SIS-254 SEGURIDAD DE INFORMACION

ING. EN TECNOLOGÍAS DE LA INFORMACIÓN Y SEGURIDAD

ING EN CIENCIAS DE LA COMPUTACION

SEMESTRE 7, 6

CAPITULO I
Introduccion

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

ACTIVOS DE INFORMACION

Los activos de información son todos aquellos datos e infraestructura tecnológica que son importantes para el buen desarrollo de la operaciones normales de una empresa.

UMRPSFXCH FACULTAD TECNOLOGÍA

SEGURIDAD DE LA INFORMACION

La seguridad de la información se refiere a las medidas tácticas para la protección de la información. Por ejemplo Políticas, análisis de riesgos, planes de contingencia.

ASFI ➡ Conjunto de medidas y recursos destinados a resguardar y proteger la información, buscando mantener la confidencialidad, integridad, y la disponibilidad de la misma.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

SEGURIDAD INFORMATICA

La seguridad informática es la disciplina encargada de implementar medidas técnicas para la protección de los activos que soportan la información. Por ejemplo Firewall, Redes Tecnológicas, etc.

La **seguridad informática**, también conocida como **ciberseguridad** es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA

ISO 27000

International Organization for Standardization

QUE VAMOS A VER.-

- Conocer los principales conceptos relacionados con Modelos y Estándares en Seguridad Informática.
- Reconocer los conceptos básicos de gestión de riesgos.
- Identificar la normatividad ISO en el proceso de gestión de la información.
- Determinar las principales normativas relacionadas con la seguridad de la información.

ISO 27000

Prof: Ing. D. Roca

FAMILIA

La **Organización Internacional de Estandarización** (ISO) recoge un extenso número de normas dentro de la familia de **ISO 27000.**

Cada norma tiene reservado una número dentro de una serie que van desde 27000 hasta 27019 y de 27030 a 27044. Vamos a realizar un repaso de las mas importantes de esta serie o familia:

Esta estandarización contiene las definiciones y los términos que se utilizarán durante toda la **serie 27000**. Para aplicar cualquier normativa necesita conocer un vocabulario perfectamente definido, por lo que así evitaremos cualquier mala interpretación de conceptos técnicos y gestión. Esta norma es gratuita a diferencia de las demás de la serie de normas que sí que suponen un coste para su implementación.

FAMILIA ISO 27000

Es la norma principal de toda la serie ya que incluye todos los requisitos de un **Sistema de Gestión de Seguridad de la Información** en las organizaciones. Es la certificación que deben obtener las organizaciones. *Norma que especifica los requisitos para la implantación del SGSI*. **Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos**. Fue publicada como estándar internacional en octubre de 2005. Revisada en septiembre de 2013. En el Anexo A se enumeran los objetivos de control y los análisis que desarrolla la **norma ISO27001** para que se puedan seleccionar las empresas durante el progreso de sus **Sistemas de Gestión de Seguridad de la Información.**

UMRPSFXCH FACULTAD TECNOLOGÍA

FAMILIA ISO 27000

EXIN INFORMATION SECURITY

ISO/IEC 27002

Gestión de la seguridad de la información

Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, **manteniendo 2005 como año de edición**. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a **SEGURIDAD DE LA INFORMACIÓN**. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

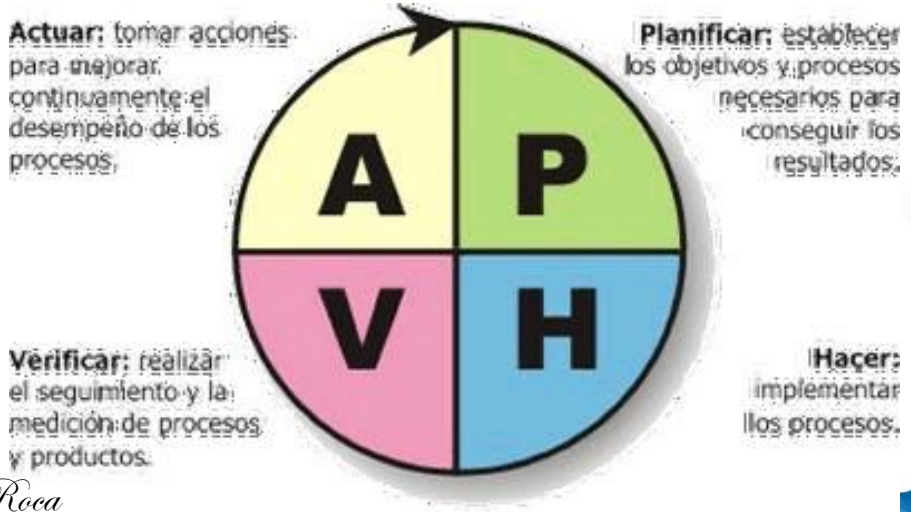
Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

Son **DIRECTRICES** para la implementación de un **SGSI**. Es el soporte de la norma ISO/IEC 27001. nos da la información necesaria para la utilización del **ciclo PHVA**(viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act") y todos los requerimientos de sus diferentes fases.



UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

ISO 27004

Publicada el 15 de Diciembre de 2009 y revisada en Diciembre de 2016. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

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.** Publicada el 7 de diciembre de 2009, no se encuentra traducida al español actualmente.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

Esta normativa establece las diferentes directrices para la **gestión de los Riesgos en la Seguridad de la Información**. Se trata de una norma de apoyo a los conceptos generales que vienen especificados en la ISO 27001 y se encuentra diseñada para ayudar a aplicar, de una forma satisfactoria, la seguridad de la información basada en un enfoque de gestión de riesgos. Para comprender a la perfección esta norma es necesario conocer todos los conceptos, modelos, procesos y términos descritos en la norma **ISO-27001 e ISO 27002**. ES LA QUE PROPORCIONA RECOMENDACIONES Y LINEAMIENTOS DE MÉTODOS Y TÉCNICAS DE EVALUACIÓN DE RIESGOS DE SEGURIDAD EN LA INFORMACIÓN

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA

ISO/IEC 27006

Este estándar específica todos los requisitos para lograr la acreditación de las entidades de auditoría y certificación de **Sistema de Gestión de Seguridad de la Información**. **ISO** ISO 27006 se trata de una versión revisada de la EA-7/03 (requisitos para la acreditación de entidades) que añade a la ISO/IEC 17021 (requisitos para entidades de auditoría y certificación de Sistemas de Gestión), los requisitos específicos de la**27001** y los del **Sistema de Gestión de Seguridad de la Información**. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1.

Prof: Ing. D. Roca

FAMILIA

Bienvenida
ISO/IEC 27007

Es un manual de **AUDITORÍA** de un **Sistema de Gestión de Seguridad de la Información**. Es un estándar Internacional el cual ha sido creado para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información (SGSI)**.
Publicada en noviembre de 2011.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

FAMILIA ISO 27000

ISO 27008

[Publicada](#) el 15 de Octubre de 2011. **No certificable.** ES UNA GUÍA DE AUDITORÍA DE LOS CONTROLES SELECCIONADOS EN EL MARCO DE IMPLANTACIÓN DE UN SGSI. En España, esta norma no está traducida. El original en inglés puede adquirirse en [iso.org.](#) Actualmente en proceso de revisión para su actualización.

Es una guía para auditar los controles seleccionados para implantar un SGSI. No es certificable. Publicada en octubre de 2011.

UMRPSFXCH FACULTAD TECNOLOGÍA

Prof: Ing. D. Roca

REFERENCIAS DE IMAGENES

Malyska , T. (2015). hombres-cinturón-salvavidas-apoyo-1002779. Recuperado de https://pixabay.com/es/hombres-cintur%C3%B3n-salvavidas-apoyo-1002779/

Altmann, Gerd.(2014). matrix-434037_1920. Recuperado de https://pixabay.com/es/matriz-comunicaci%C3%B3n-software-pc-434037/

Schwarzenberger, M.(2014). Cable-541068_1920. Recuperado de https://pixabay.com/es/cable-equipo-sata-s-ata-conexi%C3%B3n-541068/

Altmann, Gerd.(2015). hook-829942_1920. Recuperado de https://pixabay.com/es/gancho-marca-de-verificaci%C3%B3n-829942/

Linforth, P .high-security-1740431_1920. Recuperado de https://pixabay.com/es/alta-seguridad-protecci%C3%B3n-virus-1740431/

Janeb13. (2016). computer-1199488_1280. Recuperado de https://pixabay.com/es/equipo-teclado-rat%C3%B3n-pantalla-1199488/