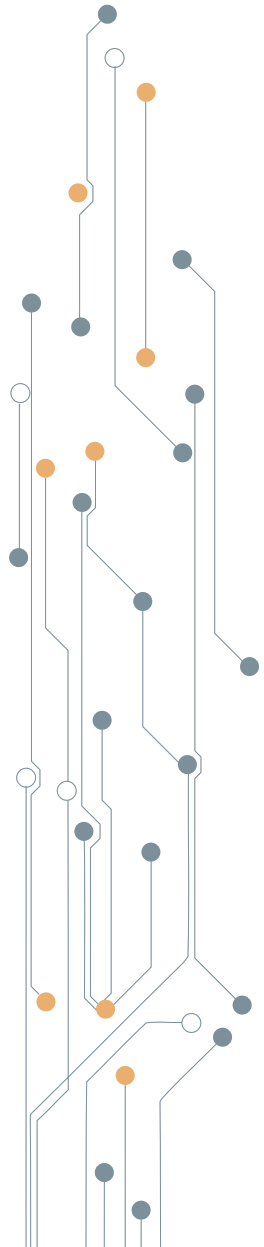
Introducción a la Seguridad y a la criptografía

Telefónica EDUCACIÓN DIGITAL

Índice



1. Seguridad Informática, seguridad de la información y criptografía

Seguridad informática y seguridad de la información

Es común confundir el término seguridad informática con el término seguridad de la información. Aunque pueda parecernos a simple vista que ambos significan lo mismo, en el fondo lo son, y cada una tiene un ámbito de aplicación bien delimitado.

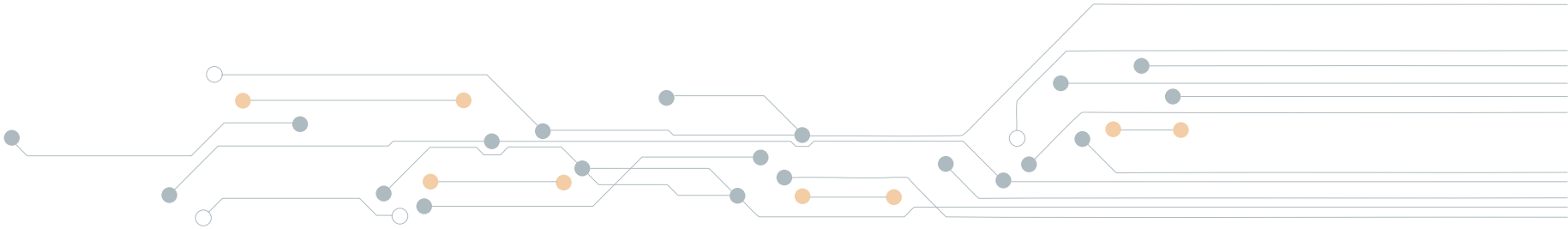
La información es el activo más importante que debe protegerse en una empresa u organización. Como veremos más adelante en este capítulo, dicha información presentará diversas vulnerabilidades y estará expuesta a un conjunto de amenazas durante todo su ciclo de vida. A saber, dicho ciclo comienza cuando ésta se genera, continúa cuando ésta se gestiona y, si corresponde, se transmite, sigue cuando ésta se almacena y, finalmente, concluye cuando ésta se destruye, si fuera el caso o bien necesidad. Por lo tanto, en cada una de estas etapas del ciclo de vida de la información, deberemos aplicar medidas de seguridad para su protección.

La seguridad informática se centrará en aquellos aspectos de protección que inciden directamente con los medios informáticos en los que la información cumple su ciclo de vida, siempre desde un punto de vista tecnológico de la informática y de la telemática. Son ejemplos de este entorno tecnológico de la seguridad los siguientes:

a) El uso de la criptografía para la protección y la seguridad de los datos.

b) Las herramientas que permiten asegurar y fortificar las redes.

c) Los métodos que añaden seguridad a las aplicaciones informáticas, programas y bases de datos.



En cambio, cuando nos referimos a seguridad de la información, centramos nuestra atención en los aspectos sistémicos de la gestión de esa seguridad, como por ejemplo las políticas y planes de seguridad que toda empresa u organización debe plantearse, la orientación de esta seguridad hacia la continuidad del negocio y sus planes estratégicos, así como la adecuación del tratamiento de esa información al entorno legal y a las normativas nacionales e internacionales, con las cuales habrá que dar un debido cumplimiento. En este caso, son ejemplos de un entorno empresarial y estratégico de la seguridad, los siguientes:

a) La gestión del riesgo y de la seguridad de la información.

b) Las políticas de seguridad que permitan el buen gobierno.

c) La adecuación de la seguridad a las normativas internacionales y a la legislación vigente.

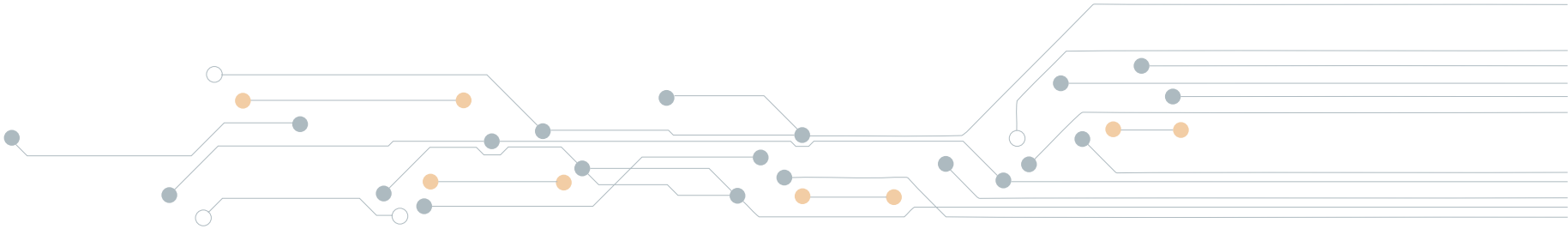
Resulta claro que el término más amplio y genérico entre los dos es el de seguridad de la información, en tanto la gestión integral de la información también abarca su protección en escenarios tecnológicos. Por ello, hoy en día resulta más común hablar de seguridad de la información que de seguridad informática, si bien ambas se complementan.

Criptografía

El ser humano ha utilizado desde tiempos inmemoriales artilugios varios para ocultar información confidencial a terceros no autorizados y proteger así sus secretos. Se tienen datos desde el siglo V antes de Cristo… pero, ¿qué es la criptografía?

Siguiendo la definición de la Real Academia Española RAE, criptografía es el "arte de escribir con clave secreta o de un modo enigmático".

En una primera instancia podríamos aceptar esta definición como válida porque, entre otras cosas, es la idea inicial que se nos viene a la cabeza por el uso que se ha hecho de ella durante la historia de la humanidad, incluso en el ámbito literario si tenemos en consideración la primera novela en la que se trata esta temática, El escarabajo de Oro de Edgar Allan Poe publicada en el año 1843, y muchas otras novelas incluso de este siglo XXI.



Pero si nos detenemos a pensar en la adecuación de dicha definición a lo que en realidad ocurre hoy en día cuando usamos la criptografía (por ejemplo, comunicaciones seguras en Internet), esa definición de la RAE no acierta en ninguna de sus afirmaciones. A saber:

1) La criptografía ya no es un arte, al contar desde mediados del siglo XX con diversos estudios matemáticos que la sustentan, iniciados por los trabajos del matemático Claude Shannon en 1948 y 1949 sobre teoría de la información y sistemas con secreto.

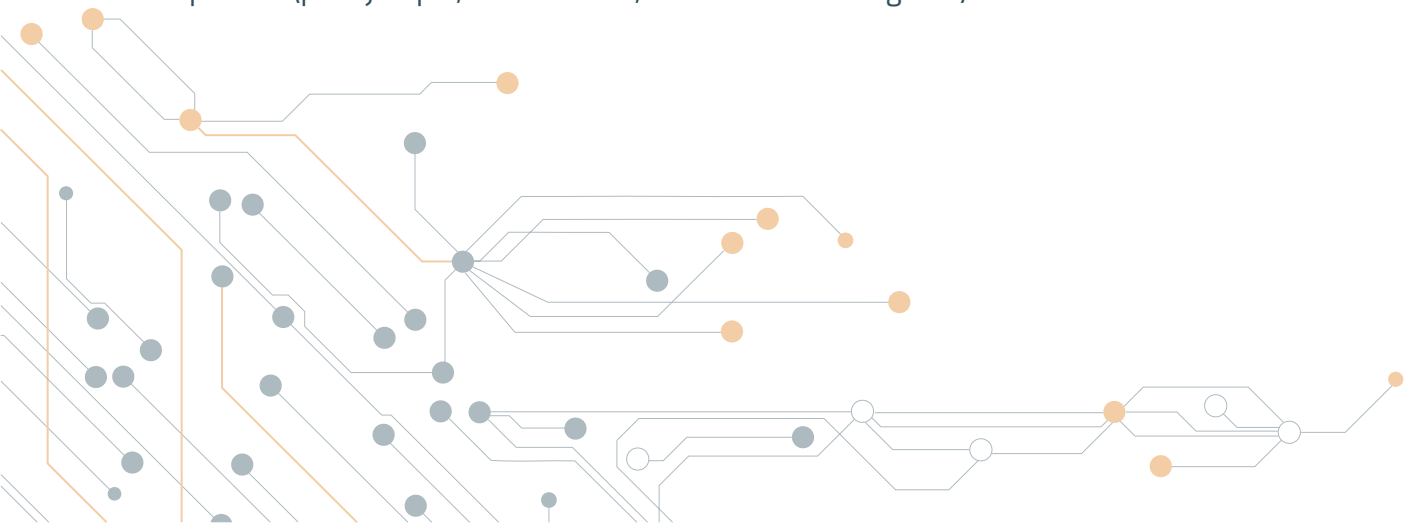
2) En realidad, ya no sólo se escriben mensajes; estos mensajes se generan con diversas herramientas y pueden ser multimedia (texto, audio, vídeo) y, además, el documento a cifrar puede ser inteligible o no para el ser humano (por ejemplo, un ejecutable, una dll, etc.).

3) Por lo general hoy en día no se usa una sola clave secreta en la cifra. Lo normal será usar dos claves (una de sesión y un vector de inicialización) y, en ciertos sistemas, usar una clave pública y otra privada (por ejemplo, banca online, servidores web seguros).

4) En cuanto a lo enigmático del criptograma, esto sólo es válido cuando el alfabeto de cifrado es diferente al alfabeto del texto en claro, especialmente si se usan signos extraños en el primero, como sucedía por ejemplo en el libro de Allan Poe citado. Hoy se cifran bits y bytes, y el resultado de la cifra dista mucho de ser algo enigmático. Da lo mismo leer la cadena de 8 bits 01100001, que corresponde a la letra a del código ASCII, que la cadena de 8 bits 11100001, que corresponde a la letra á del código ASCII. No hay nada de enigmático en esas dos cadenas de bits.

Una definición más actual y científica de la criptografía sería:

"*Conjunto de herramientas matemáticas, técnicas y algoritmos que, con el uso de una o más claves, permiten cifrar la información y, por tanto, protegerla y dotarle al menos de confidencialidad e integridad".*



2. Amenazas y vulnerabilidades

Amenazas

Las amenazas son una posible causa de un incidente no deseado, el cual puede ocasionar daño a un sistema o una organización. De una manera más técnica se define amenaza como aquella situación de daño cuyo riesgo de producirse es significativo. Destacan aquí estos tres términos:

a) Incidente. Cualquier evento inesperado y no deseado que puede comprometer las operaciones de una empresa u organización.

b) Daño. El perjuicio, económico o no, que se produce cuando una amenaza ocurre.

c) Riesgo. Es el producto entre la magnitud de un daño (d), y la probabilidad de que éste tenga lugar (p): R = d x p

Ante un incidente de seguridad en la información o los datos con los que trabajamos, aunque los daños no fuesen directamente económicos, lo cierto es que el coste asociado a la recuperación de los mismos, o el tiempo y esfuerzo necesarios para volver al estado anterior al incidente, la situación del "antes de", pueden llegar a ser muy altos y, en ciertos casos, tan extremos que pueden significar la desaparición de la organización.

Observa que una situación con un elevado nivel de daño, pero muy poco probable, puede suponer menor riesgo que una situación con un nivel de daño moderado, pero mucho más probable. Siempre y cuando hagamos una buena estimación de los daños y las probabilidades de que éstos se produzcan, obtendremos unos valores de riesgo útiles. Pero de todo ello se ocuparán otras especialidades de la seguridad de la información como, por ejemplo, el análisis y la gestión de riesgos.

La figura 1.1 resume de forma esquemática cómo se clasifican las amenazas, por la forma en que se producen (naturales, involuntarias e intencionales), y según la forma en que operan (activas y pasivas). Se trata de una adaptación simplificada del Anexo C: Ejemplos de amenazas típicas, de la norma ISO/IEC 27005 de Gestión de riesgos de la Seguridad la Información.

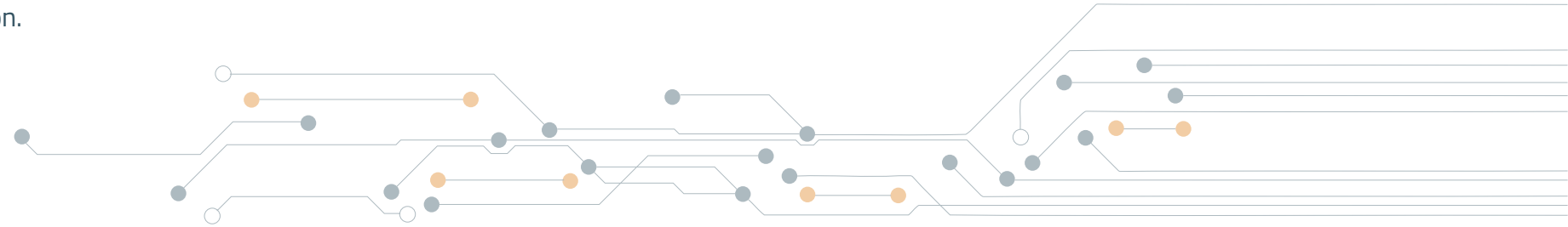


Figura 1.1. Resumen esquemático de clasificación de las amenazas.

Vulnerabilidades

¿Son lo mismo amenazas que vulnerabilidades? No.

Las vulnerabilidades son debilidades de un activo o grupo de activos que pueden ser explotadas por una o más amenazas cuando ocurre un incidente.

Por lo tanto, el riesgo será la probabilidad de que las amenazas exploten estos puntos débiles, causando pérdidas o daños a los activos e impactos al negocio. Para gestionar y si, fuera posible, eliminar o al menos minimizar este riesgo, lo primero que deberá hacerse es identificarlos, pero ello no corresponde al temario y ni a los objetivos de este curso. No obstante, sí deben considerarse aquí qué tipos de vulnerabilidades pueden afectar a la información, así como sus amenazas, en tanto en un buen número de escenarios la solución pasará por el uso de herramientas de criptografía.

Figura 1.2. Vulnerabilidades que puede presentar la información.

En la siguiente tabla se muestran algunas vulnerabilidades típicas en sistemas de información.

FÍSICAS	Instalaciones inadecuadas en el espacio de trabajo, disposición desorganizada de cables de energía y de red, ausencia de identificación de personas y de locales, etc.
NATURALES	Locales próximos a ríos propensos a inundaciones, ambientes sin protección contra incendios, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes, etc.
HARDWARE	Conservación inadecuada de los equipos, la falta de una configuración de respaldo o equipos de contingencia, etc.
SOFTWARE	La configuración e instalación inadecuada, ausencia de actualización, etc.
ALMACENAMIENTO	Plazo de validez y caducidad, defecto de fabricación, lugar de almacenamiento en locales insalubres o con alto nivel de humedad, magnetismo, moho, etc.
COMUNICACIÓN	• La ausencia de sistemas de cifrado en las comunicaciones que pudieran permitir que personas ajenas a la organización obtengan información privilegiada. • La mala elección de sistemas de comunicación para el envío de mensajes de alta prioridad de la empresa, podría provocar que no alcanzaran el destino esperado o bien se interceptara el mensaje en su tránsito.
HUMANAS	• La falta de capacitación específica para la ejecución de las actividades inherentes a las funciones de cada uno. • La falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones, etc. • Contraseñas débiles o compartidas. • Falta de uso de criptografía en la comunicación. • Compartir identificadores tales como nombre de usuario o credencial de acceso, etc. • Desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por los miembros internos de la empresa.

Tabla 1.1. Vulnerabilidades características asociadas a la información.

Para terminar, es menester indicar que la información será vulnerable y estará amenazada por acciones de interrupción, de interceptación, de modificación y de fabricación.

Ante una amenaza de **interrupción** de la información, ésta se dañará, se perderá o bien dejará de funcionar un punto del sistema. Su detección será inmediata. Como ejemplos de interrupción tenemos la destrucción del hardware, borrado de programas, borrados de datos y fallos en el sistema operativo.

Ante una amenaza de **interceptación** de la información, se producirá un acceso a la información por parte de personas no autorizadas o bien el uso de privilegios no adquiridos. Su detección puede ser difícil ya que a veces no deja huellas. Como ejemplos de interceptación tenemos las copias ilícitas de programas y la escucha en línea de datos.

Ante una amenaza de **modificación** de la información, se producirá un acceso no autorizado que cambiará el entorno para su beneficio. Su detección podría difícil si no se cuenta con herramientas de comprobación de integridad. Como ejemplos de modificación tenemos modificación de bases de datos y cambios en los elementos del hardware.

Por último, ante una amenaza de **fabricación,** en el sistema se crearán de forma no autorizada nuevos objetos. Su detección suele ser difícil y es característico en delitos de falsificación.

Como ejemplos de fabricación tenemos añadir transacciones en red y añadir registros en una base de datos.

Estas amenazas se muestran esquemáticamente en la figura 1.3.

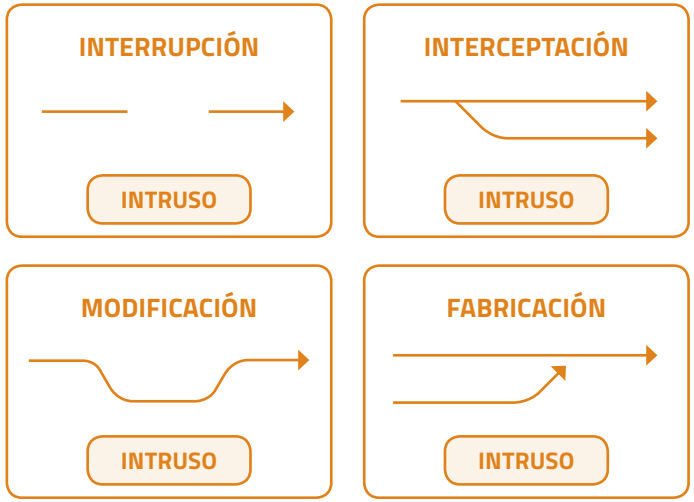


Figura 1.3. Amenazas en la información.

Estas amenazas pueden afectar a la confidencialidad, a la integridad y a la disponibilidad de la información.

3. Confidencialidad, integridad y disponibilidad

Seguiremos las definiciones de la Organización Internacional de Estandarización (ISO/IEC) en la norma ISO-27000.

Confidencialidad

"Confidencialidad es la propiedad por la que la información no se pone a disposición o se revela a individuos entidades o procesos no autorizados".

Se persigue asegurar que sólo las personas autorizadas podrán acceder a la información. La información tendrá confidencialidad si la misma debe mantenerse en secreto por alguna razón. Para lograr esta propiedad de la información segura, usaremos técnicas de criptografía.

Integridad

"*Integridad es la propiedad de salvaguardar la exactitud y completitud de los activos.".*

Se persigue garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas, preservando la exactitud y completitud de la misma y de los métodos utilizados para su procesamiento. Es común asociar el término de integridad de la información de forma genérica a la integridad de los datos, así como a la autenticación de usuarios y/o procesos.

En ambos casos también usaremos herramientas de criptografía para lograr esta propiedad de la información segura.

Disponibilidad

"Disponibilidad es la propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieran".

Se persigue asegurar que los usuarios autorizados puedan tener acceso a la información y a los medios asociados, cada vez que lo requieran. Para lograr esta propiedad de la información segura, ya no podremos usar criptografía sino otras técnicas de gestión de redes y de sistemas.

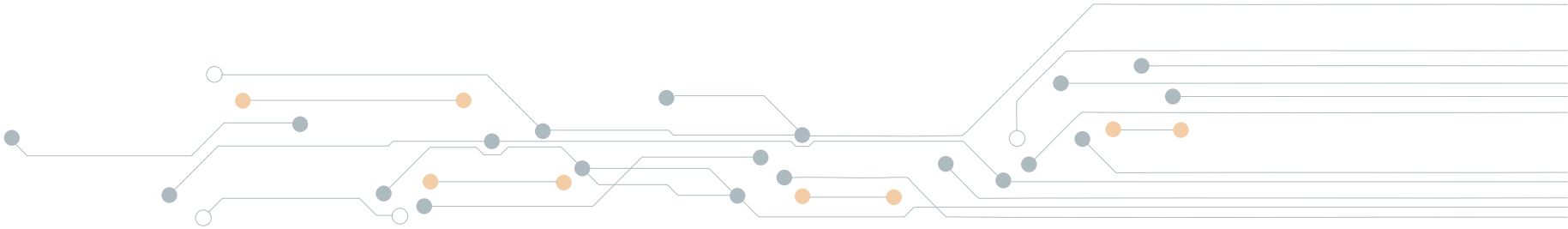
Podemos concluir entonces que la criptografía nos servirá para cumplir con dos de las tres propiedades de una información segura, la confidencialidad y la integridad. Más aún, será la única herramienta para lograr confidencialidad, integridad o bien las dos juntas.

Es común añadir a esta tríada el No repudio de emisor y de receptor. Esto tiene que ver con un intercambio de información entre un cliente y un servidor, típico en plataformas seguras de Internet, y previene que alguna de las partes involucradas en esa transacción digital niegue haber enviado o recibido un mensaje, algo que está directamente asociado a la necesaria trazabilidad de la información.

El no repudio, la autenticación y la trazabilidad se conocen como servicios de seguridad, que complementan a los tres principios básicos.

4. Elementos básicos de la criptografía

- **Texto en claro.** El principio definiremos texto en claro como cualquier información que resulta legible y comprensible por sí misma. Se le asigna normalmente la letra M de mensaje, por ejemplo, M = En un lugar de La Mancha, o M = EN UN LUGAR DE LA MANCHA. No obstante, el texto en claro podría ser cualquier documento, incluso no legible.
- **Criptograma.** Texto o conjunto de bits que resultan de la cifra de cualquier información, que no es legible ni comprensible, salvo para el destinatario legítimo de la misma cuando lo descifre. Se le asigna normalmente la letra C de criptograma. Por ejemplo, C = HPXPÑ XJDUG HÑDOD PFKD o bien C =97431381fc46703c17d2df589af508a800d462c0e6b298525b487ee4d184055d, resultados de cifrar M = EN UN LUGAR DE LA MANCHA en el primer caso con el algoritmo del César y, en el segundo caso, con el algoritmo AES y una clave de 128 unos, estando ahora la salida en formato hexadecimal.
- **Espacio de claves.** Conjunto de todas las claves posibles y válidas que pueden usarse en un algoritmo de cifra.
- **Cifrar y descifrar.** Procesos que permiten transformar un texto en claro en un criptograma y viceversa. Como es lógico, debería poder descifrar el criptograma sólo quien tenga la clave secreta y sea el destinatario de ese secreto.
- **Criptoanálisis.** Tiene un objetivo opuesto a la criptografía; por tanto, se ocupa de conseguir capturar el significado de mensajes construidos mediante criptografía sin tener autorización para ello.
- **Esteganografía y Estegoanálisis.** La esteganografía se ocupa de ocultar mensajes con información privada por un canal inseguro, de forma que el mensaje no sea ni siquiera percibido. Normalmente el mensaje es escondido dentro de datos con formatos de video, imágenes, audio o mensajes de texto. El estegoanálisis se ocupa de detectar mensajes ocultos con técnicas esteganográficas.
- **Criptología.** Ciencia que agrupa la criptografía, el criptoanálisis, la esteganografía y el estegoanálisis.



En la figura 1.4 se muestra el esquema de un sistema de cifra. Si la clave usada en el extremo emisor y el extremo receptor son la misma, se hablará de sistemas de cifra simétrica. Por el contrario, si las claves del extremo emisor y del extremo receptor son diferentes pero inversas entre sí (algo que se verá en próximos capítulos), se hablará de sistemas de cifra asimétrica.

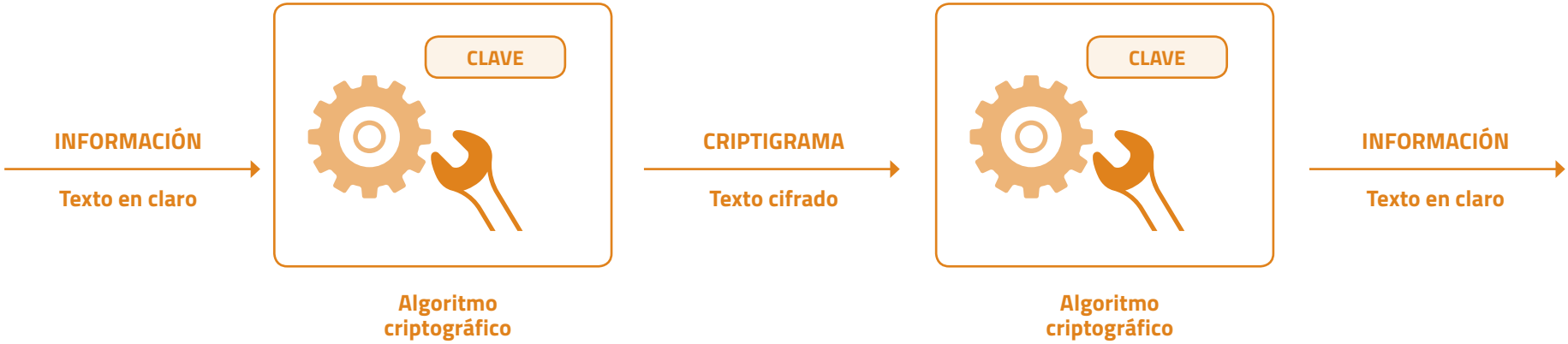


Figura 1.4. Esquema de un sistema de cifra.

Cifrar y codificar

Aunque sea un error bastante común, no hay que confundir cifrar con codificar.

Codificar, es decir asignar un código a algo, es una acción estática, en el sentido de que los valores que se asignan con ese código a sus elementos son siempre los mismos, nunca cambian. Por ejemplo, la letra A en código ASCII es el valor decimal 65 o en binario 01000001, y así será siempre, en cualquier país del mundo y en cualquier fecha. Lo mismo podemos decir de otros códigos como el Morse, Baudot, Base64, código de barras, código QR, etc.

Por el contrario, cifrar es una acción dinámica, en el sentido de que, dependiendo de una clave, un mismo mensaje podrá convertirse en diferentes criptogramas. Una clave que lógicamente cambiará con el tiempo y que como veremos se recomienda sea de un solo uso.

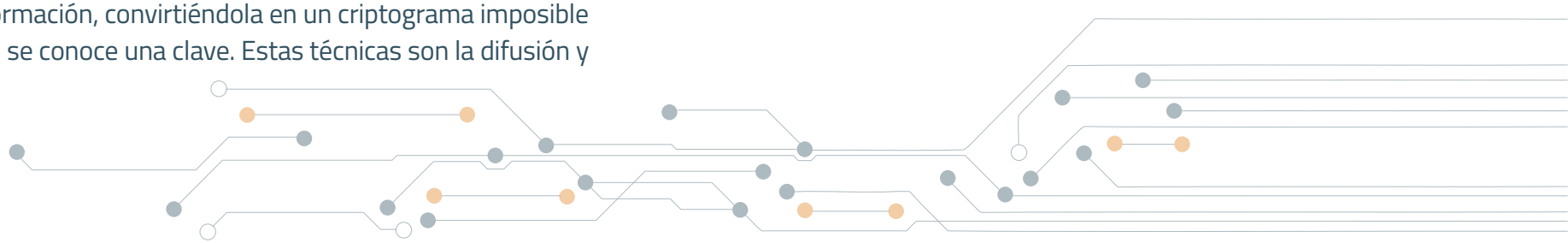
Difusión y confusión

Los algoritmos de cifra, tanto clásica como moderna, usan dos principios básicos para enmascarar el texto en claro y proteger el secreto de la información, convirtiéndola en un criptograma imposible de descifrar si no se conoce una clave. Estas técnicas son la difusión y la confusión.

Dichos principios, que se usaban ya en los orígenes de la criptografía, son refrendados en 1949 por Claude Shannon en el artículo Communication Theory of Secrecy Systems.

Como su nombre lo indica, la difusión pretende difundir las características del texto en claro en todo el criptograma, ocultando de esta forma la relación que existe entre el texto en claro y el texto cifrado. Para lograr esta difusión, al texto en claro se le aplicarán diversas operaciones de transposición o permutación de las letras, caracteres, bytes o bloques determinados, de manera que los elementos del mensaje aparecerán ahora totalmente dispersos o desordenados en el criptograma. Los sistemas que basan su cifra en este tipo operaciones se conocen como algoritmos de cifra por transposición.

Por su parte, la confusión pretende confundir al atacante, de manera que no le sea sencillo establecer una relación entre el criptograma y la clave de cifrado. Para lograr esta confusión, ahora aplicaremos al texto en claro operaciones de sustitución de un carácter, bloques determinados de texto o bien uno o más bytes, por otros elementos similares, dando origen de esta manera los algoritmos de cifrado por sustitución.



Sustituir uno o más elementos del texto en claro por uno o más elementos en el texto cifrado, como es lógico los elementos del criptograma no serán los mismos que los del mensaje original. Sin embargo, tal y como estudió Shannon a mediados del siglo pasado, todos los lenguajes tienen unas particularidades que hacen que éstos sean muy redundantes. El lenguaje castellano presenta una gran redundancia. Esto significa que en algunos criptosistemas (básicamente los de tipo clásico orientados al cifrado de caracteres) podremos aplicar esta característica para romper textos cifrados, porque dicha redundancia se manifestará también en el criptograma.

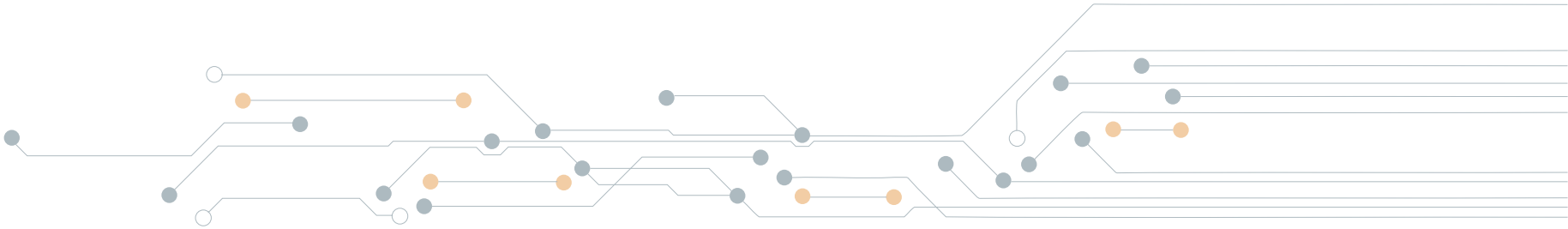
Un texto cifrado debe tener una apariencia totalmente aleatoria y deberá eliminarse cualquier relación estadística entre el mensaje original y su texto cifrado. Esto se logra con la permutación y la sustitución; sin embargo, ambas por sí solas no son suficientes para cifrar un texto de manera segura. La combinación de la sustitución y la transposición dispersa completamente la estructura estadística del mensaje sobre la totalidad del texto cifrado, dando así fortaleza a la cifra y al secreto. A estos sistemas se les conoce como cifradores de producto.

Fortaleza de los algoritmos: ataques

Algunos de los ataques más comunes en la criptografía clásica son:

Ataques por fuerza bruta. El criptoanalista descifra el criptograma probando una a una todas las claves posibles del espacio de clave de esa cifra, hasta que obtiene un mensaje con sentido. La mayoría de los sistemas de cifra moderna sólo pueden atacarse mediante esta técnica poco elegante. Observa que, si la clave del algoritmo es binaria y tiene n bits, en media deberían probarse 2n-1 claves para que prospere un ataque por fuerza bruta, puesto que dicha clave será aleatoria.

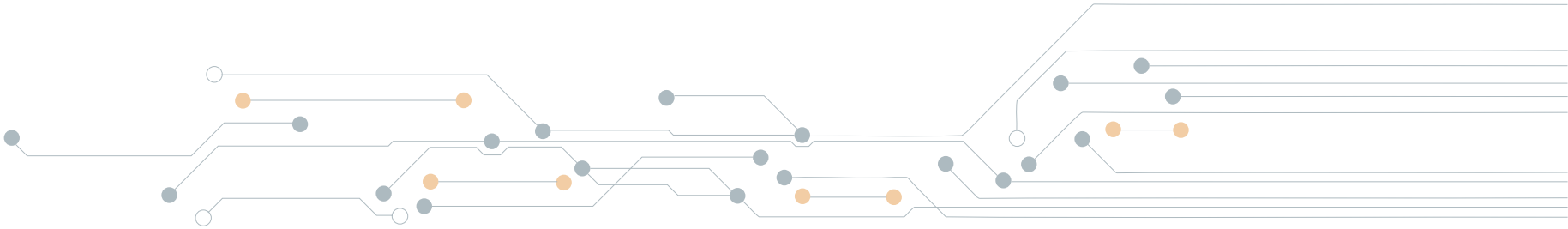
Ataques sólo con textos cifrados. El criptoanalista dispone de un texto cifrado y quiere obtener el texto en claro o la clave. Se pueden usar métodos de diccionario, probando únicamente con un subconjunto de las claves posibles; por ejemplo, si las claves son palabras, o mediante un análisis de frecuencia en el caso de los sistemas de cifra clásica. En este último caso, normalmente es importante poder disponer de suficiente texto cifrado para poder aplicar estadísticas del lenguaje.



Ataques con texto en claro conocido. El criptoanalista dispone de un texto en claro y su correspondiente texto cifrado, lo que permite reducir el espacio de búsqueda de claves u obtener estadísticas que pueden usarse para hacer deducciones en otros textos cifrados. Todos los algoritmos que se precien de seguros deben soportar un ataque con texto en claro conocido. Es decir, si se conoce cómo funciona el algoritmo, se conoce el criptograma y se conoce incluso el texto en claro, será de igual manera muy difícil encontrar la clave usada en la misma, salvo aplicando fuerza bruta.

Así, hablaremos de sistemas incondicionalmente seguros y de sistemas computacionalmente seguros. Los sistemas incondicionalmente seguros son aquellos en los que, aun disponiendo de recursos, de tiempo y de gran una cantidad de texto cifrado si fuera necesario, no es posible romper el algoritmo, esto es, descubrir la clave de cifra. Y los sistemas computacionalmente seguros son aquellos en los que sólo con suficiente poder de cálculo y tiempo para ello, el sistema podría ser roto, pero a un coste tan elevado y con un tiempo tan alto, que en la práctica resulta imposible abordar el ataque. Es normal hablar de miles de millones de años como media de tiempo para poder romper un algoritmo moderno mediante fuerza bruta.

La criptografía actual se caracteriza por usar algoritmos cuya fortaleza se basa en que el sistema es computacionalmente seguro. Para ello se usan claves de centenas de bits para un tipo de cifradores, los llamados simétricos, y claves de miles de bits para otros cifradores llamados asimétricos.

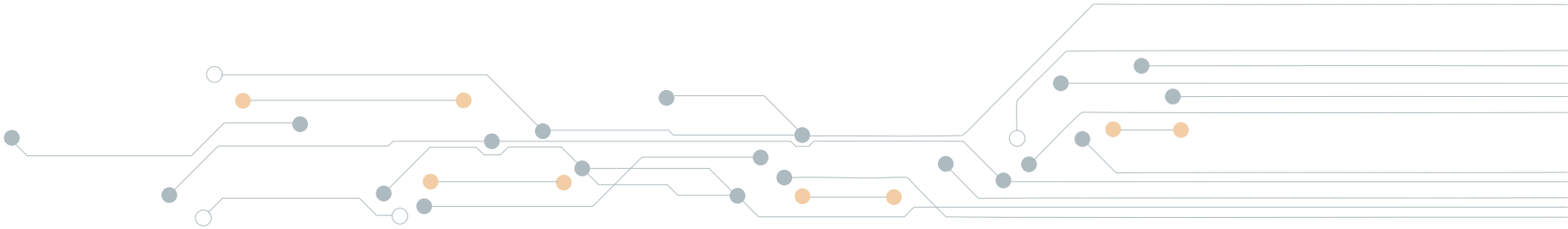


5. Los principios de Kerckhoffs

Auguste Kerckhoofs establece en 1883 los siguientes principios para la criptografía:

1. **El sistema debe ser en la práctica indescifrable, en caso de que no lo sea matemáticamente.**
2. **El sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo.**
3. **La clave del sistema debe ser fácil de memorizar y comunicar a otros, sin necesidad de tener que escribirla; será cambiable y modificable por los interlocutores válidos.**
4. **El sistema debe poder aplicarse a la correspondencia telegráfica.**
5. **El sistema debe ser portable y su uso no deberá requerir la intervención de varias personas.**
6. **El sistema debe ser fácil de usar, no requerirá conocimientos especiales ni tendrá una larga serie de reglas.**

De ellos, el más importante es el segundo, totalmente actual en nuestros días. Hoy en día hemos simplificado su enunciado diciendo simplemente que la seguridad del sistema debe recaer solamente en la clave. Por lo tanto, no es válida la opción de lograr seguridad por oscurantismo, es decir ocultando el algoritmo de cifra. El código fuente del algoritmo de cifra debe ser de dominio público.



Telefónica EDUCACIÓN DIGITAL