Introducción a los fundamentos de la seguridad informática

PID_00245595

Erik de Luis Gargallo

Universitat Oberta de Catalunya

Índice

Introducción

En la actualidad no cabe duda de que las nuevas tecnologías de la información y las comunicaciones han provocado enormes cambios en nuestra sociedad, en lo que se ha considerado una nueva revolución social. Organismos públicos y privados, hogares, centros sanitarios, transportes, entes educativos y compañías de cualquier tamaño utilizan Internet ya no para presentar un hecho diferencial, sino por las enormes posibilidades de comunicación e información que ofrece. Como se solía decir hace unos años (algo que se ha convertido ya en premisa): si no está en Internet, simplemente es que no existe.

Así, la interconexión de las distintas redes conforma la gran red o Internet, también llamada red de redes, ya que no se trata de una red de ordenadores conectados entre sí, sino de una red de redes independientes. Esta nos permite comunicarnos directamente, compartiendo servicios e información. Se convierte en una fuente de recursos inagotable.

En Internet podemos encontrar varios servicios, aunque el más extendido es la World Wide Web o WWW. Nos permite la consulta remota de páginas web. Aun así, podemos encontrar otros muchos servicios, entre los que se puede destacar el de correo electrónico, la transmisión de archivos, las conversaciones en línea, la mensajería instantánea, etc.

Pero navegar por Internet no está exento de peligros. Los riesgos en el uso de las redes de comunicaciones son muy comunes, motivo por el cual la seguridad informática se ha convertido en uno de los principales temas que se deben tratar en la actualidad.

Se suele tener la idea, aunque cada vez más caduca, de que la seguridad informática es una materia que deben afrontar únicamente las empresas. Y se dice que estas son las principales afectadas por los ataques que se sufren en la Red. Nada más lejos de la realidad: hoy en día, nadie está exento de los peligros que presenta Internet, lo que nos obliga a cada uno de nosotros a concienciarnos de los riesgos existentes y a tomar las medidas adecuadas para reducir tanto como nos sea posible el peligro de sufrir un incidente de seguridad.

En esta introducción a los fundamentos de la seguridad informática, trataremos dos temas básicos relacionados con la seguridad de la información: estudiaremos la denominada «tríada CID» y analizaremos las diferencias entre la seguridad física y lógica en el campo de las tecnologías de la información y las comunicaciones.

Objetivos

Los materiales didácticos de este módulo proporcionan los contenidos y las herramientas imprescindibles para lograr los objetivos siguientes:

1. Identificar los objetivos generales de la seguridad informática: la confidencialidad, la integridad y la disponibilidad.

2. Entender los conceptos de seguridad física y seguridad lógica, sus diferencias y las distintas medidas que se pueden aplicar en cada caso.

1. La tríada: confidencialidad, integridad y disponibilidad

Vivimos permanentemente conectados a las redes públicas. Nuestros ordenadores, móviles, tabletas, etc., intercambian en muchos casos información que queda fuera de nuestro control, en caso de estar en nuestro hogar, o de nuestra empresa en el ámbito laboral. Además debemos tener presente que cada vez disponemos de más movilidad con nuestros datos y que, día a día, se incrementan los ataques lógicos provenientes del exterior contra nuestros dispositivos electrónicos.

Hoy en día, multitud de dispositivos permanecen conectados a Internet.

Este hecho se traduce en una complejidad cada vez mayor para controlar y proteger nuestra información. Además, nadie puede asegurar la total protección con una probabilidad del cien por cien; esta es imposible de alcanzar debido normalmente al equilibrio entre el nivel de seguridad deseado y la funcionalidad que se requiere.

Muchas son las ecuaciones posibles para conseguir la seguridad deseada. ¿Cedemos en funcionalidad y hacemos más seguro nuestro sistema? ¿Cedemos en seguridad y lo hacemos más funcional? ¿Buscamos un equilibrio que quizás nos deje en parte inseguros y que, además, puede que no sea del todo eficaz?

Lo que parece estar claro es que la seguridad es proporcional al coste de las medidas de protección. No cabe duda de que sin protección se facilita enormemente el acceso a cualquier tipo de intrusión a nuestro sistema.

El objetivo de la seguridad de la información es proteger la de una organización, empresa u hogar, así como los sistemas que la tratan. Para ello buscaremos garantizar las tres características que permitirán llevar a cabo dicho propósito: la confidencialidad, la integridad y la disponibilidad.

En una empresa es importante disponer de una política de seguridad efectiva que proteja sus datos, lo que al final se traduce en proteger el patrimonio que son sus recursos de información. Es importante entender que, de la misma manera que vemos como necesidad la protección de la propiedad corporativa, los edificios de oficinas y las personas, hemos de ver también necesaria la protección del principal activo: los datos.

Comúnmente, en informática se conocen estas características como la tríada CID, en referencia a las iniciales de los conceptos que la componen (confidencialidad, integridad y disponibilidad). A continuación, pasaremos a describir en qué consiste cada uno de ellos.

1.1. Confidencialidad

La **confidencialidad** consiste en que la información solo debe estar disponible para los agentes autorizados.

Así, solo podrán acceder a la información aquellos actores autorizados (dispositivos, sistemas, ficheros, etc.), teniendo presente que, aun disponiendo de acceso, estos actores no deben convertirla en disponible para otros. Por lo tanto, la confidencialidad asegura que únicamente las personas que deseemos que accedan a la información podrán hacerlo.

Las amenazas que afectan a la confidencialidad motivan el acceso de un actor no autorizado a la información. Se denomina **interceptación**. La interceptación consiste en el acceso a la información por parte de personas no autorizadas. Algunos ejemplos pueden ser el uso de privilegios no adquiridos o la escucha en línea de datos.

1.2. Integridad

La **integridad** consiste en que la información del sistema esté disponible tal y como fue almacenada por un agente autorizado.

En el caso de la integridad, la información solo puede ser modificada por actores autorizados y de una manera controlada. En concreto, la integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

Esta propiedad permite que la información se mantenga intacta de cualquier modificación que no sea autorizada, o bien que dicha información no sea manipulada o alterada por otras personas.

Así, la amenaza que motiva la alteración no autorizada de la información (por ejemplo, la destrucción, entendida como modificación que inutiliza la información) se denomina **modificación**. Esta supone el acceso no autorizado que cambia el entorno para su beneficio, lo que, por ejemplo, puede ser la modificación no autorizada de una base de datos.

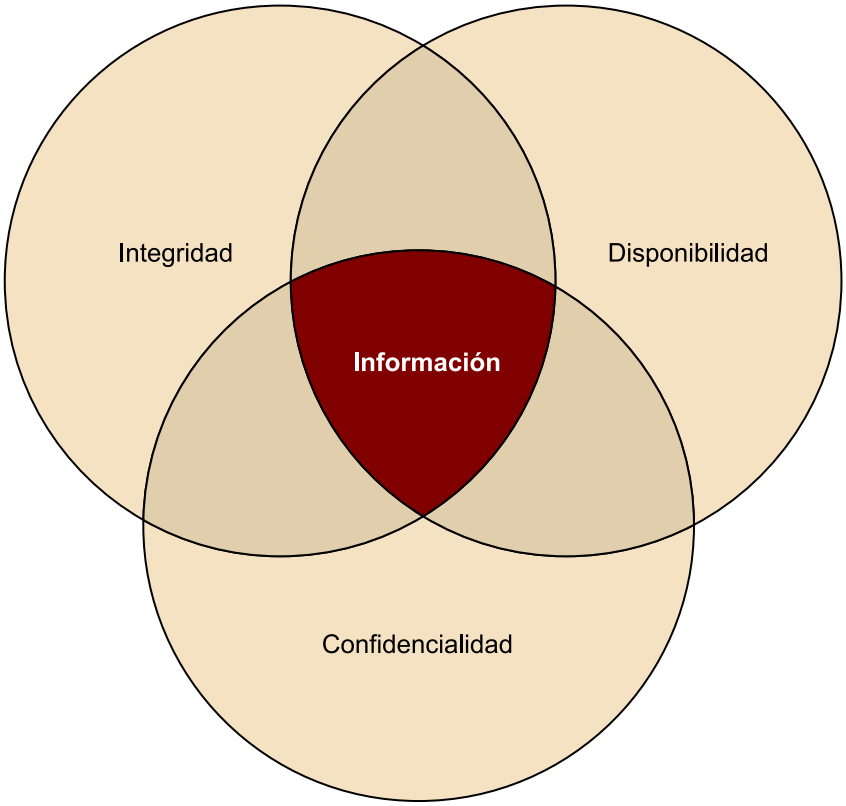
1.3. Disponibilidad

La **disponibilidad** consiste en garantizar que los recursos del sistema se encontrarán disponibles cuando sean necesarios, especialmente en caso de información crítica.

Esta característica se traduce en el hecho de que la información debe permanecer accesible para los actores autorizados, sea cual sea el momento y la manera que estos requieran.

De esta manera, las amenazas que motivan la pérdida, la inutilización o la indisponibilidad de la información derivan en una **interrupción**. Por medio de una interrupción se daña, se pierde o se inutiliza un punto del sistema. Algunos ejemplos pueden ser la destrucción del hardware, el borrado de programas o datos, o los fallos en el sistema operativo.

La tríada CID: confidencialidad, integridad y disponibilidad



1.4. Autenticidad, trazabilidad y no repudio

En los últimos años, están tomando fuerza otras propiedades aplicables a la seguridad de la información, como la autenticidad, la trazabilidad y el no repudio.

En este sentido, la **autenticidad** consiste en garantizar la legitimidad del origen de la transmisión; es decir, busca atestiguar que el emisor de un mensaje es quien dice ser. Esta propiedad guarda una relación directa con la integridad en el sentido de que ambas propiedades garantizan la integridad total del mensaje recibido.

Así, mientras la autenticidad garantiza el origen de un documento (es decir, que el documento o comunicación procede de la persona o entidad de quien dice provenir), la integridad garantiza la persistencia y completitud del contenido o documento (es decir, que dicho documento no ha sido modificado por ningún agente externo a la comunicación).

Por otro lado, la **trazabilidad** es la propiedad que certifica que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad. Dicho de otra manera, permite ponernos frente al conocimiento de operaciones, consultas o modificaciones de la información.

Finalmente, una de las propiedades que está cogiendo más empuje en los últimos años es el **no repudio**. Mediante esta propiedad, el emisor de un mensaje no puede negar haberlo enviado. En otras palabras, evita el rechazo interesado de los mensajes por parte de los comunicantes.

2. Seguridad física y seguridad lógica

Eugene Howard Spafford, profesor de ciencias informáticas en la Universidad de Purdue (Indiana, Estados Unidos) y experto asesor en seguridad de datos del Gobierno norteamericano, hizo la siguiente afirmación en marzo de 1989 en la revista *Scientific American*, en referencia a la seguridad de los sistemas informáticos:

> «The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts».
>
> Traducción: «El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de hormigón y sellado con plomo en una habitación con guardias armados... Incluso así tengo mis dudas».

Valorar la seguridad TIC como algo meramente lógico, es decir, como la simple protección de los datos, procesos y programas, no tiene cabida en la actualidad. Factores como la seguridad de las personas y las instalaciones, o el denominado cumplimiento normativo, toman tanta relevancia como los anteriores.

La seguridad física puede asociarse a la protección del sistema ante las amenazas como incendios, inundaciones, edificios, cables, control de accesos de personas, etc. Es decir, son aquellos mecanismos de prevención y detección destinados a proteger físicamente cualquier recurso. Por otro lado, la seguridad lógica se encarga de la protección de la información en su propio medio.

Es importante destacar que la seguridad informática no es un bien medible; resulta extremadamente difícil medir el grado de seguridad del que disponemos en un momento dado. En cambio, sí podríamos desarrollar diversas herramientas para cuantificar de alguna forma nuestra inseguridad informática.

A continuación veremos los dos grandes pilares en los que se divide la seguridad aplicable a los sistemas de información: la seguridad física y la seguridad lógica.

2.1. La seguridad física

Otorgar un nivel concreto de seguridad física suele basarse en la clasificación de la información, sea esta la que sea, según los requisitos de integridad, confidencialidad y disponibilidad requeridos.

Debemos, por lo tanto, valorar la información que hemos de proteger; entonces, en función de dicha valoración, suministrar las medidas de seguridad física correspondientes.

Difusión de un documento público

A título de ejemplo, imaginemos un documento público que deseamos que llegue a tantas personas como sea posible. No tendría mucho sentido aplicar sobre este una gran cantidad de medidas de seguridad, que lo único que nos generarían son barreras en el momento de acceder a él.

En grandes organizaciones, la seguridad física toma una especial relevancia, bien por la información que estas desean proteger, bien por la cantidad de personas que en ella se encuentran. En ocasiones se producen debilidades dentro de dichas organizaciones en medidas como el control de acceso a ubicaciones, la protección de la información en formato físico (documentos, soportes…) o la seguridad operativa en las instalaciones (como la política de mesas limpias, que consiste en guardar la documentación que se encuentre a la vista para evitar una fuga de información o el robo de documentos que puedan contener información confidencial…). Es necesario garantizar los aspectos relativos a la protección física de la información en todos los casos.

Los aspectos de seguridad física no solo hacen referencia a las personas, la información tangible o los edificios. El hecho de que solo personal autorizado disponga de acceso físico a los elementos principales de la red, como pueden ser los puntos de acceso y enrutadores, evitaría que un posible atacante pudiera utilizar el acceso a la red cableada y utilizarla para acceder a la red interna.

Por **seguridad física** entenderemos, por lo tanto, todas aquellas medidas cuyo objetivo es proteger físicamente un recurso del sistema, si se entiende como recurso desde un dispositivo de memoria tipo USB hasta el control de acceso de personal, pasando por la documentación de un proyecto clave para la empresa.

Así podemos concluir que nos enfrentamos a tres complejos grupos de posibles riesgos:

- **El acceso físico**. Se suele considerar el más importante. Si un atacante desea destruir un sistema informático perfectamente protegido por varias medidas de seguridad lógica, pero tiene libre acceso físico a él, toda medida, por muy cara que pueda ser, no servirá de nada. Imaginemos simplemente que un atacante pueda disponer de la cantidad de agua equivalente a un pequeño vaso, pero que es suficiente para destruir el mejor servidor del mercado.

- **Desastres naturales**. Aunque no se pueden considerar ataques voluntarios, sino más bien fruto del azar, está claro que sufrir una inundación, un terremoto o un incendio será suficiente para destruir el sistema que se debe proteger. Por tal motivo, los sistemas informáticos bien protegidos disponen de planes de contingencia para casos como los descritos anteriormente, además de políticas de seguridad que describen protocolos de realización de copias de seguridad de los sistemas en los que dicha copia

es llevada a lugares distintos del original, donde la posibilidad de coincidir el mismo desastre a la vez es casi imposible de prever. Cabe recordar y tener siempre presente que el hardware, aunque económicamente sea un problema, se puede reemplazar, pero los datos no.

- **Alteraciones en el entorno**. Pensemos simplemente en un aumento inesperado de la temperatura, pero suficiente para sobrecalentar el sistema. O en una subida de la tensión eléctrica que no se trata apropiadamente. Ambos son una muestra de una alteración que sufre el entorno que puede provocar graves consecuencias en el sistema de información.

2.2. La seguridad lógica

En lo referente a la **seguridad lógica**, esta guarda relación con la protección del software de los equipos informáticos; es decir, con la salvaguardia de las aplicaciones y los datos de usuario contra robos, pérdidas, entradas de virus informáticos, modificaciones no autorizadas, ataques desde la propia Internet, etc.

La seguridad lógica guarda relación directa con el conocido *malware* o software malicioso, cuya función es dañar el sistema o causar un mal funcionamiento en este. Aunque lo veremos más adelante, en otro módulo, es importante destacar la denominación «software malicioso» o *malware*, por encima de la denominación incorrecta de «virus informático», ya que este último no deja de ser un tipo de *malware*.

La evolución imparable del software malicioso ha acompañado, como no puede ser de otra manera, la evolución a la par de la seguridad lógica. Atrás queda el *malware* diseñado por uno o un pequeño grupo de piratas informáticos con la simple voluntad de reivindicar un hecho o simplemente molestar al usuario común.

En la actualidad, son las grandes mafias las que han encontrado en este tipo de software un filón en su lucro económico, y parece ser que la cosa no va a detenerse fácilmente; más bien al contrario, el aumento del *malware* sigue un crecimiento exponencial desde sus inicios.

***Malware* en 2015**

Tal y como informa Panda, compañía internacional especializada en el desarrollo de soluciones de seguridad, en su revista *Pandalabs' Anual Report 2015*, solo en el año 2015 se descubrieron más de ochenta y cuatro millones de nuevas muestras de *malware*, con un total de 230.000 muestras al día, lo que, a su entender, indica que el 32,13 % de los ordenadores del mundo están infectados.

Resumen

En este módulo hemos visto los fundamentos de la seguridad informática, separando el concepto de seguridad en física y lógica, y analizando la denominada «tríada de seguridad TIC».

La tríada CID (confidencialidad, integridad y disponibilidad) se basa en los tres principios rectores que, una vez garantizados, nos permitirán disponer de una adecuada seguridad en nuestro sistema informático, ya sea doméstica o empresarialmente.

La seguridad física toma una especial relevancia como base de cualquier sistema de información. Se protege ya sea de accesos ilegítimos o de personal no autorizado, o de amenazas físicas como un incendio o una inundación.

Hemos hecho hincapié en la seguridad lógica, ya que es esta la que, sobre la base de la seguridad física, permitirá garantizar la protección de la información contenida en nuestros sistemas, dada la constante evolución del *malware* o software malicioso.

En otros módulos se analizan en profundidad los distintos tipos de *malware*, así como los peligros a los que nos enfrentamos en la Red, y las posibles medidas para evitarlos o mitigar su impacto; todo ello enfocado básicamente a la protección de los menores y adolescentes en su interacción con las nuevas tecnologías.

Actividades

1. Como hemos visto en este módulo, la seguridad física de un sistema informático se basa en la aplicación de barreras físicas y procedimientos de control al hardware frente a amenazas físicas. Si en una empresa A se comienzan a planificar estrategias de acceso a las dependencias como el blindaje contra robos, un sistema de protección contra incendios o un control de acceso a los recintos donde se sitúan los ordenadores, ¿eso es seguridad física o lógica? ¿Por qué?

2. Por otro lado, la seguridad lógica de un sistema informático consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en él. Así pues, si en una empresa B se comienzan a planificar estrategias como el uso correcto de un procedimiento, la comprobación de la veracidad de la información transmitida o la creación de usuarios restringidos, ¿eso es seguridad física o lógica? ¿Por qué?

Bibliografía

Aguilera López, P. *Seguridad informática*. Editex.

Ramió Aguirre, J. (2006). *Seguridad informática y criptografía*. Madrid: Universidad Politécnica de Madrid.

Romero, L. A. *Seguridad informática. Conceptos generales*. Salamanca: Universidad de Salamanca.

Enlaces de Internet

http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica

http://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx