

# OVI SEGURIDAD INFORMATICA

* + [**INICIO**](http://docs.google.com/index.html)
  + [**MULTIMEDIA**](http://docs.google.com/multimedia.html)
  + [**LECTURAS**](http://docs.google.com/lecturas.html)
  + **ACTIVIDADES**
    - [**Actividad 1**](http://docs.google.com/actividad1.html)
    - [**Actividad 2**](http://docs.google.com/actividad2.html)
    - [**Actividad 3**](http://docs.google.com/actividad3.html)
  + [**AUTORES**](http://docs.google.com/autores.html)

## ¿Cuál es la normatividad que rige a la seguridad de la información?

### Marco Legal

###### • CONPES 3701 DE 2011 –Lineamientos CiberSeguridad y Ciberdefensa

###### • Ley 527 de 1999 – Validez jurídica y probatoria de la información electrónica;

###### • Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad;

###### • Ley 679 de 2001 – Pornografía Infantil – Responsabilidad ISPs;

###### • Ley 962 de 2005 – Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;

###### • Ley 1150 de 2007 – Seguridad de la información electrónica en contratación en línea;

###### • Ley 1266 de 2008 – Habeas data financiera, y seguridad en datos personales;

###### • Ley 1273 de 2008 – Delitos Informáticos y protección del bien jurídico tutelado que es la información;

###### • Ley 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad;

###### • Ley 1437 de 2011 – Procedimiento Administrativo y aplicación de criterios de seguridad;

###### • Ley 1480 de 2011 – Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas;

###### • Decreto Ley 019 de 2012 – Racionalización de trámites a través de medios electrónicos. Criterio de seguridad

###### • Ley 1581 de 2012 – Ley estatutaria de Protección de datos personales;

###### • Ley 1623 de 2013 – Ley de Inteligencia – Criterios de seguridad;

###### • Ley 1712 de 2014 – Transparencia en el acceso a la información pública.

Certicamara. (2017). Retrieved 19 September 2017, from https://web.certicamara.com/media/58493/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

Normas ISO sobre gestión de seguridad de la información | Seguridad Informática. (2017). Descargas.pntic.mec.es. Retrieved 19 September 2017, from http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas\_iso\_sobre\_gestin\_de\_seguridad\_de\_la\_informacin.html

SGSI - 04 Estándares de Gestión de la Seguridad de la Información. (2017). YouTube. Retrieved 27 October 2017, from https://www.youtube.com/watch?v=vWAV0bdWvtI

 Este ovi sobre seguridad informática va dirigido a estudiantes o demás personas que estén interesados en saber más de la seguridad informática y sus elementos como son la integrad,disponibilidad,privacidad,control y autenticidad de la informática .presenta una introducción, profundización e información complementaria sobre los elementos de este tema y maneras de protegerse de Universidad Nacional Abierta y a Distancia – [UNAD](#gjdgxs) - Vicerrectoría Académica y de Investigación - VIACI Escuela: Ciencias Básicas Tecnología e Ingeniería Programa: Ingeniería de Sistemas Curso: Diseños de Sitios Web Código: 301122 inseguridades en la informática como son los antivirus y colocar muy buenas contraseñas que sean difíciles de copiar entre otros.

[HIPERVINCULO](#gjdgxs)

#### **Definición Seguridad informatica**

La seguridad informática, también conocida como 'seguridad de tecnología de la información', 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 y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La ciberseguridad es la seguridad del Ciberespacio, que comprende Personas, Procesos , Infraestructura. La definición de seguridad de la información no debe ser confundida con la de «seguridad informática», ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad informática es la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación.

##### **Objetivos**

La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores. La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes: La infraestructura computacional: es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar por que los equipos funcionen adecuadamente y anticiparse en caso de fallos, robos, incendios, sabotajes, desastres naturales, fallos en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática. Los usuarios: son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable. La información: esta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios. Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no esten dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática. En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial. En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales. Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso a la compañía a través de Internet. Además, debido a la tendencia creciente hacia un estilo de vida nómada de hoy en día, el cual permite a los empleados conectarse a los sistemas de información casi desde cualquier lugar, se pide a los empleados que lleven consigo parte del sistema de información fuera de la infraestructura segura de la compañía. La seguridad informática se resume, por lo general, en cinco objetivos principales: Integridad: garantizar que los datos sean los que se supone que son Confidencialidad: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian Disponibilidad: garantizar el correcto funcionamiento de los sistemas de información Evitar el rechazo: garantizar de que no pueda negar una operación realizada. Autenticación: asegurar que sólo los individuos autorizados tengan acceso a los recursos Confidencialidad La confidencialidad consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación. Integridad La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente). Disponibilidad El objetivo de la disponibilidad es garantizar el acceso a un servicio o a los recursos.

No repudio Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada. Autenticación La autenticación consiste en la confirmación de la identidad de un usuario; es decir, la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.

##### **Necesidad de un enfoque global**

Frecuentemente, la seguridad de los sistemas de información es objeto de metáforas. A menudo, se la compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas. Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad a nivel global y que debe constar de los siguientes elementos: Concienciar a los usuarios acerca de los problemas de seguridad Seguridad lógica, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías. Seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc. Seguridad física, o la seguridad de infraestructuras materiales: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la compañía, las estaciones de trabajo de los empleados, etc.

# [**https://es.wikipedia.org/wiki/Seguridad\_inform%C3%A1tica**](#gjdgxs)

## **https://www.bitcuantico.com/2011/01/26/seguridad-informatica-conceptos-y-caracteristicas/**

Encuentranos en las redes sociales