TECNOLÓGICO NACIONAL DE MÉXICO

**Instituto Tecnológico de La Paz**

**Ingeniería en Sistemas Computacionales**

**Seguridad En Infraestructura Web**

**MSC. Armando Yuen Coria**

***Alumno***

**Enrique Missael Ramos Sepúlveda**

**ENSAYO**

**ISO/IEC 27034**

**ISO/IEC 27035**

La Paz B.C.S a 28 de agosto de 2019

ÍNDICE

[INTRODUCCIÓN 3](#_Toc17861775)

[ISO / IEC 27034 3](#_Toc17861776)

[ISO / IEC 27035 4](#_Toc17861777)

[CONCLUSIÓN 5](#_Toc17861778)

[BIBLIOGRAFÍA 5](#_Toc17861779)

# INTRODUCCIÓN

La ISO se trata de la Organización Internacional de Normalización, y se dedica a la creación de estándares para asegurar la calidad, seguridad y eficiencia de productos y servicios.

En la actualidad, existen más de 22.000 normas ISO diferentes. Cada una de ellas está centrada en la estandarización o regulación de un elemento de los servicios y/o productos.

En este presente trabajo se hablará de las normas ISO / IEC 27034 la cual trata sobre proporciona orientación para ayudar a las organizaciones a integrar la seguridad en los procesos utilizados para administrar sus aplicaciones. Y la ISO / IEC 27035 que presenta conceptos básicos y fases de la gestión de incidentes de seguridad de la información y combina estos conceptos con principios en un enfoque estructurado para detectar, informar, evaluar y responder a incidentes, y aplicar las lecciones aprendidas.

# ISO / IEC 27034

ISO / IEC 27034 ofrece orientación sobre seguridad de la información a aquellos que especifican, diseñan y programan o procuran, implementan y usan sistemas de aplicaciones, en otras palabras, gerentes de negocios y TI, desarrolladores y auditores, y en última instancia, los usuarios finales de las TIC. El objetivo es garantizar que las aplicaciones informáticas entreguen el nivel de seguridad deseado o necesario en apoyo del Sistema de Gestión de Seguridad de la Información de la organización, abordando adecuadamente muchos riesgos de seguridad de las TIC.

La norma establece que este no es un estándar de desarrollo de aplicaciones de software, ni un estándar de gestión de proyectos de aplicaciones, ni un estándar de ciclo de desarrollo de software. Su propósito es proporcionar una guía general que será apoyada, a su vez, por métodos y estándares más detallados en esas áreas;

Explícitamente adopta un enfoque de proceso para especificar, diseñar, desarrollar, probar, implementar y mantener funciones y controles de seguridad en los sistemas de aplicación. Por ejemplo, define la seguridad de la aplicación no como el estado de seguridad de un sistema de aplicación (los resultados del proceso) sino como "un proceso que una organización puede realizar para aplicar controles y mediciones a sus aplicaciones para gestionar el riesgo de usarlas".

La ISO 27034 se basa en los principios fundamentales siguientes:

* La seguridad se observa como un requisito.
* Seguridad de aplicaciones depende del contexto.
* Inversión correcta para la seguridad de las aplicaciones.
* Seguridad de las aplicaciones tiene que ser demostrada.

# ISO / IEC 27035

ISO 27035 explica un enfoque de mejores prácticas destinado a la gestión de la información de incidentes de la seguridad. Los controles de la seguridad de la información no son perfectos debido a que pueden fallar, pueden trabajar solo parcialmente o incluso, a veces, están ausentes, es decir, no están en funcionamiento. Debido a esto, los incidentes pasan debido que los controles preventivos no son totalmente eficaces o fiables.

La gestión de incidentes da lugar a que existan controles de detección y correctivas que estarán destinadas a reducir los impactos desfavorables y aprender las lecciones sobre mejoras en el SGSI. La norma proporciona un enfoque estructurado para:

* Identificar, comunicar y evaluar los incidentes de la seguridad de la información
* Contestar, gestionar los incidentes de la seguridad de la información
* Identificar, examinar y gestionar las vulnerabilidades de seguridad de la información
* Aumentar la mejora de la continuidad de la seguridad de la información y de la gestión de los incidentes, como respuesta a la gestión de incidentes de la seguridad de la información y de las vulnerabilidades.

La orientación de la seguridad de la información en ISO-27035 se puede aplicar a todas las organizaciones, ya sean pequeñas, medianas o grandes. Además, se da orientación de forma específica para las empresas que presten servicios de gestión de incidentes de seguridad de información.ISO-27035 constituye un proceso con cinco etapas que son claves:

* Preparase para enfrentarse a los incidentes.
* Reconocer los incidentes de seguridad de la información.
* Examinar los incidentes y tomar las decisiones sobre la forma en que se han llevado a cabo las cosas.
* Dar respuesta a los incidentes, lo que quiere decir, investigarlos y resolverlos.
* Aprender de las lecciones.

# CONCLUSIÓN

Las Normas ISO son un referente de calidad a nivel mundial y permiten a las organizaciones la estandarización y mejoramiento de sus procesos, su funcionamiento y reconocimiento, lo cual es de vital importancia para la sobrevivencia de las empresas. En el caso de la ISO 27034 ayuda a las organizaciones a integrar la seguridad sin problemas durante todo el ciclo de vida de sus aplicaciones. Por otra parte la ISO 27035 proporciona orientación sobre aspectos de la gestión de incidentes de seguridad de la información en las siguientes partes correspondientes.

# BIBLIOGRAFÍA

<https://www.iso.org/standard/44378.html>

<https://blog.rapid7.com/2017/04/20/introduction-to-isoiec-27035-the-iso-standard-on-incident-handling/>

<https://www.iso.org/obp/ui/#iso:std:iso-iec:27034:-1:ed-1:v1:en>

<https://www.pmg-ssi.com/2014/04/iso-27034-seguridad-de-aplicaciones/>

<https://www.iso27001security.com/html/27034.html>

<https://www.iso.org/standard/62071.html>