.html

Instituto de Ética Informática

Proporcionar una brújula moral para el océano de la tecnología de la información

Hogar Sobre CEI Eventos Publicaciones CEI en la Prensa



Como líder en el campo, el Computer Ethics Institute ha proporcionado un foro y un recurso avanzado para identificar, evaluar y responder a los problemas éticos asociados con el avance de las tecnologías de la información en la sociedad. A través de actividades de asesoramiento y consulta, investigación y educación, y difusión pública, CEI ha estimulado la conciencia de los problemas que pueden surgir a medida que la tecnología continúa desarrollándose.

Una encuesta revela que el personal de TI



está fisgoneando ¿Hay gente fisgoneando en los archivos de su computadora personal en el trabajo? Una nueva encuesta muestra que mirar archivos confidenciales es bastante común. John Henrehan informa sobre Fox 5 News y muestra lo que ha hecho CEI para educar a los profesionales de TI y al público sobre la ética informática.

Computer Ethics Institute

A moral compass for cyberspace

Diez mandamientos de la ética informática

Los Diez Mandamientos de la ética informática han sido yn código de ética muy eficaz para el uso adecuado de la tecnología de la información.



Entes éticos reguladores





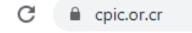


ACM actualiza el código de ética

ACM actualizó recientemente su Código de Ética Conducta Profesional . El Código de Ética revisado shorda 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.

Descarque un PDF del folleto del Código ACM (A)

Entes éticos reguladores





LA INSTITUCIÓN

ACTIVIDADES

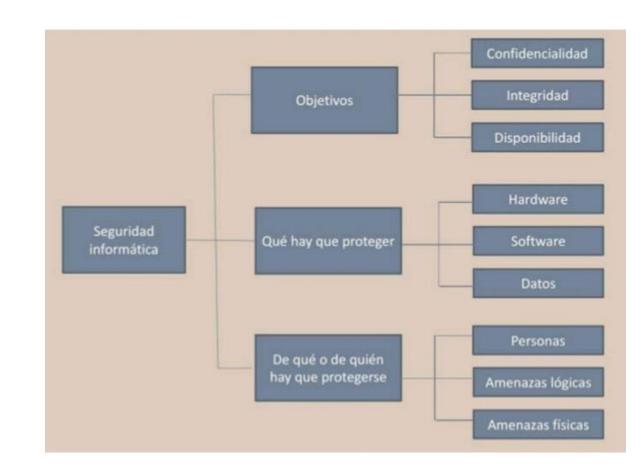
Colegio de Profesionales en Informática y Computación

El Colegio de Profesionales en Informática y Computación (CPIC), es un ente no estatal de derecho público con plena capacidad jurídica y patrimonio propio, creado mediante la Ley No.7537 del 1 de noviembre de 1995. Dentro de sus principales objetivos están el promover el progreso de los profesionales en informática y computación, así como emitir opinión y asesorar en materia de su competencia a los Poderes del Estado, organismos, asociaciones, e instituciones públicas y privadas.



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





Culminación del módulo



- ISO27000/1/2
- COBIT
- ITIL
- Entes éticos reguladores
- Ley en CR



Ley 9048 Delitos informáticos Costa Rica





COBIT[®]



