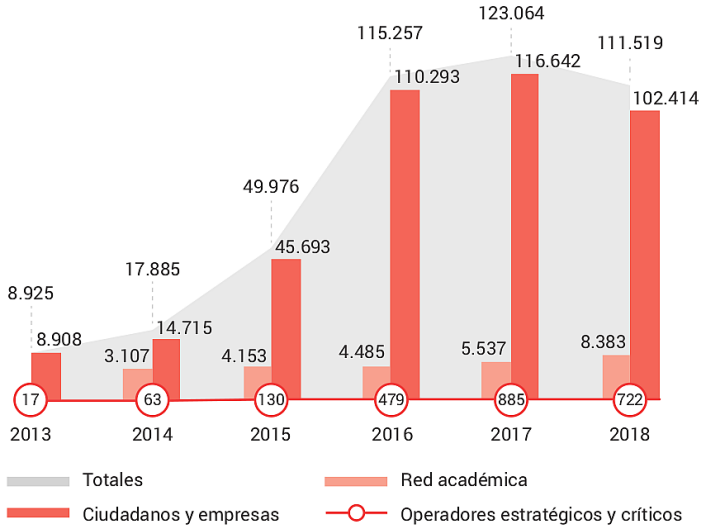
1. Introducción

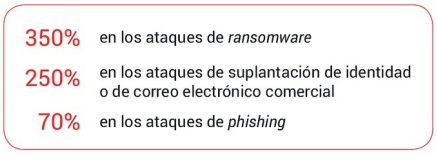
Los motivos por los que la seguridad debe formar parte de la agenda de cualquier organización, independientemente de su sector económico o de su tamaño, son muchos y variados, algunos de los cuales se pueden leer en la prensa con mucha frecuencia: fraudes electrónicos, casos de phishing en la banca, filtraciones no deseadas de información o de datos personales, cortes en las comunicaciones, etc. Los perjuicios que ocasionan los incidentes de seguridad son, cuando menos, incómodos y en muchos casos económicamente gravosos: paradas de producción, pérdidas de clientes, pérdida de reputación, etc.

Desde hace unos años INCIBE[1] realiza estudios sobre el sector de la seguridad TIC en España donde se puede comprobar una tendencia al alza en incidencias de seguridad. Principalmente son ataques de ransomware, secuestro de sistemas, fugas de información, ciberestafas y técnicas de engaño como el phising.



Fuente: INCIBE

En un estudio similar realizado por Google en 2018, se estimó que el coste medio de un ciberataque a una pyme es de unos 35.000€ y que el 60% de las pymes cierra 6 meses después del haber sufrido el ciberataque. Ese mismo año el porcentaje de ataques a nivel mundial aumentó:



2. Seguridad Informática, Seguridad TIC y Seguridad de la Información

Es generalmente aceptado que el objetivo de la seguridad es proteger los activos (personal, información, material, instalaciones) y las actividades de una organización. Por tanto, según sea el recurso a proteger se utilizan los términos de seguridad del personal, seguridad de la información, seguridad del material, seguridad de las instalaciones o seguridad de las operaciones.

Al hablar de informática y seguridad aparecen varios términos que aún siendo parecidos no significan lo mismo y que a lo largo de los años ha cambiado:

- **Seguridad Informática:**
  - Nació en la época en la que no existían las redes de banda ancha, los teléfonos móviles o los servicios de internet como las redes sociales o las tiendas virtuales.
  - Centrada en proteger los sistemas; es decir, los ordenadores, las redes y el resto de infraestructuras de nuestra organización.
  - Es un concepto fundamentalmente técnico, lo que la aleja del punto de vista de un usuario o gerente.
- **Seguridad TIC:**
  - Además de proteger el ordenador como elemento central de una infraestructura tecnológica, hace especial hincapié en las infraestructuras de comunicaciones y amplía el ámbito de protección a los dispositivos móviles; y en general, a cualquier dispositivo capaz de almacenar, transmitir o tratar

[1]INCIBE: Insituto Nacional de Ciberseguridad - https://www.incibe.es/

información. Pero, además, abarca la protección de elementos no físicos, como son los servicios (correo electrónico, la navegación web, etc.).
- La Seguridad TIC sigue siendo de carácter fundamentalmente tecnológico.

- **Seguridad de la Información:**
  - Protección de la información, independientemente de su formato, localización, naturaleza, etc.
  - Se tienen en cuenta varios puntos de vista: técnico, organizativo, normativo y legal.

3. Seguridad de la Información

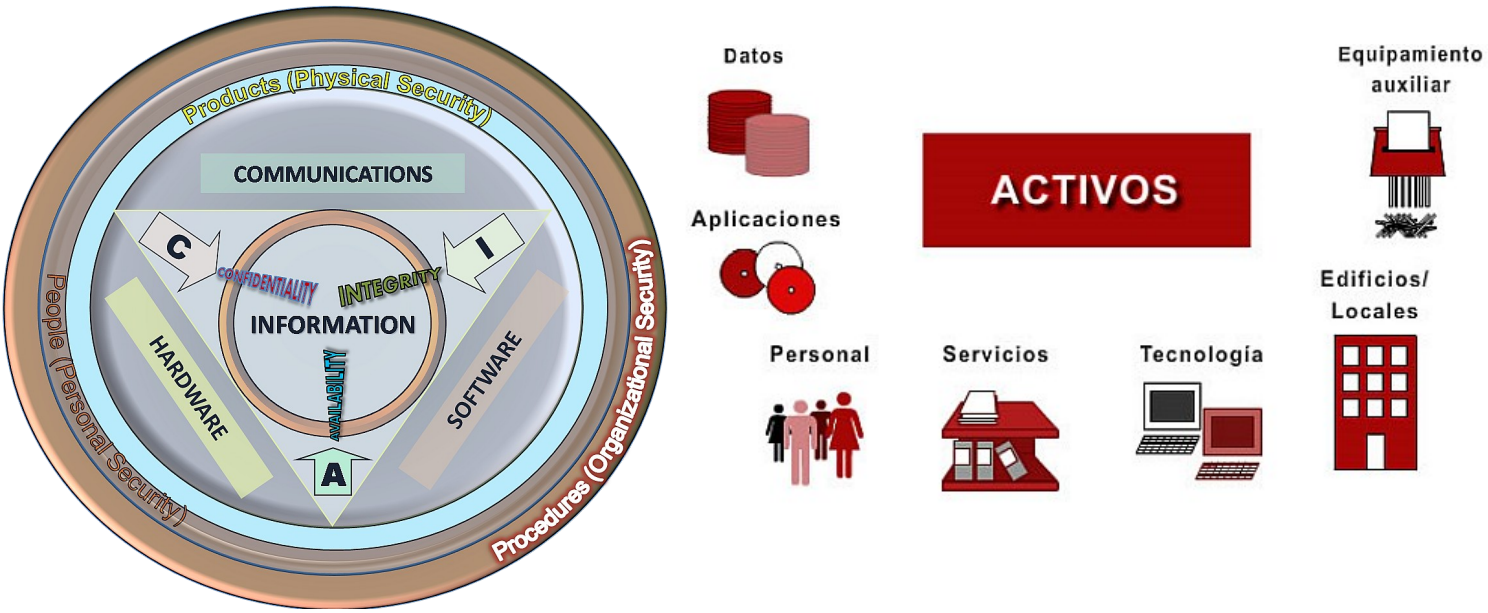
Al analizar que se hace cuando se protege un ordenador, un iPAD, un teléfono móvil, una infraestructura de comunicaciones o un servicio se llega a la conclusión que lo que en realidad se está haciendo, es proteger la información almacenada, enviada, transmitida y modificada en dichos servicios, infraestructuras o dispositivos.

La información es un activo; es decir, un elemento que tiene valor para las empresas. En torno a ella se crean y desarrollan procesos y tareas; sin la información, esas tareas y procesos, no sirven para nada o no pueden llevarse a cabo adecuadamente. En muchos casos, la información y su seguridad están directamente relacionadas con la supervivencia del negocio o el aseguramiento de ingresos:

- Fallos de energía eléctrica que imposibiliten acceder a la información.
- Robo o extravío de equipamiento con información (portátiles, PDAs, etc.).
- Venta de información interna a competidores.
- Ataque a sistemas informáticos con robo de información sobre clientes, con posible repercusión mediática y violación de legislación o normativa.
- Incendios donde se destruyan equipamiento, oficinas, etc.

Debido a su importancia, se busca la protección de la información, independientemente de su formato, localización, naturaleza, etc. Al hablar de Seguridad de la Información no hay por qué referirse a incidentes relacionados con el malware, el robo de información u otros incidentes de tipo tecnológico, sino que la información puede verse afectada también por un incendio, una inundación, un empleado descontento, etc.

La Seguridad de la Información se puede definir como la **protección de la confidencialidad, integridad y disponibilidad** de los activos de información[2] según sea necesario para alcanzar los objetivos de negocio de la organización.

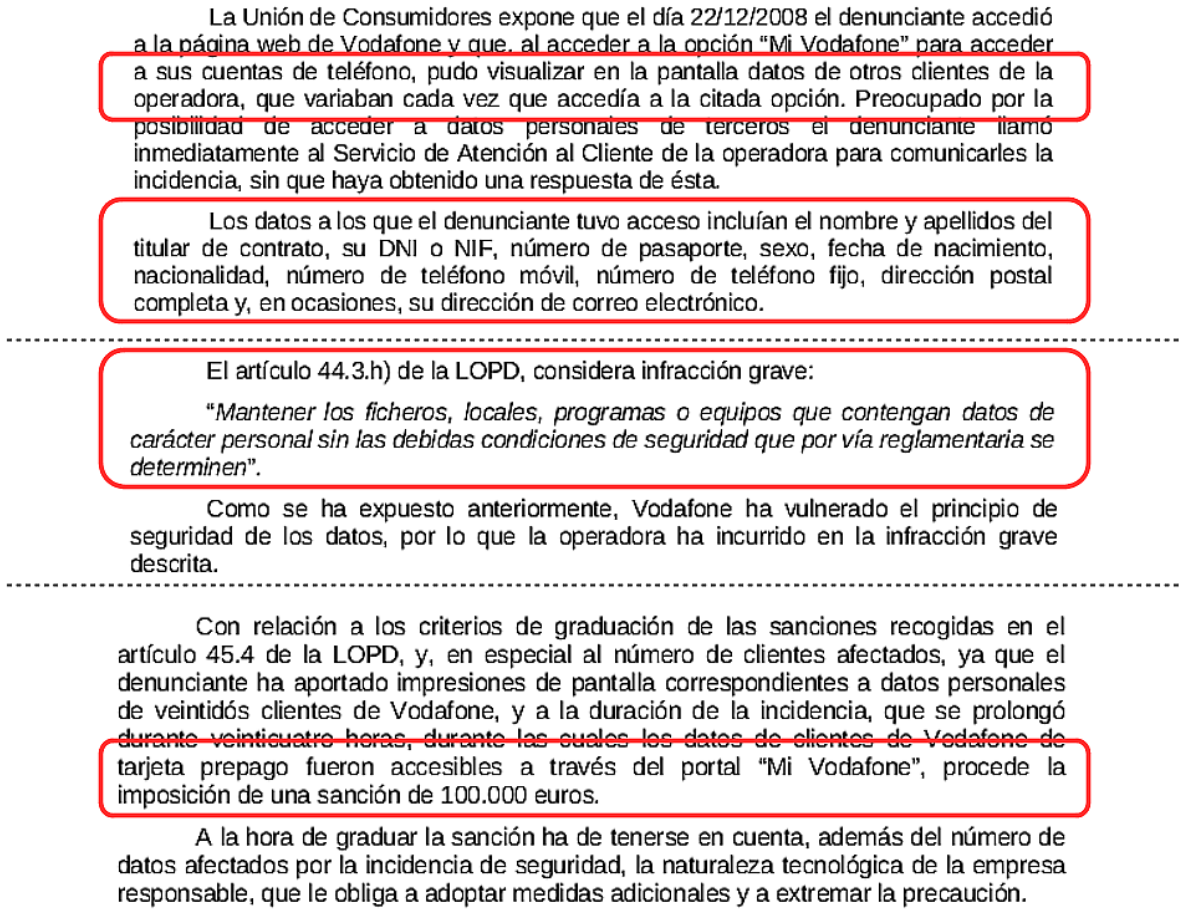


Es lo que se conoce como la triada C.I.A. por sus siglas en inglés: Confidentiality-Integrity-Availavility. Estos tres parámetros básicos de la seguridad se definen como:

- **Confidencialidad (*confidentiality*):**
  - A la información únicamente pueden acceder las personas autorizadas para ello.
  - La información se revela exclusivamente a los usuarios autorizados.

[2] Activos de información: los datos, los equipos, las aplicaciones, las personas, que se utilizan para crear, gestionar, trasmitir y destruir la información

- Para garantizar la confidencialidad hay que prevenir la divulgación de información a personas/sistemas no autorizadas.
- Si accediera a ella alguien de la competencia podría utilizarla para conseguir beneficios económicos, o bien denunciar a la organización ante la Agencia de Protección de Datos para que se le impusiera una multa si se demuestra que se vulneró la Ley de Protección de Datos de Carácter Personal, o publicarla en la prensa para dañar la imagen de la organización.



La Unión de Consumidores expone que el día 22/12/2008 el denunciante accedió a la página web de Vodafone y que, al acceder a la opción "Mi Vodafone" para acceder a sus cuentas de teléfono, pudo visualizar en la pantalla datos de otros clientes de la operadora, que variaban cada vez que accedía a la citada opción. Preocupado por la posibilidad de acceder a datos personales de terceros el denunciante llamó inmediatamente al Servicio de Atención al Cliente de la operadora para comunicarles la incidencia, sin que haya obtenido una respuesta de ésta.

Los datos a los que el denunciante tuvo acceso incluían el nombre y apellidos del titular de contrato, su DNI o NIF, número de pasaporte, sexo, fecha de nacimiento, nacionalidad, número de teléfono móvil, número de teléfono fijo, dirección postal completa y, en ocasiones, su dirección de correo electrónico.

El artículo 44.3.h) de la LOPD, considera infracción grave:

"*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen*".

Como se ha expuesto anteriormente, Vodafone ha vulnerado el principio de seguridad de los datos, por lo que la operadora ha incurrido en la infracción grave descrita.

Con relación a los criterios de graduación de las sanciones recogidas en el artículo 45.4 de la LOPD, y, en especial al número de clientes afectados, ya que el denunciante ha aportado impresiones de pantalla correspondientes a datos personales de veintidós clientes de Vodafone, y a la duración de la incidencia, que se prolongó durante veinticuatro horas, durante las cuales los datos de clientes de Vodafone de tarjeta prepago fueron accesibles a través del portal "Mi Vodafone", procede la imposición de una sanción de 100.000 euros.

A la hora de graduar la sanción ha de tenerse en cuenta, además del número de datos afectados por la incidencia de seguridad, la naturaleza tecnológica de la empresa responsable, que le obliga a adoptar medidas adicionales y a extremar la precaución.

Fig. Partes de una sanción impuesta por la AEPD [3]

- **Integridad (*integrity*):**
  - La información ha de estar completa y correcta en todo momento.
  - Se mantienen los datos libres de modificaciones no autorizadas. La información se modificada sólo por personal autorizado.
  - La integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
  - Si la información se corrompe, se podrían enviar cartas o facturas erróneas a los clientes, con la confusión y las quejas de los afectados que acarrearía, más el trabajo y el tiempo que habría que emplear para corregir los errores y restaurar a su estado correcto la información. Que la información permanezca íntegra en todo momento es más importante de lo que a primera vista pueda parecer.

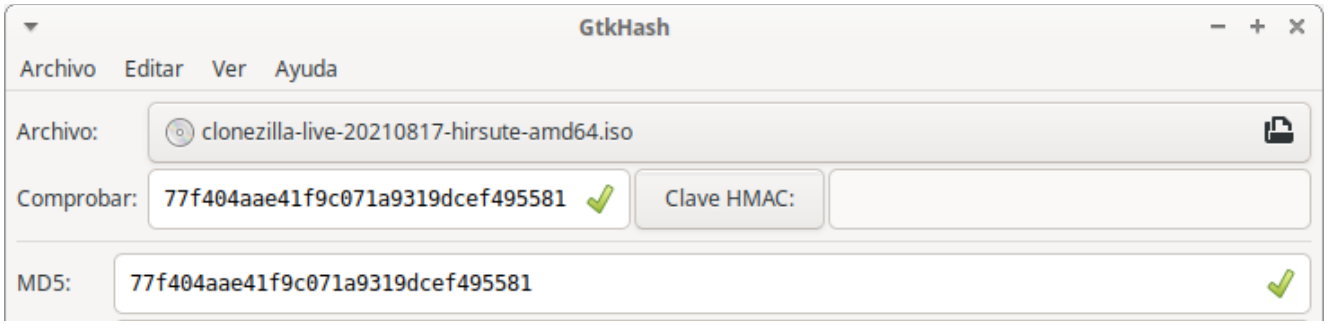


Fig. Comprobación de la integridad de un archivo usando MD5

[3]AEPD: Agencia Española de Protección de Datos - https://www.aepd.es/es

- **Disponibilidad (*availability*):**
  - La información estará lista para acceder a ella o utilizarse cuando se necesita.
  - Las personas/sistemas/aplicaciones pueden acceder a la información.
  - Para garantizar la disponibilidad hay que lograr que la información sea utilizable cuándo y cómo lo requieran los usuarios autorizados.
  - Si el equipo en que reside esta información se estropea y no se puede acceder a ella, simplemente no se puede funcionar, no se puede dar servicio, lo que implica que se deja de ganar dinero y en casos extremos se puede perder, si el cliente decide marcharse y adquirir el servicio en otro proveedor. Un fallo de disponibilidad tiene siempre un impacto económico directo en la organización, por leve que sea, ya que se deja de trabajar, hay una parte de la organización que ha parado, por lo que ha dejado de generar beneficio.

Un rayo tumbó parte de la nube de Amazon en Europa

"Un rayo que cayó en Dublín (Irlanda) puso los servicios de nube de Amazon Europa sin funcionar en domingo, y se esperaba que algunos clientes quedaran sin conexión hasta dos días.

Las fuentes de energía primaria y secundaria quedaron anuladas con el mismo rayo que cayó durante una intensa tormenta eléctrica el domingo 7 de agosto en la ciudad de Dublín, donde Amazon opera su centro de datos de la zona europea. El rayo causó que un transformador explotara, causando un incendio en la red de la compañía eléctrica que suministra luz a Amazon; pero ese mismo meteoro también fulminó los generadores de respaldo de la firma. Una 'desviación eléctrica', originada por el rayo, viajó por los cables y eliminó el sistema de control, que normalmente habría activado los generadores de respaldo del centro de datos, según informaron a los usuarios europeos los operadores de Amazon que trabajan en el Service Health Dashboards de la nube EC2.

El rayo también fulminó el data center de Microsoft que provee la suite de aplicaciones de su Business Productivity Online, de acuerdo con DataCenterKnowledge.com, sitio de operaciones de centros de datos."

Fig. Resumen de una noticia sobre una caída de servicio provocada por un rayo

Además de los anteriores también se habla de:

- **Autenticidad:**
  - La información es lo que dice ser o el transmisor de la información es quién dice ser.

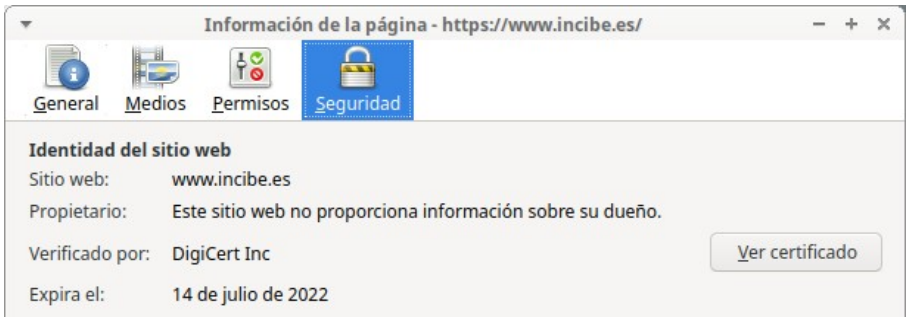


Fig. El uso de certificados digitales en https permite garantizar que el servidor es realmente el equipo con el que queremos hablar

- **Trazabilidad:**
  - Poder asegurar en todo momento quién hizo qué.
  - Poder asegurar en todo momento cuándo lo hizo.

```
/var/log/auth.log
Sep 20 12:40:39 x99 sudo:   manuel : TTY=pts/2 ; PWD=/home/manuel ; USER=root ; COMMAND=/usr/bin/apt update
Sep 20 12:40:39 x99 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 20 12:40:48 x99 sudo: pam_unix(sudo:session): session closed for user root
Sep 20 12:55:06 x99 sudo:   manuel : TTY=pts/2 ; PWD=/home/manuel ; USER=root ; COMMAND=/usr/bin/apt full-upgrade
Sep 20 12:55:06 x99 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Sep 20 12:55:07 x99 sudo: pam_unix(sudo:session): session closed for user root
```

Fig. Líneas del fichero de log `/var/auth/log` donde se registran los comandos ejecutados con `sudo`

Como asegura el Centro Criptológico Nacional[4], la seguridad absoluta es imposible de alcanzar ya que las medidas de seguridad a implementar deben ser proporcionales a los riesgos. Es necesario adoptar un compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada.

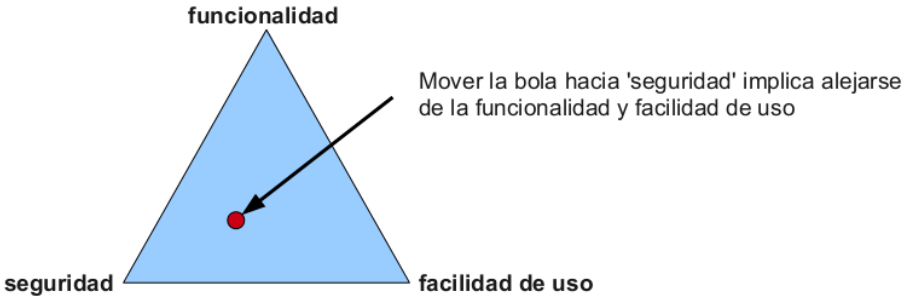


Fig. Seguridad frente a facilidad de uso y funcionalidades

4. Sistemas de Gestión de la Seguridad de la Información

La Seguridad de la Información tiene en cuenta la protección de la información desde tres varios puntos de vista: **técnico, organizativo, normativo y legal**. Por tanto, estamos protegiendo la información pero, además, lo hacemos desde varias facetas distintas, y para ello, necesitamos a su vez implementar medidas de tipo técnico, organizativo, normativo y legal.

Podemos tender a centrarnos únicamente en las medidas de tipo técnico; sin embargo, la experiencia nos dice que dejar de lado las medidas de tipo organizativo-normativo-legal es un error. Por ejemplo, analizando incidentes de seguridad aparece muchas veces el factor humano como culpable. Los ataques de ingeniería social son muy efectivos, a veces por la ingenuidad del usuario y otras por la ignorancia de buenas prácticas de seguridad y falta de concienciación. Cuanto más sofisticadas sean las tecnologías empleadas para proteger la información, más centrados estarán los ataques en explotar las debilidades del personal.

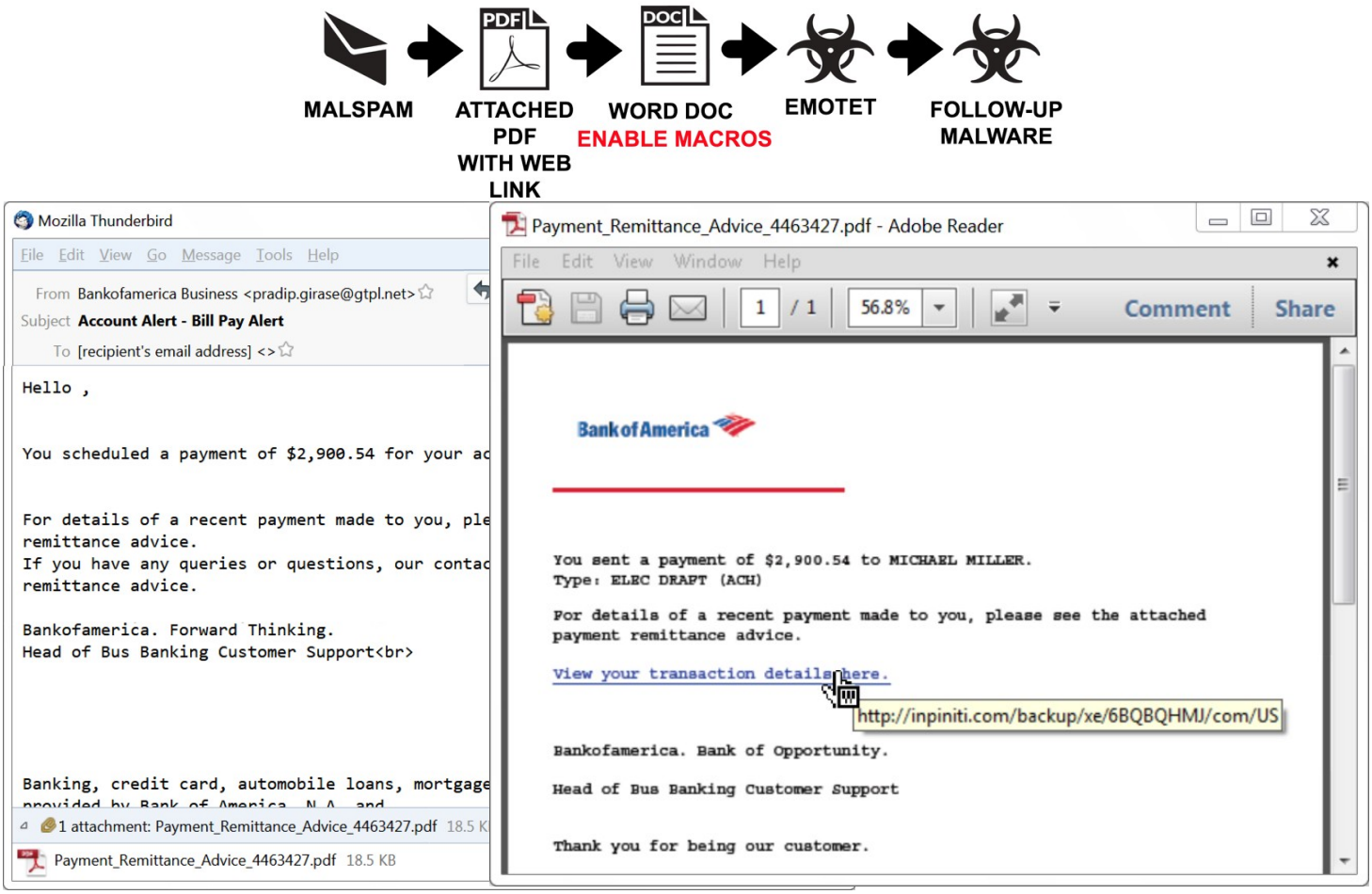


Fig. Cadena de infección del malware Emotet y ejemplo de mensaje y pdf con enlace a documento infectado

[4]CCN-Cert: Centro Criptológico Nacional - Organismo dependiente del Ministerio de Defensa - https://www.ccn-cert.cni.es/

La Seguridad de la Información se ha convertido en el enfoque de referencia actual ya que cuenta con una ventaja sobre los anteriores: dispone de **normas estandarizadas** que permiten la implantación de un **Sistema de Gestión de la Seguridad de la Información**. Seguir unos criterios, metodología y medidas estandarizadas facilita mucho la labor a la hora de aplicar e implementar la Seguridad de la Información.

El estándar más reconocido por las empresas es la **familia de normas ISO 27000**, destacando la **ISO 27001** y la **ISO 27002**, en donde se definen 14 capítulos de controles que contienen un total de 114 controles de seguridad. Se trata de una guía de buenas prácticas que describe objetivos de control y controles recomendables relativos a la seguridad de la información. A modo de ejemplo se ponen los puntos a considerar en el control 9. Control de accesos:

9. CONTROL DE ACCESOS.
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso.
9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.
9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

Resumiendo, la implementación de seguridad es un problema de ingeniería, un compromiso entre costes y facilidad de uso frente a protección. Se deben planificar y tener en cuenta los pasos siguientes:

1. Análisis de Riesgos: estudiar los riesgos posibles y valorar las consecuencias de los mismos sobre los activos (información).
2. Gestión de Riesgos: valorar las diferentes medidas de protección y decidir la solución que más se adecué a la organización (determinación del riesgo residual).
3. Política de Seguridad: adaptar operativa habitual de la organización a las nuevas medidas de seguridad.
4. Mantenimiento: observación continua de las medidas de seguridad, así como la adecuación de las mismas a la aparición de nuevas tecnologías.
5. Planes de Contingencia: determinación de las medidas a adoptar ante un incidente de seguridad.

5. Riesgos, amenazas y vulnerabilidades

Un análisis de riesgos permite estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Existen diversas metodologías para abordar de forma sistemática el análisis de riesgos, como la española MAGERIT, OCTAVE, ISO 27005, etc.

Asociados al análisis de riesgos aparecen los siguientes términos:

- **Vulnerabilidad:**
  - Existencia de agujeros o debilidades en el sistema o en alguna de las medidas de seguridad implementadas que podrían permitir o facilitar la actuación de una amenaza.
  - A modo de ejemplo, ordenadores sin antivirus o con antivirus desactualizados, ausencia de copias de seguridad, contraseñas de acceso débiles y que no se cambian, ausencia de control de cambios, usuarios sin formación, ...

- En general, una vulnerabilidad en un sistema se puede agrupar bajo uno de los siguientes apartados en función de su naturaleza:
  - Vulnerabilidad debido al uso incorrecto del sistema por parte de usuarios autorizados.
  - Vulnerabilidad debido a que no se controla el acceso al sistema.
  - Vulnerabilidad generada por procedimientos ineficaces.
  - Vulnerabilidad generada por averías o fallos en el hardware y software.
  - Vulnerabilidad intrínseca de los sistemas debido a su complejidad y desconocimiento de sus posibilidades o limitaciones.

- **Amenaza:**
  - Ocurrencia de uno o más acontecimientos de los que se deriva una situación en la que la información puede sufrir una pérdida de confidencialidad (acceso, difusión, observación, copiado, robo), integridad (modificar, sustituir, reordenar, distorsionar) o disponibilidad (destruir, dañar, contaminar, dejar fuera de servicio).
  - Las amenazas a los sistemas van desde desastres naturales tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos y virus, con un origen tanto interno como externo.
  - En función de su origen de la amenaza se clasifican en:
    - **Amenaza interna:** la que representa cualquier persona que esté asociada con el sistema o con su información produciendo un daño no intencionado (uso incorrecto, fallo humano o accidente) o la amenaza que representan personas deshonestas o de mala fe que ocasionan un daño intencionado a un sistema o a la información que contiene.
    - **Amenaza externa:** la que representan personas externas al sistema (p.e. hackers) produciendo un daño intencionado o no intencionado, que puede ser ocasionado por un acceso no autorizado a la información o por la introducción de software dañino.
    - **Amenaza física:** la que afecta a la existencia real y a la condición física de las instalaciones del sistema (robo de equipos, daños por fuego, inundaciones, sabotajes, desastres naturales, ...).
    - **Amenaza lógica:** relacionadas con el software que causa un mal funcionamiento en el sistema y que ha sido creado de manera intencionada o no. Por ejemplo, malware, ataques de denegación de servicio (DoS), ...

- **Impacto:**
  - Consecuencias de que la amenaza ocurra.
  - A modo de ejemplo, divulgación de información confidencial, retraso en la ejecución y la conclusión de actividades de negocio, pérdida de credibilidad frente a clientes, ...

- **Riesgo intrínseco:**
  - Cálculo del daño probable a un activo si se encontrara desprotegido.
  - Los riesgos indican la posibilidad de que se materialice o no una amenaza aprovechando las vulnerabilidades

- **Salvaguarda:**
  - Medida técnica, organizativa y/o legal que ayuda a paliar el riesgo.
  - A modo de ejemplo, guardias, control de acceso, cortafuegos, detectores de intrusos, antivirus, monitorización, auditorías, respaldo de seguridad, cursos de actualización de conocimientos, cursos de mentalización, sanciones, planes de contingencia, ...

- **Riesgo residual:**
  - Riesgo remanente tras la aplicación de salvaguardas. En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la Dirección.

Fig. Relación entre términos

6. Auditorías de seguridad, análisis de penetración y análisis forense.

Una **auditoría** es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones. Las auditorías deben realizarse de manera periódica y sus resultados han de quedar registrados y ser notificados a los responsables para que tomen las medidas oportunas.

En función de los objetivos y el alcance podemos encontrar varios tipos de auditoría; a modo de ejemplo:

- Auditoría legal del Reglamento de Protección de Datos.
- Auditoría de la seguridad física.
- Auditoría de seguridad interna.
- Auditoría de seguridad perimetral.
- Análisis de penetración (*Pentest*): evaluación de la seguridad de un sistema informático o red simulando un ataque procedente de un agente malicioso (Black Hat hacker o cracker).
- Auditoría de código de aplicaciones: revisión del código de las aplicaciones en busca de errores de programación que puedan comprometer la seguridad del sistema.

Las auditorías deben ser sistemáticas, por lo que se suele seguir alguna metodología, destacando COBIT (Objetivos de Control para Tecnologías de Información y relacionadas) y la norma ISO 27007 (guía para la realización de auditorías de un SGSI).

Un tipo especial de auditoría es el **análisis forense**; se trata, de un estudio exhaustivo de un sistema del que se quiere conocer su historia. Normalmente se aplica a sistemas de los que se tiene la sospecha o la certeza de que han sido víctimas de una intrusión, un ataque o se han utilizado para realizar alguna acción maliciosa. El analista forense tratará de responder a cuestiones como:

- ¿En qué momento exacto se ha producido la intrusión o actuación maliciosa?.
- ¿Quién ha sido el sujeto que realizó la acción?.
- ¿Qué metodología ha seguido?.
- ¿Cuál es el alcance del incidente?¿Qué daños y modificaciones ha producido el sujeto en el sistema?.

Además, el informe del forense debe indicar que medidas se deben tomar para solventar el incidente y que medidas se deben adoptar para evitar que se repita. En base a lo anterior, la organización podrá depurar responsabilidades e incluso, tomar medidas legales; motivo por el cual, es muy importante el proceso de recogida de evidencias y su posterior preservación.

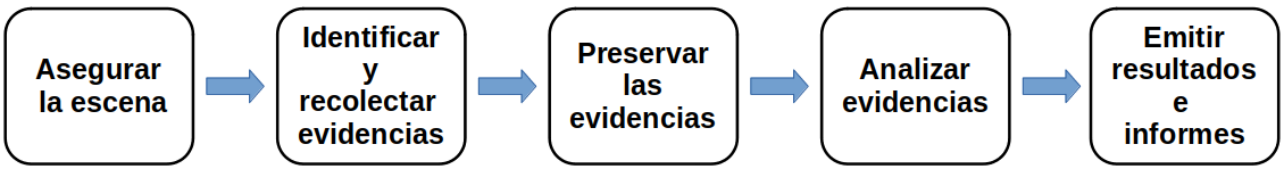


Fig. Análisis forense digital

7. Clasificación/Taxonomía de los ciberincidentes

Como los ciberincidentes no poseen las mismas características ni la misma peligrosidad, es necesario disponer de una taxonomía de los ciberincidentes, lo que ayudará posteriormente a su análisis, contención y erradicación. El trabajo de diversas organizaciones internacionales ha sido adoptado por el Incibe y clasifica los incidentes en:

- **Contenido abusivo**
  - **SPAM**: correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
  - **Delito de odio**: contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
  - **Pornografía infantil, contenido sexual o violento inadecuado**: material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
- **Contenido dañino**
  - **Sistema infectado**: sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.

  - **Servidor C&C (Command and Control)**: conexión con servidor de Mando y Control (C&C o C2) mediante malware o sistemas infectados.
  - **Distribución de malware**: recurso usado para distribución de malware. Ejemplo: recurso de una organización empleado para distribuir malware.
  - **Configuración de malware**: recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de webinjects para troyano.
  - **Malware dominio DGA**: nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).
- **Obtención de información**
  - **Escaneo de redes (scanning)**: envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.
  - **Análisis de paquetes (sniffing)**: observación y grabación del tráfico de redes.
  - **Ingeniería social**: recopilación de información personal sin el uso de la tecnología. Ejemplos: mentiras, trucos, sobornos, amenazas.
- **Intento de intrusión**
  - **Explotación de vulnerabilidades conocidas**: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ejemplos: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
  - **Intento de acceso con vulneración de credenciales**: múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.
  - **Ataque desconocido**: ataque empleando exploit desconocido.
- **Intrusión**
  - **Compromiso de cuenta con privilegios**: compromiso de un sistema en el que el atacante ha adquirido privilegios.
  - **Compromiso de cuenta sin privilegios**: compromiso de un sistema empleando cuentas sin privilegios.
  - **Compromiso de aplicaciones**: compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.
  - **Robo**: intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.
- **Disponibilidad**
  - **DoS (Denegación de Servicio)**: ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
  - **DDoS (Denegación Distribuida de Servicio)**: ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
  - **Sabotaje**: sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.
  - **Interrupciones**: interrupciones por causas externas. Ejemplo: desastre natural.
- **Compromiso de la información**
  - **Acceso no autorizado a información**: acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
  - **Modificación no autorizada de información**: modificación no autorizada de información. Ejemplos: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
  - **Pérdida de datos**: pérdida de información. Ejemplos: pérdida por fallo de disco duro o robo físico.
- **Fraude**
  - **Uso no autorizado de recursos**: uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ejemplo: uso de correo electrónico para participar en estafas piramidales.

- **Derechos de autor**: ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez.
- **Suplantación**: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
- **Phishing**: suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

- **Vulnerable**
  - **Criptografía débil**: servicios accesibles públicamente que pueden presentar criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.
  - **Amplificador DDoS**: servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.
  - **Servicios con acceso potencial no deseado**: servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.
  - **Revelación de información**: acceso público a servicios en los que potencialmente pueda revelarse información sensible. Ejemplos: SNMP o Redis.
  - **Sistema vulnerable**: sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
- **Otros**
  - **Otros**: todo aquel incidente que no tenga cabida en ninguna categoría anterior.
  - **APT**: ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.
  - **Ciberterrorismo**: uso de redes o sistemas de información con fines de carácter terrorista.
  - **Daños informáticos PIC**: borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una infraestructura crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.