FASE 3 CONSTRUCCIÓN - SEGURIDAD INFORMÁTICA
NORMAS ISO 27000

HERNAN DE JESUS QUINTANA
JUAN IGNACIO BOLIVAR
OMAR YOVANY FORERO DIAZ

CARLOS ALBERTO SOSA
TUTOR

GRUPO: 301122_29

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
DISEÑO DE SITIOS WEB
JUNIO 2019

NORMAS ISO 27000

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.

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) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos o procesos autorizados cuando lo requieran.

ISO/IEC 27001

Ya hemos indicado que "la norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI documentado dentro del contexto global de los riesgos de negocio de la organización. Especifica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de organizaciones individuales o partes de estas".
El objetivo es la mejora continua y se adopta el modelo Plan-Do-Check-Act (PDCA o ciclo Demming) para todos los procesos de la organización.

Las fases de este modelo son:

Planificación (Plan) [establecer el SGSI]

Establecer la política, objetivos, procesos y procedimientos relativos a la gestión del riesgo y mejorar la seguridad de la información de la organización para ofrecer resultados de acuerdo con las políticas y objetivos generales de la organización.

- Identificar lo que se quiere mejorar.
- Recopilar datos del proceso que se quiere mejorar.
- Analizar los datos recogidos.
- Establecer los objetivos de mejora.
- Detallar los resultados esperados.
- Definir los procesos necesarios conseguir los objetivos.

Ejecución (Do) [implementar y gestionar el SGSI]

Implementar y gestionar el SGSI de acuerdo con su política, controles, procesos y procedimientos. En la medida de lo posible debería hacerse en un entorno de prueba para poder verificar sus resultados antes de implantarlo en el sistema real.

A continuación les dejamos algunos detalles de cada uno de los estándares que están incluidos en la familia de ISO 27000.

- **ISO 27000:** contiene el vocabulario en el que se apoyan el resto de las normas. Es similar a una guía/diccionario que describe los términos de todas las normas de la familia.
- **ISO 27001:** es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar.
- **ISO 27002:** se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles.
- **ISO 27003**: es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.
- **ISO 27004:** describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la Seguridad de la Información. Especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos.
- **ISO 27005:** es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.
- **ISO 27006:** es un conjunto de requisitos de acreditación para las organizaciones certificadoras.
- **ISO 27007**: es una guía para auditar SGSIS. Establece qué auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc.

REFERENCIA BIBLIOGRAFICA

- Gobierno de España normas ISO 27000 Recuperado de: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

- Intedya, ISO 27000 y el conjunto de estándares de Seguridad de la Información Recuperado de: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjunto-de-estandares-de-seguridad-de-la-informacion.html