Unidad 1: Principios de seguridad y alta disponibilidad

[**1**](#_heading=h.2jxsxqh) **Introducción 2**

[**2**](#_heading=h.z337ya) **Propiedades CIDAN 3**

[**3**](#_heading=h.3j2qqm3) **Alta disponibilidad 5**

[3.1.1](#_heading=h.1y810tw) Ejemplo 6

[**4**](#_heading=h.4i7ojhp) **Elementos de seguridad 7**

[*4.1*](#_heading=h.2xcytpi) *Activos 7*

[*4.2*](#_heading=h.1ci93xb) *Vulnerabilidad 9*

[*4.3*](#_heading=h.3whwml4) *Amenazas 9*

[*4.4*](#_heading=h.2bn6wsx) *Riesgos 10*

[4.4.1](#_heading=h.qsh70q) Proceso del análisis de riesgos 10

[**5**](#_heading=h.3as4poj) **Auditoría de seguridad 11**

[*5.1*](#_heading=h.1pxezwc) *Servicios de una auditoría 11*

[*5.2*](#_heading=h.49x2ik5) *Tipos de auditorías 12*

# Introducción

Los hábitos de vida del ser humano le han llevado a depender enorme y exageradamente de los sistemas informáticos; de ahí que la seguridad informática se haya convertido en algo de suma relevancia. De hecho, es cierto que todo —o casi todo— está controlado por ordenadores:

* Nuestras cuentas bancarias.
* El comercio internacional.
* Plantas de energía eléctrica
* Ejército
* Satélites
* Sistema judicial
* Sistema sanitario

La protección de los sistemas y redes de ordenadores es, por lo tanto, crítica; sin esa protección, podrían ocurrir desastres de toda índole; cabe recordar, a estas alturas ya en clave de humor, que en los años previos al año 2000, el llamado “Efecto 2000” —ocasionado por un error de previsión increíble— puso en alarma a todo el planeta: los sistemas informáticos dejarían de ser seguros el 1 de enero de 2000 convirtiendo la vida de las personas en un gran caos; sirvan estos tres vídeos como recordatorio de lo ocurrido:

[Anuncio Gobierno de España en 1999](https://www.youtube.com/watch?v=Y0y2Bnv1djA)

[Recordatorio de TVE del Efecto 2000](http://www.rtve.es/alacarta/videos/te-acuerdas/efecto-2000-acuerdas/978703/)

[Cortometraje finalista de Jameson Notodofilmfest en 2014](https://www.youtube.com/watch?v=BYeYe84seCY)

Cuando hablamos de seguridad informática, lo hacemos de un término que podría definirse de cientos de maneras; he aquí algunas posibles definiciones:

* El conjunto de servicios y mecanismos que aseguren la integridad y privacidad de la información que los sistemas manejen.
* El conjunto de servicios, mecanismos y políticas que aseguren que el modo de operación de un sistema sea seguro.
* El conjunto de protocolos y mecanismos que aseguren que la comunicación entre los sistemas esté libre de intrusos.

Estos son algunos de los principales objetivos de la seguridad informática:

* Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos
* Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
* Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
* Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

La comunidad de usuarios y profesionales en materia de seguridad informática mantiene al día al resto de los usuarios mediante noticias y post en blogs y webs especializadas: el [Basque Cibersecurity Centre](https://www.basquecybersecurity.eus/es/) es la organización designada por el Gobierno Vasco para promover la ciberseguridad en Euskadi, y cuenta con numerosos servicios tanto para usuarios como para empresas; el Instituto Nacional de Ciberseguridad (INCIBE): <https://www.incibe.es/> dispone de la Oficina de Seguridad del Internauta, que, entre otros servicios, pone a disposición de los ciudadanos varios test sobre seguridad informática: <http://www.osi.es/es/cuanto-sabes> .

# Propiedades CIDAN

Se considera seguro un sistema que cumple con las propiedades de integridad, confidencialidad y disponibilidad de la información.

Disponibilidad

Garantiza que el sistema y los datos estarán disponibles para los usuarios; se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidentalmente o intencionadamente se hayan dañado o destruido.

Confidencialidad

Garantiza que el acceso a la información no se produce de forma no autorizada; dicho de otra forma: los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

Para prevenir errores de confidencialidad, debe diseñarse un control de accesos al sistema: quién puede acceder, desde dónde, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

Integridad

Garantiza que la información no ha sido modificada sin autorización; es decir: los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

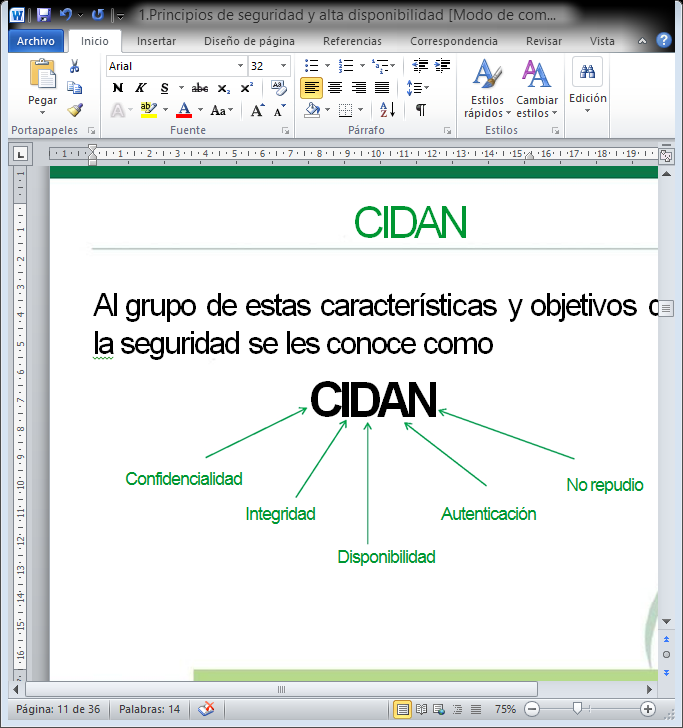
Para evitar riesgos relacionados con la integridad, se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y traten y resuelvan los errores que se han descubierto.

Autenticación

Garantiza que un documento ha sido elaborado (o pertenece) por quien el documento dice. Se trata, por lo tanto, de que la identidad del emisor no sea suplantada. Entraría en juego aquí la criptografía.

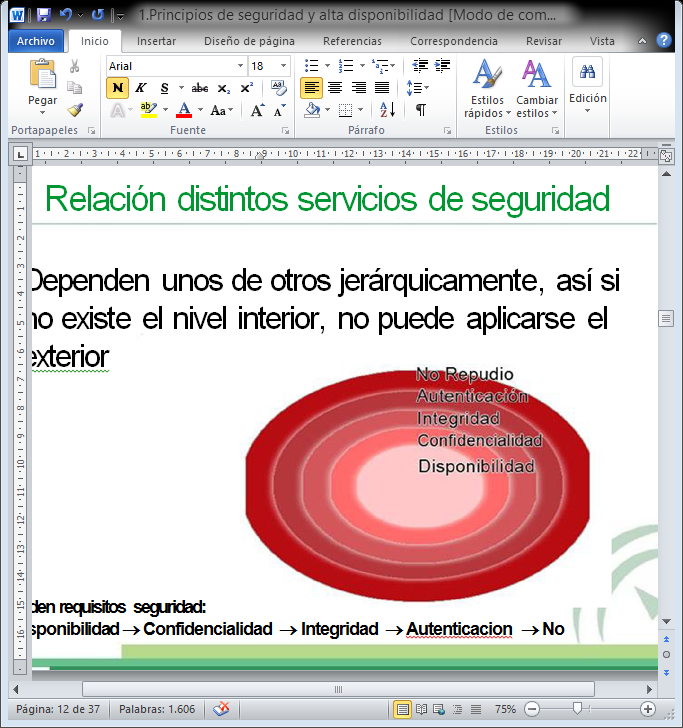
No repudio

Impide que el emisor niegue haber estado involucrado en una comunicación. Puede ser:

* No repudio en origen: el emisor no puede negar el envío; la prueba la crea el emisor y la recibe el destinatario.
* No repudio en destino: el receptor no puede negar la recepción ya que el emisor tiene pruebas de la recepción, creadas por el receptor y recibidas por el emisor.
* 

Esquema CIDAN

Dependen unos de otros jerárquicamente; así, si no existe el nivel interior, no puede aplicarse el exterior.



# Alta disponibilidad

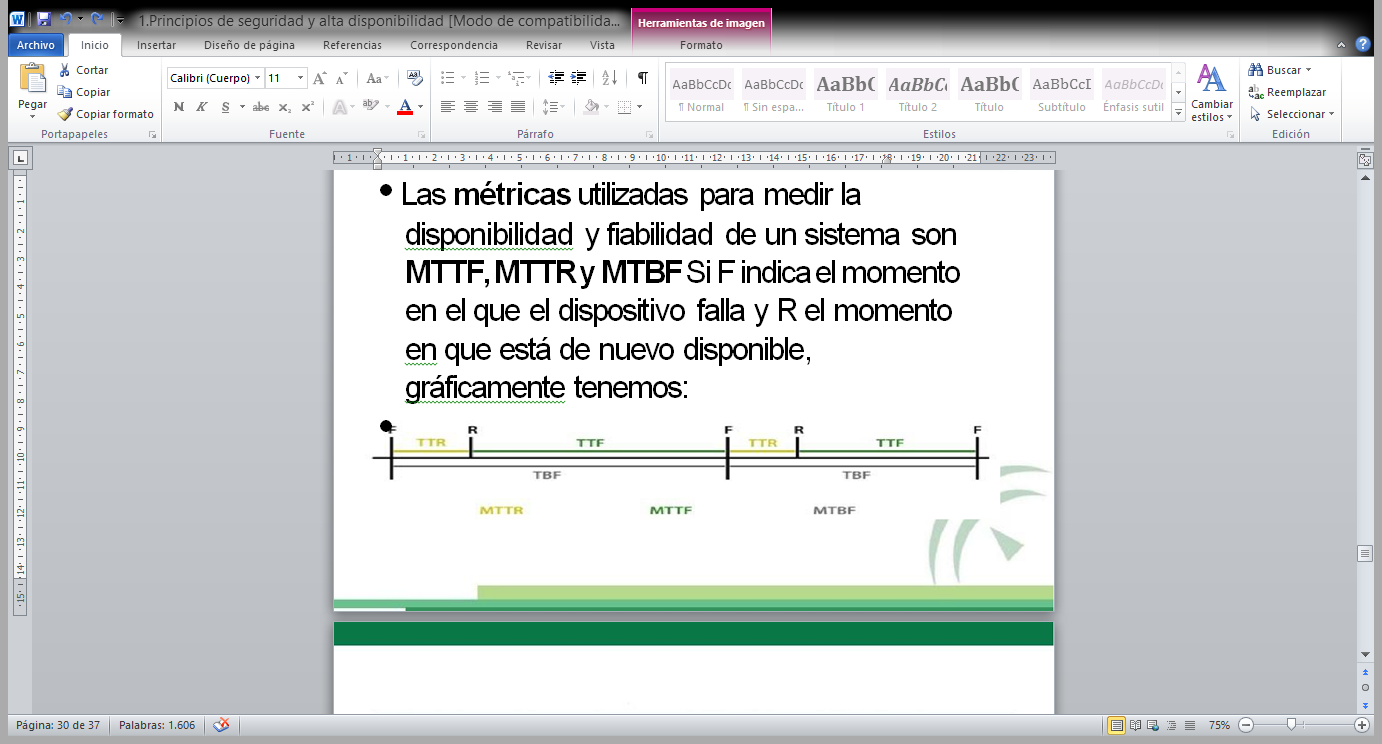
La alta disponibilidad (High Availability) es la capacidad de que las aplicaciones y los datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones.

Estos son los tipos de interrupciones principales:

* Previstas: ocurren cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
* Imprevistas: suceden por acontecimientos imprevistos (apagón, error de hardware/software, problemas de seguridad, desastre natural, virus...).

Métricas

Las métricas utilizadas para medir la disponibilidad y fiabilidad de un sistema son MTTF, MTTR y MTBF; si F indica el momento en el que el dispositivo falla y R el momento en que está de nuevo disponible, gráficamente tenemos:



* TTR (Time to repair): tiempo que se necesita para volver a poner en marcha el sistema; dicho de otra manera: tiempo que se tarda en reparar el fallo.
* TTF (Time to failure): tiempo que pasa desde que el sistema empieza a funcionar hasta que falla; es decir: el tiempo que el sistema está funcionando ininterrumpidamente, sin fallos.
* TBF (Time between failures): tiempo transcurrido entre el inicio de un fallo y el inicio del siguiente fallo.
* MTTF (Mean time to failure): tiempo medio de funcionamiento ininterrumpido hasta que se produce un fallo.

MTTF = (Tiempo total de funcionamiento correcto) / (nº fallos)

* MTTR (Mean time to repair) Tiempo medio que se tarda en poner de nuevo en marcha el sistema cuando ocurre un fallo.

MTTR = (Tiempo total de inactividad) / (nº de fallos)

* MTBF (Mean time between failures): tiempo medio entre fallos.

MTBF = (Tiempo total) / (nº de fallos)

Existen muchos niveles de disponibilidad, estando el mayor nivel de exigencia en “los cinco nueves” (99,999%), lo cual implica que se aceptan unos 5 minutos de inactividad anuales.

### Ejemplo

*Tenemos que calcular el MTTR, MTTF y MTBF de un servidor que ha tenido 5 caídas en los últimos 3 meses. Las tres primeras se solucionaron en 5 minutos, pero las dos últimas supusieron un tiempo de inactividad de 30 y 40 minutos respectivamente.*

5 fallos en 3 meses

* 3 meses -> 24 x 60 x 90 = 129600 minutos.
* 5 fallos -> 5 + 5 + 5 + 30 + 40 = 85 minutos.
* 129600 – 85 = 129515 minutos de funcionamiento correcto.
* **MTTR = 85 m / 5 = 17 minutos.**
* **MTTF = 129515 / 5 = 25903 minutos.**
* **MTBF = 129600 / 5 = 25920 minutos.**

¿Qué porcentaje de disponibilidad ha tenido el servidor del caso anterior?

Tiempo funcionamiento/Tiempo total = 129515/129600= 0,9993 → **99,93%**

¿Cuánto tiempo puede estar inactivo al mes un equipo para conseguir la disponibilidad de 5 nueves?

1 mes x 30 días/mes x 24 horas/mes x 60 min/hora = 43200 minutos tiene un mes

100 -> 43200 m

99,999 -> x

 x = 43200 min. x 99,999 / 100 = 43199,568 minutos que tiene que estar funcionando

 43200 – 43199,568 = 0,432 minutos (o sea, 25,92 s) de inactividad al mes, como máximo.

# Elementos de seguridad

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema.

Para comenzar a analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta algunos elementos: activos, amenazas, riesgos, ataques e impactos.

## Activos

Recursos que pertenecen al propio sistema de información o están relacionados con éste. La presencia de los activos facilita el funcionamiento de la empresa y la consecución de sus objetivos.

Hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido en otro.

Datos

Representan el núcleo de toda organización. Se puede considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente, están organizados en bases de datos.

Software

Son los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos. Reciben y gestionan o transforman datos para darles el fin que tenga establecido.

Hardware

Son los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento y almacenan los datos; también los periféricos y elementos accesorios (modém, router, instalación eléctrica...) para asegurar el correcto funcionamiento.

Redes

Desde las redes locales de la propia organización hasta las metropolitanas o Internet. Representa la vía de comunicación y transmisión de datos a distancia.

Soportes

Se trata de los lugares donde la información queda registrada y almacenada (CD, discos...e incluso papel).

Instalaciones

Lugares que albergan los sistemas de información y de comunicaciones (oficinas, despachos... incluso vehículos).

Personal

Conjunto de personas que interactúan con el sistema de información (administradores, programadores, usuarios internos y externos y resto del personal de la empresa)

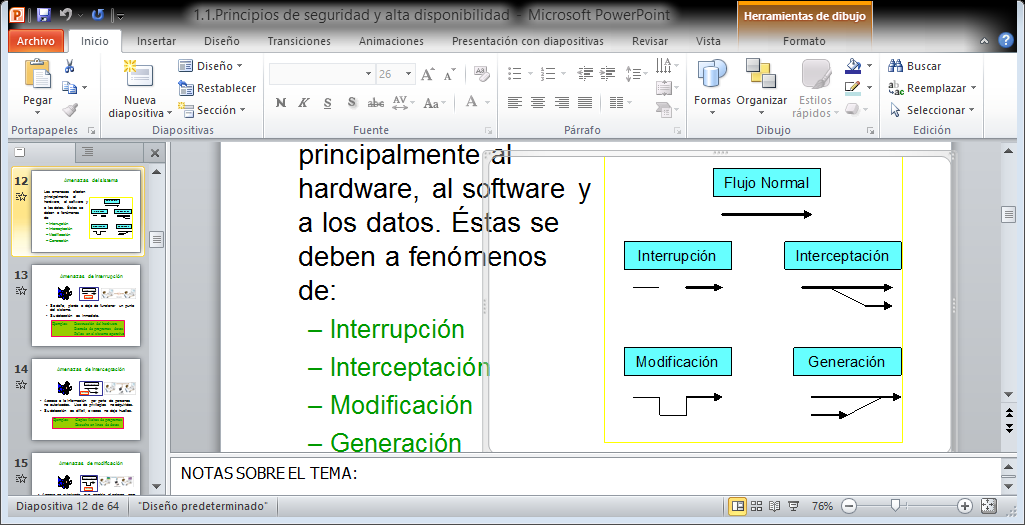
Servicios

Se trata de servicios que se ofrecen a clientes o usuarios: productos, sitios Web, foros, correo electrónico...

## Vulnerabilidad

Se considera vulnerabilidad a todo aquello que puede provocar que nuestros sistemas informáticos funcionen de manera diferente a como estaba pensado que lo hicieran, afectando a la seguridad de los mismos, y pudiendo derivar, entre otras cosas, en la pérdida y robo de información sensible.

## Amenazas

Son factores de diversa índole (personas, máquinas o sucesos) que, aprovechándose del nivel de vulnerabilidad del sistema, podrían atacar a éste produciéndole daños. Afectan principalmente al hardware, al software y a los datos y se deben a fenómenos de: interrupción, interceptación, modificación y generación.

Amenazas de interrupción

Se daña, pierde o deja de funcionar un punto del sistema; su detección es inmediata. Ejemplos: destrucción del hardware; borrado de programas y datos; fallos en el sistema operativo.

Amenazas de interceptación

Se produce el acceso a la información por parte de personas no autorizadas, debido al uso de privilegios no adquiridos. Su detección es difícil, ya que a veces no deja huellas. Ejemplos: copias ilícitas de programas; escucha en la línea de datos.

Amenazas de modificación

Tienen que ver con el acceso no autorizado que cambia el entorno para su beneficio; su detección es, a menudo, difícil. Ejemplos: modificación de bases de datos; modificación de elementos del HW.

Amenazas de generación

Están relacionadas con la creación de nuevos objetos dentro del sistema; su detección es difícil, pudiendo darse delitos de falsificación. Ejemplos: añadir transacciones en la red; añadir registros en una base de datos.

## Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad, ni una vulnerabilidad cuando no existe amenaza para la misma.

### Proceso del análisis de riesgos

Para implantar una política de seguridad en un sistema de información es necesario seguir un esquema lógico:

* Hacer el inventario y una valoración de los activos.
* Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.
* Identificar y evaluar las medidas de seguridad existentes.
* Identificar y valorar las vulnerabilidades de los activos a las amenazas que les afectan.
* Identificar los objetivos de seguridad de la organización.
* Determinar sistemas de medición de riesgos.
* Determinar el impacto que produciría un ataque.
* Identificar y seleccionar las medidas de protección.

# Auditoría de seguridad

Es el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades.

Entre los objetivos de una auditoría destacan estos:

* Revisar la seguridad de los entornos y sistemas.
* Verificar el cumplimiento de la normativa y legislación vigente (Ley de protección de datos).
* Elaborar un informe independiente.

## Servicios de una auditoría

He aquí algunos de los servicios que ofrece una auditoría:

* Enumeración de sistemas operativos, servicios, aplicaciones, topologías y protocolos de red.
* Detección, comprobación y evaluación de vulnerabilidades.
* Medidas específicas de corrección.
* Recomendaciones sobre implantación de medidas preventivas.

## Tipos de auditorías

Auditoria de seguridad interna

Nivel de seguridad de las redes locales y de carácter interno.

Auditoria de seguridad perimetral

Nivel de seguridad del perímetro de la red local, conectado a redes públicas.

Test de intrusión

Se intenta acceder a los sistemas para comprobar el nivel de resistencia a la intrusión.

Análisis forense

Análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema.