



Universidad Nacional  
Abierta y a Distancia

Escuela de Ciencias Básicas, Tecnología e Ingeniería

# Normas

204039-Seguridad Informática

Grupo:301122\_25 Diseño de Sitios Web

*7 de Junio de 2019*

# Normas para la Seguridad Informática

## ISO 27001:



Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. (ISOTools , 2019)



# Normas para la Seguridad Informática



## ISO 27001:



El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. *(ISOTools , 2019)*



# Normas para la Seguridad Informática

## ISO 27001:



CO-SI-CER535520

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. (ISOTools , 2019)

La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. (ISOTools , 2019)



## Estructura de la norma ISO 27001:



**1.Objeto y campo de aplicación:** La norma comienza aportando unas orientaciones sobre el uso, finalidad y modo de aplicación de este estándar. (*ISOTools* , 2019)

**2.Referencias Normativas:** Recomendla la consulta de ciertos documentos indispensables para la aplicación de ISO27001. (*ISOTools* , 2019)

**3.Términos y Definiciones:** *Describe la terminología aplicable a este estándar.* (*ISOTools* , 2019)



# Normas para la Seguridad Informática

## Estructura de la norma ISO 27001:



**4.Contexto de la Organización:** Este es el primer requisito de la norma, el cual recoge indicaciones sobre el conocimiento de la organización y su contexto, la comprensión de las necesidades y expectativas de las partes interesadas y la determinación del alcance del SGSI. (*ISOTools* , 2019)

**5.Liderazgo:** Este apartado destaca la necesidad de que todos los empleados de la organización han de contribuir al establecimiento de la norma. Para ello la alta dirección ha de demostrar su liderazgo y compromiso, ha de elaborar una política de seguridad que conozca toda la organización y ha de asignar roles, responsabilidades y autoridades dentro de la misma. (*ISOTools* , 2019)



## Estructura de la norma ISO 27001:



**6.Planificación:** Esta es una sección que pone de manifiesto la importancia de la determinación de riesgos y oportunidades a la hora de planificar un Sistema de Gestión de Seguridad de la Información, así como de establecer objetivos de Seguridad de la Información y el modo de lograrlos. (*ISOTools* , 2019)

**7.Soporte:** En esta cláusula la norma señala que para el buen funcionamiento del SGSI la organización debe contar con los recursos, competencias, conciencia, comunicación e información documentada pertinente en cada caso. (*ISOTools* , 2019)





# Normas para la Seguridad Informática



## Estructura de la norma ISO 27001:



**8.Operación:** Para cumplir con los requisitos de Seguridad de la Información, esta parte de la norma indica que se debe planificar, implementar y controlar los procesos de la organización, hacer una valoración de los riesgos de la Seguridad de la Información y un tratamiento de ellos. (*ISOTools* , 2019)

**9.Evaluación del Desempeño:** En este punto se establece la necesidad y forma de llevar a cabo el seguimiento, la medición, el análisis, la evaluación, la auditoría interna y la revisión por la dirección del Sistema de Gestión de Seguridad de la Información, para asegurar que funciona según lo planificado. (*ISOTools* , 2019)

**10.Mejora:** Por último, en la sección décima vamos a encontrar las obligaciones que tendrá una organización cuando encuentre una no conformidad y la importancia de mejorar continuamente la conveniencia, adecuación y eficacia del SGSI. (*ISOTools* , 2019)



## Novedades de la ISO 27001:2013:



CO-SI-CER535520

Esta norma fue publicada recientemente, aportó una serie de cambios con respecto a su antecesora que los usuarios de los SGSI tienen que asimilar para continuar gestionando de forma eficaz la Seguridad de la Información. Las novedades que manifiesta son: (ISOTools , 2019)

- *No aparece la sección “Enfoque a procesos” con su respectiva metodología basada en el ciclo PHVA, ahora ofrece mayor flexibilidad. (ISOTools , 2019)*
- *Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad. (ISOTools , 2019)*
- *Se han revisado los requisitos y controles. (ISOTools , 2019)*
- *Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación. (ISOTools , 2019)*

## Novedades de la ISO 27001:2013:



Esta norma fue publicada recientemente, aportó una serie de cambios con respecto a su antecesora que los usuarios de los SGSI tienen que asimilar para continuar gestionando de forma eficaz la Seguridad de la Información. Las novedades que manifiesta son: (ISOTools , 2019)

- *No aparece la sección “Enfoque a procesos” con su respectiva metodología basada en el ciclo PHVA, ahora ofrece mayor flexibilidad. (ISOTools , 2019)*
- *Se elimina la obligatoriedad de algunos documentos, conservando únicamente la declaración de aplicabilidad. (ISOTools , 2019)*
- *Se han revisado los requisitos y controles. (ISOTools , 2019)*
- *Se apuesta por un enfoque del análisis del riesgo en la fase de planificación y operación. (ISOTools , 2019)*

# Lista de Referencias



- ISOTools . (2019). Software ISO Riesgos y Seguridad. Obtenido de <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>



Universidad Nacional  
Abierta y a Distancia

**¡GRACIAS POR SU  
ATENCIÓN!**