Universidad Nacional Experimental del Táchira (UNET)
Vicerrectorado Académico Decanato de Docencia
Departamento de Ingeniería Informática
Asignatura: Seminario

Familia de estándares ISO/IEC 27000

Realizado por:
Jessica Ramírez C.I: 21.219.949
Cristopher Cáceres C.I: 20.120.542
Edwin Sierra C.I: 21.000.079
Johan Vargas C.I: 20.626.255

El sistema de Gestión de seguridad de la información consiste de una serie de políticas, directrices, procedimiento, pautas, recursos y actividades que se encuentran gestionadas, cuya búsqueda es la protección de los activos de información de una organización.

Los estándares proporcionan orientación para los diversos aspectos en la implementación del SGSI, permite dirigirse a un proceso específico, conocer las normas para obtener un control, asimismo la orientación específica de algún sector .La familia de estándares del SGSI consta de normas interrelacionadas, que se encuentran publicadas o en desarrollo, estos componentes se centran en estándares que describen los requisitos del SGSI (ISO/IEC27001) y del organismo de certificación (ISO/IEC 27006) para todo aquellos que se certifican con la norma ISO/IEC 27001.

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Esta serie contiene un conjunto coherente de acciones que han dado un buen servicio recomendadas por las medidas preventivas y reactivas de la Seguridad de la Información para poder implementar, desarrollar y mantener las especificaciones para los sistemas de gestión de la seguridad de la información (SGSI).

ISO/IEC 27000: Es un vocabulario estándar para el SGSI

Alcance: Este estándar Internacional permite proporcionar a las organizaciones e individuos:

- Proporciona una visión general de los estándares que componen la familia de SGSI;
- una introducción a los sistemas de gestión de seguridad de la información (SGSI); y
- Una breve descripción del proceso Plan-Do-Check-Act y términos, asimismo de las definiciones utilizados en la familia de estándares de SGSI.

Propósito: El ISO/IEC 27000 describe los fundamentos de los sistemas de gestión de seguridad de la información, que son la esencia de la familia de estándares de SGSI, y define los términos relacionados.

ISO/IEC 27001: La norma ISO 27001 fue aprobada y publicada como estándar internacional el 15 de octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Es la norma principal y más importante de la familia y contiene la especificación de los requisitos para la implantación del sistema de gestión de seguridad de la información. Este estándar es la certificación

que deben obtener las organizaciones. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.

Alcance: Esta norma internacional especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI) dentro del contexto de los riesgos globales de negocio de la organización. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Esta norma exige el desarrollo de una gestión documental completa, que cubra todo lo relativo a la gestión de cambios y versiones y estandarice el proceso de revisión y validación formal de la misma, garantizando su viabilidad y operatividad, puede ser utilizada por todas las organizaciones, sin importar el tipo, el tamaño y la naturaleza.

Propósito: Proporciona requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y amortiguamiento de los riesgos asociados a los activos de información que la organización pretende proteger al operar sus SGSI. Verifica independientemente que los riesgos de la organización estén correctamente identificados como evaluados y gestionados los procesos, los procedimientos y documentación de protección de la información, asimismo cumple los requisitos establecidos y demuestra a los clientes que la seguridad de su información es primordial.

ISO/IEC 27006: 1 de Marzo de 2007. Esta norma específica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

Alcance: Esta norma internacional especifica los requisitos y proporciona una guía para los organismos que realizan la auditoría y la certificación de SGSI según ISO / IEC 27001, además de los requisitos contenidos en la norma ISO / IEC 17021. Se destina principalmente para apoyar la acreditación de organismos de certificación que prestan SGSI la certificación según la norma ISO / IEC 27001.

Propósito: ISO / IEC 27006: 2011 especifica los requisitos y proporciona una guía para los organismos que realizan la auditoría y certificación de un sistema de gestión de seguridad de la información (SGSI), además de los requisitos contenidos en la norma ISO / IEC 17021 e ISO / IEC 27001. Se piensa sobre todo para apoyar la acreditación de organismos de certificación que ofrecen la certificación del SGSI. Los requisitos contenidos en la norma ISO / IEC 27006: 2011 permite demostrar en términos de competencia y fiabilidad por parte de cualquier organismo que proporcionan la certificación del SGSI, y las orientaciones contenidas en la norma ISO / IEC 27006: 2011 proporciona interpretación

adicional de estos requisitos para cualquier organismo que proporciona la certificación del SGSI.

ISO/IEC 27002: Es un estándar para la seguridad de la información publicado por la International Organization for Standardization y la Comisión Electrotécnica Internacional**.** La versión más reciente es la ISO/IEC 27002:2013.

Alcance: Esta Norma Internacional proporciona una lista de objetivos de control comúnmente aceptados y las mejores prácticas controlan para ser utilizado como una guía de implementación en la selección y la aplicación de controles para lograr la seguridad de la información.

Propósito: Proporciona orientación sobre la aplicación de los controles de seguridad de la información. Específicamente las cláusulas 5 y 18 son las que proporcionan asesoramiento e implementación específica como la orientación sobre las mejores prácticas en apoyo a los controles especificados en las cláusulas A.5 a A.18 de la norma ISO / IEC 27001.

ISO/IEC 27003: Publicada el 1 de Febrero de 2010. Focaliza su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información.

Alcance: Se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO / IEC 27001:2005. Se describe el proceso de especificación del SGSI y el diseño desde el inicio hasta la elaboración de planes de ejecución. En él se describe el proceso de obtener la aprobación de la gestión para implementar un SGSI, se define un proyecto para implementar un SGSI (denominado en la norma ISO / IEC 27003:2010 como el proyecto de SGSI), y da pautas sobre cómo planificar el proyecto de SGSI, resultando en una SGSI proyecto final de ejecución del plan.

Propósito: Proporciona un enfoque orientado al proceso para la implementación ISMS acorde con la ISO/IEC 27001 por lo tanto tiene como objetivo servir como guía para la implementación de un Sistema de Gestión para la Seguridad de la Información de acuerdo al estándar ISO/IEC 27001:2005.

ISO/IEC 27004: Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

Alcance: Son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad

de la información. Tiene orientación y asesoramiento sobre el desarrollo y el uso de mediciones con el fin de evaluar la eficacia de ISMS

Propósito: ISO / IEC 27004 proporciona un marco de medición que permite una evaluación del SGSI de manera eficaz que se mide de acuerdo con la norma ISO / IEC 27001 por lo tanto. Expone que el tipo de medidas requeridas dependerá del tamaño y complejidad de la organización, de la relación coste beneficio y del nivel de integración de la seguridad de la información en los procesos de la propia organización.

ISO/IEC 27005: Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

Alcance: Ofrece directrices para la gestión de riesgos de seguridad de la información. El método descrito en esta norma es compatible con los conceptos generales especificados en ISO / IEC 27001.Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.

Propósito: ISO / IEC 27005 proporciona orientación sobre la implementación de un proceso de gestión de riesgos orientado y enfocado en ayudar de forma satisfactoria la implementación y el cumplimiento de la gestión del riesgo de acuerdo con la ISO / IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.

ISO/IEC 27007: Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

Alcance: Específica la guía para auditar el SGSI basándose en normas contenidas en la ISO 19011 que es aplicada a los sistemas en general así como también provee información sobre las conductas externas e internas para auditar un SGSI. Esta Norma Internacional proporciona orientación sobre la realización de auditorías de SGSI, así como orientación sobre la competencia de los auditores de sistemas de gestión de seguridad de la

información, además de la orientación que figura en la norma ISO 19011, que es aplicable a los sistemas de gestión en general.

Propósito: Proporciona orientación a las organizaciones que necesitan gestionar un programa de auditoría SGSI en contra de los requisitos especificados en la norma ISO / IEC 27001.

ISO/IEC TR 27008: Esta norma es un informe técnico o también se le puede llamar auditoría técnica complementa la norma ISO / IEC 27007. Se concentra en la auditoría de los controles de seguridad de la información, mientras que '27007 se centra en la auditoría de los elementos del sistema de gestión de los SGSI.

Alcance: Esta norma trabaja sobre la información de las auditorias para los controles de seguridad, es un elemento que provee técnicas de reportes para la revisión la implementación y operación de los controles todas esta información conlleva a que las organizaciones cumpla con estándares más sin embargo no comprende

Propósito: Proporciona un enfoque en la revisión de los controles de seguridad de la información, incluyendo la comprobación de la conformidad técnica, frente a un estándar de implementación de seguridad de la información establecido por la organización. No pretende proporcionar ninguna orientación específica sobre el cumplimiento de la demostración respecto a la medición, evaluación de riesgos o auditoría de un SGSI según lo especificado en la norma ISO / IEC 27004, ISO / IEC 27005 o ISO / IEC 27007, respectivamente. Este Informe Técnico no está destinado a la gestión auditorías de sistemas

ISO/IEC 27013: Esta norma proporciona orientación sobre la implementación de un sistema de seguridad de la información y la gestión de servicios, basada tanto en la norma ISO / IEC 27001: 2005 (SGSI) e ISO / IEC 20000-1.

Alcance: La relación entre la seguridad de la información y la gestión de los servicios es muy estrecha, puesto que muchas organizaciones ya han reconocido los beneficios de adoptar los lineamientos de las normas mencionadas anteriormente. Es importante mencionar que dichas normas tienen un enfoque muy similar en cuanto a procesos y actividades, incluido el importante principio de mejora continua, es por esto que la norma ISO/IEC 27013 proporcionar una mejor comprensión de las características, similitudes y diferencias de la norma ISO / IEC 27001 e ISO / IEC 20000-1 para ayudar en la planificación de una gestión integrada sistema que se ajusta a ambas normas internacionales.

Propósito: Proporcionar a las organizaciones una mejor comprensión de las características, similitudes y diferencias de la norma ISO / IEC 27001 e ISO / IEC 20000-1

para ayudar en la planificación de un sistema de gestión integrado que se ajusta a las normas Internacionales.

ISO/IEC 27014: Esta norma facilita orientación sobre los principios y conceptos para gobernar la seguridad de la información. A través de esta, las organizaciones podrán dirigir, comunicar, evaluar y controlar la seguridad de la información que está relacionada con sus actividades.

Alcance: La ISO-27014 indica seis principios de gobiernos de la seguridad de información los cuales son: a) Establecer seguridad de la información en toda la empresa, b) Seguir un enfoque basado en el riesgo, c) Establecer la dirección de las decisiones de inversión, d) Confirmar el cumplimento de los requisitos externos e internos. e) Promover un ambiente de seguridad positiva, f) Evidenciar el rendimiento en relación con los resultados del negocio.

Propósito: La seguridad de la información se ha convertido en una cuestión clave para las organizaciones. No sólo hay aumento de los requisitos normativos, sino también a la falta de medidas de seguridad de la información de una organización puede tener un impacto directo en la reputación de una organización. Por lo tanto, los órganos de gobierno, como parte de sus responsabilidades de gobierno, se requieren cada vez de tener la supervisión de seguridad de la información para garantizar que se alcancen los objetivos de la organización.

ISO/IEC TR 27016: Es el estándar que define la economía organizacional para la gestión de información de seguridad. Dado que esta norma se encuentra todavía en la versión preliminar, es teóricamente posible que se publique en 2013, sin embargo, 2014 es mucho más realista como un año de publicación.

Alcance: Su Informe Técnico proporcionará una metodología que permite a las organizaciones a comprender mejor económicamente cómo valorar con mayor precisión sus activos de información claramente identificados, el valor del potencial de riesgo para los activos de información, apreciar el valor que los controles de protección dan a la información y lo que estos ofrecen a los activos, y determinar el nivel óptimo de los recursos que se aplicarán en la obtención de estos activos.

Propósito: Este Informe Técnico complementará la familia de normas de SGSI mediante la superposición de una perspectiva de la economía en la protección de los activos de información de una organización en el contexto del entorno social más amplio al que una organización opera, y proporcionar orientación sobre cómo aplicar economía de organización de la seguridad de la información mediante el uso de modelos y ejemplos.

ISO / IEC 27010: Tecnología de la información - Técnicas de seguridad - Gestión de seguridad de la información.

Alcance: Proporciona orientación sobre la información , seguridad y comunicaciones entre las industrias, en diferentes sectores de la industria y con los gobiernos, ya sea en tiempos de crisis y para proteger la infraestructura crítica o para el reconocimiento mutuo en circunstancias normales de negocios para satisfacción legal, reglamentario y obligaciones contractuales.

Propósito: La norma proporciona orientación sobre los métodos, modelos, procesos, políticas, controles, protocolos y otros mecanismos para el intercambio de información de forma segura con contrapartes de confianza en el entendimiento de que se respetarán los principios de seguridad de la información importante.

El establecimiento de enfoques generales hacia los aspectos de seguridad de información del proceso (por ejemplo, la escritura y la implementación de políticas y procedimientos, junto con actividades de formación y sensibilización para los involucrados en el proceso y la evaluación concebiblemente independiente o auditorías para confirmar que los acuerdos se ajustan a la norma ISO / IEC 27010 y / u otras normas aplicables ISO27k como 27001, 27002 y 27005);

Las relaciones de confianza con otras organizaciones que también pueden estar implicados (por ejemplo, si las comunicaciones se enrutan a través de algún tipo de agencia), o son atraídos en algún modo a la situación, incluyendo socios de negocios y aquellos que pueden tener para estar informado o participando en el proceso como un legal o de otro tipo de servicio.

La evaluación y la aceptación de riesgos y obligaciones de seguridad (por ejemplo, en algún tipo de contrato o acuerdo, cuya existencia y contenido también puede ser confidencial);

Comunicar información de forma segura (por ejemplo, el uso de controles criptográficos adecuados), evitando que sea enviada a las entidades de contrapartida equivocadas, interceptados, borrados, falso, duplicar, repudiado, dañado, modificado o de otro modo puesto en duda deliberadamente por un tercero o por medio de controles inadecuados y errores. Versión de controles y autorización apropiada tanto para la divulgación y la aceptación de la información valiosa; Los riesgos y los controles relacionados con la recopilación, el análisis, la propiedad, la protección y en adelante la divulgación de información sobre la situación actual de las partes beneficiarias que participan en una investigación.

Proteger adecuadamente la información y tal vez otros activos confiados a las organizaciones receptoras y de los individuos

ISO / IEC 27011: Tecnología de la información - Técnicas de seguridad - Directrices de gestión de seguridad de información para las organizaciones de telecomunicaciones basados en la norma ISO / IEC 27002

Alcance y propósito: Esta norma fue diseñada para las organizaciones de telecomunicaciones, la información y los procesos de apoyo, instalaciones de telecomunicaciones, redes y líneas son activos comerciales importantes. A fin de que los organismos de telecomunicaciones para gestionar adecuadamente estos activos empresariales y continuar correctamente y con éxito sus actividades de negocio, gestión de seguridad de la información es extremadamente necesario. Esta Recomendación proporciona los requisitos de gestión de seguridad de la información para las organizaciones de telecomunicaciones.

Esta especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema documentado de gestión de seguridad de la información (SGSI) en el contexto de los riesgos de negocio globales de la telecomunicación. Especifica los requisitos para la aplicación de controles de seguridad adaptados a las necesidades de telecomunicaciones individuales o partes de los mismos.

ISO / IEC TR 27015: Tecnología de la información - Técnicas de seguridad - Directrices de gestión de seguridad de la información para los servicios financieros

Alcance: Este Informe Técnico ofrece directrices, además de la orientación dada en la norma ISO / IEC 27000 familia de normas, para iniciar, implementar, mantener y mejorar la seguridad de la información dentro de las organizaciones que prestan servicios financieros.

Propósito: Aunque el sector de servicios financieros ya trabaja bajo una vasta franja de riesgo y las normas de seguridad (tales como ISO TR 13569 "Guía de seguridad la información bancaria", SOX y Basilea II / III), la guía de implementación de SGSI desarrollado por SC 27 refleja la norma ISO / IEC 27001 y 27.002, junto con diversos estándares de seguridad de uso general tales como los requisitos de PCI-DSS y COBIT.

ISO / IEC TR 27015 amplifica y extiende algunas de las recomendaciones de la norma ISO / IEC 27002 para las organizaciones de servicios financieros - por ejemplo, la recomendación

en la sección 6.2.2 que las actividades de sensibilización de seguridad deben cubrir los clientes, no sólo a los empleados.

ISO 27799: Informática de la salud - Información gestión de la seguridad en materia de salud mediante la norma ISO / IEC 27002

Alcance: Especifica un conjunto de controles detallados para la gestión de seguridad de la información de salud y proporciona información sobre directrices sobre mejores prácticas. Mediante la implementación de esta norma internacional, las organizaciones de salud y otros custodios de la información de salud serán capaces de garantizar un nivel mínimo de seguridad requerido, adecuada a las circunstancias de su organización y que mantendrá la confidencialidad, integridad y disponibilidad de la información de salud personal.

Propósito: Se aplica a la información de salud en todos sus aspectos; cualquiera de sus formas la información toma (palabras y números, grabaciones de sonido, dibujos, vídeo e imágenes médicas), todos los medios se usan para almacenarla (impresión o escribir en papel o de almacenamiento electrónico) y todos los medios se utilizan para transmitirlo (a mano, por fax, a través de redes informáticas o por correo), ya que la información siempre debe ser protegido de manera apropiada.

Esta Norma Internacional proporciona orientación a las organizaciones sanitarias y otros custodios de información personal de salud sobre la mejor manera de proteger la confidencialidad, integridad y disponibilidad de dicha información mediante la implementación de la norma ISO / IEC 27002. En concreto, esta norma se ocupa de las necesidades de gestión de seguridad de la información especiales del sector de la salud y sus entornos operativos únicos. Si bien la protección y seguridad de la información personal es importante para todas las personas, empresas, instituciones y gobiernos, existen requisitos especiales en el sector de la salud que deben cumplirse para asegurar la confidencialidad, integridad, y la disponibilidad de información de salud personal.