Fundamentos de seguridad informática

PID_00269891

Amadeu Albós Raya

Tiempo mínimo de dedicación recomendado: 5 horas

Universitat Oberta de Catalunya

Amadeu Albós Raya

Ingeniero informático por la Universitat Oberta de Catalunya.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Helena Rifà (2019)

Primera edición: septiembre 2019

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

La tecnología se ha vuelto ubicua con el paso del tiempo, no solo porque los servicios que ofrece son cada vez más numerosos y accesibles desde casi cualquier lugar, sino porque la sociedad la ha aceptado de pleno y la explota cada día con más objetivos y en situaciones diferentes.

Las tecnologías de la información y la comunicación facilitan que la información pueda fluir continuamente en todas direcciones, sin muchas complicaciones técnicas o fronteras que sean perceptibles. Pero la información es un activo valioso que debe protegerse, ya que con esta omnipresencia está expuesta continuamente a todo tipo de riesgos. A veces habrá que asegurar que la información no haya sido modificada sin autorización, otras veces que solo puedan acceder a ella determinados usuarios y otras, garantizar que se pueda acceder a ella en cualquier circunstancia. Los sistemas informáticos son el medio para procesar la información y extraer el máximo provecho de dicha información, pero también pueden materializar todos los riesgos con aquellas tecnologías que no disponen de los mecanismos de seguridad adecuados.

La complejidad de los sistemas informáticos y la evolución constante de las amenazas obligan a que la seguridad no sea ni estática ni esté centrada en un solo elemento, sino que esté basada en un conjunto coherente de medidas dinámicas que pretenden reducir (y si puede ser, eliminar completamente) el impacto que puedan tener esas amenazas.

A lo largo de las próximas secciones veremos cómo es un sistema informático y cuáles son las medidas habituales para garantizar, por un lado, la seguridad física y perimetral, y por otro, la seguridad de los servicios y las comunicaciones.

Objetivos

1. Conocer el sistema informático, sus componentes y su funcionamiento.

2. Identificar los riesgos de seguridad de la información que procesa el sistema informático.

3. Comprender las medidas de seguridad física y perimetral de un sistema informático.

4. Comprender las medidas de seguridad de los servicios y las comunicaciones de un sistema informático.

5. Entender la cohesión y complementariedad de las medidas de seguridad informática.

6. Reflexionar sobre la evolución de los riesgos y la dinámica de la seguridad informática.

1. El sistema informático

La tecnología es esencial para automatizar el proceso de la información. Todos los elementos que intervienen en el sistema deben estar bien organizados y actuar conjuntamente para lograr este objetivo, pero las tecnologías son diversas por naturaleza y presentan diferentes ritmos evolutivos, lo que genera un amplio abanico de escenarios posibles.

Todas las medidas para garantizar la seguridad de la información recaen sobre los componentes del sistema informático y en la interacción que se da entre ellos; por lo tanto, no se podrán implementar adecuadamente sin conocer su funcionamiento y su organización.

1.1. El contexto informático

Hoy en día, difícilmente se pueden concebir tecnologías basadas en elementos aislados los unos de los otros. Si bien se pueden encontrar situaciones concretas que pueden justificar este planteamiento,[1] los requisitos actuales para el tratamiento de datos imponen cada vez más la cooperación y la comunicación entre todos los elementos.

[(1)]Por ejemplo, un ordenador que se dedique exclusivamente al cálculo no tiene muchos más requisitos para el desempeño de su objetivo que el programa de cálculo y los datos que se deben procesar.

Un **sistema informático** es un conjunto organizado de recursos humanos, materiales y lógicos que actúan en el proceso automático de la información.

Veamos esta definición con más detalle:

- El sistema informático requiere una estructura adecuada y coherente que permita integrar, con eficacia, la capacidad y la función que puede aportar cada uno de los recursos al proceso de la información.

- Los recursos materiales son todos aquellos elementos tangibles que se pueden encontrar en el sistema. Sería el caso de los ordenadores, las tabletas, los servidores, el cableado, los conmutadores, los proyectores, los rúteres, las impresoras, etc.

- Los recursos lógicos son todos aquellos elementos intangibles que son necesarios para utilizar el hardware y obtener las prestaciones que este ofrece, el software (por ejemplo, los sistemas operativos o las aplicaciones de usuario) o las configuraciones que definen el comportamiento del sistema

(por ejemplo, las reglas de filtrado de un cortafuegos o la definición de los permisos de acceso a una carpeta compartida).

- Los recursos humanos son todas aquellas personas que interactúan con el sistema para realizar diferentes tareas, como los usuarios, los administradores, los desarrolladores, los técnicos, etc.

- La acción conjunta de los diferentes recursos del sistema es necesaria para conseguir el resultado esperado. Por ejemplo, para consultar el buzón de correo, un usuario deberá utilizar un ordenador conectado a la red que tenga instalado el sistema operativo y la aplicación necesaria para conectar con el servicio de correo electrónico.

En general, se considera que cualquiera de los recursos puede suponer una amenaza para la seguridad del sistema. Por ejemplo, un usuario puede comprometer el acceso a la información almacenada si deja a la vista las claves de acceso al sistema, un sistema operativo puede presentar vulnerabilidades[2] dentro del código que podrían ser explotadas para obtener privilegios de ejecución[3]; del mismo modo, los errores en el diseño de un procesador pueden facilitar el acceso no autorizado a datos de otros procesos.

(2)A menudo, las vulnerabilidades se denominan con el término inglés *bugs*.

(3)Las acciones que se ejecutan en un sistema están enmarcadas en el propio contexto, a excepción de aquellas de administración o de supervisión que pueden tener privilegios en otros contextos diferentes del propio.

1.2. La infraestructura del sistema

La **infraestructura de un sistema informático** es el conjunto de soportes y dispositivos que procesan, transmiten o almacenan la información. Representa los recursos esenciales sobre los que se llevarán a cabo las acciones, por lo que su ausencia impide que el sistema informático pueda llevar a cabo una o más funciones.

Forman parte de la infraestructura todos aquellos soportes materiales sobre los que se sustenta el sistema, como podrían ser el cableado y los armarios de red, y todos aquellos dispositivos electrónicos que, junto con el software de base, desempeñan una o más funciones, por ejemplo, los ordenadores y los servidores con el sistema operativo o las impresoras y los proyectores con el *firmware*[4] que incorporan.

(4)El *firmware* (o soporte lógico inalterable) implementa las funciones básicas de control de un dispositivo, por lo que está relacionado con las características físicas y electrónicas del hardware sobre el que está integrado.

A grandes rasgos, se pueden distinguir tres grupos de recursos dentro de la infraestructura: aquellos que tienen relación con los usuarios, los relacionados con los servicios y aquellos relativos a las comunicaciones.

1.2.1. Los recursos de usuario

Todos los usuarios necesitan utilizar el sistema informático con los dispositivos adecuados, de manera que puedan completar una o más de las acciones en torno al proceso de la información que deban realizar.

Los **recursos de usuario** son todos aquellos dispositivos que materializan la interfaz entre el hombre y la máquina, de manera que la interacción conduzca a la realización de alguna tarea concreta con el sistema informático.

Por ejemplo, son recursos de usuario los ordenadores, las tabletas, los teléfonos inteligentes, las impresoras, los proyectores o las pizarras digitales, entre otros. Estos dispositivos disponen de un soporte electrónico (hardware) sobre el que se ejecuta la lógica de funcionamiento (software) que facilita la operación con el usuario y la realización de las acciones. Se pueden clasificar según varios criterios, pero, desde la perspectiva de la seguridad, se distinguirán principalmente los siguientes tipos:

- Los **dispositivos corporativos**, que adquiere y administra la propia organización para que los usuarios puedan realizar las tareas que tienen encomendadas. Se consideran fiables porque la organización elige sus especificaciones, instala el software adecuado a ellos y determina la configuración necesaria para que se integren en el sistema con garantías de seguridad.

- Los **dispositivos de terceros**, que, a pesar de estar presentes en el sistema y acceder a uno o más de los servicios que ofrece, son propiedad de los usuarios (como trabajadores o colaboradores) o incluso de otras organizaciones (como clientes, proveedores o invitados); por lo tanto, normalmente, se encuentran fuera del control administrativo de la organización. De hecho, cada vez son más las organizaciones que aceptan esta política, denominada BYOD[5], pese a los riesgos que para la seguridad puede suponer la integración de dispositivos desconocidos o poco fiables dentro del sistema. De estos dispositivos se desconoce su estado de mantenimiento y de protección, así como los riesgos a los que pueden haber sido sometido o las amenazas que pueden generar dentro del sistema.

(5)BYOD es el acrónimo del inglés *bring your own device*, una filosofía que propone la incorporación al sistema de los dispositivos que aportan los usuarios.

Los recursos de usuario se ubican en el extremo del sistema informático y suelen considerare la puerta de entrada para romper la cadena de seguridad, por ejemplo, con la introducción de software malicioso[6] que explote vulnerabilidades, el robo de dispositivos que contengan información no cifrada o la obtención ilícita de las claves de acceso al sistema. Muchas veces, la actuación de los usuarios puede ser determinante a la hora de controlar los riesgos y evitar

(6)El software malicioso (*malware* en inglés) es todo aquel software que tiene objetivos nocivos para los dispositivos, por ejemplo, corromper el sistema operativo o robar datos.

la propagación de incidentes hacia el resto del sistema. Por ejemplo, evitando la acción de software malicioso, analizando sistemáticamente las llaves de memoria o evitando la retransmisión de mensajes fraudulentos.

1.2.2. Los recursos de servicio

La implantación de un sistema informático supone un incremento del coste, la complejidad, el mantenimiento y los riesgos de seguridad, por lo que no tiene sentido si no se utiliza para prestar servicios de valor añadido a la organización.

Los **recursos de servicio** son todos aquellos dispositivos que proveen de alguna funcionalidad específica al resto del sistema, tanto si los clientes del servicio son recursos de usuario como si se trata de otros recursos de servicio (que pueden necesitar otros servicios para proporcionar el suyo propio con efectividad).

Por ejemplo, es un recurso de servicio un directorio de usuarios que organiza los permisos de estos y da servicio a un servidor de ficheros para autorizar el acceso a determinadas carpetas compartidas.

En términos generales, se pueden considerar dos grandes grupos de recursos de servicio:

- Los **dispositivos compartidos**, que son recursos que ofrecen funcionalidades limitadas y específicas de acuerdo con la capacidad o las características que tienen en particular, como podrían ser las impresoras en red, las cámaras de vigilancia, los proyectores conectados a la red, los sensores ambientales, etc. En general, estas funcionalidades se ofrecen gracias al *firmware* que incorporan, aunque pueden necesitar la instalación de software en el recurso que quiere acceder al servicio (por ejemplo, para visualizar las imágenes o el vídeo de una cámara de vigilancia puede ser necesaria la instalación de un navegador web o de una aplicación específica).

- Los **servidores**, que son los recursos por excelencia a la hora de proveer al resto del sistema de servicios de alto nivel, dada su capacidad de proceso y de adaptación a cualquier contexto. Con el software adecuado, los servidores pueden ofrecer servicios web, de correo electrónico, de bases de datos, de aplicaciones, de tiempo, de compartición de ficheros y un largo etcétera. Los servidores disponen de hardware y software específico capaces de soportar la carga de trabajo que se les pueda exigir para mantener las prestaciones y su funcionamiento a lo largo del tiempo[7].

(7)La redundancia de los componentes físicos (como las fuentes de alimentación o los discos de almacenamiento) es una manera habitual de mantener la estabilidad de funcionamiento en caso de fallos.

Los recursos de servicio, especialmente los servidores, centralizan información que es valiosa para la organización, por lo que suelen considerarse uno de los centros de atención a la hora de implantar medidas de seguridad. Por ejemplo, la sobretensión eléctrica puede malograr un servidor y detener los servicios que presta (incluso corromper los datos en proceso), o las vulnerabilidades presentes en el sistema operativo (o en el hipervisor[8]) pueden facilitar el acceso a datos sin autorización.

[8]El hipervisor (también llamado monitor de máquinas virtuales) permite la ejecución simultánea de varios sistemas operativos con su propio contexto de funcionamiento (máquinas virtuales) sobre el mismo servidor físico.

1.2.3. Los recursos de comunicación

Para que todos los recursos presentes en la infraestructura puedan cooperar en el proceso de la información, es imprescindible establecer canales que permitan el envío y la recepción de datos entre los diferentes componentes.

Los **recursos de comunicación** son todos aquellos soportes, dispositivos, programas y protocolos que permiten la transmisión o el intercambio de datos entre los diferentes elementos del sistema (que normalmente serán recursos de usuario o de servicio, pero también otros recursos de comunicación).

La infraestructura de comunicaciones toma la forma de red informática. Los recursos (nodos) se conectan con una interfaz adecuada al soporte de transmisión[9] que habilita en el software instalado la transferencia de paquetes de datos[10] utilizando protocolos de comunicación estándar.

[9]Los soportes o medios de transmisión más utilizados son el par trenzado de cobre (sobre todo para el cableado interno), la fibra óptica (especialmente en las conexiones a internet) y el vacío (para las conexiones inalámbricas).

Las redes informáticas requieren la instalación de cajas o puntos de conexión (con cables) y de puntos de acceso (inalámbricos) para conectar los nodos, los dispositivos para transmitir las comunicaciones entre los nodos (conmutadores[11]) y aquellos dispositivos que sirven para conectar con los nodos ubicados en otras redes (rúteres[12]), como, por ejemplo, internet. También es necesario implantar algunos servicios básicos para el buen funcionamiento de la red, como el servicio de direccionamiento de recursos (para asignar a cada nodo una dirección identificativa que permita localizarlo) o la resolución de los nombres de los nodos (para obtener las direcciones que tienen asignadas a partir del nombre común, y viceversa).

[10]El paquete de datos es la unidad básica de transferencia y contiene tanto la información que se quiere transmitir como otros datos de control (emisor, receptor, marca de tiempo, orden del paquete, etc.).

[11]El conmutador es un dispositivo que transmite paquetes de datos entre los nodos que están directamente conectados.

[12]Los rúteres son dispositivos que permiten intercambiar paquetes de datos entre dos o más redes diferentes.

Como el resto de los elementos de la infraestructura, los recursos de comunicación también son uno de los objetivos habituales para romper la seguridad del sistema, dada la función de facilitar la transmisión de datos en todas direcciones[13]. La interceptación de datos, la modificación indebida de información, la suplantación del emisor o del receptor, la redirección de paquetes de datos

[13]Por defecto, los datos se transmiten por la red en claro (sin cifrar) y los conmutadores no filtran ni los nodos que se conectan a ella ni los paquetes de datos que envían o reciben.

o la denegación de servicios son riesgos inherentes a las comunicaciones, que pueden comprometer la seguridad de cualquiera de los nodos presentes en el sistema.

1.3. Los servicios del sistema

Los **servicios de un sistema informático** son todas aquellas funcionalidades que proporciona el sistema que tienen un valor directo[14] para los usuarios y para la organización en general. Representan el objetivo principal por el que se implanta el sistema y justifican el aumento de costes, riesgos y complejidad con beneficios concretos en uno o más aspectos del proceso de la información dentro de la organización.

(14)Cabe diferenciar los servicios que ofrece el sistema a los usuarios (que tienen el objetivo de añadir valor a sus tareas) de los que son necesarios para el funcionamiento de la infraestructura de soporte (que son de gestión y explotación de los recursos y no implican directamente al usuario).

Forma parte de los servicios del sistema todo el software que provee a los usuarios de procesos, capacidades o funcionalidades de alto nivel que son relevantes para el objeto de negocio de la organización, por ejemplo, la manipulación, el almacenamiento, la presentación o la comunicación de información. A diferencia del software instalado en los recursos de usuario (por ejemplo, procesadores de texto, hojas de cálculo, herramientas de presentación, etc.), los servicios requieren una infraestructura completa para acceder a las prestaciones que ofrecen. El correo electrónico, la compartición de ficheros, la transmisión de voz o de vídeo, los servicios web, la mensajería instantánea o los juegos en línea son ejemplos de servicios de uso habitual entre los usuarios.

Desde la perspectiva de la seguridad, se diferencian aquellos servicios que se prestan localmente desde el propio sistema de la organización, de aquellos que se ofrecen desde el exterior (por ejemplo, desde internet) y de aquellos que combinan las características anteriores.

1.3.1. Los servicios locales

Tradicionalmente, la opción por defecto de cualquier organización ha sido implantar todos los servicios necesarios en la infraestructura local, lo que permite tener el control total de los procesos y de los servicios corporativos.

Los **servicios locales** son todas aquellas funcionalidades que se diseñan, se implantan, se explotan y se mantienen dentro de la infraestructura de la organización. Este planteamiento no implica necesariamente que sea la propia organización la que realiza las tareas de administración o de gestión de los servicios[15], sino que representa un objetivo en su concepción, ubicación y utilización.

(15)La organización puede delegar las tareas de administración del sistema a un tercero (por ejemplo, una empresa especializada) cuando no puede (o no quiere) asumir la gestión de su sistema.

Veamos las particularidades de implantar los servicios en el sistema de la organización:

- La organización mantiene el control total de los servicios que ofrece y puede ajustar de manera directa, dinámica y precisa cualquiera de los aspectos de seguridad a cualquier nivel (desde los componentes físicos hasta los de aplicación).

- La implantación local de los servicios requiere la infraestructura necesaria para funcionar con garantías de seguridad[16] y personal capaz de construirlos y mantenerlos a lo largo del tiempo[17], con las implicaciones económicas y organizativas que esto comporta.

- Las medidas de seguridad de los servicios locales han de ser proporcionales al contexto, coherentes con las soluciones informáticas implantadas y administradas de manera proactiva para garantizar la consistencia del servicio y la protección de la información.

(16)Algunos servicios pueden necesitar hardware con mucha capacidad o con configuraciones específicas, y software con costes de licencia que dependen de la máquina en la que se instala o del número de usuarios que lo utilizan.

(17)Si bien las herramientas actuales facilitan parte de las tareas, es necesario un conocimiento profundo de ello para garantizar la seguridad y la coherencia de la configuración.

Es bastante habitual considerar el sistema local como un entorno seguro y fiable para desplegar los servicios de la organización, pero este es un error que ha propiciado multitud de incidentes de seguridad (por ejemplo, el secuestro, el robo o la destrucción de datos), ya que los riesgos y las amenazas no tienen fronteras y el sistema local puede no ser tan fiable como cabría esperar que fuera a efectos de seguridad informática[18].

(18)La tendencia actual a la hora de implantar medidas de seguridad en las organizaciones es considerar que el sistema local es un entorno poco o nada fiable.

1.3.2. Los servicios remotos

La democratización del acceso a internet de banda ancha ha propiciado la proliferación de la oferta de servicios fuera de las organizaciones, lo que facilita, cada vez más, la sustitución o la ampliación de todos aquellos servicios que tradicionalmente se han implantado localmente en el propio sistema de las organizaciones.

Los **servicios remotos** son todos aquellos servicios que se utilizan desde la organización (aunque también podrían ser accesibles desde cualquier otro lugar) pero que no están implantados en su sistema. Normalmente, son ofrecidos por proveedores con quienes se contrata la prestación de estos servicios con unas condiciones específicas.

Las condiciones pueden estar relacionadas con el software o las funcionalidades provistas, el apoyo y la atención al usuario, el mantenimiento y las medidas de seguridad, el coste de los servicios principales y complementarios, etc.

De entre los ejemplos posibles, seguramente los servicios de portal web y correo electrónico corporativo son de los más habituales, pero se podrían añadir muchos más, como la conexión a escritorios remotos[19], los sistemas de información empresariales, las herramientas cooperativas y de trabajo en grupo, la mensajería instantánea o la televisión bajo demanda. En general, se puede considerar que los sistemas informáticos actuales están preparados para utilizar servicios remotos a cualquier nivel, por ejemplo, actualizar el sistema operativo de un ordenador a partir de los depósitos de software remotos que proporciona el propio fabricante, o enviar y recibir mensajes con la aplicación de mensajería instantánea de un teléfono inteligente.

(19)El acceso a escritorios remotos es una tecnología que permite interactuar con un ordenador que se encuentra físicamente distante como si se estuviera delante, es decir, se visualiza la misma interfaz de usuario y se pueden ejecutar las mismas acciones (incluso con la redirección de impresoras o de discos locales).

Si bien en la decisión de externalizar servicios se suelen tener en cuenta varios factores (como los costes, el mantenimiento, la responsabilidad, etc.), la seguridad del servicio y de la información que se procesa es un aspecto de especial importancia. De hecho, el aprovisionamiento externo de un servicio no lo excluye de los riesgos y las amenazas de seguridad, más bien al contrario, puesto que la exposición a los ataques aumenta por el hecho de ser directamente accesible desde cualquier nodo de internet. Para mitigar esta situación, los proveedores de servicio implementan en los centros de datos[20] un amplio abanico de medidas altamente efectivas para garantizar sus servicios ante riesgos físicos (como las intrusiones, los incendios o los cortes eléctricos) o lógicos (como la protección de vulnerabilidades, la salvaguarda de la información, la prevención contra ataques organizados o el software malicioso) con tecnologías específicas y profesionales cualificados que difícilmente son abordables por muchas organizaciones.

(20)Los centros de datos (en inglés, *data centers*) son instalaciones preparadas para alojar una gran cantidad de recursos destinada a proveer de servicios a los clientes que los contratan.

Si bien la externalización de servicios aumenta la dependencia con respecto a los proveedores de tecnología (entre otros aspectos), la ubicación real del servicio no se considera actualmente un factor determinante a la hora de garantizar la protección de la información. En cualquier caso, serán las medidas que se puedan implantar junto con el servicio (ya sea local o remoto) las que lo dotarán de garantías de seguridad reales[21].

(21)No es difícil encontrar servicios en centros de datos más seguros y protegidos que los equivalentes implantados en sistemas locales. El almacenamiento y la compartición de ficheros es un buen ejemplo de ello.

1.3.3. Los servicios híbridos

La implantación de servicios locales y remotos suele dar respuesta a buena parte de los requisitos habituales de las organizaciones, pero se pueden dar circunstancias que necesiten soluciones que se encuentren a medio camino entre las dos opciones.

Los **servicios híbridos** son aquellos servicios que necesitan disponer de recursos locales y remotos para cumplir su función, eventualmente, de manera distribuida o descentralizada. Si bien esta dualidad establece dependencias para que el servicio sea efectivo, abre un abanico de posibilidades nuevas que pueden ayudar a resolver requisitos particulares de la organización.

Veamos algunos ejemplos de estos servicios:

- Es posible que sea necesario publicar en el exterior algún servicio de la organización con el objetivo de que otros usuarios o servicios puedan acceder a él. Los casos más habituales corresponden a los servicios de portal web y correo electrónico corporativo con dominio de la organización, pero puede haber muchos otros. La exposición de servicios al exterior supone un riesgo elevado para el sistema, tanto por el aumento de requisitos de seguridad como por la ampliación de la superficie de ataque[22].

(22)Los servicios web y de correo electrónico se sitúan habitualmente entre los más atacados, y muchas veces sirven de plataforma para atacar otros sistemas, sean estos locales o remotos.

- A veces será necesario que los usuarios ajenos a la organización puedan utilizar los recursos del sistema local como si se encontraran físicamente dentro de las instalaciones, como sería el caso de los comerciales que visitan a los clientes (y deben acceder a los servicios internos) o del trabajo a distancia de los empleados de una organización (que acceden desde casa, a menudo con tecnologías de conexión a escritorios remotos). La implementación de estos servicios también supone un riesgo elevado para la organización, ya que permiten el acceso al sistema (y a una información que puede ser privilegiada o confidencial) desde el exterior, por no mencionar las facilidades que se abren para la propagación de software malicioso.

- A veces será necesario conectar permanentemente dos sistemas informáticos que se encuentran físicamente distantes el uno del otro pero accesibles a través de un medio que puede ser hostil (como internet). Sería el caso de una organización que tenga diferentes oficinas, sedes o sucursales repartidas a lo largo del territorio y que, por las circunstancias de su funcionamiento, deben intercambiar datos de manera automática y permanente. Como en el caso anterior, los riesgos para la seguridad aumentan debido a la ampliación de la superficie de ataque y de la facilidad de propagación de incidentes entre todos los sistemas conectados (que actúan como si fuera uno solo).

- También es posible que un servicio necesite distribuir el procesamiento de la información entre recursos internos y externos, de manera que una parte del proceso se realice de manera remota y la otra local. Por ejemplo, sería el caso de aquellos servicios de computación distribuida donde se divide y reparte la resolución de una tarea (eventualmente compleja) entre dos o más recursos, como las aplicaciones de igual a igual[23] o proyectos

(23)El paradigma de computación de igual a igual (en inglés *peer-to-peer*, P2P) se fundamenta en una red de nodos que pueden actuar como cliente o servidor al mismo tiempo. Uno de los usos más populares es la compartición de ficheros.

como SETI@home[24]. Los riesgos para la seguridad siguen siendo elevados debido a la necesidad de interacción entre sistemas distantes (y quizá desconocidos) y a la automatización de esta interacción (no siempre es fácil detectar las acciones que realiza); pero al mismo tiempo resulta variable en función del servicio que se esté ejecutando (por ejemplo, los servicios de compartición de ficheros pueden comprometer más fácilmente la información que los servicios dedicados al cálculo masivo de datos).

(24)El proyecto SETI@home es una gran red de nodos particulares (todo el mundo puede inscribirse en él libremente) que utiliza los momentos de inactividad de los equipos informáticos para procesar señales de radio del espacio exterior a partir de los datos en bruto obtenidos por las antenas.

Aunque estos servicios (o posibles variantes) son bastante utilizados porque son relativamente fáciles de implementar con el hardware y el software actuales, cada vez es más recurrente la reconversión en servicios remotos ofrecidos por proveedores de servicio. Esto es así porque la industria de la externalización de servicios informáticos es un mercado que no deja de ingeniar nuevas tecnologías que facilitan cada vez más la ubicuidad de los servicios y reivindican facilidades tanto en la explotación de estos servicios como en la contratación y la gestión del coste, a la vez que mantienen las garantías de funcionamiento propias de los servicios remotos. Por ejemplo, sería el caso de la conexión remota al sistema de la organización o a las plataformas para administrar o centralizar los dispositivos de la internet de las cosas[25].

(25)La internet de las cosas, más conocida como IoT (sigla del inglés *Internet of things*), representa la conexión de los dispositivos cotidianos o comunes a la red (eventualmente internet), de manera que puedan interactuar con otros y ser controlados o monitorizados a distancia. Son ejemplos de estos dispositivos las cámaras de vigilancia, los cierres de puertas, los diferentes sensores (de temperatura, presión, etc.) y un largo etcétera cada vez más numeroso.

No hay que olvidar que la utilización de estos servicios supone el establecimiento de una dependencia con el proveedor que se debe plasmar en un contrato de prestación de servicios, donde debería haber una mención especial a la seguridad y protección de la información que se procesa.

1.4. La estructura y el funcionamiento del sistema

La estructura de un sistema informático puede ser tan simple o compleja como los requisitos que debe cumplir. El sistema ha de ser un reflejo de la organización y evolucionar al mismo ritmo, sin subestimar las posibilidades que, a su vez, pueden ofrecer los adelantos tecnológicos para favorecer o mejorar los objetivos, el funcionamiento o la capacidad de la organización.

Pese a la diversidad de escenarios posibles, los sistemas informáticos siguen una estructura funcional común, tanto desde la vertiente de infraestructura como desde la de servicios.

1.4.1. El diseño y la operativa de la infraestructura

A continuación se presenta, de manera simplificada, el funcionamiento general de la infraestructura de los sistemas informáticos:

- En general, los recursos de usuario (por ejemplo, ordenadores) y los recursos de servicio (por ejemplo, servidores) se conectan a los recursos de comunicación (como los conmutadores) creando un segmento de red que

habilita la comunicación entre todos ellos. Conectando dos o más conmutadores se extiende o se amplía el segmento de red hacia más nodos.

- En los segmentos de red inalámbricas (por ejemplo, wifi[26]), los nodos se conectan a la red (que se identifica con un SSID[27]) a través de puntos de acceso[28]. Como cualquier otro recurso, para habilitar la comunicación con el resto de los nodos solo hay que conectar los puntos de acceso a los conmutadores.

- La interfaz de red de cada dispositivo tiene dos direcciones: la dirección física (llamada MAC[29]), que identifica el dispositivo pero no habilita la comunicación a nivel global, y la dirección lógica, que se asigna de acuerdo con la ubicación real del nodo conectado y las características de la red donde se encuentra, lo que habilita el envío y la recepción de paquetes de datos con otros nodos, ya sean estos locales o remotos.

- En el modelo de comunicaciones más extendido hoy en día en todo tipo de redes, el modelo TCP/IP[30], el direccionamiento lógico se basa en las direcciones IP[31], que junto con la máscara de red[32], habilitan la comunicación directa entre los nodos que se encuentran en la misma red[33] o a través de un rúter si se encuentran en redes diferentes. En general, la mayoría de los sistemas poseen un recurso de servicio (por ejemplo, un rúter o un servidor) que distribuye automáticamente las direcciones lógicas a los dispositivos que se conectan a él utilizando protocolos específicos de asignación de direcciones (el más habitual es DHCP[34], aunque hay otros, como BOOTP[35]).

- Desde el punto de vista general de la seguridad, el direccionamiento IP puede ser público o privado. Las direcciones públicas se asignan a nodos conectados a internet, para que se pueda tener acceso a ellas directamente desde cualquier otro nodo. En cambio, las direcciones privadas están reservadas y los paquetes con estos destinos no salen nunca de la red local (los rúteres no los transfieren a internet), por lo que todos los particulares y las organizaciones pueden utilizarlas para las comunicaciones internas[36]. De acuerdo con el estándar, las direcciones privadas que se excluyen del ámbito de internet son 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

(26)Wifi es la abreviatura de *wireless fidelity*, un tipo de red inalámbrica muy extendida y que se utiliza habitualmente para conectar dispositivos de usuario a la red de una organización.

(27)SSID es el acrónimo inglés de *service set identifier*.

(28)Los puntos de acceso inalámbricos se conocen popularmente como AP, acrónimo inglés de *access point*.

(29)La dirección física o dirección MAC (acrónimo del inglés *media access control*) es un identificador de 48 bits único para cada interfaz de red, que se representa con un número en formato hexadecimal (por ejemplo, 12:34:56:78:9A:BC) y se asigna en función del fabricante y del tipo de dispositivo.

(30)TCP/IP es el modelo de comunicaciones resultante de la creación de internet, y debe su nombre a la conjunción de sus dos protocolos principales: TCP (*transport control protocol*) e IP (*internet protocol*).

(31)La dirección IP es un identificador de 32 bits que se representa con cuatro números decimales (entre 0 y 254) separados por puntos (por ejemplo, 192.168.21.37). Se estructuran en clases y algunos rangos están reservados a propósitos específicos.

(32)La máscara de red actúa como filtro de una dirección IP para identificar el nodo dentro de la red. Por ejemplo, 192.168.21.37/24 indica que los 24 primeros bits corresponden a la red (máscara) y el resto, al nodo. Es decir, la dirección corresponde al ordenador 37 de la red 192.168.21.0/24.

(33)Los nodos 192.168.12.77/24 y 192.168.21.78/24 no se podrán comunicar directamente entre sí porque se encuentran en redes diferentes: el primero está en la red 192.168.12.0/24 y el segundo, en la 192.168.21.0/24.

(34)DHCP es la sigla del inglés *dynamic host configuration protocol.*

(35)BOOTP es el acrónimo del inglés *bootstrap protocol*.

(36)Muchos rúteres están configurados de fábrica con el direccionamiento privado 192.168.1.0/24 para la red interna.

- Para conectar el sistema a internet es necesario un rúter, que es el dispositivo que asegura el intercambio de paquetes entre las redes de ámbito público (internet) y privado de la organización. Para realizar su función, dispone de una dirección IP privada en la interfaz de red local y de una dirección IP pública en la interfaz conectada a internet (que asigna el proveedor de telecomunicaciones[37]). Para que los nodos de la red local se puedan conectar con recursos externos, es necesario que tengan configurada la dirección IP del rúter como puerta de enlace[38] a otras redes (que constituye una de las opciones de configuración de los protocolos de asignación de direcciones).

(37)A veces se hace referencia al proveedor de telecomunicaciones con el acrónimo inglés ISP (*internet service provider*).

(38)La puerta de enlace se conoce popularmente por el inglés *gateway*.

- Para localizar los recursos de internet es habitual utilizar el servicio DNS[39], que resuelve las direcciones públicas de los nodos a los que se quiere acceder a partir de su nombre de dominio[40]. En general, el proveedor de telecomunicaciones asigna los servicios DNS a la interfaz pública del rúter (aunque se pueden utilizar otros servidores diferentes a los asignados), para que pueda retransmitir las peticiones de los nodos de la red local (para hacerlo, hace falta que los nodos internos tengan configurada la dirección privada del rúter como servidor DNS, otra de las opciones de configuración de los protocolos de asignación de direcciones).

(39)DNS es el acrónimo del inglés *domain name system*.

(40)El nombre completo de dominio se conoce como FQDN, acrónimo inglés de *fully qualified domain name*, que consiste en el nombre del nodo seguido de los dominios a los que pertenece, por orden jerárquico y separados por puntos.

1.4.2. El diseño y la operativa de los servicios

Veamos ahora cómo es el funcionamiento habitual de la prestación de servicios en los sistemas informáticos:

- Aunque hay diferentes paradigmas de prestación de servicios, uno de los más utilizados es el llamado *cliente/servidor*, donde uno de los recursos (el servidor) está a la espera de recibir las peticiones de los otros recursos (los clientes), que son quienes toman la iniciativa de solicitar el servicio y asumen la parte activa de la conexión. Una vez recibida la petición, el servidor puede analizar su conveniencia y su adecuación antes de prestar (o no) el servicio. Por ejemplo, la navegación web sigue el paradigma cliente/servidor porque es el usuario (cliente) el que pide al servidor web que le transmita el contenido de alguno de los recursos web que posee.

- En la mayoría de los casos, para poder acceder a los servicios que se ofrecen e interactuar con ellos, es necesario disponer de una aplicación adecuada (ya sea estándar o creada *ad hoc*), sin la cual o bien no será posible acceder al servicio, o bien será complicado interactuar con él. Por ejemplo, este sería el caso del navegador web, que permite descodificar el lenguaje HTML[41] de las páginas web para mostrar visualmente el resultado de manera amigable para los humanos. También sería el caso de los clientes de correo electrónico, que presentan de manera organizada la lista de mensajes y el contenido de aquellos que se quieren visualizar.

(41)HTML es el acrónimo del inglés *hypertext markup language*, el lenguaje utilizado para crear y distribuir páginas web.

- En el modelo TCP/IP, cada servicio tiene asociado un protocolo de aplicación que establece los requisitos necesarios para interactuar con el servicio y obtener el resultado esperado. Estos protocolos son estándares y muy cercanos al usuario, como, por ejemplo, HTTP[42] (para la transferencia de páginas web), FTP[43] (para la transferencia de ficheros), NTP[44] (para sincronizar el reloj de los equipos), POP3[45] (para recuperar los mensajes del buzón), SMTP[46] (para transmitir mensajes electrónicos) y un largo etcétera de protocolos que resuelven multitud de situaciones concretas.

(42)HTTP es el acrónimo del inglés *hypertext transfer protocol*.

(43)FTP es el acrónimo del inglés *file transfer protocol*.

(44)NTP es el acrónimo del inglés *network time protocol*.

(45)POP3 es el acrónimo del inglés *post office protocol*, en la tercera versión del protocolo.

- Los protocolos de aplicación requieren utilizar protocolos de transporte para establecer la comunicación entre ambos extremos. Existen dos protocolos de transporte en el modelo TCP/IP, el TCP[47], que es un protocolo que se asegura de que todos los paquetes de datos que se envían llegan a destino (entre otras medidas), y el UDP[48], que es más ligero y rápido pero no garantiza que el receptor reciba todos los paquetes que se le envían. Si bien la mayoría de los protocolos de aplicación utilizan TCP en las comunicaciones para garantizar el servicio, otros han optado por el UDP por la rapidez que ofrece en su transmisión aunque se pierda algún paquete (por ejemplo, los servicios en tiempo real).

(46)STMP es el acrónimo del inglés *simple mail transfer protocol*.

(47)TCP es el acrónimo del inglés *transport control protocol*.

(48)UDP es el acrónimo del inglés *user datagram protocol*.

- Cada servicio tiene asignado un puerto concreto sobre el que presta su función, es decir, una puerta de entrada abierta en la que espera las peticiones de servicio. Los puertos toman la forma de un número entre 0 y 65535 (ambos incluidos) y están asociados a los protocolos de transporte. Por ejemplo, el servicio DNS utiliza el puerto 53 de los protocolos TCP y UDP (TCP/53 y UDP/53), el servicio HTTP utiliza el puerto 80 del protocolo TCP (TCP/80), el servicio SMTP utiliza el puerto 25 del protocolo TCP (TCP/25), el servicio RDP[49] utiliza el puerto 3389 del protocolo TCP (TCP/3389), el servicio SSH[50] utiliza el puerto 22 del protocolo TCP (TCP/22), el servicio SMB[51] utiliza el puerto 445 del protocolo TCP (TCP/445) o el servicio IPP[52] utiliza el puerto 631 del protocolo TCP (TCP/631).

(49)RDP es el acrónimo del inglés *remote desktop protocol*, un protocolo que permite la conexión a escritorios remotos basado sobre todo en MS Windows.

(50)SSH es el acrónimo del inglés *secure shell*, una interfaz de administración propia de los sistemas GNU/Linux.

(51)SMB es el acrónimo de *server message block*, un protocolo para compartir ficheros en una red local.

- Si bien los estándares definen los puertos que debe utilizar cada servicio (como los vistos anteriormente), en la práctica nada impide que se puedan cambiar por otros. Por ejemplo, no es extraño encontrar servidores web

(52)IPP es el acrónimo de *internet printing protocol*, un protocolo para imprimir documentos en una impresora en red.

que ofrezcan el servicio HTTP desde el puerto TCP/8080, en lugar del estándar TCP/80.

(53)Un servidor tendrá tantos puertos abiertos como servicios esté prestando.

- Para poder acceder a un servicio hay que conocer la dirección IP del servidor, los protocolos de aplicación y de transporte que utiliza, y también el puerto sobre el que está a la espera de peticiones[53]. Con esta información, se deben enviar los paquetes de datos necesarios con la estructura, el formato y los datos que requieran los protocolos al puerto concreto de la dirección IP del servidor. Si todo es correcto, el servidor devolverá una respuesta de acuerdo con la definición de los protocolos a la dirección IP del cliente que ha solicitado el servicio, y así sucesivamente hasta completar toda la interacción.

1.4.3. La seguridad del sistema informático

Como se puede entrever en las secciones anteriores, difícilmente puede haber un mecanismo de seguridad que pueda cubrir todas las necesidades de seguridad (ni siquiera la mayoría) de un sistema informático que puede ser tan diverso y complejo como las amenazas y los riesgos a los que está expuesto.

Para garantizar la seguridad de la información no hay ninguna otra vía sino la de combinar múltiples mecanismos de seguridad a lo largo y ancho de todo el sistema informático de manera adecuada, coherente y proporcional.

Muchas veces, la implantación de medidas de seguridad sigue un modelo por capas o niveles (desde el soporte físico hasta el factor humano), pero con independencia del despliegue que se haga (que deberá ser conexo con el contexto), lo importante es garantizar toda la cadena de seguridad de la información de principio a fin (por ejemplo, creación, almacenamiento, acceso, modificación y destrucción).

Con todo, también habrá que tener en cuenta otros aspectos que pueden influir en la definición y planteamiento de la seguridad del sistema:

- La evolución (o la actualización) de la tecnología implantada en el sistema puede comportar cambios en el funcionamiento o la operativa de los componentes, y requerir el ajuste de las medidas de seguridad (o incluso promover la implantación de otras nuevas). Por ejemplo, la actualización del software de servicios puede descartar la utilización de los protocolos de aplicación que se consideren inseguros, obsoletos o comprometidos. Es el caso de las primeras versiones de los protocolos SMB o SSH, entre muchos otros.

- En general, las nuevas tecnologías presentan requisitos de seguridad más exigentes, por lo tanto, la incorporación al sistema puede provocar la necesidad de ajustar o de implementar nuevas medidas para garantizar su cohesión y el funcionamiento global. Por ejemplo, los servicios de compartición de ficheros[54] se están sustituyendo progresivamente por servicios en línea a los que se accede por medio de un navegador web.

(54)Los servicios de ficheros utilizan normalmente protocolos orientados a una red local, como SMB o NFS.

- La organización evoluciona con el tiempo y el sistema informático debe reflejar algunos de estos cambios. A veces solo será necesario realizar ajustes en la configuración de seguridad (por ejemplo, la actualización de los permisos de acceso a la información), pero en otros casos quizá habrá que dar respuesta a nuevas necesidades que requieran la reevaluación completa de la política de seguridad del sistema (por ejemplo, implantar nuevos servicios que sean accesibles desde el exterior de la organización).

- Los riesgos y las amenazas contra la seguridad de cualquiera de los componentes del sistema también evolucionan (y se perfeccionan) con el tiempo, por lo tanto, debe ser habitual la revisión periódica de la política de seguridad del sistema para considerar las novedades que vayan surgiendo. Por ejemplo, es muy conocida la capacidad que tiene el software malicioso de explotar las vulnerabilidades de día cero[55].

(55)Los ataques de día cero aprovechan la ventana de tiempo existente entre la identificación de una vulnerabilidad y la publicación de la actualización que la corrige.

A menudo, cuando se trata de la seguridad de los sistemas informáticos se suele citar una frase que, con el tiempo, se ha convertido en toda una referencia:

> «El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él».
>
> Prof. Eugene Spafford (Universidad Purdue)

Es cierto que conseguir que un sistema informático sea completamente seguro es imposible, pero decididamente se pueden implementar políticas y mecanismos que ofrezcan garantías suficientes, como veremos en las próximas secciones.

2. La seguridad física y perimetral

Sin ningún tipo de duda, uno de los primeros aspectos que cabe considerar a la hora de proteger la información es el acceso al sistema informático. De nada sirve implementar las tecnologías y las medidas de seguridad más eficaces si se descuidan aspectos tan básicos como, por ejemplo, no cerrar con llave la sala de servidores o dejar a la vista las credenciales de usuario.

En las próximas secciones se abordarán tanto los aspectos físicos de seguridad como todos aquellos aspectos lógicos relacionados con el acceso y la conexión a la infraestructura del sistema.

2.1. Los conceptos básicos de seguridad

Los mecanismos de seguridad de la infraestructura están orientados a proteger los diferentes recursos presentes en el sistema, tanto en su vertiente material como en la de su explotación (esto es, la capa básica de software que habilita el uso de los recursos).

A menudo, muchas de estas medidas están encaminadas a controlar el acceso (físico o lógico) a los diferentes recursos (de usuario, de servicio o de comunicaciones), de manera que todos los intentos fraudulentos[56] para acceder a él sean detectados, controlados y filtrados, y se evite, dentro de lo posible, la propagación de los incidentes hacia el resto del sistema.

(56)El establecimiento de políticas de seguridad debe permitir, precisamente, el establecimiento de criterios claros, coherentes y bien definidos respecto al acceso a los recursos.

Las actuaciones que se pueden llevar a cabo para proteger la infraestructura del sistema no están exclusivamente ligadas a la implementación de medidas técnicas en uno o más de los componentes, sino que también pueden requerir las acciones de los usuarios o incluso dar forma a la estructura física o lógica del sistema informático. Por ejemplo, se pueden crear zonas con diferentes requisitos de seguridad, donde el intercambio de comunicaciones puede estar filtrado o directamente bloqueado.

2.2. La seguridad física del sistema

Uno de los principios básicos de seguridad de toda infraestructura es la protección física de los recursos, no solamente ante accesos no autorizados, sino también frente a los riesgos físicos y naturales inherentes a la localización donde se encuentran estos ubicados.

Veamos algunos de estos riesgos:

- El libre acceso a la zona en la que se encuentran los recursos por parte de personas no autorizadas implica un riesgo de robo, manipulación o destrucción que se puede resolver cerrando el espacio y limitando su acceso. La sala de servidores[57] es uno de los ejemplos más habituales, pero el acceso a los armarios de datos o de comunicaciones (entre otros) también debería estar controlado, pues constituyen accesos directos al sistema.

(57)Cuando la importancia de la información almacenada lo requiere, las salas de servidores se pueden proteger con controles biométricos de entrada y con materiales y aislamientos de todo tipo.

- La protección contra los riesgos inherentes a todo espacio físico, como, por ejemplo, los incendios o las inundaciones. Si bien el hardware tiene un valor económico tangible, lo que realmente tiene valor (quizá incalculable) es la información almacenada en el sistema (la pérdida total de la información podría comprometer la actividad de la organización). Los servidores suelen centralizar la información más importante, y, por lo tanto, constituyen uno de los principales objetivos que hay que proteger.

- Las fluctuaciones o los cortes en el suministro eléctrico son otro de los riesgos físicos para cualquier sistema. Los picos de tensión pueden ser nefastos para cualquier material electrónico y pueden requerir la sustitución de alguno de los componentes para que vuelvan a funcionar (por ejemplo, la fuente de alimentación). En general, se considera que se deberían proteger los recursos de servicio (principalmente, servidores) y de comunicaciones (principalmente, conmutadores, rúteres y puntos de acceso) con sistemas de alimentación ininterrumpida[58].

(58)Los sistemas de alimentación ininterrumpida (SAI) son dispositivos que filtran las sobretensiones de la corriente eléctrica. Pueden incorporar baterías para mantener la alimentación durante un tiempo en caso de corte en el suministro eléctrico.

- Los componentes internos de los dispositivos también pueden fallar por muchos motivos y dejar el recurso fuera de servicio rápidamente. Los servidores son, una vez más, el primer objetivo que hay que proteger aprovechando la capacidad que tienen para redundar los componentes más susceptibles de fallo (por ejemplo, la fuente de alimentación y los discos de almacenamiento) y así mantener la continuidad de los servicios.

- La pérdida o el fallo total del sistema también es un escenario que se debe prever, por muy fatalista que pueda parecer (de hecho, el funcionamiento de la organización puede depender de él completamente). Realizar regularmente copias de seguridad[59] de la información más importante es una medida imprescindible y totalmente ineludible en cualquier sistema (ya sea doméstico o corporativo). Las exigencias y los planteamientos pueden ser muy diversos en función del contexto y de la información que haya que salvaguardar, pero una estrategia simple y popular es la llamada 3-2-1, que sostiene el mantenimiento de tres copias de los datos (la de datos del sistema en producción y dos más) en dos soportes diferentes, con una de ellas fuera de las instalaciones de la organización[60].

(59)Las copias de seguridad se conocen popularmente por el inglés *backup*.

(60)Cabe tener en cuenta que, con la proliferación de los servicios remotos (a menudo denominados «en la nube»), también se han diversificado las estrategias de copias de seguridad (algunas de ellas reinterpretando la de 3-2-1).

Seguramente, los centros de datos son el ejemplo más claro de cómo se debe proteger un sistema contra todo tipo de riesgos, dado que implementan las buenas o mejores prácticas del sector (por ejemplo, controles de acceso en las

instalaciones, materiales específicos contra degradaciones diversas, regulación térmica de temperatura y de humedad, protección contra alteraciones en la corriente eléctrica, múltiples sistemas de alta disponibilidad, etc.), a expensas de contrapartidas económicas muy importantes.

Puede ser que la mayoría de las organizaciones no pueda asumir la implementación de todas las medidas de seguridad posibles; por lo tanto, se impone el principio de proporcionalidad a la hora de ponderar los requisitos que tiene el sistema y seleccionar los mecanismos adecuados, necesarios y coherentes con la casuística de la organización.

2.3. La seguridad de los recursos

Mantener la información segura a lo largo de la cadena de proceso es responsabilidad de todos los recursos implicados, de principio a fin. Considerar que el sistema es seguro por haber implantado mecanismos en algunos de los recursos es desconsiderar la concepción global de lo que ha de ser un entorno seguro y fiable facilitando la materialización de los riesgos y la proliferación de los incidentes de seguridad.

Los mecanismos que pretenden asegurar los recursos del sistema persiguen un doble objetivo, por un lado, proteger el propio recurso del proceso que realiza, y por otro, protegerlo del sistema o de los otros recursos con los que pueda tener interacción.

2.3.1. Los recursos de usuario

Los recursos de usuario son uno de los objetivos a la hora de proteger la cadena de seguridad de la información, ya que se ubican en el extremo (el inicio y el final) de buena parte de las transacciones del sistema, ejecutan múltiples aplicaciones que conectan con servicios de entornos muy diferentes que manipulan todo tipo de datos, no siempre disponen de todos los mecanismos de seguridad necesarios para proteger la información, y el usuario que utiliza estos recursos no tiene por qué conocer todas las actuaciones que deben llevarse a cabo para garantizar, en todo momento, la seguridad de las transacciones que realiza.

La diversidad de riesgos que deben afrontar los recursos de usuario es muy conocida y alimenta la proliferación de todo tipo de amenazas que los explotan. La formación de los usuarios en materia de seguridad y el control de los recursos que utilizan son dos de los pilares fundamentales para proteger este extremo de la cadena, pero la adopción rápida de las políticas BYOD en las organizaciones promueve la implantación de medidas específicas para conte-

(61)MDM es la sigla de *mobile device management*, un software que permite gestionar, asegurar y monitorizar dispositivos móviles.

ner este nuevo escenario (por ejemplo, la segmentación de la red inalámbrica de invitados o la implantación de sistemas MDM[61] para aceptar dispositivos que deban acceder a los servicios del sistema).

Veamos algunas de las medidas de seguridad habituales que son aplicables a casi cualquier dispositivo de usuario:

- Mantener el sistema operativo y todas las aplicaciones siempre actualizadas.
- No descargar ni instalar aplicaciones de orígenes desconocidos.
- Utilizar la cuenta de supervisor únicamente para realizar tareas administrativas, como, por ejemplo, la configuración del dispositivo o la instalación de aplicaciones.
- Utilizar claves de acceso robustas[62].
- Si es posible, implementar controles de acceso a la información o a las aplicaciones.
- Bloquear la interfaz de interacción con el sistema cuando no se deba utilizar.
- Instalar y configurar mecanismos de protección contra ataques (por ejemplo, un cortafuegos local[63]) y software malicioso (por ejemplo, un antivirus).
- Realizar copias de seguridad de la información en dispositivos externos de manera regular.
- Mantener la prudencia a la hora de interactuar con los servicios, especialmente con aquellos implantados en la nube. Hay que revisar detenidamente el contrato de prestación de los servicios remotos para garantizar que los datos que se confían no son objeto de actividades inadecuadas.
- Cifrar con claves y algoritmos robustos[64] la información que se deba almacenar en los dispositivos (especialmente aquellos que sean móviles).
- Si procede, fijar los dispositivos móviles con cadenas u otros soportes para evitar los posibles robos.

(62) Los mínimos que se consideran para la robustez de las claves son cada vez más altos. Actualmente, se considera robusta una clave formada por una frase que incluya todo tipo de símbolos.

(63) En este contexto, el cortafuegos es un software que filtra las conexiones de la red hacia el dispositivo (y viceversa), y descarta aquellas que puedan ser sospechosas o fraudulentas.

(64) Por ejemplo, el sistema operativo puede cifrar completamente un volumen de datos, o algunos lápices de memoria incorporan zonas protegidas dentro del espacio de almacenamiento.

Estas medidas son genéricas y no excluyen la consideración de otras soluciones que puedan ser aplicables a contextos específicos, como podría ser el caso de algunos ámbitos públicos (por ejemplo, los sectores educativo, sanitario o la Administración pública en general) o privados (por ejemplo, organizaciones de investigación y desarrollo o empresas de alta tecnología).

Aunque algunos mecanismos de seguridad se pueden automatizar, como, por ejemplo, la búsqueda de virus, la actualización del sistema o la realización de copias de seguridad, el usuario se mantiene en la primera línea de protección de la cadena de seguridad y las actuaciones que realiza pueden ser determinantes. La formación de los usuarios es tan decisiva como la creación de hábitos y costumbres en materia de seguridad y protección de la información dentro de la organización.

2.3.2. Los recursos de servicio

Los recursos de servicio comparten la funcionalidad con el resto del sistema, por lo que están más expuestos a los riesgos, y el hecho de que fallen genera un impacto mayor en la organización que la disrupción eventual de otros recursos (como los de usuario). Garantizar la estabilidad y la disponibilidad del recurso, y preservar las características y las propiedades de los servicios que presta son objetivos esenciales.

Los riesgos a los que puede estar sometido un recurso de servicio pueden ser muy diversos, y pueden ir desde el fallo de alguno de los componentes materiales del recurso que detengan completamente su funcionamiento (como el fallo de la fuente de alimentación o de un disco de almacenamiento), hasta la vulneración de uno o más de los componentes lógicos que puedan comprometer la información que procesa (por la acción de software malicioso presente en los recursos de usuario).

Los dispositivos compartidos (como las impresoras o los proyectores) suelen tener pocas opciones de seguridad porque su función es limitada y no suelen suponer un gran riesgo ni para su propia seguridad ni para la del sistema en general. La mayoría de las veces, las opciones se limitan a la activación de unas pocas medidas, como el bloqueo de la interfaz de configuración con una clave de acceso, la restricción de la prestación del servicio a un conjunto de recursos concreto o la limitación de las funciones según el perfil de usuario.

En cambio, los servidores son los recursos de servicio que más riesgos de seguridad acumulan, considerando la centralización de datos y las funciones dentro del sistema. Veamos algunas de las medidas más habituales:

- En el plano físico, los servidores tienen cajas con ventilación y fuentes de alimentación mejoradas, y también una cerradura para cerrar con llave

el acceso a los componentes internos. Además, existen tanto en formato torre, para colocarse preferentemente en el suelo o sobre una plataforma, como en formato *rack*, que se instalan dentro de un armario de datos (cerrado con llave y ubicado en espacios menos accesibles). Algunos servidores de torre también se pueden instalar en estos armarios gracias a unas guías opcionales.

- Respecto al hardware, las medidas de seguridad principales se centran en redundar los componentes críticos del servidor para que sean tolerantes a los fallos (cuando un componente falla, hay otro que permite mantener el funcionamiento sin interrupciones). Por ejemplo, es habitual disponer de más de una fuente de alimentación eléctrica instalada o más de una interfaz de conexión a la red. También disponen de varios discos (controlados por hardware o por software) sobre los que se distribuyen los datos[65], de tal manera que, si uno falla, no solo no se detiene el servicio ni se pierden los datos, sino que si se sustituye el disco problemático por uno nuevo, pueden escribirse los datos que debería tener (a partir de la información del resto de los discos) y se recupera, así, la estabilidad que se había perdido.

(65) Uno de los mecanismos de redundancia más utilizados es RAID, acrónimo del inglés *redundant array of inexpensive disks*, que se puede implementar tanto por hardware como por software. Ofrece varios niveles de redundancia de acuerdo con los discos disponibles y los objetivos que se quieran lograr (rendimiento, protección, etc.).

- Los datos no siempre deben estar físicamente en el mismo servidor que procesa las transacciones, sino que pueden ubicarse en otros recursos de servicio accesibles a través de la red (y que pueden estar en ubicaciones todavía más seguras). Sería el caso del almacenamiento en red[66] o de las redes de almacenamiento[67], que si bien puede parecer un juego de palabras, son dos conceptos completamente diferentes: mientras que el primero actúa como un servidor de ficheros, el segundo se presenta como un disco local pero el acceso se redirige hacia la red de almacenamiento. Ambas opciones añaden complejidad al sistema y, como cualquier otro servicio, requieren medidas de seguridad específicas (especialmente las redes de almacenamiento, donde es fácil cometer errores de configuración que puedan comprometer la seguridad).

(66) El almacenamiento en red es conocido por la sigla NAS, del inglés *network attached storage*.

(67) Las redes de almacenamiento se conocen con la sigla SAN, del inglés *storage area network*.

- En cuanto al software, implantar soluciones de proveedores contrastados y que ofrezcan un buen soporte, adecuadas a la función que deben realizar y descartando cualquier opción que no forme parte del ámbito empresarial son aspectos esenciales para garantizar la seguridad. Si bien la actualización regular del software es vital para corregir vulnerabilidades, también es importante que la configuración (especialmente del sistema operativo o del hipervisor) no deje margen a la explotación de riesgos (por ejemplo, con mecanismos de aislamiento y control de los procesos en ejecución[68]), por lo que es posible necesitar a los conocimientos de profesionales del área para garantizar estos aspectos de seguridad.

(68) Los sistemas operativos de nivel empresarial pueden controlar la actividad que realizan los procesos que se ejecutan y bloquearlos si las acciones que pretenden realizar no corresponden con su perfil (por ejemplo, si intentan acceder a un fichero de configuración que no es propio).

- Uno de los servicios imprescindibles que todo servidor ha de mantener siempre activo y bien configurado es el cortafuegos. El filtrado que proporciona de las conexiones garantiza que solo sean accesibles los puertos de los servicios que se están prestando, que se descarten los paquetes de datos corruptos o fraudulentos y que las comunicaciones de los clientes sigan los patrones de interacción previstos. El cortafuegos permite el filtrado de conexiones en cualquier sentido de la comunicación, de manera que también es posible evitar que la instalación de un servicio fraudulento en el servidor pueda contactar o enviar datos a sistemas desconocidos, frecuentemente hostiles[69].

(69)Hay listas de recursos de internet que son conocidos porque son el origen de ataques o de la difusión de correo basura o de software malicioso.

Los recursos de servicio son el objeto habitual de múltiples amenazas de seguridad pero, en general, hay suficientes mecanismos de seguridad en prácticamente todos los niveles como para ofrecer garantías de protección de la información, con la condición de adecuarlas y configurarlas de acuerdo con el contexto y la exposición que tengan.

2.3.3. Los recursos de comunicación

Los recursos de comunicación establecen canales para la transmisión de datos entre extremos, pero esta facilidad también expone los recursos del sistema y los datos que se intercambian entre ellos a diferentes riesgos. Evitar los accesos ilícitos y el control fraudulento de los recursos de comunicación son objetivos habituales de la política de seguridad.

Veamos algunas de las disfunciones que pueden sufrir los componentes básicos de las comunicaciones y las implicaciones para la seguridad de la información:

- El cableado se puede estropear con el tiempo, especialmente los conectores y los cables de los recursos. No siempre es fácil identificar el elemento que genera el fallo (a veces, pueden ser parciales o intermitentes), pero pueden provocar la corrupción de los datos que se transmiten o incluso la pérdida total de la transmisión.

- Las interfaces de red también pueden presentar problemas de funcionamiento, sobre todo debido a un fallo de los componentes electrónicos que las integran. Además de la posibilidad de pérdida o corrupción de los datos que se transmiten, también pueden propagar problemas hacia el conmutador debido a la transmisión de señales disruptivas (por ejemplo, la repetición en bucle del proceso de activación y desactivación de la línea) que pueden afectar a su función si no disponen de los mecanismos de detección y desactivación de líneas problemáticas[70] (lo cual dejaría al recurso sin acceso a la red).

(70)Cada vez es más frecuente encontrar conmutadores que implementan la desactivación de líneas problemáticas. A menudo, el protocolo de activación no se desencadena hasta que se desconecta y reconecta el recurso.

- Los conmutadores o los puntos de acceso pueden dejar de funcionar por fallo eléctrico o electrónico (como es el caso de las interfaces de red). A veces, estos problemas no detienen completamente el dispositivo, sino que se traducen en un comportamiento errático que puede provocar la corrupción de los datos que se transmiten, la pérdida parcial o total de la conectividad de los recursos o la disfunción del segmento de red que controlan (por ejemplo, impidiendo la comunicación con otros segmentos).

Más allá de las disfunciones en un plano físico (que son inherentes a la electrónica de los soportes), el foco de atención principal suele recaer en la capa de software de los diferentes recursos que implementan las funcionalidades propias de la comunicación:

- El principio de mantener actualizado el *firmware* de cada dispositivo es garantía de corrección de errores y de prevención de vulnerabilidades, como en cualquier otro recurso del sistema informático.

- Otro principio básico de todos los dispositivos que se adquieren es la necesidad de cambiar las claves de acceso que el fabricante establece en los productos por defecto, en favor de unas claves propias suficientemente robustas como para resistir los ataques habituales de fuerza bruta[71].

(71)Los ataques de fuerza bruta consisten en probar sistemáticamente todas las combinaciones posibles de contraseñas hasta conseguir la credencial válida.

- Proteger la interfaz de configuración del dispositivo, tanto del acceso desde ubicaciones no autorizadas (por ejemplo, internet) como de los usuarios no autorizados (controlando los permisos de administración o supervisión) y de la captura ilícita de transmisiones (activando las variantes seguras de los protocolos, por ejemplo, HTTPS[72]). Los cambios fraudulentos en la configuración de algunos recursos de comunicación (especialmente en los rúteres) pueden redirigir la transmisión de datos hacia sistemas ilegítimos.

(72)HTTPS es la variante segura del protocolo HTTP, protocolos ampliamente utilizados para configurar dispositivos de red.

- Por defecto, la conexión física de cualquier dispositivo a la red ya lo habilita a establecer comunicación con el resto de los recursos que están presentes, lo que puede suponer un riesgo para la seguridad. Para mitigar esta situación es necesario desactivar todas aquellas interfaces de los conmutadores y rúteres que no tienen ningún recurso asignado, o bien imponer filtros de acceso por dirección física (MAC) en aquellos casos en los que sea necesario mantener un control estricto del dispositivo[73].

(73)Las opciones de filtrado por dirección física son propias de rúteres y puntos de acceso inalámbricos.

- El acceso físico a los recursos de comunicación, como los conmutadores y los rúteres, puede facilitar la manipulación fraudulenta de las conexiones del resto de los dispositivos o incluso la conexión al sistema de dispositivos externos que podrían realizar cualquier actividad ilegítima, como la escucha de las comunicaciones[74], la introducción de software malicioso o el bloqueo de servicios[75]. Las medidas de seguridad principales se centran

(74)Las herramientas de escucha pueden recuperar los paquetes de datos que circulan por la red para analizar su contenido.

(75)Los ataques de denegación de servicio son conocidos popularmente por la sigla en inglés DoS (*denial of service*).

en ubicar los recursos de comunicación en armarios cerrados con llave y limitar su acceso al personal autorizado.

Las organizaciones dependen cada vez más de los recursos de comunicación para acceder a los servicios que sustentan su actividad; por lo tanto, cualquier disfunción puede parar parcial o totalmente su actividad. Proteger la infraestructura de comunicaciones resulta esencial hoy en día, para garantizar tanto los recursos conectados como la información que estos transfieren.

2.3.4. La internet de las cosas

La internet de las cosas representa todo un reto de seguridad porque provee de alguna funcionalidad que puede ser importante o confidencial para la organización a partir de un dispositivo que es relativamente simple (o incluso limitado) que se conecta directamente a la red (ya sea esta una red local o internet). Por ejemplo, con estos dispositivos se puede controlar la apertura y el cierre de puertas, monitorizar sensores ambientales de salas o proporcionar imágenes o vídeos de ubicaciones concretas (entre otras muchas posibilidades).

Veamos algunas de las particularidades en torno a la seguridad de la información que supone la explotación de estos dispositivos:

- Utilizan diversidad de tecnologías tanto para el hardware como para el software. El amplio abanico de posibilidades que resulta de ello dificulta tanto la estandarización de la administración como la implementación de medidas de seguridad generales.

- A menudo, los dispositivos deben implantarse en la misma ubicación donde es necesaria su función, lo que a veces origina que tanto el propio dispositivo como la conexión a la red sean físicamente accesibles y manipulables.

- La sencillez de muchos de estos dispositivos se traduce en prestaciones limitadas, tanto en el hardware (dificultad para realizar cálculos complejos, como los necesarios para el cifrado) como en el *firmware* (que disponen de interfaces de control con pocas opciones de seguridad).

- Los proveedores de estos dispositivos no siempre mantienen una línea de actualización del *firmware* de los dispositivos que comercializan (como sí suele hacerse con las aplicaciones o los sistemas operativos), lo que puede dejar los dispositivos desprotegidos ante ataques que exploten las vulnerabilidades detectadas pero no corregidas.

La fuerte implantación que están teniendo estos dispositivos (tanto en particulares como en todo tipos de organizaciones), las carencias o limitaciones que pueden presentar en materia de seguridad y la accesibilidad de muchos de ellos desde internet han propiciado que estos dispositivos sean uno de los objetivos habituales para romper la cadena de seguridad de la información.

A continuación se plantean algunas medidas generales para mejorar la seguridad de estos dispositivos:

- Seleccionar dispositivos con suficiente capacidad de procesado y prestaciones de seguridad, de fabricantes implantados sólidamente en el mercado que puedan proveer de actualizaciones de *firmware* los productos que comercializan.

- Actualizar regularmente el *firmware* para corregir errores y prevenir vulnerabilidades, como cualquier otro recurso del sistema.

- Cambiar la clave de acceso por defecto por una contraseña propia de robustez suficiente. Si es posible, diferenciar el acceso de administración del dispositivo (que permite realizar cambios en la configuración) del de operador (que permite consultar y ejecutar la función que realiza).

- Habilitar las funciones de cifrado disponibles en el dispositivo, tanto para proteger las comunicaciones con la interfaz de configuración como para transmitir los datos que genera su función.

- Habilitar el filtrado de conexiones para asegurar que el dispositivo solo da servicio a los equipos o sistemas legítimos y protegerlo, así, de posibles ataques o de accesos ilícitos desde otros sistemas.

- Intercalar un recurso nuevo que asegure las funciones básicas de seguridad si el dispositivo no es capaz de ello. Además, este recurso también puede ayudar en el procesado de todos los datos que genera el dispositivo[76] (que, a veces, pueden ser en tiempo real).

(76)El término *edge computing* hace referencia a los recursos que centralizan y procesan los datos de los dispositivos IoT antes de enviar los resultados al sistema de la organización.

La internet de las cosas es un área que continúa en curso de desarrollo, especialmente en cuanto a los aspectos de seguridad de la información. La implementación real de los mecanismos de seguridad dependerá en gran medida de los dispositivos concretos que se deban proteger y de su contexto.

2.4. La seguridad de la red

Las organizaciones dependen, cada vez más, de las comunicaciones para apoyar todo el flujo de información que generan y consumen los recursos del sistema. Con razón, buena parte de las actuaciones de seguridad que se suelen implantar globalmente se centran en los recursos de comunicación.

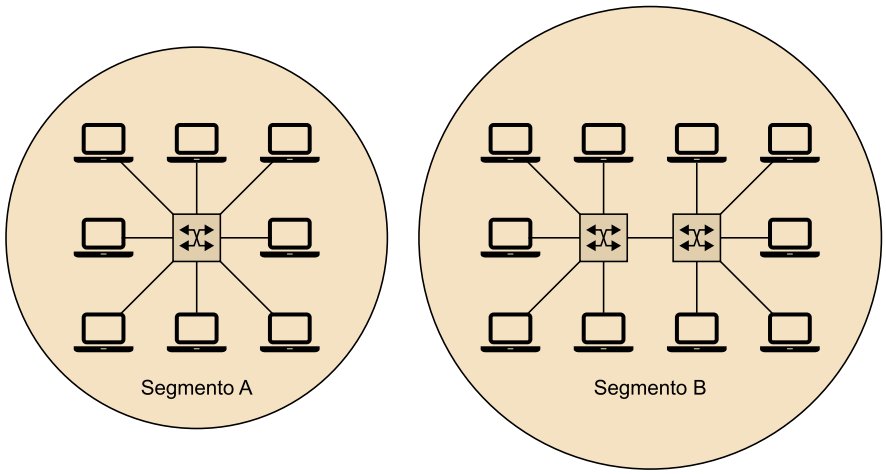
Los mecanismos de seguridad de la red persiguen proteger los accesos y mantener el control de las comunicaciones para minimizar los riesgos que supone tener una infraestructura permanentemente activa y conectada. En los apartados siguientes se hace un recorrido por los más habituales.

2.4.1. La segmentación de la red

El principio fundamental de todas las redes es facilitar la comunicación entre todos los nodos que están conectados a ellas. En la topología en estrella[77], el conmutador es el dispositivo central que permite enlazar los extremos de la comunicación y, si se quiere ampliar la red, en general, solo hay que añadir más conmutadores y conectarlos entre sí de manera que exista un camino entre cualquier par de nodos.

[77]La topología en estrella es la estructura de red más utilizada hoy en día, y consiste en conectar cada nodo a un punto central por el que pasan todas las comunicaciones.

Figura 1. Dos segmentos de red en estrella aislados, uno de ellos (B) con dos conmutadores que amplían el segmento hacia más nodos



Veamos las medidas de seguridad que se pueden implementar en este nivel:

- Por defecto, el conmutador permite la comunicación sin restricciones entre todos los recursos que se conectan. A veces, se pueden dar situaciones que hagan necesario el aislamiento de uno o más grupos de nodos, de manera que únicamente se puedan comunicar dentro de cada grupo. Para hacer posible esta situación hay que segmentar o dividir la red, ya sea de manera física o virtual.

- La segmentación física consiste en aislar los conmutadores que conectan los nodos de cada grupo, descartando cualquier enlace físico con los conmutadores de otros grupos de nodos. Si bien la segmentación física cumple con el objetivo, es compleja de organizar y costosa de implantar, pues debe contar con al menos tantos conmutadores como grupos de nodos se quieran segmentar.

- Para resolver los inconvenientes de la segmentación física, algunos conmutadores implementan el estándar IEEE 802.1Q[78], que ayuda a la creación de segmentos virtuales en la red, denominados VLAN[79], asociando cada interfaz del conmutador con un segmento determinado y etiquetando cada uno de los paquetes que transmite con el número de VLAN al que pertenece. A pesar de que comparten el mismo recurso físico, se considera que las VLAN garantizan el aislamiento de los nodos al mismo nivel que la segmentación física.

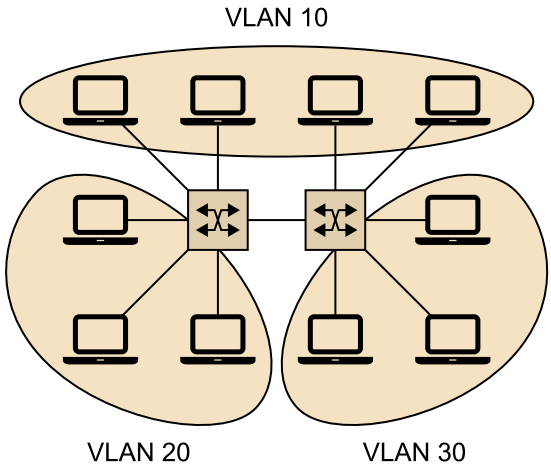
- En el supuesto de que sea necesario comunicar los diferentes segmentos de una red, ya sean físicos o virtuales, es imprescindible que cada segmento tenga un direccionamiento diferente[80] y que un rúter asegure la comunicación entre cada segmento. En este punto, si procede, el rúter puede establecer los filtros necesarios para dejar pasar únicamente los paquetes que cumplen los criterios que se han definido (por ejemplo, habilitar únicamente un sentido de la comunicación o filtrar los servicios que se solicitan en la transmisión).

(78)El estándar IEEE 802.1Q define la segmentación con el etiquetado de los paquetes de datos, insertando un campo que identifica el segmento al que pertenece el paquete.

(79)VLAN es el acrónimo inglés de *virtual local area network*.

(80)La manera más fácil de crear direccionamientos diferentes es ajustar la máscara de red. Por ejemplo, las redes 192.168.21.0/24 y 192.168.73.0/24 son dos redes privadas diferentes.

Figura 2. Segmentación virtual (VLAN) de una red en estrella con dos conmutadores



Segmentar la red interna en varios segmentos presenta la ventaja de poder gestionar varios perfiles de seguridad (uno para cada zona), a costa de aumentar la complejidad del diseño, el coste económico y la dedicación para crear y mantener la infraestructura.

2.4.2. Las redes inalámbricas

En la actualidad, la conexión de los dispositivos inalámbricos es un aspecto tan importante para la organización como lo es la conectividad por cable, a pesar de los riesgos que supone mantener una zona abierta donde cualquie-

(81)Si la cobertura de la red inalámbrica se extiende más allá de las instalaciones de la organización, nada impide que pueda ser atacada por dispositivos externos.

ra puede intentar introducirse en el sistema[81]. A veces, buena parte de estos dispositivos inalámbricos pueden estar asociados al fenómeno BYOD, lo que aumenta todavía más los riesgos de seguridad para el sistema.

Veamos algunas de las particularidades habituales en torno a la seguridad de las redes inalámbricas (por ejemplo, las redes wifi[82]):

(82)Es el acrónimo inglés de *wireless fidelity*, un tipo de red inalámbrica que desarrolla la familia de protocolos estándar IEEE 802.

- Los puntos de acceso son dispositivos conectados a la red del sistema que difunden una red inalámbrica que puede extender la red cableada (utilizando el mismo direccionamiento) o puede ser independiente (creando un nuevo segmento de la red con un direccionamiento específico para los dispositivos inalámbricos). En este último caso, el mismo punto de acceso actuaría como rúter entre ambas redes.

- Algunos de los parámetros de configuración de la red inalámbrica pretenden mitigar los riesgos inherentes a esta tecnología, como la capacidad de crear una red invisible, limitar el número máximo de equipos que se pueden conectar a ella, definir portales cautivos[83] para utilizar la red, habilitar un filtro de dispositivos válidos basado en direcciones MAC, definir una contraseña para acceder a la red, establecer algún tipo de cifrado[84] a la hora de transmitir los datos o, en algunos recursos, incluso la posibilidad de limitar la comunicación directa entre los diferentes dispositivos conectados a la red inalámbricas del punto de acceso[85], entre otros.

(83)Los portales cautivos son mecanismos para autorizar el acceso a la red, por ejemplo, con nombre de usuario y contraseña.

(84)De entre los métodos de seguridad wifi que están estandarizados por la industria, el WPA2 ya no se considera suficientemente seguro y se opta por la utilización de WPA3 siempre que esté disponible.

(85)A veces, esta funcionalidad se denomina *red de invitados* (en inglés, *guest network*).

- Si bien algunos puntos de acceso pueden incorporar servicios de gestión de la red como DHCP y DNS, es bastante habitual delegar esta tarea a los recursos que abastecen la red cableada. De la configuración de estos servicios dependerá la difusión que se hace a los clientes inalámbricos de las particularidades de la red interna del sistema, como, por ejemplo, conocer el nombre del dominio o las direcciones de los servicios implantados.

- Los puntos de acceso no suelen incorporar la capacidad de filtrar los paquetes de datos que se transmiten entre la red inalámbrica y la red cableada. Será necesario segmentar la red inalámbrica y establecer reglas de filtrado entre ambas redes por medio del rúter si se quiere controlar el flujo de las comunicaciones (como sucede en cualquier otro segmento de red).

Cada vez es más fácil garantizar las conexiones inalámbricas dentro de la organización gracias a la evolución de la tecnología, pero la adopción del BYOD requiere profundizar con detenimiento en la complementariedad del conjunto de medidas para garantizar la seguridad del conjunto.

2.4.3. El cortafuegos

En cuanto a la red, un cortafuegos es un dispositivo que implementa las funciones de rúter y que puede examinar los paquetes de datos que recibe para determinar si acepta o rechaza su retransmisión.

Los cortafuegos se ubican en la frontera entre dos o más redes (ya sea entre segmentos internos o entre el sistema e internet), de manera que pueda filtrar las comunicaciones desde el perímetro de cada red.

Veamos las particularidades principales de su funcionamiento:

- Los cortafuegos analizan los paquetes de datos en función de las reglas de filtrado definidas: cuando los atributos de un paquete coinciden con los definidos en una regla, se ejecuta la acción que se ha definido (se acepta, se deniega o se rechaza el paquete). Por ejemplo, «acepta todos los paquetes de datos provenientes de la red interna que solicitan el servicio DNS (UDP/53)». En general, el paquete de datos se descarta si no coincide con ninguna de las reglas definidas.

- Las reglas de filtrado pueden examinar varios atributos y propiedades de los paquetes. Por ejemplo, la dirección de origen o de destino del paquete, el protocolo utilizado y el número de puerto, si el paquete está iniciando una conexión nueva o forma parte de una comunicación ya establecida, el sentido y la dirección de la comunicación, etc. Además, las reglas pueden combinar varias de estas características al mismo tiempo para ajustar al máximo el filtrado de la situación que se acepta, se rechaza o se deniega, aunque cabe tener en cuenta que, cuanto más atributos se verifiquen y más reglas haya, mayor será el coste computacional que deberá soportar el cortafuegos y más retardará el tráfico de paquetes.

- La seguridad que proporciona el cortafuegos es proporcional a cómo de adecuadas son las reglas del filtrado. En este sentido, es habitual partir de una configuración que deniega todas las conexiones (tanto de entrada como de salida del sistema) y solo aceptar las estrictamente necesarias (delimitando las direcciones, los protocolos, los puertos, etc.). Evidentemente, la configuración se deberá adaptar al contexto exacto de la organización (por ejemplo, si la organización publica su propio servicio web habrá que habilitar las conexiones entrantes para prestar el servicio al exterior).

- Una de las funciones interesantes que desempeñan los cortafuegos es la capacidad de registrar la actividad que realizan en forma de diarios[86]; de este modo se puede saber de primera mano cuál es el comportamiento del cortafuegos ante las diversas situaciones a las que debe enfrentarse día a día (por ejemplo, la cantidad y las características de los ataques que se están filtrando).

[86]Los diarios (en inglés, *logs*) es una de las utilidades más interesantes y útiles de los cortafuegos.

- Dado que es un dispositivo de red, el cortafuegos también puede realizar otras funciones, por ejemplo, asignar direcciones a los dispositivos de la red, resolver los nombres de los recursos, enrutar los paquetes entre los diferentes segmentos de red (sean estos físicos o virtuales) o conectar cada uno de los segmentos a internet. Si bien se trata de funciones que habitualmente se asignan al cortafuegos, en instalaciones grandes se delegan a otros dispositivos para liberarlo de cualquier tarea que no sea la propia (con el inconveniente de que añade coste y complejidad a la instalación).

- El mercado ofrece muchas soluciones basadas en cortafuegos que amplían las funciones ya comentadas con otros servicios, como la protección antivirus, los servidores intermediarios[87], los filtros de aplicación[88] o incluso la integración de puntos de acceso inalámbricos en el propio dispositivo. Toda esta combinación de funcionalidades rompe la finalidad primera que ha de tener el cortafuegos, y las buenas prácticas del área recomiendan delegar estos servicios a otros dispositivos.

[87]El servidor intermediario actúa de mediador entre el cliente y el servidor para proteger al primero de los contenidos ofrecidos por el segundo. El caso más habitual es el servidor intermediario de servicios web.

[88]Los filtros del nivel de aplicación (a menudo llamados *Layer 7* o simplemente *L7*) intentan identificar la aplicación o el servicio que hay detrás de una conexión mediante su comportamiento, de manera que esta se pueda filtrar (lo que no es posible realizar a nivel de red).

El cortafuegos es un elemento imprescindible para la seguridad del sistema informático. Si bien su objetivo principal es proteger de riesgos externos, no hay que olvidar que también existen riesgos en el interior del sistema, por lo que también se pueden establecer reglas para limitar las conexiones que salen hacia internet (y así quizá detectar posibles aplicaciones fraudulentas que operen dentro del sistema).

[89]Las redes privadas virtuales son conocidas popularmente como VPN, el acrónimo inglés de *virtual private network*.

2.4.4. Las redes privadas virtuales

A veces, las organizaciones se ven obligadas a permitir la conexión remota a su sistema para que un usuario (o todo un sistema informático distinto) se pueda conectar a él y utilizar los recursos de los que dispone como si estuviera presente localmente. Para garantizar la seguridad de estas conexiones se utilizan las redes privadas virtuales[89]:

- Una red privada virtual se fundamenta en la creación de un canal de comunicaciones seguro a través de un medio inseguro (como podría ser internet). Este canal es como un túnel de extremo a extremo donde la información se transmite de manera segura.

- Dentro del sistema, el dispositivo que normalmente se encarga de establecer las conexiones de red privada virtual es el cortafuegos, gracias a su ubicación en la frontera con internet y a su capacidad de enrutar paquetes de datos. En instalaciones grandes, a veces se derivan estas funciones a servidores específicos.

- Hay diferentes implementaciones de redes privadas virtuales; probablemente, una de las más utilizadas en todas partes es IPSec[90], puesto que

[90]IPSec es la contracción de IP (*internet protocol*) y Sec (*security*).

buena parte de los sistemas operativos (y muchas veces, también del *firmware*) lo incorporan por defecto.

- En general, para establecer el canal seguro hace falta que los extremos conozcan o compartan algunos parámetros de la conexión, por ejemplo, la pasarela[91], la clave compartida de la conexión, las credenciales del usuario que se conecta o los certificados digitales para autenticar los extremos. El número de parámetros depende del tipo de conexión y de los mecanismos de seguridad exigidos para establecer el canal seguro (algunos de ellos son acumulables).

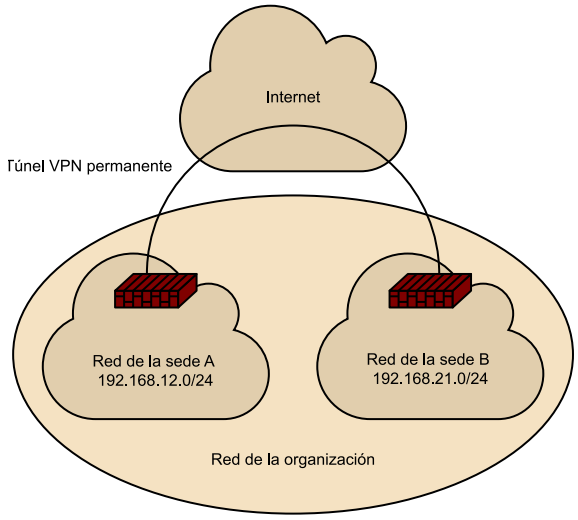
(91)La pasarela del túnel VPN es la dirección del sistema al que se quiere conectar, es decir, la dirección IP pública del rúter.

- Una vez que se ha establecido el túnel, toda la información que se envía o se recibe por este canal está cifrada de tal manera que cualquiera que pueda capturar los paquetes de datos no podrá conocer su contenido si desconoce las claves utilizadas.

- Los usos más habituales de las redes privadas virtuales son la conexión de usuarios remotos[92] o la interconexión de sistemas informáticos. En el primer caso se crea y se destruye el túnel (y el segmento de red virtual asociado) bajo demanda del equipo remoto. En el segundo caso se establece un canal seguro, permanente y cifrado entre los sistemas, lo que permite la accesibilidad continua entre todos los nodos presentes en las redes conectadas. En ambos casos se pueden establecer reglas de filtrado en las comunicaciones, aunque no es lo habitual.

(92)En el argot propio, al usuario remoto que se conecta a un sistema a través de una red privada virtual se le denomina *road warrior*.

Figura 3. Red privada virtual (VPN) permanente entre dos sedes de una misma organización



- El objetivo principal de las redes privadas virtuales es extender la red a todos los equipos o sistemas remotos, lo que aumenta la superficie de ataque y los riesgos de seguridad en general. Por defecto, se considera que los equipos remotos que se conectan a través de una red privada virtual han de ser igual de confiables que los equipos locales, aunque es recomenda-

ble implantar filtros para controlar los accesos y evitar la propagación de riesgos.

- La utilización de redes privadas virtuales supone más coste computacional en los equipos que establecen el túnel debido a las operaciones criptográficas que se deben realizar para asegurar los paquetes de datos que se transmiten, pero también por las posibles reglas de filtrado que se puedan haber establecido.

Las redes privadas virtuales son una de las opciones más utilizadas para conectar equipos o sistemas de manera segura a través de internet, pero cada vez son más las alternativas que proponen externalizar las conexiones seguras a través de servicios de terceros[93] o inclusos directamente reconvertir hacia la nube todos aquellos servicios a los que deben acceder los usuarios remotos (así se evita cualquier actuación en el sistema local).

[93] Normalmente, estos servicios de conexión segura a través de un servicio externalizado requieren la instalación de software específico en los dos extremos de la conexión (por ejemplo, el servicio de escritorio remoto).

2.4.5. La detección y la protección contra intrusos

No parece fácil detectar las intrusiones que pueda haber en unos sistemas que están orientados plenamente a facilitar la utilización y la comunicación entre los recursos. Además, a los posibles atacantes también les interesa hacer prueba de discreción si consiguen introducirse en el sistema, y evitan (o eliminan) cualquier rastro que puedan dejar.

Los sistemas de detección y de protección contra intrusos[94] intentan mantener bajo control esta situación; veamos cómo funcionan:

[94] Los sistemas de detección de intrusos son conocidos popularmente por el acrónimo inglés IDS (*intrusion detection system*) y los sistemas de protección contra intrusos, por IPS (*intrusion protection system*).

- El sistema de detección de intrusos monitoriza la actividad del sistema buscando patrones o comportamientos que puedan ser sospechosos y, en caso de encontrarlos, emitir una alerta.

- En general, la detección consiste en monitorizar varios elementos buscando patrones de comportamiento ya conocidos (como los del software malicioso) o anómalos (como la acción repetitiva de acciones contra un mismo recurso o el envío de paquetes mal estructurados). La detección se puede realizar en varios niveles; los más habituales se encuentran en la red, en el sistema operativo y en las aplicaciones. Por ejemplo, que una aplicación intente modificar o acceder a ficheros que no forman parte de su contexto de ejecución podría activar una alerta que indique que quizá se trata de software malicioso.

- El sistema de protección contra intrusos puede actuar sobre los elementos del sistema para contener el impacto que pueda tener una alerta previamente detectada (por ejemplo, activar reglas específicas del cortafuegos) y así evitar que se pueda producir un incidente de seguridad.

- Existe la posibilidad de que la monitorización genere falsos positivos e identifique como un ataque o incidente una situación que no tiene por qué serlo. En general, se recomienda realizar una primera fase de detección para ajustar el comportamiento de las herramientas antes de poner en marcha la protección (que activaría los mecanismos necesarios para bloquear los elementos que han generado la alerta).

En el mercado hay muchas utilidades que realizan las funciones de detección y protección ante intrusiones, si bien muchas veces usan nomenclaturas diversas para referirse a estas funcionalidades. Por ejemplo, la mayoría de los sistemas operativos controlan el número de intentos fallidos a la hora de introducir las credenciales de usuario, y bloquean durante unos minutos la entrada a partir de un cierto número de errores consecutivos.

2.4.6. Las zonas desmilitarizadas

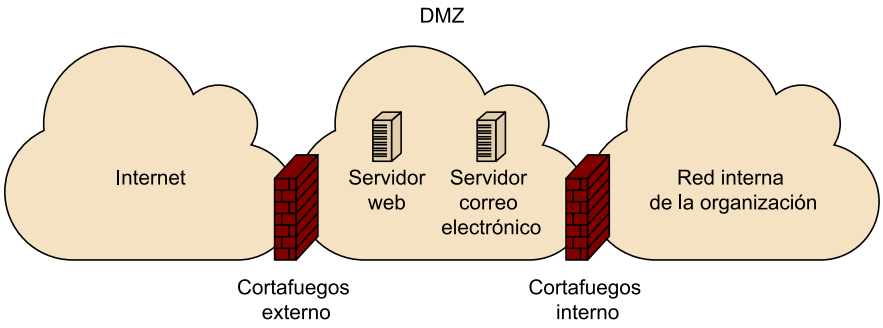
A veces, la organización necesita publicar alguno de los servicios que ofrece su sistema, ya sea para que el público general pueda acceder a él (como un portal web) o por necesidades de funcionamiento del propio servicio (como sería el caso de un servidor de correo electrónico, al que se necesita acceder desde el exterior para recibir el correo entrante de los dominios que administra).

Ofrecer estos servicios supone un riesgo para el sistema, por lo que suele crear una zona desmilitarizada[95] para garantizar la seguridad:

[95]La zona desmilitarizada, del inglés *demilitarized zone* (DMZ), se basa conceptualmente en su homónimo de la vida real para indicar una zona de exclusión que pretende evitar riesgos mayores.

- La zona desmilitarizada es un segmento de la red del sistema que se crea cuando se duplica el cortafuegos. Es decir, el espacio de red resultante entre el cortafuegos externo (que hace de frontera con internet) y el interno (que hace de frontera con el sistema local) actúa como una zona desmilitarizada. También es posible crear la zona con un solo cortafuegos dedicando una de las interfaces de red disponibles a crear este segmento nuevo.

Figura 4. Zona desmilitarizada (DMZ) basada en dos cortafuegos (interno y externo) con dos servicios accesibles desde el exterior (web y correo electrónico)



- En la zona desmilitarizada se ubican los recursos a los que se debe poder acceder desde el exterior. El cortafuegos externo permitirá el acceso remoto a los recursos de la zona, mientras que el cortafuegos interno mantendrá

aislado el sistema local y limitará así el impacto de los posibles incidentes de seguridad.

- La implantación de una zona desmilitarizada es costosa en términos económicos porque supone la adquisición del material para implementar la zona (cortafuegos, conmutadores, servidores, etc.), pero también por la inversión en horas de profesionales para garantizar la seguridad global de toda la infraestructura, que estará más expuesta.

- La publicación de servicios aumenta los riesgos y facilita la explotación de vulnerabilidades que no solo pueden afectar a los propios servicios, sino también servir de plataforma para atacar los cortafuegos o el sistema local (o incluso otros sistemas[96]).

(96)Las redes zombis son redes de ordenadores que están bajo el control de los atacantes y sirven de plataforma para cometer ataques contra otros sistemas.

Si bien las zonas desmilitarizadas continúan teniendo sentido en organizaciones medianas y grandes que necesitan publicar servicios en el exterior y poseen la capacidad suficiente para garantizar el funcionamiento y la seguridad, cada vez es más habitual migrar estos servicios a centros de datos especializados, de manera que sean ellos quienes asuman todos los requisitos de seguridad necesarios para publicar los servicios.

3. La seguridad de los servicios y de las comunicaciones

El sistema se crea y se mantiene para procesar la información que requiere el funcionamiento de la organización; por lo tanto, además de las medidas necesarias para asegurar la infraestructura del sistema, también hay que proteger la explotación de los servicios y de las comunicaciones de alto nivel.

En este sentido, las actividades diarias de los usuarios de la organización, como, por ejemplo, acceder al sistema, modificar ficheros compartidos, acceder al sistema de información de la organización o consultar el buzón de correo electrónico debe tener la cobertura necesaria para garantizar que la información se mantenga segura en cualquier circunstancia.

A lo largo de los próximos apartados se verán los mecanismos más habituales que se implementan para asegurar las acciones que los usuarios, los dispositivos y los procesos realizan en el sistema, tanto en los servicios como en las comunicaciones.

3.1. Los conceptos básicos de seguridad

Los mecanismos de seguridad de los servicios y de las comunicaciones se centran en proteger toda aquella información que es productiva para la organización y que, en consecuencia, forma parte de su objeto de negocio.

De acuerdo con el estándar ISO/IEC 27001[97], **la seguridad de la información** consiste en preservar las tres propiedades esenciales de la información: la confidencialidad, la integridad y la disponibilidad[98].

(97)El estándar ISO/IEC 27000 es la normativa de referencia para definir, desplegar y mantener medidas de seguridad en un sistema informático.

(98)Las propiedades de seguridad de la información son fácilmente extensibles según el contexto donde se aplica, y pueden incluir aspectos como la autenticidad, la trazabilidad, la responsabilidad y el no repudio.

Veamos los mecanismos principales que se implementan habitualmente para garantizar la seguridad de cada una de estas propiedades.

3.1.1. La confidencialidad

Mantener la información accesible para un conjunto de personas y secreta para el resto ha sido desde siempre uno de los aspectos fundamentales a la hora de proteger la información. Si la información es poder, tal y como reza el dicho, mantenerla secreta parece un requisito indispensable para todo aquel que la posee.

(99)Hoy en día, todos los métodos para cifrar y descifrar la información son públicos y ampliamente conocidos, por lo tanto, la calidad de la protección recae exclusivamente en la clave de cifrado.

La **confidencialidad** es la propiedad que garantiza que la información es únicamente accesible para aquellos que están autorizados a utilizarla.

En general, para garantizar la confidencialidad de una información (tanto si está almacenada como en circulación por la red) se utilizan mecanismos criptográficos que transforman un texto en claro en un texto cifrado (y viceversa) gracias a la utilización de algoritmos y claves criptográficas, de manera que el texto solo es accesible si se posee la clave utilizada para cifrar[99].

Para el contexto que nos ocupa, hay dos grandes métodos de cifrado (o criptosistemas):

- Los **criptosistemas de clave privada**, también llamados *criptosistemas de clave simétrica o compartida*, utilizan la misma clave de cifrado tanto para cifrar como para descifrar la información (por lo tanto, la clave ha de ser compartida entre ambos usuarios, dispositivos o procesos que deben acceder a la información cifrada). El algoritmo más representativo es el AES[100], que es el estándar actual, mientras que DES[101] y Triple DES[102] (o 3DES) ya no son recomendables, aunque hayan sido ampliamente utilizados en diversidad de ámbitos.

- En los **criptosistemas de clave pública**, también llamados *criptosistemas de clave asimétrica*, cada usuario posee un par de claves: una pública, accesible para todo el mundo, y una privada, que solo conoce cada usuario. Ambas claves tienen la particularidad de poder descifrar lo que ha cifrado la otra y, a su vez, impedir que se pueda obtener la clave privada a partir de la pública. Los algoritmos más utilizados son RSA[103], ElGamal[104] y la criptografía de curva elíptica (CCE[105]). El funcionamiento es simple: si se quiere que un usuario pueda acceder a determinada información, se cifra con su clave pública para que después la pueda descifrar con su clave privada y así recuperar la información original.

Veamos algunas particularidades de estos criptosistemas:

- Los procesos de cifrado y descifrado de datos tienen un coste computacional elevado para los dispositivos debido a la intensidad de los cálculos matemáticos de los algoritmos. En este sentido, los criptosistemas de clave pública son claramente más costosos que los de clave privada.

- La distribución de claves compartidas en los criptosistemas de clave privada es un proceso muy costoso porque para cada usuario nuevo es necesario generar una clave nueva con cada uno de los otros usuarios del sistema. Este proceso sigue una progresión exponencial respecto al número de usuarios que no es escalable en la práctica.

(100)AES es el acrónimo inglés de *advanced encryption standard*.

(101)DES es el acrónimo inglés de *data encryption standard*, un algoritmo de cifrado que ha sido el estándar durante años, muy utilizado en servicios informáticos y de telecomunicaciones.

(102)El Triple DES es una variante del DES que encadena tres veces el algoritmo; se introdujo al demostrar que el DES se podría romper fácilmente y obtener de él la información en claro.

(103)RSA es la sigla de Rivest, Shamir y Adleman, sus creadores, y se basa en las matemáticas de los números primos.

(104)El sistema de encriptación ElGamal se basa en el intercambio de claves de Diffie-Hellman.

(105)La criptografía de curva elíptica se basa en las matemáticas homónimas.

- A menudo se utilizan los criptosistemas de clave pública para intercambiar de manera segura una clave compartida que servirá para cifrar el intercambio de información. En general, esta clave compartida se utiliza exclusivamente durante un periodo de tiempo limitado y después se destruye (por ejemplo, la sesión de un usuario en el sistema). La clave es larga y se obtiene de funciones aleatorias, por lo que se considera suficientemente segura como para poderse obtener de manera fraudulenta durante el tiempo de la interacción. Con este planteamiento se evitan tanto los problemas de la distribución de claves compartidas como del sobrecoste computacional que requiere el cifrado de clave pública.

Los criptosistemas de clave pública todavía tienen otra problemática que resolver, que no es otra sino garantizar que las claves públicas son efectivamente de quienes dicen ser. Es decir, que la clave pública que se puede obtener de un usuario (o de un dispositivo) sea la que corresponde realmente con su clave privada, y no con la de ningún otro que haya podido suplantar su identidad. Para resolver esta situación se creó la infraestructura de clave pública.

La **infraestructura de clave pública**[106] es el conjunto de recursos físicos, lógicos, humanos, políticos y procedimentales necesarios para crear y gestionar certificados digitales basados en criptografía de clave pública.

(106)La infraestructura de clave pública se conoce popularmente por el acrónimo inglés PKI (*public key infrastructure*).

La infraestructura consta de varios elementos que interactúan para garantizar su objetivo; los más relevantes son los siguientes:

- Los **certificados**[107] son el centro de toda la infraestructura, contienen datos identificativos del usuario, el servicio o la organización a la que hacen referencia, así como la clave pública y la fecha de validez del certificado (entre otros datos). La clave privada no se almacena en el certificado, sino en una estructura o fichero de datos separado.

(107)El formato de certificado más habitual sigue el estándar internacional X.509 en su tercera versión (v3).

- La **autoridad de certificación**[108] es la entidad de confianza que garantiza que los certificados que emite (y revoca) corresponden a los usuarios, servicios u organizaciones legítimos (lo que comporta su verificación real). Si se confía en una autoridad de certificación y se dispone del certificado (porque se ha obtenido por canales seguros), se podrá garantizar la identidad de cualquiera de los usuarios, servicios u organizaciones a los que haya emitido un certificado solo comprobando su validez. Esta confianza se estructura de manera jerárquica: si se confía en la autoridad de certificación, se confía en todos los certificados que haya emitido (y así en adelante, para todos los niveles).

(108)La autoridad de certificación se conoce por la sigla CA del inglés *certification authority*.

- Los **repositorios** son las estructuras en las que se almacena toda la información de la infraestructura de clave pública, en especial los certificados y las listas de revocación de certificados[109] (que son listas que incluyen los certificados que han dejado de ser válidos antes de la fecha prevista).

[109]Las listas de revocación de certificados se conocen como CRL, acrónimo del inglés *certification revocation list*.

La infraestructura de clave pública proporciona todas las garantías de confianza que son necesarias para implementar el cifrado de clave pública en multitud de entornos, tanto del sector público (por ejemplo, en la Administración pública con la generación del DNI electrónico) como del privado (por ejemplo, el sector bancario o financiero en general).

3.1.2. La integridad

Otra de las propiedades esenciales para dotar de garantías a la información es que represente la realidad de manera fidedigna. Es decir, que la información no haya sido creada o manipulada por un tercero sin autorización y, en consecuencia, haya dejado de tener el valor original o, peor todavía, que conduzca a una interpretación errónea.

La **integridad** de la información es la propiedad que garantiza la correspondencia respecto a la realidad original que representa, sin alteraciones fraudulentas de ningún tipo.

Para garantizar la integridad de la información se utilizan funciones de resumen[110], que son funciones matemáticas que establecen una correspondencia unidireccional entre la información y una representación simbólica de medida fija. Es decir, cualquier alteración o modificación en la información original generará un resumen diferente[111] que delataría la pérdida de integridad.

[110]Las funciones de resumen se conocen habitualmente como funciones *hash*.

[111]Aunque el resumen tiene medida fija, es muy difícil que el resumen de dos informaciones sea el mismo.

Los algoritmos de resumen SHA-1[112] y MD5[113] han sido habituales durante mucho tiempo, pero ya no son recomendables porque presentan algunas vulnerabilidades. Actualmente, los algoritmos de resumen recomendables para ser utilizados son los de la familia SHA-2 y SHA-3, que presentan novedades respecto a las versiones anteriores y varias variantes en función de la longitud del resumen que se quiere obtener.

[112]SHA es la sigla del inglés *secure hash algorithm*.

[113]MD es la sigla del inglés *message digest*.

Cuando se hace referencia a la integridad de una información cabe considerar dos dimensiones:

- La **integridad del contenido**, que garantiza que la información representa realmente aquello que debe representar, es decir, que es exacta, fidedigna, creíble y fiable en todos los aspectos. Para garantizar la integridad del contenido de una información, el emisor ha de calcular la función resumen y hacerla accesible para el receptor, que, por su parte, calculará el resumen de la información que haya obtenido y comprobará que ambos resúmenes

coincidan para validar que la información no se haya alterado. Un ejemplo habitual de la integridad del contenido es la descarga de software desde medios inseguros (como internet), donde el productor publica el resumen de los ficheros en su portal de descarga para que los usuarios lo puedan contrastar con los de la copia descargada.

- La **integridad de la fuente** tiene como objetivo garantizar que la información proviene de la entidad que la debe proporcionar, y no de ninguna entidad ilegítima que haya suplantado a la original. Para garantizar la integridad de la fuente se utiliza el cifrado de clave pública: el emisor calcula el resumen de la información y lo cifra con su clave privada, de manera que el receptor pueda descifrarlo con la clave pública del emisor y comprobar si corresponde con el resumen que ha calculado de la información obtenida (solo coincidirá si la información no ha sido alterada y la clave pública utilizada es la del emisor). Un ejemplo de integridad de la fuente es la autenticación de un mensaje de correo o de un documento electrónico[114], donde el emisor quiere garantizar que se trata efectivamente del autor.

[114]Algunas aplicaciones de ofimática incorporan funciones de cifrado para garantizar la confidencialidad y la integridad de mensajes, documentos, etc., utilizando certificados.

Una consecuencia directa de superar la verificación de la integridad es que el emisor no puede repudiar la información *a posteriori*. Por ejemplo, el fabricante de software no puede eludir su responsabilidad si los ficheros descargados de su portal son íntegros pero contienen software malicioso (por ejemplo, un virus o un troyano). De hecho, la propiedad de integridad de la información asienta las bases necesarias para la firma digital de documentos gracias a los mecanismos técnicos para vincular diferentes entidades (integridad de la fuente) con una misma información (integridad del contenido).

3.1.3. La disponibilidad

Hoy en día, la información es más necesaria que nunca, porque sin ella ni se pueden realizar las actividades previstas ni se pueden tomar las decisiones adecuadas. La información siempre ha de estar disponible para aquellas entidades que tienen pleno derecho de acceder a ella.

La **disponibilidad** es la propiedad que garantiza que la información siempre sea accesible para todos los usuarios o procesos que están autorizados a ello.

Garantizar el objetivo de disponibilidad puede requerir un amplio abanico de medidas técnicas, muchas de ellas propias de los ámbitos físico y de infraestructura; revisemos las más relevantes:

Ved también

Para más detalle, ved el módulo dedicado a la seguridad física y de infraestructura.

- Proteger el soporte físico de la información de los accesos no autorizados o de los riesgos físicos y naturales.

- Redundar los componentes críticos del sistema para evitar interrupciones del servicio.
- Realizar copias de seguridad de manera regular para poder restablecer los servicios cuanto más rápido mejor.
- Segregar los dispositivos potencialmente peligrosos a segmentos de red controlados.
- Implantar medidas de prevención contra amenazas y vulnerabilidades.
- Controlar el acceso y la utilización de los dispositivos que contienen datos.
- Implantar políticas y controles para asegurar que no se puede alterar libremente el acceso a la información (por ejemplo, parando los servicios).
- Implantar políticas y controles para asegurar que la información no se elimina de manera fortuita o deliberada por parte de usuarios o procesos no autorizados.
- Establecer mecanismos de detección y de protección de amenazas que secuestren los datos o impidan su acceso (por ejemplo, los ataques de denegación de servicio[115]).

[115]Los ataques de denegación de servicio son conocidos por la sigla DoS, del inglés *denial of service*. Hay una variante que explota todavía más los recursos de la red llamada DDoS, *distributed denial of service*.

A diferencia de las medidas técnicas para garantizar las otras propiedades de seguridad de la información, la pérdida de la disponibilidad de la información es posiblemente la menos fácil de lograr, ya que se pueden dar circunstancias que quedan fuera del alcance de las actuaciones previstas. Por ejemplo, un corte en el suministro eléctrico bastante largo puede acabar con la capacidad de las baterías del sistema de alimentación ininterrumpida y parar los servidores; el fallo de más de un disco del servidor puede provocar la parada inmediata del servicio (o incluso la pérdida de los datos almacenados) o que el centro de datos donde se haya ubicado el sistema de información empresarial sea atacado por una red de zombis[116] que retarde o desatienda las peticiones de servicio que se realizan.

[116]Una red de zombis (*botnet*) es un conjunto de dispositivos conectados a la red (como ordenadores, teléfonos inteligentes o dispositivos IoT) que están bajo el control de terceros gracias a software malicioso y que se utilizan para perpetrar ataques como la denegación de servicio distribuida (DDoS), enviar correo basura o robar datos.

Implantar medidas de seguridad para prever todas las circunstancias posibles es complejo y costoso. Una vez más, el principio de proporcionalidad se impone para seleccionar la información que es crítica para la organización y los mecanismos que pueden asegurarla de acuerdo con el contexto y la situación particular.

3.2. La seguridad de los usuarios

Muchas veces, la seguridad de un sistema informático (y de la información que procesa) se fundamenta en controlar los accesos y las acciones que se realizan. Para conseguirlo, primero hay que verificar que los usuarios son efectivamente quienes dicen ser, y segundo que pueden realizar las operaciones que pretenden.

Las medidas de **seguridad de usuario** agrupan todos aquellos mecanismos que permiten definir y controlar las acciones que puede hacer cada uno de ellos, lo que requiere la verificación previa de su identidad.

En este contexto, se consideran usuarios tanto las personas que interactúan con el sistema como los procesos que se ejecutan en él. De hecho, todos los procesos están ligados a un usuario del que retoman el contexto de seguridad que necesitan para realizar sus acciones, con independencia de si este usuario representa una persona física o una función dentro del sistema[117].

(117)La creación de usuarios impersonales con permisos limitados a la función que realizan es una medida de seguridad habitual en los sistemas.

En las próximas secciones se revisarán los mecanismos principales tanto para garantizar la identidad del usuario como para controlar su interacción con el sistema.

3.2.1. La autenticación

Buena parte de la seguridad del sistema (especialmente la de los servicios que ejecuta) se basa en saber quién lo está utilizando, porque no todos los usuarios deben poder realizar las mismas acciones o acceder a la misma información. Esta necesidad va más allá de la distribución de tareas o de funciones propia de los departamentos de una organización, ya que está regulada por la legislación nacional e internacional. Por ejemplo, está tipificado que un usuario únicamente debe poder acceder a la información que requiere para realizar sus tareas hasta que las complete.

La **autenticación** es el proceso por el que se valida la identidad de un usuario, es decir, se verifica que el usuario es efectivamente quien dice ser antes de utilizar el sistema.

En función de los requisitos de seguridad que pueda imponer la organización, el sistema puede exigir la autenticación en diferentes niveles:

- A la hora de poner en marcha un recurso, ya sea en la BIOS[118] o en el soporte de arranque del sistema.

(118)BIOS es el acrónimo de *basic input output system*, un *firmware* que controla el hardware.

- Cuando se quiere utilizar el sistema operativo del recurso y se inicia así una nueva sesión del usuario que se valida.

- Para acceder y utilizar una aplicación, programa o servicio, ya sea este local o remoto.

Estas medidas son acumulables, es decir, es posible que el sistema requiera la autenticación en solo uno, en dos o en los tres niveles antes de que se pueda utilizar.

El proceso de autenticación del usuario se basa en diferentes factores complementarios, de manera que el sistema puede exigir más de uno para validar la identificación. Veamos cuáles son estos factores:

- Los **factores que conoce el usuario**, como, por ejemplo, una contraseña, una frase, la respuesta a una pregunta o un PIN[119].

- Los **factores que posee el usuario**, como las tarjetas inteligentes[120], los testigos de autenticación[121] o incluso dispositivos implantados (como microchips bajo la piel).

- Los **factores que tiene el usuario**, por ejemplo, los identificadores biométricos como la huella digital, el patrón de la retina o del iris del ojo, la voz, la escritura, la geometría de la mano o de la cara, la secuencia de ADN del individuo, etc.

(119) PIN es la sigla del inglés *personal identification number*.

(120) Las tarjetas inteligentes (en inglés, *smart cards*) tienen la capacidad de almacenar información protegida con mecanismos criptográficos.

(121) Los testigos de autenticación permiten calcular contraseñas desechables o almacenar claves de cifrado, se pueden implementar en hardware (un llavero) o en un software que se instala en un dispositivo (un teléfono inteligente).

Los factores que conoce el usuario suelen ser los más vulnerables porque muchas veces se acaban apuntando en algún lugar (ya que la contraseña es difícil de recordar), son excesivamente simples (como una serie de letras del abecedario o del teclado) o son deducibles a partir de la información del usuario (como una fecha de aniversario o el nombre de familiares). A continuación se revisan algunas de las medidas recomendadas a la hora de seleccionar las credenciales:

- Utilizar contraseñas largas (frases) y fáciles de recordar, evitando palabras o series de caracteres que puedan ser deducibles (fechas, nombres, secuencias, etc.).

- Establecer un periodo de validez y de reutilización de la contraseña coherente con el riesgo que tiene el servicio al que da acceso.

- Memorizar la contraseña, no dejarla nunca por escrito y evitar que otras personas la puedan ver. No tirar papeles con contraseñas que otras puedan leer.

También se puede pensar que los factores que posee el usuario (por ejemplo, las tarjetas inteligentes) son vulnerables por el riesgo de pérdida del objeto o incluso de robo, pero hay que tener en cuenta que estos elementos suelen tener protecciones adicionales para acceder al contenido. Por ejemplo, a las tarjetas solo se puede acceder si se introduce correctamente el PIN y muchas de ellas tienen capacidad de procesado, de manera que la información almacenada no sale nunca de la propia tarjeta.

Se considera que cuanto más factores de autenticación requiera el sistema de autenticación, más garantías tendrá de la identidad del usuario.

Por ejemplo, hoy en día es habitual que los servicios tengan la posibilidad de requerir dos factores de autenticación[122]: primero se introducen las credenciales en el sistema o el servicio que se quiere utilizar (normalmente, usuario y contraseña) y, una vez comprobadas, el sistema envía al teléfono inteligente del usuario una alerta (a través de un mensaje o de una aplicación específica) para validar el intento de conexión al sistema. Además de añadir factores a la autenticación, este sistema también permite detectar cuándo las credenciales del usuario han sido comprometidas y es necesario cambiarlas de inmediato (por ejemplo, si se recibe la notificación para validar una conexión que no se ha realizado). Una variante de este ejemplo consiste en la utilización de contraseñas de una sola vez[123], donde el sistema es capaz de transmitir al usuario (a través de un mensaje o de una aplicación) una contraseña que únicamente es válida para una sesión o para un tiempo determinado.

[122] La autenticación basada en dos factores es popularmente conocida como 2FA, la sigla de *two factors of authentication*.

[123] La autenticación basada en contraseñas desechables se conoce por la sigla en inglés OTP (*one-time password*).

3.2.2. La autorización

La identificación del usuario es el primer paso para establecer una interacción segura, pero esto no implica que automáticamente tenga acceso a la información o que pueda realizar cualquier operación en el sistema.

La **autorización** es el proceso por el que se verifica que el usuario tiene el permiso para realizar las operaciones que pretende llevar a cabo, como acceder a informaciones determinadas o ejecutar acciones o programas concretos.

Por ejemplo, los clientes de banca electrónica se pueden autenticar con éxito en el portal porque han introducido correctamente los factores de autenticación que se exigen, pero cada uno de ellos solo podrá acceder las cuentas bancarias que tienen asociadas su usuario y no a las del resto.

Aunque la autorización suele ser un proceso que depende de la autenticación, puede haber servicios (por ejemplo, los servicios web o de ficheros) en los que un usuario anónimo[124] (no autenticado) puede acceder a determinadas informaciones o ejecutar un conjunto de operaciones en el sistema de manera legítima y sin romper la política de seguridad establecida.

(124)A menudo, a los usuarios anónimos se los conoce como invitados (*guest*) y utilizan el contexto de seguridad de cuentas de usuario homónimos.

En términos generales, la autorización define el contexto de seguridad de un usuario por medio de políticas de control de acceso a los recursos o a los servicios del sistema.

Las políticas de control de acceso definen con concreción y determinismo las acciones que puede realizar cada usuario (a menudo, esta definición se aplica a grupos de usuarios para facilitar su gestión). La implementación de estas políticas es muy diversa porque depende en gran medida del contexto de utilización, pero se pueden identificar dos tendencias mayoritarias:

- El **control de acceso por usuario o por dispositivo**, que define el contexto de seguridad en el propio perfil de cada usuario o dispositivo, es decir, todas aquellas operaciones que ha de ser capaz de realizar en el sistema. Esta implementación es propia de los sistemas operativos (entre otros), que permiten definir la pertenencia de los usuarios o dispositivos a determinados grupos, de manera que el simple hecho de pertenecer a un grupo concreto sea suficiente para realizar un conjunto determinado de operaciones. Por ejemplo, podrán conectarse al ordenador de manera remota[125] todos aquellos usuarios que pertenezcan al grupo de usuarios remotos para los que está habilitado el permiso para establecer este tipo de conexión. Todos los usuarios que no pertenezcan a este grupo no podrán establecer ninguna conexión remota con el ordenador, aunque mantendrán el inicio de sesión local (si lo tienen activado).

(125)La conexión remota al ordenador utiliza software y protocolos específicos, que a veces son propios de cada sistema operativo. Por ejemplo, SSH para los entornos GNU/Linux y RDS para MS Windows.

- El **control de acceso por recurso** se define por los recursos o por los servicios del sistema a los que se puede acceder de manera que cada uno de ellos pueda tener su propia lista de control de acceso[126], una matriz donde se definen las operaciones que puede realizar cada usuario (o grupo) por aquel recurso o servicio concreto. Esta implementación es propia del nivel de servicios del sistema y se puede considerar un estándar *de facto* debido a su implementación en multitud de entornos. Por ejemplo, los servidores de ficheros pueden establecer una lista de control de acceso en cada una de las carpetas compartidas, definiendo qué usuarios (o grupos de usuarios) pueden realizar las operaciones de lectura y/o de escritura dentro de la carpeta y en las subcarpetas que contiene. Algunos servicios pueden ser más granulares a la hora de definir los permisos. Por ejemplo, la creación, la modificación, la visualización, la eliminación, etc.

(126)Las listas de control de acceso son conocidas por el inglés *access control list* (ACL).

En el contexto de los servicios de un sistema, es habitual acumular y combinar los controles de acceso por usuario (o dispositivo) y por recurso para garantizar que el ajuste de la seguridad sea el óptimo respecto al contexto de utilización.

Cabe tener en cuenta que la mayoría de las soluciones, por defecto, implementan el principio de mínimo privilegio[127], que determina que cada usuario solo deberá tener aquellos permisos que son estrictamente necesarios para realizar sus tareas. En la práctica, este principio se traduce con la activación de los permisos más bajos que tiene el usuario; por ejemplo, si el usuario hereda del grupo un permiso de lectura en una carpeta y un permiso de escritura a nivel de recurso, el servidor de ficheros únicamente activará el permiso de lectura siguiendo el principio de mínimo privilegio.

(127) En inglés, *principle of least privilege*.

3.2.3. La gestión de la identidad

La verificación de la identidad de los usuarios y el control de sus accesos siempre ha sido un aspecto esencial de la seguridad de todo sistema informático. Con el paso del tiempo se han desarrollado (y se continúan desarrollando) diversidad de métodos y protocolos para cubrir estos requisitos, que se pueden utilizar tanto de manera independiente como integrados de múltiples maneras.

En general, es bastante habitual implementar un **servicio de identidad o de directorio** en el sistema que centralice la información y la administración de los usuarios y provea, al mismo tiempo, de autenticación y/o de autorización al resto de los servicios y dispositivos del sistema.

Veamos algunas de las características que pueden tener estos servicios de identidad:

- El servicio de identidad puede almacenar todo tipo de información de los usuarios, como datos generales (nombre, apellidos, teléfonos, domicilio, etc.), credenciales diversas (cuentas de usuario y contraseñas), certificados de seguridad y claves de cifrado (claves públicas y privadas), atributos biométricos (huella digital, geometría de la cara o de la mano, etc.), pertenencia a grupos de usuario; incluso es capaz de almacenar autorizaciones, derechos o permisos en todo el sistema. Algunas de estas características solo están disponibles en determinadas soluciones que integran múltiples funcionalidades en un solo producto.

- La información se almacena en estructuras de datos específicos guardados en ficheros o en bases de datos, a las que se puede acceder mediante el servicio de identidad utilizando uno o más protocolos, por ejemplo, LDAP[128], Kerberos[129], RADIUS[130] o incluso SQL[131] en el caso de bases de datos relacionales.

- En general, cada servicio del sistema requiere completar el proceso de autenticación del usuario, lo que puede resultar pesado si el usuario ha de acceder a muchos servicios diferentes. Una manera de resolver esta situación es el servicio de inicio de sesión único[132], donde el usuario debe realizar el registro de la sesión una sola vez en el servicio de identidad y todos los servicios que dependen de él aceptan automáticamente su validez. Kerberos es uno de los protocolos más habituales para proveer el inicio de sesión único dentro de un sistema informático local, pero los servicios accesibles desde internet utilizan otros estándares y protocolos; algunas de las tecnologías que se utilizan habitualmente son OpenID[133], OAuth[134] o SAML[135], entre muchas otras.

Con la implementación conjunta de estas tecnologías se logra uno de los requisitos esenciales para la seguridad de todo el sistema, que no es otro que identificar a los usuarios que realizarán las acciones en el sistema y gestionarán la información que se procesa en él. Además, las diferentes soluciones de gestión de la identidad que se ofrecen en el mercado también permiten materializar las políticas de seguridad definidas en la organización, por ejemplo, el periodo de validez de la contraseña de los usuarios o los requisitos de complejidad que deben tener cuando se impone el cambio, aunque también otras funciones que son invisibles para los usuarios pero útiles para la gestión de la seguridad, como el establecimiento de relaciones de confianza entre diferentes dominios de seguridad y permitir así la interoperabilidad de los usuarios entre ambos sistemas.

(128) LDAP es la sigla en inglés de *lightweight directory access protocol*, un protocolo para acceder y mantener un servicio de directorio de usuarios.

(129) Kerberos es un protocolo para validar la identidad de usuarios y servicios mediante tiques de duración limitada.

(130) RADIUS es el acrónimo de *remote authentication dial-in service*, un protocolo que puede autenticar usuarios contra varias fuentes locales o remotas.

(131) SQL es el acrónimo de *structured query language*, un lenguaje para manipular bases de datos relacionales.

(132) El servicio de inicio de sesión único se denomina, en inglés, *single sign-on* (SSO).

(133) OpenID es un estándar y un protocolo para la autenticación descentralizada.

(134) OAuth es un estándar para la delegación de la autenticación ampliamente utilizado en internet.

(135) SAML es la sigla de *security assertion markup language*, un lenguaje estándar para intercambiar datos de autenticación y de autorización entre entidades.

3.3. La seguridad de los servicios y las comunicaciones

La finalidad principal de todo sistema informático es, por un lado, proveer servicios de alto nivel para la organización, y, por otro, facilitar el acceso de los usuarios a estos servicios. A menudo, estos servicios procesan, almacenan y transmiten información de valor que ha de mantenerse segura, lo que supone una exposición del servicio y de las comunicaciones a diversidad de ataques, riesgos y amenazas.

Las medidas de **seguridad de servicios y comunicaciones** agrupan todos aquellos mecanismos para garantizar las propiedades de seguridad de la información en la prestación del servicio, es decir, tanto en el proceso de la información que realizan como en la comunicación con el usuario.

La relación entre servicio, usuario y comunicaciones es indisoluble porque los usuarios (o los procesos) interactúan con los servicios que se ofrecen en el sistema (sean estos locales o remotos) a través de la red de comunicaciones implantada. Mantener la seguridad a lo largo de toda esta cadena de elementos tan diversos y susceptibles de ser atacados de múltiples maneras supone un esfuerzo importante para la organización.

En las próximas secciones se verán algunos de los mecanismos más habituales para garantizar esta cadena de seguridad de la información.

3.3.1. Los servicios

Sin ningún tipo de duda, todos los servicios son un posible objetivo de ataques por el simple hecho de existir, con independencia de si son públicos o privados, internos o externos a un sistema, etc. Hay muchos tipos de servicios, pero todos tienen en común que de alguna manera permiten el acceso a los datos subyacentes o el control de algún mecanismo, lo que los posiciona en el punto de mira de cualquier atacante o software malicioso.

La **seguridad de los servicios** se centra en garantizar que el servicio no se pueda comprometer a ningún nivel, especialmente en cuanto al funcionamiento y los datos que procesa.

Los servicios están sometidos permanentemente a todo tipos de riesgos y amenazas de seguridad por su propia idiosincrasia; veamos algunos de los más habituales:

- La existencia de puertas ocultas[136] o vulnerabilidades no corregidas en las soluciones informáticas que proveen el servicio podrían habilitar el acceso de usuarios ilegítimos sin la autenticación necesaria, obtener el control administrativo de dicho servicio o incluso espiar o secuestrar la información que se procesa.

- En el supuesto de que las soluciones que proveen el servicio no estén preparadas para controlar o contener situaciones de funcionamiento anómalas (por ejemplo, la recepción de un gran número de solicitudes de servicio[137], eventualmente mal formateadas[138]), se podría producir la parada del

(136)Las puertas ocultas, en inglés, se denominan *backdoors*.

(137)Inundar de peticiones un servicio forma parte de los ataques de denegación de servicio más comunes (en inglés, *denial of service*, DoS).

servicio, la exposición de información confidencial o facilitar la inserción de software malicioso en la memoria de trabajo de la solución informática.

- Las posibles deficiencias en las interfaces o en la configuración de las soluciones, y las limitaciones para soportar las medidas de seguridad más actuales, también pueden ser el objetivo de ataques o de software malicioso, y pueden permitir el robo, el secuestro o la destrucción de datos, incluso la redirección fraudulenta del servicio, ya sea parcial o total, hacia los equipos de los atacantes. A menudo, estos aspectos de seguridad se relacionan con los dispositivos IoT, pero en ningún caso existe exclusividad.

(138)El envío de peticiones mal formateadas (o con códigos específicos) es propio de los ataques de inyección de código (los más populares son los ataques*SQL Injection*).

Todos estos aspectos dependen en gran medida de la calidad y la adecuación de las soluciones informáticas que proveen el servicio, especialmente de su diseño y construcción. Veamos ahora algunas de las características que favorecen la seguridad de estas soluciones y que pueden determinar su adopción:

- Las soluciones se pueden asegurar desde el diseño, estableciendo medidas de seguridad por defecto, implementando el principio de mínimo privilegio, revisando el código fuente por terceros[139], manteniendo diarios de actividad o reduciendo el tiempo de respuesta en la corrección de errores o vulnerabilidades[140].

(139)El software libre no solo utiliza comunidades de desarrolladores para hacer evolucionar el código fuente, sino que se publica en abierto y todo el mundo lo puede revisar y notificar incidencias o problemas de seguridad.

(140)Una vez más, la importancia de la corrección del software y la actualización permanente de los sistemas resulta vital para la seguridad de la información.

- La arquitectura interna de las soluciones también puede favorecer los aspectos de seguridad cuando se priorizan las medidas que se materializarán en las diferentes funcionalidades previstas, por ejemplo, la implementación de buenas prácticas[141] del sector o de normativas de seguridad vigentes.

(141)ITIL (*information technology infrastructure library*) es una biblioteca de buenas prácticas ampliamente reconocida y utilizada en la gestión de servicios de tecnologías de información.

- La incorporación de funcionalidades de seguridad dentro de las propias soluciones también facilita el proceso de asegurar la información, como los mecanismos para autenticar y autorizar a los usuarios, el apoyo de criptosistemas para proteger la información o la inclusión de mecanismos de filtrado de las conexiones (cortafuegos) o de detección de intrusiones (por ejemplo, cuando un usuario intenta iniciar sesión reiteradamente sin éxito).

- Las soluciones han de permitir configurar las opciones de seguridad incorporadas alertando o evitando opciones que puedan abrir brechas de seguridad[142] en el sistema, pero la organización también debe considerar a profesionales cualificados que puedan extraer el máximo provecho de las posibilidades de seguridad que ofrecen las soluciones instaladas.

(142)Algunas aplicaciones avisan al usuario cuando quiere cambiar una configuración que podría tener efectos negativos en la seguridad.

Todos estos planteamientos inciden en la necesidad de disponer de soluciones sólidas y de proveedores fiables, que tengan capacidad para diseñar y construir herramientas que incorporen los mecanismos necesarios para garantizar la seguridad de la información que procesan.

3.3.2. Las comunicaciones

Actualmente, las redes de comunicaciones son imprescindibles para poder aprovechar los servicios, pero la circulación permanente de datos entre clientes y servidores genera un riesgo constante y sostenido para la seguridad de la información.

La **seguridad de la comunicación** agrupa todas aquellas medidas orientadas a proteger la información que se transmite entre extremos a través de las redes informáticas.

Hay que tener en cuenta que buena parte de los protocolos del modelo de comunicaciones TCP/IP[143] no están concebidos teniendo en cuenta la seguridad, así que a no ser que se utilicen sus variantes seguras, cabe considerar que la información viaja a través de la red en claro[144] por defecto. Por ejemplo, el protocolo HTTP es inseguro, mientras que el protocolo HTTPS es su equivalente seguro.

Con los servicios permanentemente expuestos en la red y la transmisión de datos en claro, las posibilidades de atacar las comunicaciones de un sistema son amplias. Veamos una clasificación simple de los tipos de ataque:

- Los **ataques pasivos** se centran sobre todo en capturar los datos que circulan por la red (con la monitorización o el análisis del tráfico[145]) o determinar los servicios que provee un sistema (con el escaneo de puertos abiertos o la transmisión de paquetes fraudulentos[146]).

- Los **ataques activos** son muy variados, pero todos tienen en común la voluntad de corromper el funcionamiento normal de las comunicaciones o directamente conseguir acceso a cualquier nodo presente en la red. Estos ataques utilizan software malicioso, la escucha ilegítima de comunicaciones, los ataques de denegación de servicio[147], la redirección de paquetes a un tercero[148] o los ataques de interceptación[149]. Muchos de estos ataques

(143)La pila TCP/IP es el modelo de comunicaciones que utiliza internet y el más habitual en todo tipo de sistemas, aunque su desarrollo data de los años sesenta del siglo pasado.

(144)Que un paquete de datos contenga información en claro quiere decir que cualquiera que sea capaz de capturarlo podrá leer su contenido sin restricciones mayores.

(145)Una conexión entre dispositivos o sistemas de telecomunicaciones no autorizados se denomina, en inglés, *wiretapping*.

(146)El escaneo de los puertos que mantiene abiertos un servidor se conoce como *port scan*, mientras que la transmisión fraudulenta de paquetes para averiguar los servicios se denomina *idle scan*.

(147)Los ataques de denegación de servicio tienen variantes, una de las más habituales es la versión distribuida (DDoS), en la que un conjunto de equipos (normalmente bajo control fraudulento) envía paquetes de solicitud de servicio o de control (ICMP) de manera masiva a un mismo servicio.

disponen de múltiples variantes que explotan vulnerabilidades conocidas en sistemas que no están actualizados.

El mecanismo de seguridad principal para garantizar las comunicaciones de los servicios de un sistema y prevenir buena parte de los ataques activos es la utilización de la criptografía:

- Cifrando los datos de usuario de los paquetes que se transmiten por la red se garantiza que, a pesar de capturarlos y analizarlos, se mantenga la confidencialidad siempre que no se disponga de la clave de cifrado.

- Con el cifrado de los datos se puede detectar fácilmente la manipulación de los paquetes, gracias al control de la integridad de los datos que proporciona, y también comprobar la autenticidad del emisor, especialmente si se utilizan certificados digitales.

- La utilización de la infraestructura de clave pública añade garantías de identidad entre extremos y de robustez si se emplean claves asimétricas (que suelen ser largas). Asimismo, existen métodos para compartir claves de cifrado a través de un medio inseguro, por ejemplo, el intercambio de claves Diffie-Hellman (que normalmente se utilizan para generar claves de sesión).

- La criptografía no puede prevenir o evitar los ataques contra la disponibilidad de los servicios, que es una cuestión desvinculada de la protección de los datos y que se debe gestionar con los mecanismos ya vistos.

Hay diferentes librerías y protocolos que implementan métodos criptográficos para garantizar la seguridad de las comunicaciones, pero sin ningún tipo de duda, el más utilizado es TLS.

TLS (*transport layer security*)[150]) es un conjunto de protocolos criptográficos diseñados para proporcionar confidencialidad e integridad en la transmisión de datos a través de una red.

Veamos las características principales de TLS:

- Proporciona una conexión privada o confidencial entre extremos porque cifra los datos utilizando una clave para cada sesión (que se negocia al inicio de cada conexión con un protocolo de intercambio seguro de claves).

- Se autentican los extremos de la conexión mediante certificados provenientes de la infraestructura de clave pública, que si bien es optativa, nor-

(148)Uno de los ataques de redirección es el *DNS spoofing*, que consiste en corromper el servicio de resolución de nombres cambiando la dirección IP de un servicio para redirigirlo hacia el sistema del atacante, de manera que le puedan llegar todos los paquetes que emite el usuario hacia el que cree que es el sistema legítimo.

(149)El ataque de interceptación es conocido por el inglés *man-in-the-middle*, y consiste en redirigir la comunicación entre dos extremos hacia un intermediario sin su consentimiento, de manera que este la pueda escuchar y, si quiere, alterar.

(150)La mayoría de las librerías y referencias mantienen el nombre SSL (*secure sockets layer*), el antecesor ya obsoleto de TLS, a pesar de implementar los nuevos protocolos.

malmente se requiere por parte de al menos uno de los extremos de la conexión (normalmente el servidor).

- Se mantiene la integridad de los datos que se transmiten porque se envían acompañados de un código de autenticación de mensaje[151], que controla tanto la alteración de los datos transmitidos como la pérdida de algún paquete durante la transmisión.

- Puede garantizar que cualquier reutilización de las claves de cifrado no pueda descifrar comunicaciones anteriores. Esta propiedad se denomina *forward secrecy*.

- Puede soportar diferentes métodos de intercambio de claves, de cifrado y de autenticación de mensajes, pero no todas las combinaciones posibles generan las propiedades anteriores.

(151)El código de autenticación de mensaje se denomina, en inglés, *message authentication code* (MAC).

La mayoría de las variantes seguras de los protocolos del modelo de comunicaciones TCP/IP utilizan TLS para asegurar las conexiones. Además del cambio en el nombre del protocolo (por ejemplo, HTTPS es la versión segura de HTTP), muchos protocolos seguros también cambian el número de puerto del servicio (por ejemplo, HTTPS utiliza el puerto TCP/443 en lugar del TCP/80 del protocolo inseguro HTTP). Otros protocolos no cambian el puerto (o tienen ambas variantes, como LDAP) pero utilizan una solicitud específica para iniciar la conexión segura llamada «STARTTLS».

Cabe destacar que TLS (como otros protocolos criptográficos) proporciona un túnel seguro de extremo a extremo, por lo que garantiza que ninguno de los dispositivos o recursos a través de los que se transmiten los datos puedan acceder al contenido de los paquetes de datos. Pero esta privacidad también se aplica a cualquier dispositivo de seguridad perimetral que pueda haber en el sistema (por ejemplo, un cortafuegos o un servidor intermediario[152]); por lo tanto, si se transmite cualquier ataque o amenaza a través de la conexión segura, el equipo final será el único elemento capaz de contenerlos o mitigarlos (lo que tendría que motivar la implantación de medidas de seguridad en este extremo de la conexión).

(152)Los servidores intermediarios se conocen popularmente como *proxy* y el ejemplo más habitual es el *proxy* de servicios HTTP, que además de hacer las funciones de intermediación, también pueden filtrar los contenidos o verificar la presencia de software malicioso, entre otros.

3.3.3. Los usuarios

De poco sirve la implantación de todos los mecanismos técnicos para garantizar la seguridad del sistema si los usuarios finales no toman conciencia de que también forman parte de la cadena de seguridad de la información.

La **seguridad de los usuarios** agrupa todas aquellas actuaciones que pretenden integrar las acciones de los usuarios dentro de la política de seguridad del sistema.

Tradicionalmente, la seguridad informática se ha querido resolver desde una perspectiva técnica, pero con el paso del tiempo se ha demostrado que resulta imprescindible implicar a todos los agentes que interactúan con el sistema, especialmente a los usuarios finales, ya que han de garantizar el extremo de la cadena de proceso de la información. Por ejemplo, algunos usuarios pueden tener dificultades para gestionar correctamente las diferentes credenciales de que disponen o para reconocer páginas web fraudulentas o adjuntos de mensajes potencialmente peligrosos (entre otros), lo que puede suponer un riesgo para la seguridad de todo el sistema.

En este sentido, son muy conocidos los ataques de ingeniería social, cuyo objetivo es persuadir a los usuarios para que revelen secretos que permitan a los atacantes conseguir cualquier tipo de información que puedan utilizar contra el sistema o contra ellos mismos (por ejemplo, credenciales de acceso a servicios, los números y códigos de tarjetas de crédito, etc.). Probablemente, uno de los casos más conocidos son los ataques de pesca de credenciales, que pretenden engañar a los usuarios[153] presentando un portal web aparentemente conocido pero que redirige la información proporcionada (por ejemplo, las credenciales de acceso a un servicio) a los servidores de los atacantes.

(153)El engaño se implementa por medio de correo electrónico o mensajería instantánea (*spoofing*) y crea una situación que requiere la atención del usuario, por ejemplo, un descubierto bancario.

Este tipo de ataques son difíciles de prever (incluso desde el punto de vista técnico); por lo tanto, la mejor manera de gestionarlos es con la formación de los usuarios y la promoción de una cultura de la seguridad en la organización que fomente tanto la identificación de estas situaciones como la prudencia a la hora de actuar.

3.4. La seguridad de los contenidos

Si bien todos los mecanismos de seguridad son bienvenidos para apoyar a la cadena de seguridad, a veces lo que interesará es garantizar alguna de las propiedades de seguridad en elementos de información individuales (como un documento o un mensaje).

La **seguridad del contenido** pretende aplicar mecanismos de seguridad a elementos o soportes de información particulares, que a menudo están asociados al trabajo que realizan los usuarios para garantizar alguna de sus propiedades.

Por ejemplo, a veces se querrá proteger un lápiz de memoria de accesos indebidos o garantizar la validez de documentos (como contratos o acuerdos). En ocasiones, estos elementos de información se quedan al margen de las políticas de seguridad general implantadas en el sistema, pero su cobertura es necesaria para asegurar algunas de las situaciones que se pueden dar en la organización. En las próximas secciones se revisan algunos casos interesantes.

3.4.1. El cifrado

Como se ha visto en apartados anteriores, el mecanismo principal para garantizar la confidencialidad de la información es el cifrado de los datos, ya sea mediante criptosistemas de clave privada o pública. Con las soluciones existentes, hoy en día es relativamente fácil poder cifrar la información:

- Muchos sistemas operativos permiten el cifrado de los discos del ordenador (incluso de aquellos donde se instala el sistema) con una contraseña, de manera que de los intentos de recuperar directamente los datos del disco no se pueda obtener resultado en claro.

- En soportes extraíbles (como los lápices de memoria) se pueden crear áreas privadas utilizando el mismo software de cifrado que proporciona el fabricante del soporte o por medio de un software de terceros.

- Algunas aplicaciones ofimáticas permiten bloquear determinadas acciones en los documentos que manipulan o cifrar completamente el contenido con contraseñas (o incluso con certificados digitales).

- El correo electrónico permite el cifrado y descifrado de los mensajes con criptosistemas de clave pública, teniendo en cuenta que es necesario haber configurado previamente los certificados de los usuarios implicados en la comunicación[154], ya sea con la instalación directa de los certificados o el acceso a los repositorios donde están almacenados.

[154]Normalmente, la clave pública y privada que corresponde a un usuario se empaqueta en un fichero con formato PKCS#12 (extensión .p12) protegido con una contraseña de acceso.

El número de aplicaciones con soporte para el cifrado de los contenidos continúa en crecimiento (sobre todo aquellas que implementan la infraestructura de clave pública), síntoma inequívoco de la importancia que tiene proteger la información.

3.4.2. La firma digital

La integridad de la información es una de las propiedades de seguridad importantes en sistemas informáticos donde el coste de copia o de modificación es prácticamente inexistente[155]. Una de las aplicaciones más interesantes de la criptografía aplicada a la integridad es la firma digital de documentos o mensajes:

[155]En cualquier sistema informático, copiar un dato de un lugar a otro o modificarlo directamente no se considera costoso, ni en términos computacionales ni temporales.

- La firma digital utiliza la infraestructura de clave pública, donde cada uno de los usuarios o entidades que firman el documento tienen su par de claves (pública y privada).

- Del documento que hay que firmar (un contrato, un acuerdo, un mensaje, etc.) se extrae un resumen (*hash*), que se cifra con la clave privada de cada usuario[156] y se añade al documento para que el resto pueda descifrarlo con la clave pública correspondiente y verificar la coincidencia con el resumen del documento (lo que significaría que se ha firmado el documento original).

- En general, cada vez que se abre el documento se comprueban las firmas, por lo que requiere disponer de los certificados instalados en el sistema o el acceso a los repositorios que los contienen.

- Con la firma digital se logra también otra de las propiedades de la seguridad de la información (si bien no esencial), que es el no repudio. Una vez verificada la firma del documento o del mensaje, el usuario no puede negar su acción porque técnicamente se puede demostrar lo contrario.

- La firma digital se puede combinar con el cifrado del contenido, pero hay que tener en cuenta que se trata de dos operaciones diferentes: el cifrado del contenido se realiza con la clave pública del destinatario (para que lo pueda descifrar con su clave privada) y la firma digital utiliza la clave privada del emisor (para que el receptor la pueda descifrar con la clave pública del emisor).

- Las administraciones públicas (entre otros organismos) pueden proporcionar certificados digitales legalmente válidos a las personas físicas y jurídicas para realizar las operaciones anteriores con los mismos efectos legales que una firma física (por ejemplo, los documentos de identidad electrónica).

(156)En lugar de cifrar todo el documento únicamente se suele cifrar el resumen para reducir el coste computacional de la operación. El resultado es, a efectos prácticos, perfectamente equivalente.

Del mismo modo que con el cifrado, el número de aplicaciones que soportan las operaciones de firma digital continúa creciendo, especialmente aquellas destinadas a validar la información que puede tener implicaciones legales (por ejemplo, la firma de contratos o las declaraciones de impuestos).

3.4.3. El esteganografía

Si el objetivo de la criptografía es modificar la información para que solo puedan acceder a ella aquellos que tienen la clave de cifrado, la esteganografía agrupa todas aquellas técnicas que sirven para ocultar la información privada entre datos públicos (sin alterar la percepción del conjunto).

Los casos más habituales consisten en introducir un texto dentro de un fichero de imagen o de sonido, modificando los bits menos significativos (aquellos que no producen alteraciones destacables en el resultado) para incluir la información deseada. El tamaño y la apariencia del fichero serán los mismos, por lo tanto será muy difícil constatar las diferencias entre el fichero original y el modificado, excepto en el resultado de la función resumen, que será diferente porque la codificación interna del fichero ha sido alterada.

Aunque el uso de la esteganografía requiere técnicas y software especializado para introducir los datos en los ficheros y poder recuperarlos, es una buena manera de proteger la información con medios aparentemente irrelevantes.

Resumen

No parece fácil garantizar las propiedades de seguridad de la información en un mundo como el actual. La omnipresencia de la información, la complejidad de la tecnología, la exposición constante de los servicios, la evolución rápida de los riesgos o la contención de los ataques son solo algunas de las situaciones a las que se debe hacer frente para asegurar la información.

Si bien conseguir que el sistema sea completamente seguro en toda circunstancia es un hito difícilmente alcanzable, la tecnología ofrece suficientes mecanismos de seguridad para proteger la información en la mayoría de las situaciones. La implantación de medidas requiere el análisis de la organización, la identificación correcta de los requisitos de seguridad, la buena selección y combinación de los mecanismos (técnicos, organizativos, etc.), y la implantación coherente y el mantenimiento proactivo posterior de todas las medidas para que la seguridad sea una realidad efectiva y durable.

De hecho, en el contexto de seguridad informática no se puede perder nunca la visión de conjunto, porque un sistema es tan seguro como lo es la cadena de proceso de la información que soporta. Este ciclo de vida es el que tiene que guiar todas las actuaciones dirigidas a garantizar las propiedades de seguridad de la información.

Bibliografía

Codolà, S. *Seguridad y auditoría de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Colobran, M. *Gestión de incidentes de seguridad*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Colobran, M.; Morón Lerma, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC.

Cruz, A. *Análisis de riesgos*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Domingo, J.; Herrera, J.; Rifà, H. *Criptografía*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

García, J.; Perramon, X. *Seguridad en redes de computadoras*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Introducción a la seguridad de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Implantación de un sistema de gestión de la seguridad de la información (SGSI)*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Jimeno, M. T.; Míguez, C.; Matas, A. M.; Pérez, J. (2008). *Guía práctica hacker*. Madrid: Anaya Multimedia.

Perramon, T. *Sistemes de comunicacions*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Prieto, J. *Comunicacions sense fils*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Rifà, H. *Infraestructura de clave pública*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.