INGENIERÍA EN COMPUTACIÓN

Seguridad Informática Básica

Ejercicio Normatividad

Integrantes:
Chilpa Navarro Alan Salvador- 319207738
Medina Rubalcava Natalia Michell - 319207336
Murillo Rodríguez Sarah Sofia- 422130448
Ortega de la Paz Rafael - 420054085
Romero García Diana Sofía - 319339264

Grupo : 2

Semestre: 2027-1

Profesora: Dra. Cintia Quezada Reyes

Fecha: 1 septiembre 2026

- TCSEC
  Siglas: Trusted Computer System Evaluation Criteria (Criterios de Evaluación de Sistemas Informáticos de Confianza).
- **Año y lugar de creación**: Desarrollado en los Estados Unidos y publicado en agosto de 1983
- **Objetivos**:
  - Proporcionar una metodología rigurosa para evaluar las características de seguridad y confiabilidad de los sistemas operativos comerciales.
  - Servir de guía técnica a los fabricantes para incorporar controles de seguridad basados en la confidencialidad estricta de los datos.
  - Ofrecer una base de clasificación jerárquica que permitiera al gobierno de EE. UU. seleccionar de forma segura los sistemas destinados al procesamiento de información clasificada o sensible.
- **Características**:
  - Enfoque monolítico: Evaluaba el sistema como un bloque cerrado e indivisible (unificando la funcionalidad del software con las garantías del hardware).
  - Orientación militar: Su diseño priorizaba casi exclusivamente la confidencialidad de la información y la defensa frente a fugas de datos de inteligencia, restando peso a la integridad o disponibilidad de los sistemas.
  - Base en la TCB: Todo el análisis de protección radicaba en la Trusted Computing Base (Base de Computación de Confianza), el conjunto de componentes de hardware, firmware y software que ejecutan activamente las políticas de seguridad.
- **Nivel de seguridad que emplea**:
  - El estándar TCSEC clasifica la robustez de los sistemas informáticos utilizando cuatro divisiones jerárquicas, donde A representa la máxima seguridad y D la ausencia de protección real:
  - **División D** (Protección Mínima (Minimal Protection). Sistemas evaluados que no cumplen con los requisitos de ninguna de las categorías superiores. No ofrecen seguridad confiable (p. ej., MS-DOS antiguo).
  - **Clase C1** (Protección Discrecional de Seguridad). Control de acceso basado en la identidad de usuarios individuales o grupos. Requiere una separación básica entre usuarios y datos.
  - **Clase C2** (Protección de Acceso Discrecional Controlado). Mayor granularidad en los permisos de usuario. Introduce obligatoriamente auditorías de seguridad (audit trails) y reutilización segura de objetos en memoria.
  - **Clase B1** (Protección de Seguridad Etiquetada). Primer nivel de la Seguridad Mandatoria (MAC). Exige etiquetar jerárquicamente cada objeto informático (p. ej., "Secreto", "Confidencial") para limitar el acceso de los sujetos.
  - **Clase B2** (Protección estructurada). El sistema operativo se divide en módulos independientes. Se mitigan formalmente los canales encubiertos (covert channels) y se implementa la gestión separada de perfiles de administración.

- **Clase B3** (Dominios de seguridad). El mecanismo de control de acceso debe ser demostrablemente a prueba de manipulaciones. Exige una recuperación del sistema altamente estructurada tras fallos generalizados.
- **División A1** (Protección verificada). No añade nuevas funciones respecto a B3, pero exige un análisis matemático estricto y una verificación formal del diseño arquitectónico del software.
- **Secciones que lo componen:**

  Se divide estructuralmente en los siguientes bloques analíticos básicos:

  1. Criterios de Evaluación (Parte I): Define de forma precisa las cuatro divisiones jerárquicas (A, B, C y D) con sus respectivas subclases de control.
  2. Lineamientos de Diseño (Parte II): Recomendaciones dirigidas a los ingenieros de software sobre cómo implementar el Monitor de Referencia y los dominios de aislamiento.
  3. Apéndices Técnicos: Tablas de correspondencia de requisitos, glosario de términos específicos y directrices operacionales para administradores de TI.
- **Años de actualización**:

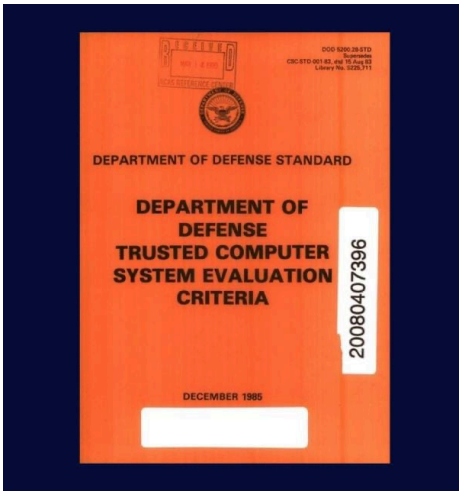
  Tras su lanzamiento en 1983, se publicó una revisión menor corregida y aumentada en el año 1985.

- **Última actualización/versiónñ** La edición de 1985 (registrada bajo el código DoD 5200.28-STD) constituyó su versión definitiva.
- **Vigencia actual:**

  No se encuentra vigente. Fue cancelado formalmente por el Departamento de Defensa de los EE. UU. el 24 de octubre de 2002. Fue sustituida por el estándar internacional Common Criteria (Criterios Comunes / ISO/IEC 15408) publicado originalmente a finales de la década de 1999/2005 debido a sus limitaciones (rigidez comercial y falta de enfoque en redes modernas).

- **Sitio web oficial:**

  Al ser un documento militar histórico descontinuado, no cuenta con un dominio web activo propio.



- ITSEC
- **Siglas:** Information Technology Security Evaluation Criteria (Criterios de Evaluación de la Seguridad de las Tecnologías de la Información).
- **Año y lugar de creación:** Publicado por primera vez en mayo de 1990 por Francia, Alemania, los Países Bajos y el Reino Unido; la versión definitiva (1.2) se publicó en junio de 1991 por la Comisión de las Comunidades Europeas.
- **Objetivos:**
    - Ofrecer un marco de evaluación armonizado entre varios países europeos, en lugar de que cada nación mantuviera su propio criterio de seguridad por separado.
    - Permitir evaluar tanto productos como sistemas completos (a diferencia del TCSEC, que se centraba en sistemas operativos).
    - Emitir un informe imparcial sobre si el objeto evaluado (Target of Evaluation, TOE) cumple la meta de seguridad declarada por el propio fabricante, con el nivel de confianza correspondiente.
- **Características:**
    - **Separación funcionalidad/aseguramiento:** a diferencia del TCSEC, que ataba la funcionalidad de seguridad al nivel de confianza, el ITSEC evalúa por separado qué hace el sistema (funciones de seguridad) y qué tan bien está comprobado que lo hace (nivel de garantía).
    - **Enfoque flexible:** el fabricante define sus propios objetivos de seguridad en un documento llamado Security Target, y el sistema se evalúa contra eso, no contra una lista fija de requisitos.
    - **Alcance más amplio que TCSEC:** puede evaluar sistemas que solo cubren autenticación o integridad, sin necesidad de cubrir confidencialidad, algo que el TCSEC no permitía.
- **Niveles de seguridad que emplea:** Siete niveles de evaluación, de E0 a E6. E0 representa confianza inadecuada (o nula); E1 es el punto de entrada mínimo de confianza útil; E6 es el nivel de mayor confianza y rigor de evaluación.
- **Secciones que lo componen:** Se estructura alrededor del Security Target (que define objetivos de seguridad, amenazas y funciones de seguridad exigidas), el proceso de

evaluación de corrección (revisión de la implementación) y el proceso de evaluación de efectividad (pruebas funcionales y de penetración, con mecanismos clasificados en resistencia "básica", "media" o "alta").

- **Años de actualización:** Solo tuvo una revisión formal, publicada como versión 1.2 en junio de 1991.
- **Última actualización o versión:** Versión 1.2 (1991); no hubo versiones posteriores.
- **¿Sigue vigente?** No. Fue absorbido, junto con el TCSEC estadounidense y el CTCPEC canadiense, en el proyecto conjunto que dio origen al Common Criteria / ISO-IEC 15408 en 1993-1999.
- **Sitio web oficial:** Al ser un documento europeo histórico descontinuado y absorbido por el estándar Common Criteria, no cuenta con un dominio web oficial activo.

Information Technology Security Evaluation Criteria (ITSEC)

- CTCPEC
- **Siglas:** Canadian Trusted Computer Product Evaluation Criteria (Criterios Canadienses de Evaluación de Productos Informáticos de Confianza).
- **Año y lugar de creación:** Se ideó inicialmente en 1988 con la fundación del Centro Canadiense de Seguridad de Sistemas. Su primer borrador se publicó en abril de 1992 y su versión final y oficial se lanzó en enero de 1993 en Ottawa, Canadá.
- **Objetivos**

  Nació con metas claras para subsanar los vacíos estructurales de los estándares de su época (como el "Libro Naranja" o TCSEC de EE. UU.):

  1. **Garantizar la Tríada CIA completa:** A diferencia de TCSEC (que casi exclusivamente se enfocaba en la Confidencialidad), el CTCPEC incluyó requerimientos estrictos para la Integridad y la Disponibilidad de los datos.
  2. **Flexibilidad de Evaluación:** Permitir que cada producto informático pudiera definir sus propios objetivos de seguridad antes de ser evaluado, adaptándose al mercado comercial y no solo al militar.
  3. **Separación de Conceptos:** Dividir de forma independiente la evaluación de las Funcionalidades de Seguridad (lo que el producto hace) y la Garantía de Seguridad (la certeza de que realmente funciona bien).
- **Características:**

    - **Enfoque Híbrido:** Combinó de forma orgánica la rigidez del modelo estadounidense (TCSEC) con el dinamismo y la flexibilidad del modelo europeo (ITSEC).
    - **Evaluación del Ciclo de Vida:** Introdujo la necesidad de auditar los procesos de desarrollo del software (desde el diseño hasta el código fuente) y no únicamente el producto terminado.
    - **Análisis Dual de Caja:** Admitía dos metodologías de pruebas técnicas:
        1. **Caja Blanca:** Para evaluar a fondo un producto específico a nivel de arquitectura.
        2. **Caja Negra:** Para evaluar la correcta integración del sistema operativo e instalaciones completas.
- **Niveles de seguridad:**

  Siguiendo el esquema de niveles de confianza heredado del ITSEC, el CTCPEC implementó 7 niveles jerárquicos de Garantía (Assurance) para medir qué tan confiable es un producto, enumerados de menor a mayor rigurosidad:

- T-0. Inseguro: El producto falló en las pruebas o no proporciona garantías evaluables.
- T-1. Pruebas Básicas: Garantía informal; análisis básico de que las funciones operan.
- T-2 Pruebas Estructuradas: El desarrollo del producto se realiza bajo controles documentados.
- T-3 Metódicamente Probado y Verificado: Revisión detallada del diseño y de los entornos de prueba.
- T-4 Diseñado y Probado Metódicamente: Análisis estricto de la arquitectura modular y aislamiento de fallos.
- T-5 Semiformalmente Diseñado y Probado: Se aplican modelos matemáticos y lógicos parciales para validar la seguridad.
- T-6 Formalmente Verificado: Máximo nivel de confianza; diseño verificado mediante pruebas matemáticas formales de extremo a extremo.

- **Secciones que lo componen:**

  El estándar estructuraba los requerimientos en cuatro criterios fundamentales de control (servicios de seguridad):

  1. Confidencialidad: Prevención del acceso no autorizado a la información.
  2. Integridad: Protección contra la modificación, adición o eliminación no autorizada de datos.
  3. Disponibilidad: Garantía de que los usuarios autorizados tengan acceso continuo a los recursos.
  4. Controlabilidad (Accountability): Aseguramiento de que las acciones de cualquier entidad puedan ser rastreadas e identificadas de manera unívoca (mecanismos de identificación, autenticación y auditoría).

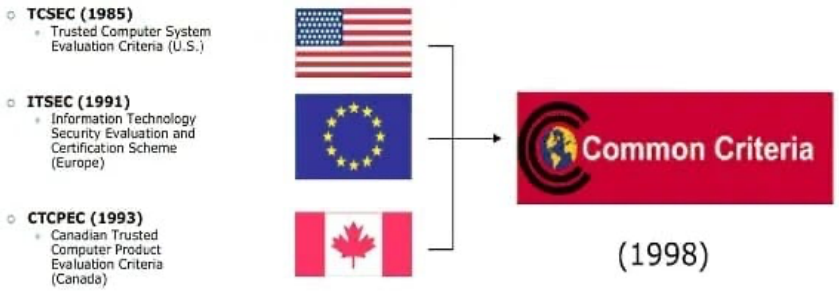
- Años de actualización

  Contó con iteraciones iniciales tempranas en mayo de 1989 (versión 1.0) y diciembre de 1990 (versión 2.0).

- **Última actualización/versión**. La Versión 3.0, publicada en enero de 1993.
- **¿Sigue vigente?** No. El CTCPEC se encuentra formalmente obsoleto y reemplazado. En 1996, el CSE de Canadá unió fuerzas con los gobiernos de EE. UU. y la Unión Europea para fusionar el TCSEC, el ITSEC y el CTCPEC. Esta alianza dio vida al estándar internacional definitivo: los Criterios Comunes (Common Criteria / ISO/IEC 15408), que es el sistema global utilizado actualmente para certificar software y hardware de alta seguridad.
- **Sitio web oficial.** Debido a su antigüedad, el CTCPEC ya no cuenta con un sitio web interactivo propio. Sin embargo, su evolución, registros históricos y el programa que lo sustituyó pueden consultarse en los canales gubernamentales de Canadá: Para revisar el estado de certificaciones de seguridad actuales en Canadá, visite el Centro Canadiense para la Ciberseguridad **(Cyber.gc.ca).**

- CITSE 15408 (Criterios comunes)

  También conocida como ISO/IEC 15408 (Common Criteria o Criterios Comunes) es el estándar técnico enfocado en la evaluación de la seguridad de productos de tecnología de la información. son el resultado de la unificación de las diferentes normativas internacionales confluyendo en un estándar único y común reconocido a nivel mundial. Este marco nos va a proporcionar un conjunto de requisitos estándar para la funcionalidad de la seguridad y al mismo tiempo medidas de aseguramiento.



  Lo que va a permitir que los productos sean evaluados de forma independiente contra normas reconocidas. Este implica que se va a tener una métrica para determinar las propiedades de seguridad en productos TIC.

  La certificación va a asegurar que los productos informáticos cumplan con estrictos estándares de seguridad a través de un enfoque estructurado de evaluación y ensayos, para ello es necesario cumplir con lo siguiente:

- **Desarrollo del Target de Seguridad (ST):** Definir los requisitos y especificaciones de seguridad del producto.
- **Evaluación por un laboratorio acreditado:** Realizar una evaluación exhaustiva en base al ST y al Nivel de Garantía de Evaluación (EAL) seleccionado.
- **Ensayos y revisión:** Realizar ensayos, revisar los procesos de diseño y desarrollo del producto y examinar las características de seguridad.
- **Emisión de la certificación:** Recibir la certificación de un organismo certificador, confirmando que el producto cumple con los estándares de seguridad y niveles de garantía especificados.

Para entender cómo opera esta norma en la práctica, es fundamental conocer sus conceptos clave, los cuales definen tanto el objeto que se evalúa como los documentos y métricas que validan su nivel de seguridad:

- **Enfoque en el producto (no en la empresa):** La norma 15408 evalúa hardware, software o sistemas específicos (por ejemplo, un sistema operativo, un dispositivo criptográfico o un firewall) para comprobar que son seguros frente a ataques.
- **Perfiles de Protección (Protection Profiles - PP):** En esta parte se encuentran los documentos que definen los requisitos de seguridad para una clase específica de productos (por ejemplo, lectores de huellas o tarjetas inteligentes).
- **Objetivos de Seguridad del Objetivo (Security Targets - ST):** Es la especificación técnica concreta que cumple un producto comercial específico que quiere ser evaluado.
- **Niveles de Garantía (EAL 1 al 7):** Determinan qué tan profunda y rigurosa fue la evaluación de laboratorio que se le hizo al producto, siendo el EAL1 el análisis básico y el EAL7 el nivel más estricto utilizado en entornos militares o de máxima seguridad.

- BS 7799.
  Aparece por primera vez en 1995, publicado por “ The British Standards Institution”, para proporcionar a las empresa un conjunto de buenas prácticas para la gestión de la seguridad de la información.Se publicó primero como una guía británica (PD 0003) sobre seguridad de la información. Después de revisarla con el público, se convirtió en la norma oficial BS7799-1:1995, a la que se le sumó una segunda parte (BS7799-2:1998) en febrero de 1998. Al inicio solo se usaba en empresas Británicas, pero con el paso del tiempo se fue extendiendo a otras empresas de diferentes países.

- **Buenas prácticas:** Ofrecer una guía basada en las mejores prácticas para implementar una seguridad de la información adecuada en las organizaciones.
- **Confianza comercial**: Facilitar el intercambio comercial entre empresas, al generar confianza compartida
- **Continuidad**: Asegurar la continuidad del negocio y minimizar posibles daños.
- **Autoevaluación**: Ayudar a identificar las fortalezas y debilidades en los procesos de gestión de la seguridad de la información.
- **Mejora continua**: Planificar acciones de mejora que apoyen el cumplimiento de los objetivos de la organización.

Antes de la BS 7799, la seguridad informática se veía solo como un tema técnico de contraseñas y respaldos de TI. Esta norma introdujo el concepto de Sistema de Gestión de Seguridad de la Información (SGSI), tratándolo como un proceso de gestión de riesgos a un nivel empresarial en el que participa toda la organización.Dividió sus partes entre un código de buenas prácticas (la parte 1) y una especificación estricta que permitía certificar a las empresas de forma independiente (la parte 2). Esto les daba confianza comercial ante clientes y socios internacionales.

- **ISO/IEC 17799**
- **Siglas:** ISO/IEC 17799 (Tecnología de la información — Técnicas de seguridad — Código de práctica para la gestión de la seguridad de la información).
- **Objetivos**
  - Proporcionar una base común e internacionalmente reconocida para que las organizaciones desarrollaran sus propias normas de gestión de seguridad de la información.
  - Ofrecer una guía práctica y eficaz de gestión de la seguridad, dirigida a los responsables de iniciar, implantar o mantener la seguridad dentro de una organización.
  - Recoger un conjunto de controles y objetivos de control considerados buenas prácticas exitosas en la industria, aplicables a cualquier tipo de organización.
- **Características**
  - Es un código de práctica (recomendaciones), no una especificación de requisitos: describe qué controles conviene aplicar, pero no dicta obligatoriamente cómo implementarlos.
  - No es certificable por sí mismo; la certificación de un Sistema de Gestión de Seguridad de la Información (SGSI) se realizaba mediante la norma complementaria BS 7799-2 (posteriormente ISO/IEC 27001).
  - Aborda la seguridad de la información de forma integral, no solo técnica, cubriendo aspectos organizacionales, físicos, legales y de recursos humanos, basándose en la tríada de confidencialidad, integridad y disponibilidad.

- **Nivel de seguridad que emplea:** No maneja niveles jerárquicos de seguridad como TCSEC o Common Criteria; contiene 39 objetivos de control y 133 controles agrupados en 11 dominios temáticos (política de seguridad, seguridad organizacional, control de acceso, gestión de continuidad del negocio, cumplimiento, entre otros).
- **Secciones que lo componen:** Se estructura en dominios de control que cubren, entre otros: política de seguridad, organización de la seguridad de la información, clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos, desarrollo y mantenimiento de sistemas, gestión de incidentes, gestión de continuidad del negocio y cumplimiento normativo.
- **Años de actualización:** Publicado inicialmente en diciembre de 2000 (ISO/IEC 17799:2000); revisado y ampliado en 2005 (ISO/IEC 17799:2005); corregido técnicamente en 2007 mediante ISO/IEC 17799:2005/Cor 1:2007, año en el que además fue renombrada como ISO/IEC 27002:2005.
- **Última actualización/versión:** Su última versión bajo el nombre ISO/IEC 17799 fue la edición de 2005, con su corrección técnica de 2007. A partir de ahí, la norma continuó su desarrollo bajo el nombre ISO/IEC 27002, cuya versión vigente es ISO/IEC 27002:2022 (véase el apartado g.2 de este trabajo).
- **Vigencia actual:** No se encuentra vigente bajo el nombre ISO/IEC 17799. Según el sitio oficial de ISO, la norma fue retirada (Withdrawn) y sustituida el 1 de julio de 2007 por ISO/IEC 27002:2005, la cual a su vez fue retirada y sustituida por ISO/IEC 27002:2022, versión actualmente activa.
- **Sitio web oficial:** Al estar retirada, no cuenta con un dominio propio activo; su ficha histórica se encuentra en el sitio oficial de ISO: https://www.iso.org/standard/39612.html

- **ISO/IEC 27000**
  La familia ISO/IEC 27000 reúne las normas internacionales orientadas a la gestión de la seguridad de la información, la ciberseguridad y la protección de la privacidad. Su propósito general es proporcionar un marco que permita a organizaciones de cualquier tamaño y sector proteger la información que manejan, incluidos datos financieros, propiedad intelectual, información de empleados y datos proporcionados por terceros.

La versión más actualizada el 3 de julio de 2026, fue desarrollada por el comité técnico ISO/IEC JTC 1/SC27, responsable de las normas relacionadas con seguridad de la información, ciberseguridad y protección de la privacidad.

Su objetivo es proporcionar una visión general de los Sistemas de Gestión de Seguridad de la Información y explicar los conceptos y principios fundamentales que sustentan este tipo de sistemas. Ayuda a una organización a comprender cómo funciona el conjunto de normas ISO/IEC 27000 antes de empezar a implementar un SGSI.

g.1) ISO/IEC 27001: Su nombre completo es Information security, cybersecurity and privacy protection — Information security management systems — Requirements. La versión más actualizada se publicó en octubre de 2022 y corresponde a la tercera edición. Cabe mencionar que está relacionada a una enmienda que se publicó en 2024.

Su objetivo es establecer los requisitos necesarios para crear, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información. ISO indica que puede ser utilizada por organizaciones de cualquier tamaño y pertenecientes a cualquier sector. El SGSI permite administrar los riesgos relacionados con la información que una organización posee, procesa o tiene bajo su responsabilidad.

Utiliza principalmente un enfoque basado en riesgos, lo que significa que la organización debe analizar qué información proteger, cuáles son las amenazas que existen, qué vulnerabilidades pueden ser explotadas, cuáles serían las consecuencias de un incidente, qué probabilidad existe de que ocurra y qué controles deben implementarse.Con ello se busca que la seguridad se administre como un proceso organizacional continuo y no sólo mediante herramientas tecnológicas.

La estructura de la ISO/IEC 27001 contempla las siguientes cláusulas:

1. Alcance
2. Referencias Normativas
3. Términos y definiciones

4. Contexto de la organización
5. Liderazgo: Implica establecer políticas, asignar responsabilidades, proporcionar recursos y garantizar que la seguridad de la información se integre dentro de los procesos generales de la organización.
6. Planificación: La organización debe determinar qué controles utilizará para reducir los riesgos encontrados.
7. Apoyo: Comprende los recursos necesarios para mantener el SGSI.
8. Operación: Se realizan evaluaciones y tratamientos de riesgos de seguridad de la información.
9. Evaluación de desempeño: La organización debe comprobar que SGSI funciona de manera correcta y se incluye el monitoreo, medición, auditorías internas y revisión por parte de la dirección.
10. Mejora: Corregir los problemas que se identifiquen para mejorar continuamente el sistema.

Es certificable, una organización puede someter su SGSI a una auditoría realizada por un organismo de certificación para demostrar que cumple los requisitos establecidos por ISO/IEC 27001. La conformidad con la norma significa que la organización dispone de un sistema para administrar los riesgos relacionados con la seguridad de sus datos de acuerdo con las prácticas y principios establecidos por el estándar

g.2) ISO/IEC 27002: Su nombre completo es Information security, cybersecurity and privacy protection — Information security controls. La versión más actual se publicó en marzo de 2022 y corresponde a la tercera edición. Su objetivo es proporcionar recomendaciones, controles y buenas prácticas para gestionar los riesgos relacionados con la seguridad de la información. ISO indica que la norma permite a las organizaciones adoptar un enfoque preventivo frente a riesgos de ciberseguridad y proteger información crítica frente a acceso no autorizado y pérdida.

Esta última edición reorganizó los controles dividiéndolos en cuatro categorías:

1. Organizacionales: Contempla 37 y están relacionados con políticas, responsabilidades, gestión de activos, relaciones con proveedores, gestión de incidentes, cumplimiento y otros procesos administrativos.

2. Humanos: Contempla 8 y tratan principalmente aspectos como selección de personal, responsabilidades, capacitación y concientización, acuerdos de confidencialidad, trabajo remoto, reporte de incidentes de seguridad.
3. Físicos: Contempla 14 que buscan principalmente proteger las instalaciones, equipos y otros recursos físicos. Incluye algunos aspectos como acceso físico, protección de oficinas, vigilancia, protección de equipos, almacenamiento, eliminación segura de dispositivos.
4. Tecnológicos: Contempla 34 y se enfoca en sistemas y tecnología, comprende temas como autenticación, privilegios de acceso, malware, vulnerabilidades técnicas, configuración, eliminación de información, prevención de fugas de datos, respaldos, registro de eventos, monitoreo, seguridad de redes y desarrollo seguro.

Algunos beneficios son que su aplicación puede contribuir a identificar y gestionar riesgos de seguridad, proteger información crítica, aumentar la confianza de clientes y otras partes interesadas, facilitar el cumplimiento de requisitos legales y contractuales, aumentar la resiliencia operacional, reducir la posibilidad de incidentes de seguridad. Ésta ISO/IEC 27002 no es directamente certificable ya que más bien funciona como una guía de las buenas prácticas y controles, más bien ésta se utiliza como apoyo para que una organización se certifique con la ISO/IEC 27001.

- **HIPAA**
  - Siglas: Ley de Portabilidad y Responsabilidad del Seguro Médico (Health Insurance Portability and Accountability Act).
  - Año y lugar de creación: Ley federal de los Estados Unidos promulgada en 1996.
  - Objetivos: Proteger la privacidad y seguridad de la información médica de las personas, establecer reglas para su uso y divulgación y normalizar determinadas transacciones electrónicas del sector salud.
  - Características detalladas: una ley federal estadounidense aplicable principalmente a planes de salud, proveedores de servicios médicos, cámaras de compensación de atención médica y sus asociados comerciales. Protege la PHI (Protected Health Information) y, mediante la Security Rule, la ePHI almacenada o transmitida electrónicamente. Exige controles de acceso,

análisis de riesgos, políticas de seguridad, protección física, capacitación y procedimientos ante incidentes.
    - Niveles de seguridad que emplea: La Security Rule divide las salvaguardas principalmente en tres grupos: administrativas, físicas y técnicas.
    - Secciones que lo componen:Transactions and Code Set Standards, Identifier Standards, Privacy Rule, Security Rule, Enforcement Rule y Breach Notification Rule.
    - Años de actualización: 2000, Privacy Rule; 2002, modificaciones de privacidad; 2003, Security Rule; 2009, HITECH; 2013, Omnibus Final Rule; 2016, modificaciones específicas de privacidad; 2024-2025, nuevas modificaciones y propuestas relacionadas con privacidad y ciberseguridad.
    - Última actualización o versión: En 2025 HHS propuso una actualización importante de la Security Rule, pero sigue siendo una propuesta y no sustituye todavía la regla vigente. Parte de las modificaciones de privacidad de 2024 fueron anuladas judicialmente en junio de 2025.
    - Sigue vigente: Sí. HIPAA continúa siendo legislación federal vigente en Estados Unidos.
    - Página oficial: https://www.hhs.gov/hipaa/index.html

- NIST
    - Siglas: National Institute of Standards and Technology o Instituto Nacional de Estándares y Tecnología
    - Año y lugar de creación: 3 de marzo de 1901 en Washington, D.C., Estados Unidos.
    - Objetivos: Promover la innovación y la competitividad industrial de Estados Unidos mediante el desarrollo de estándares, mediciones y directrices científicas y tecnológicas
    - Características detalladas: Es una agencia federal no reguladora. Realiza investigación científica y desarrolla estándares, metodologías, guías y recomendaciones utilizadas por organismos gubernamentales y empresas. Trabaja en áreas como ciberseguridad, inteligencia artificial, criptografía, comunicaciones, manufactura, nanotecnología, ingeniería y metrología. En seguridad informática es especialmente conocido por sus publicaciones FIPS y la serie Special Publication 800.

- Niveles de seguridad que emplea: No establece un único conjunto de niveles de seguridad. Sus diferentes estándares y publicaciones definen controles, niveles, categorías o requisitos dependiendo de su propósito. Por ejemplo, las publicaciones de la serie NIST SP 800 proporcionan controles y metodologías para identificar, evaluar y administrar riesgos de seguridad de la información.
- Secciones que lo componen: Su estructura incluye la Oficina del Director, programas de laboratorios, servicios de innovación e industria y áreas de administración. Sus principales laboratorios incluyen Communications Technology Laboratory, Engineering Laboratory, Information Technology Laboratory, Material Measurement Laboratory, Physical Measurement Laboratory y NIST Center for Neutron Research.
- Años de actualización: NIST, como institución, no tiene versiones. Sin embargo, uno de sus principales marcos de ciberseguridad, el NIST Cybersecurity Framework (CSF), fue publicado en 2014 como CSF 1.0, actualizado en 2018 a CSF 1.1 y nuevamente en 2024 a CSF 2.0.
- Última actualización o versión: Como institución, NIST no maneja una versión general. Tomando como referencia su Cybersecurity Framework, la versión vigente es NIST CSF 2.0, publicada el 26 de febrero de 2024.
- Sigue vigente: Sí. NIST continúa activo como una agencia del Departamento de Comercio de Estados Unidos y mantiene investigación, estándares y publicaciones en múltiples áreas científicas y tecnológicas.
- Página oficial: https://www.nist.gov/

- COBITSiglas: Control Objectives for Information and Related Technologies.
  - Año y lugar de creación: 1996, Estados Unidos
  - Objetivos: Proporcionar un marco para gobernar y administrar la información y tecnología de una organización, buscando generar valor, controlar riesgos, utilizar adecuadamente los recursos y alinear TI con los objetivos empresariales.
  - Características detalladas: Se centra en gobierno y gestión de TI a nivel empresarial. Permite diseñar un sistema de gobierno adaptado a cada organización mediante objetivos, procesos, factores de diseño, métricas y componentes. Puede integrarse con otros estándares y marcos como NIST.
  - Niveles de seguridad que emplea: Utiliza niveles de capacidad de procesos del 0 al 5, donde 0 representa un proceso con capacidad insuficiente y 5 un proceso altamente desarrollado y optimizado.
  - Secciones que lo componen: Su Core Model contiene 40 objetivos de gobierno y gestión agrupados en cinco dominios: EDM (Evaluate, Direct and Monitor),

APO (Align, Plan and Organize), BAI (Build, Acquire and Implement), DSS (Deliver, Service and Support) y MEA (Monitor, Evaluate and Assess). También considera siete componentes del sistema de gobierno, como procesos, estructuras organizacionales, información, personas y tecnología.

- Años de actualización: 1996, primera edición; 1998, segunda edición; 2000, tercera edición; 2005, COBIT 4.0; 2007, COBIT 4.1; 2012, COBIT 5; 2018, lanzamiento de COBIT 2019.
- Última actualización o versión: COBIT 2019. Aunque lleva "2019" en el nombre, fue lanzado inicialmente a finales de 2018 y sus publicaciones principales continuaron apareciendo durante 2018-2019.
- Sigue vigente: Sí. ISACA mantiene COBIT 2019 como su marco vigente para gobierno y gestión de información y tecnología.
- Página oficial: https://www.isaca.org/resources/cobit

Referencias

Akamai. (s/f). ¿Qué es la HIPAA? Akamai.com. Recuperado el 1 de septiembre de 2026, de https://www.akamai.com/es/glossary/what-is-hippa

Alonso, C. (2022, enero 25). ¿Qué es COBIT y para qué sirve? GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-es-cobit/

Canadian Centre for Cyber Security. (s.f.). Common Criteria. Government of Canada. https://www.cyber.gc.ca/en/tools-services/common-criteria

Carrero, E. (2023, julio 24). *¿Qué es el NIST?* Mobbeel Solutions. Mobbeel. https://www.mobbeel.com/blog/que-es-el-nist/

Commission of the European Communities. (1991, junio). Information technology security evaluation criteria (ITSEC): Preliminary harmonised criteria (versión 1.2, documento COM(90) 314). https://web.archive.org/web/20060523094527/http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

G., A. (2020, 28 de enero). CISSP concepts – Trusted computing base/TCEC, ITSEC and common criteria. Cyber Management Alliance. https://www.cm-alliance.com/cybersecurity-blog/trusted-computing-base/-tcec-itsec-and-common-criteria

IBM. (2025, agosto 20). ¿Qué es el marco de ciberseguridad del NIST? *Ibm.com*. https://www.ibm.com/mx-es/think/topics/nist

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model (Norma ISO/IEC 15408-1:2022). https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-4:v1:en

International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.* Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/27001?utm_source

International Organization for Standardization. (2022). *ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información*. ISO. Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/75652.html?utm_source

International Organization for Standardization. (2024). *ISO/IEC 27001:2022/Amd 1:2024. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. Enmienda 1: Cambios relacionados con la acción climática*. ISO. Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/88435.html?utm_source

International Organization for Standardization. (2026). *ISO/IEC 27000:2026. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.* Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/27000?utm_source

International Organization for Standardization. (s. f.). ISO/IEC 17799:2005. ISO. Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/39612.html

International Organization for Standardization. (s. f.). ISO/IEC 17799:2005/Cor 1:2007. ISO. Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/46381.html

International Organization for Standardization. (s. f.). ISO/IEC 27002:2005. ISO. Recuperado el 1 de septiembre de 2026, de https://www.iso.org/standard/50297.html

International Organization for Standardization. (s. f.). Familia ISO/IEC 27000: Gestión de la seguridad de la información. ISO. Recuperado el 1 de septiembre de 2026, https://www.iso.org/standard/iso-iec-27000-family?utm_source

Li, H., King, G., Ross, M. y Staples, G. (2000). BS7799: A suitable model for information security management. AMCIS 2000 Proceedings, 142. https://aisel.aisnet.org/amcis2000/142