Conceptos básicos de seguridad

Curso 2013/14

Grado Gestión Informática Empresarial

Asignatura Auditoría y Seguridad Informática

Profesores Alfredo Cuesta Infante
alfredo.cuesta@ajz.ucm.es
Alberto Herrán González
aherran@ajz.ucm.es

Contenidos

Intuición

Seguridad Informática

Cada una de esas dos palabras evoca varias ideas.
Algunas pueden ser:

Seguridad	Informática
Proteger	Información
Defender	Datos
Mantener en secreto	Programas
Prohibir el paso	Ordenadores
Estar fuera de peligro	Internet

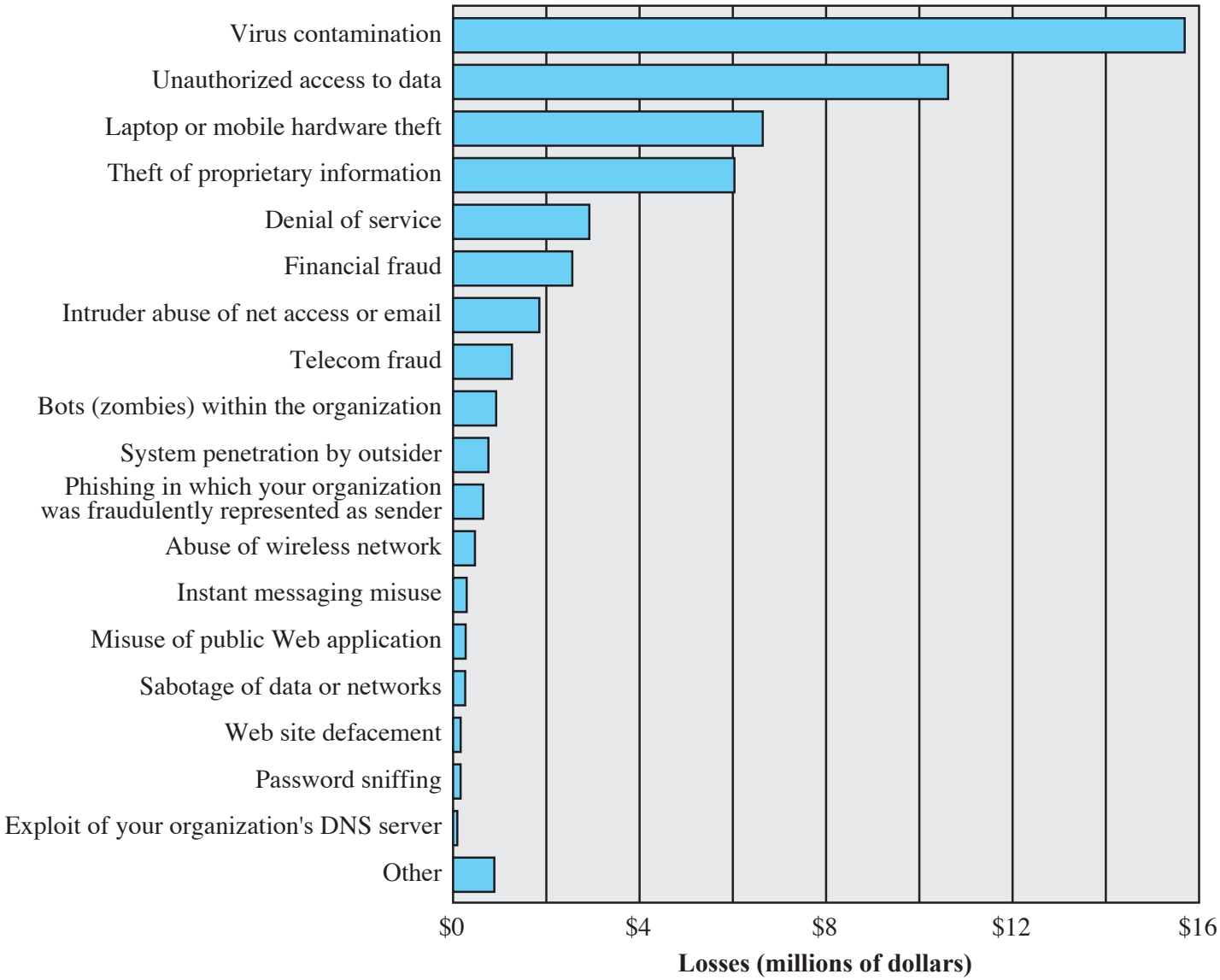
- El concepto de seguridad existe porque algo que consideramos **valioso** se encuentra **amenazado** o **atacado**.
- 100 % de seguridad $\rightarrow$ Sin amenazas ni ataques.
- Por tanto es imposible alcanzar la seguridad total.

Preguntas claves

1. ¿Qué es valioso?
2. ¿Cómo está amenazado / atacado?
3. ¿Cuáles son nuestras armas?

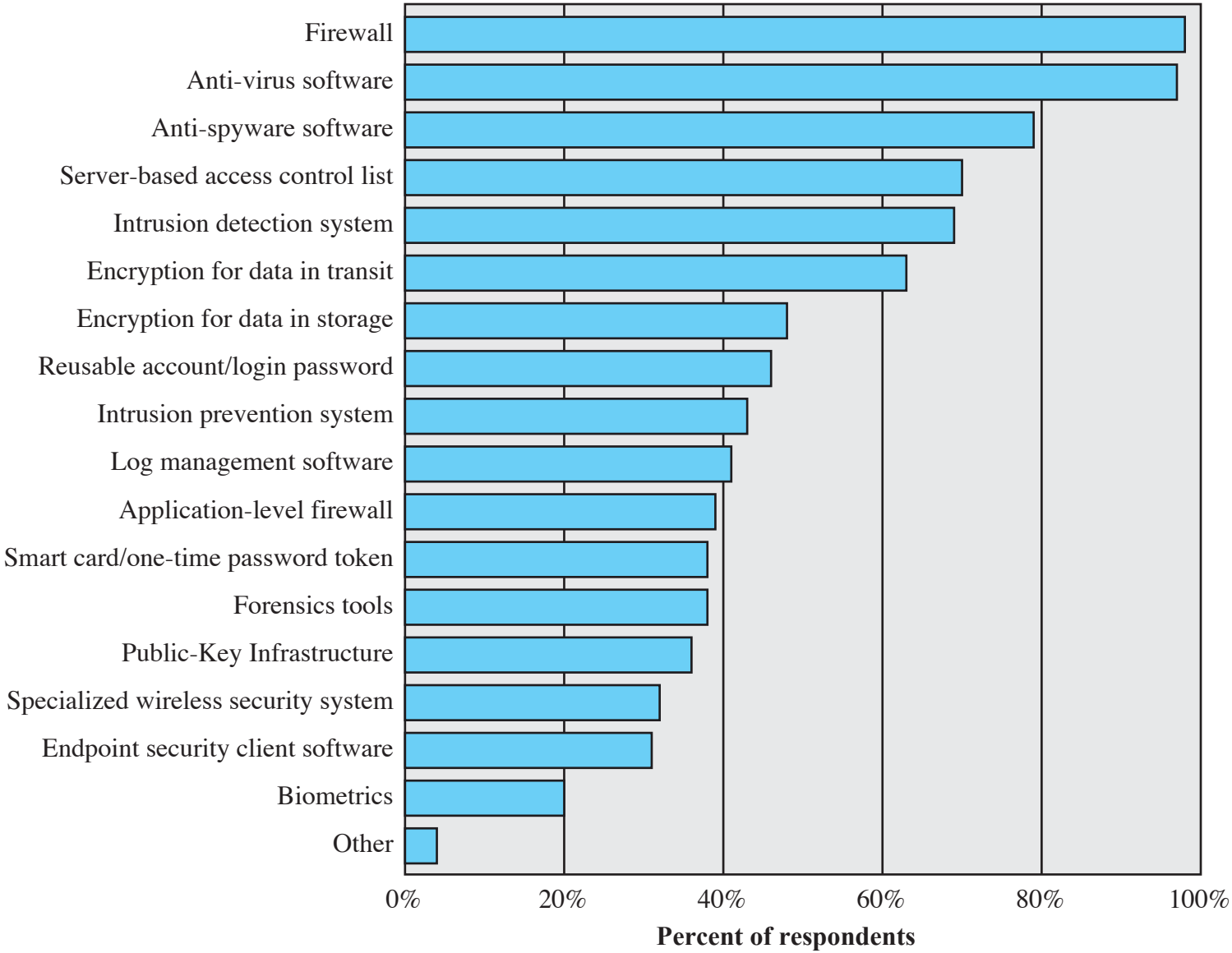
Algunos datos estadísticos

Perdidas motivadas por diferentes ataques



Algunos datos estadísticos

Tecnologías de seguridad más empleadas



¿Qué es valioso?

Activos

En inglés *asset*.
La 9ª entrada del DRAE lo define como *el conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo, y que se reflejan en su contabilidad*.

Activos informáticos

En seguridad informática tomaremos prestado el termino y llamaremos **activos informáticos** a:

- Equivalentes electrónicos del papel (pdfs, documentos, ...)
- Procesos automatizados o aplicaciones (hojas de cálculo, ...)
- Descripción de procedimientos (código fuente, planos, procesos químicos, ...)
- Información recopilada, bases de datos, ...
- Servidores, Unidades de almacenamiento masivo, ...

En definitiva es:

- toda aquella información relevante para la empresa
- que se encuentra almacenada en un soporte
- que puede ser procesado por sistemas informáticos
- así como los propios sistemas informáticos

Elementos vulnerables

- Tan importante como los activos informáticos.
- También deben ser identificados y asegurados.

Activos informáticos

El valor de la informática en la empresa

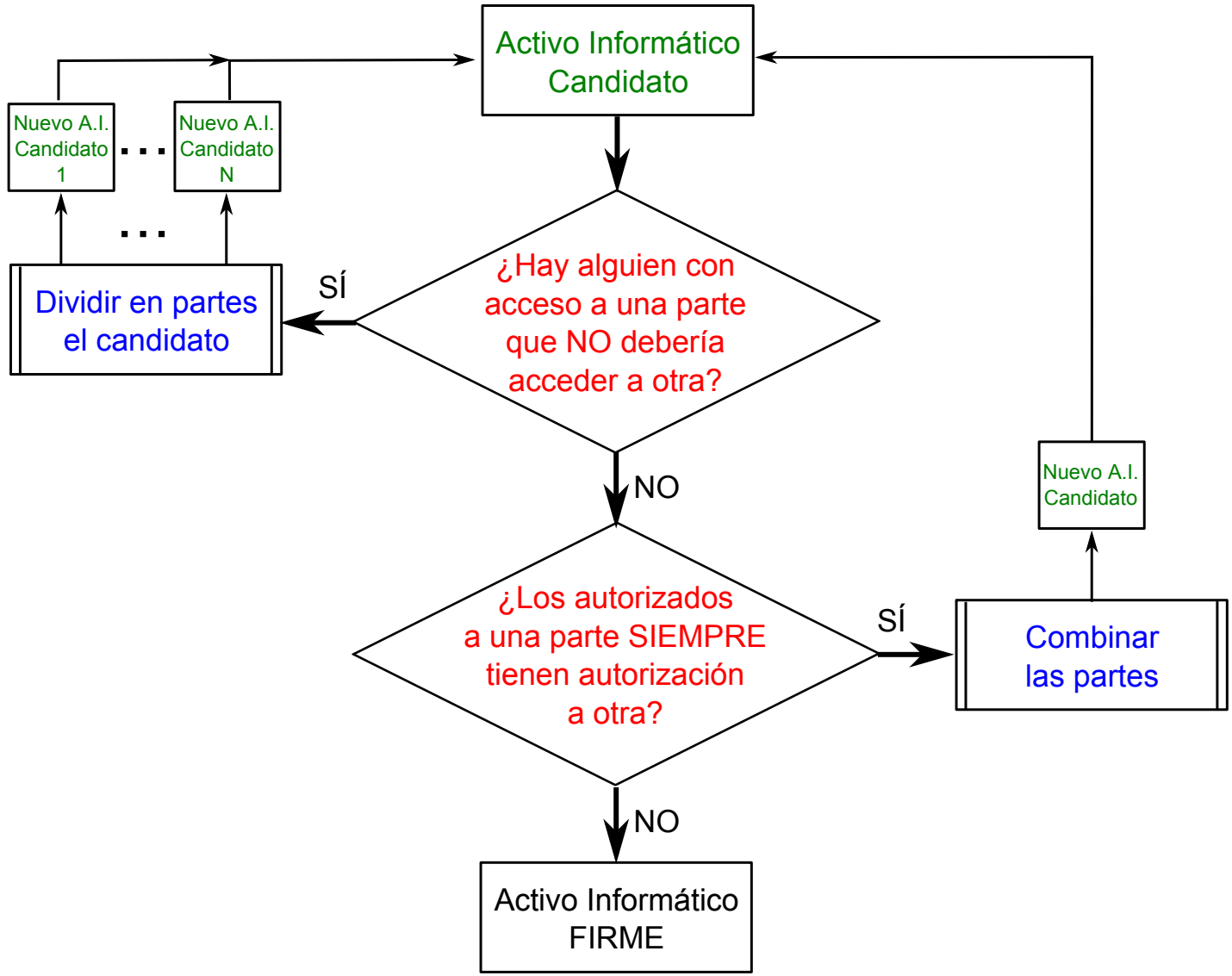
En esta asignatura consideraremos un nuevo activo de la empresa.
El **Activo informático** es toda aquella información relevante para la empresa almacenada en un soporte que puede ser procesado por sistemas informáticos; así como los mismos sistemas informáticos. Por ejemplo:

- Equivalentes electrónicos del papel (pdfs, documentos, ...)
- Procesos automatizados o aplicaciones (hojas de cálculo, ...)
- Descripción de procedimientos (código fuente, planos, procesos químicos, ...)
- Información recopilada, bases de datos, ...
- Servidores, Unidades de almacenamiento masivo, ...

¿Dónde está el tesoro?

En este punto se plantea el siguiente problema:
Dado un candidato X perteneciente a alguno de los casos enumerados arriba u otro similar; decidir si tiene la suficiente importancia o entidad para ser considerado como activo informático.
La respuesta casi nunca será SI/NO ya que la información relevante está mezclada con otra que no lo es. Por tanto el problema es equivalente a:
Dado un candidato X; dividirlo hasta llegar a sus *átomos*, que serán activos informáticos.
Así que la estrategia a seguir es *Divide y Vencerás*: resolver un problema grande mediante la resolución de los subproblemas que lo componen.

Divide y Vencerás para identificar activos informáticos



En lo sucesivo *Activo informático* se representará a/i .

¿Cómo está amenazado?

¿Por qué los a/i no son seguros?

La regla de oro es:

> Identificar quien PUEDE y quien DEBE acceder a un a/i y comparar.

El acceso puede ser legal o ilegal.

Acceso legal

Los a/i pueden estar amenazados incluso si nadie los ataca.
El sistema de seguridad puede no estar a la altura si:

- La tecnología requeríada no existía o era inaccesible cuando fue implantado.
- Hay una política de seguridad mal diseñada.
- Los empleados no tienen la formación necesaria.

Acceso ilegal

Los sistemas de seguridad se diseñan para minimizar las amenazas.
Ejemplo:

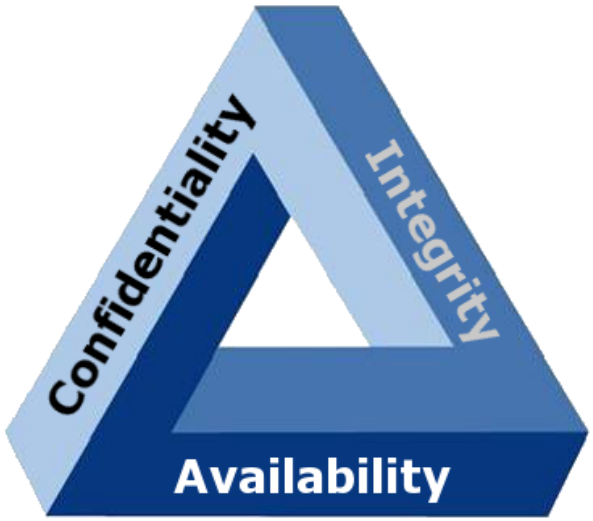
- Imponemos contraseñas para impedir el acceso al ordenador.
- El ordenador estará más amenazado si la contraseña es una palabra que si es una mezcla de caracteres, números y símbolos.
- Un ataque es la acción de llevar a cabo la amenaza, usando un diccionario para probar palabras por ejemplo.

Blancos clave de las amenazas

Las amenazas y ataques a los activos informáticos están dirigidos contra alguna de las **características fundamentales** para que un activo informático sea seguro.

El modelo anglosajón:
The CIA triad

- Confidentiality
- Integrity
- Availability



Su versión española podría ser:
El CID de la seguridad

El CID de la seguridad

Confidencialidad

- **Confidencialidad de los datos**
  - La información no es desvelada a individuos no autorizados
- **Privacidad**
  - Otrogar a los individuos control total o parcial sobre qué información relacionada con ellos puede ser recogida, almacenada y a quién puede ser desvelada

La perdida de confidencialidad supone una revelación no autorizada de información.

Integridad

- **Integridad de los datos**
  - La información o los programas cambian SÓLO de un modo conocido y autorizado
- **Integridad del sistema**
  - El sistema funciona libremente tal y como fue diseñado; sin restricciones ni funcionalidades añadidas no autorizadas

La perdida de integridad supone la modificación o destrucción de información.

Disponibilidad

- Asegurar que los sistemas responden a las peticiones y el servicio no es denegado a personas autorizadas.

La perdida de dispinibilidad supone la imposibilidad de acceder o usar la información.

Otros aspectos importantes

Imputabilidad

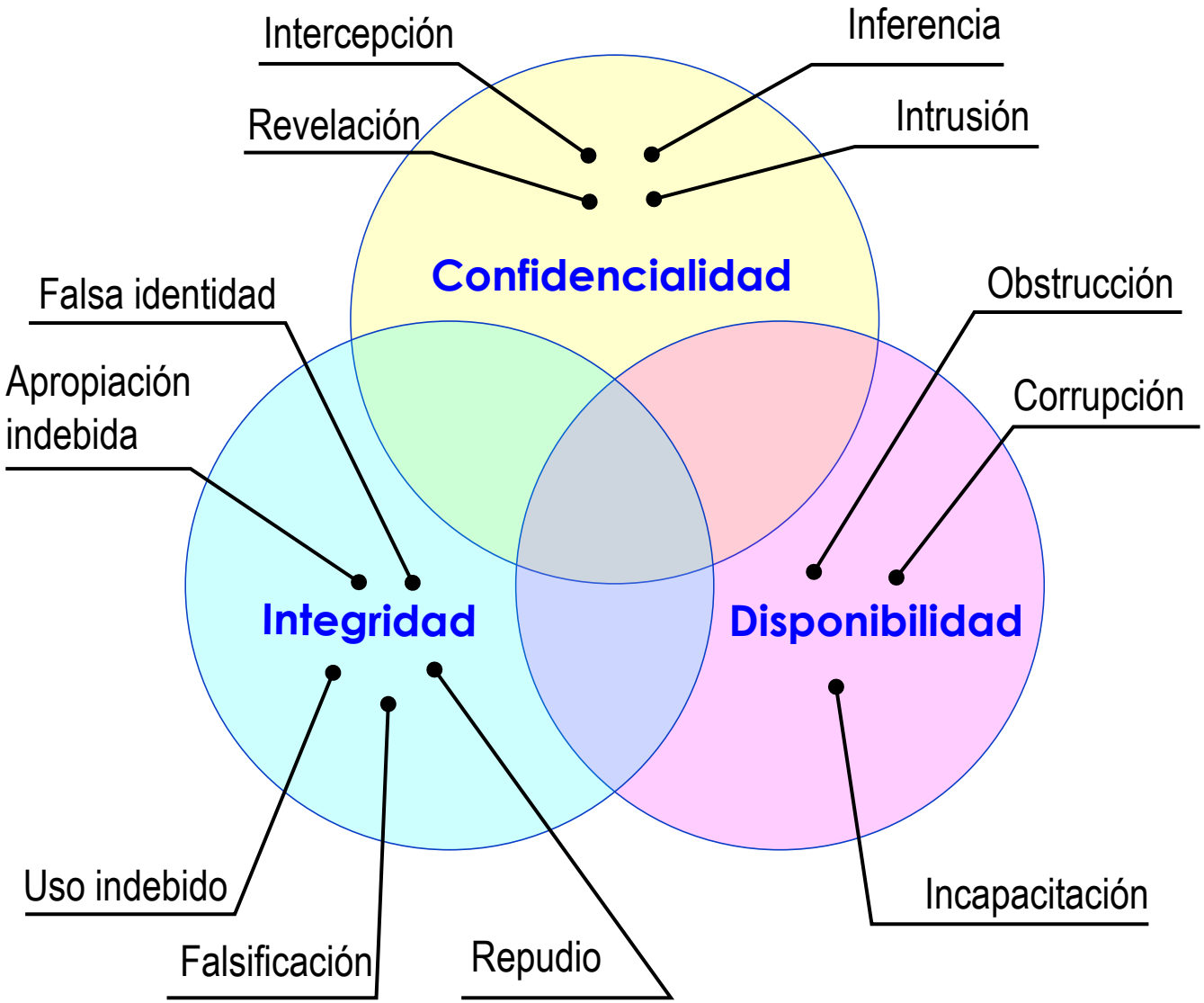
- En inglés *Accountability*
- Se plantea como objetivo poder trazar todas las acciones realizadas por una entidad de tal modo que el rastro le lleve de manera única a dicha entidad.

Autenticidad

- En inglés *Authenticity*
- Es la propiedad de ser genuino, de poder ser verificado y confiable.
- Debe verificar dos puntos:
  - Que los usuarios son quienes dicen ser.
  - Que su punto de llegada es una fuente confible.

- Confidencialidad, Integridad, Disponibilidad, Imputabilidad y Autenticidad son cualidades de la información cuando esta es segura.
- Pero la seguridad exige un esfuerzo y por tanto un coste.
- ¡ Hay que decidir que información es valiosa !

Ataques


Intercepción
Inferencia
Revelación
Intrusión
Confidencialidad
Falsa identidad
Obstrucción
Apropiación indebida
Corrupción
Integridad
Disponibilidad
Uso indebido
Incapacitación
Falsificación
Repudio

Ataques

Ejemplos

Revelación (*Exposure*) Alguien de dentro desvela información a alguien externo. Tambien puede no ser deliberada si una cadena de errores informáticos provoca que cierta información aparezca en la web de la empresa.

Intercepción (*Interception*) Lograr acceder al tráfico de red de una LAN.

Inferencia (*Inference*) Inferir información a partir de patrones de tráfico de red, aunque estén codificados.

Intrusión (*Intrusion*) Llegar a la información saltándose el sistema de control de acceso

Falsa identidad (*Masquarade*) Alguien no autorizado accede con la ID. de alguien autorizado.

Apropiación indebida (*Misappropiation*) En los ataques de denegación de servicio (Denial of Service, DoS) un programa se apropia del procesador de varios equipos conectados a red y saturan de tráfico el host contra el que van dirigidos.

Uso indebido (*Misuse*) Alguien no autorizado accede a un sistema y desactiva las medidas de seguridad.

Falsificación (*Falsification*) Cambiar datos validos por otros falsos en un fichero

Repudio (*Repudation*) El usuario niega el envío, recepción o posesión de ciertos datos.

Obstrucción (*Obstruction*) Impedir la comunicación entre dispositivos por ejemplo.

Corrupción (*Corruption*) Alguien modifica datos o el funcionamiento de algunos servicios.

Incapacitación (*Incapacitation*) Impedir el acceso al sistema desactivando el servicio o estropeando directamente el dispositivo físico.

Ejemplos

La siguiente tabla muestra como diferentes ataques dirigidos contra blancos relacionados con la informática afectan a la disponibilidad (availability), confidencialidad (confidentiality) e integridad (integrity)

	Availability	**Confidentiality**	**Integrity**
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Fuente: 'Computer Security'; W. Stallings y L. Brown

¿Cuáles son nuestras armas?

En este curso veremos los siguientes elementos en mayor o menor detalle.

Para defendernos

- Antivirus
- Criptografía

Para protegernos

- Firewalls
- Autenticación y control de acceso
- Detección de intrusos

Para anticiparnos

- Políticas de seguridad
- Auditorías
- Planes de contingencia

Resumen de conceptos y relaciones