Tema 4

Conceptos de seguridad de los sistemas de información. Seguridad física. Seguridad lógica. Amenazas y vulnerabilidades. Infraestructura física de un CPD: acondicionamiento y equipamiento. Sistemas de gestión de incidencias. Control remoto de puestos de usuario.

Guion-resumen

1. **Introducción**
2. **Conceptos de seguridad de los sistemas de información**
   - 2.1. Planificación de la seguridad
   - 2.2. Elaboración de planes
3. **Seguridad física**
   - 3.1. La identificación personal
   - 3.2. Técnicas biométricas
4. **Seguridad lógica**
   - 4.1. Subestados de la seguridad de la información
   - 4.2. Métodos de protección
5. **Amenazas y vulnerabilidades**
   - 5.1. Amenazas y vulnerabilidades físicas
   - 5.2. Amenazas y vulnerabilidades lógicas
   - 5.3. Catástrofes
6. **Infraestructura física de un CPD: acondicionamiento y equipamiento**
   - 6.1. Diseño de un CPD
   - 6.2. Implementación de un CPD
7. **Sistemas de gestión de incidencias**
   - 7.1. Tipología de incidencias. Niveles de urgencia.
   - 7.2. Marco normativo
   - 7.3. Acuerdos de nivel de servicio
   - 7.4. Herramientas y soluciones de gestión de incidencias
8. **Control remoto de puestos de usuario**

1. Introducción

Antes de abordar el estudio de los conceptos de seguridad habituales sobre sistemas de información, hay que definir conceptos de seguridad un poco más generales, como son los de activo, riesgo o vulnerabilidad.

Por activo se entiende aquello que debe protegerse. En general es información, pero también se refiere a personas e infraestructuras. La información destaca como activo, porque de ella puede depender la existencia o el colapso de una organización.

Por amenaza se entiende aquello que puede causar un mal.

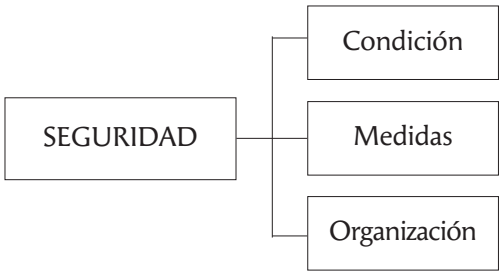
Por vulnerable se entiende algo a lo que se puede amenazar, sobre lo que se puede proyectar un daño.

Por riesgo se entiende la contingencia o proximidad de un daño, que causa impacto.

La relación entre los cuatro conceptos sería, un activo sometido a amenazas, es vulnerable y entonces supone un riesgo. Expresado en forma negativa: un activo vulnerable, que no cause impacto no constituye un riesgo.

A pesar de la importancia de la seguridad, es curioso que las pérdidas asociadas a fallos de seguridad crezcan debido a causas internas, en particular el uso que las personas hacen de los sistemas e información. Estos serán objeto de la seguridad, intentando garantizar, en la medida de lo posible, confidencialidad, integridad y disponibilidad. Al hablar de seguridad se aceptan, de forma genérica, tres grandes significados del término:

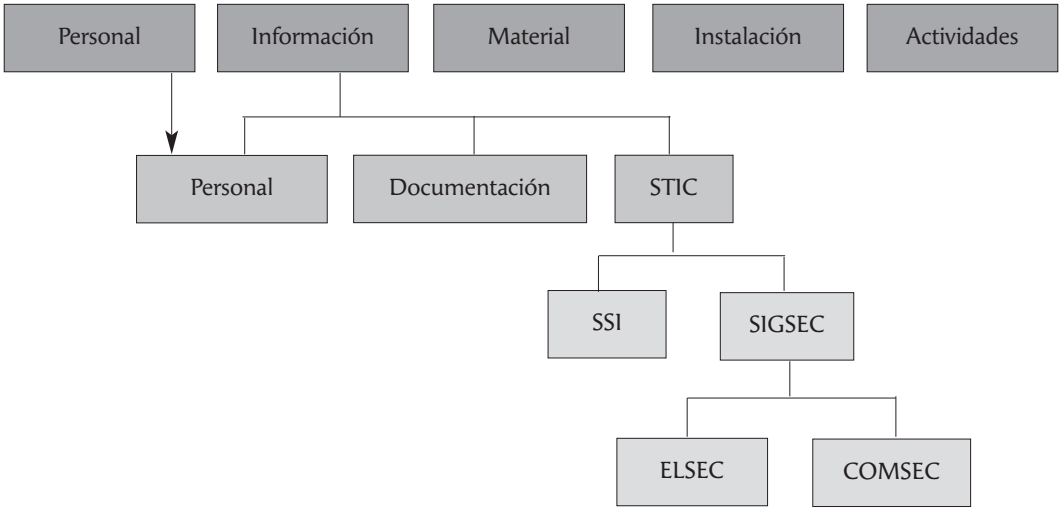
1. Condición alcanzada por un activo al protegerlo de forma adecuada.
2. Conjunto de medidas de protección.
3. organización que proporciona esa condición.



También se acepta que el objetivo de la seguridad es proteger activos y actividades. Según el tipo de activo a proteger, se usan los términos de seguridad del personal, de información, material, de las instalaciones y las de operaciones. Referida a la información, esta puede existir en las personas, en la documentación o en sistemas TIC, acuñándose entonces el término STIC (Seguridad TIC).

La seguridad del personal se repite, a un primer nivel y como dependiente de la seguridad de la información.

Esto se debe a que son dos aspectos los que se cubren, la protección personal, en especial la física y la protección personal, en cuanto a información que se maneja, lo que implica aspectos como habilitaciones, necesidad de conocer o concienciación.



La seguridad de los sistemas de información es una tarea muy compleja. Existen numerosas aproximaciones, clasificaciones y metodologías que buscan facilitar la tarea a los responsables en las organizaciones.

Un ejemplo lo constituye la propuesta de una de las entidades españolas más prestigiosas en materia de seguridad: el Centro Criptográfico Nacional (CCN). En una de sus guías de referencia se establece que la seguridad TIC (STIC) se refiere a la protección de la información en los sistemas de información (SSI) y la de las señales (SIGSEC). La seguridad de las señales, a veces distingue entre la seguridad electrónica (ELSEC) y la de los sistemas de comunicaciones (COMSEC). La ELSEC se aplica a sistemas que no son de comunicaciones como sensores o sistemas de navegación. Esta distinción se debe al establecimiento de un paralelismo con la terminología de inteligencia, que identifica la inteligencia de señales (SIGINT) y distingue la inteligencia de comunicaciones (COMINT) e inteligencia electrónica (ELINT).

Según la definición del término STIC, la seguridad de la información y sistemas que la tratan puede conseguirse protegiendo cada recurso que compone su configuración. Así, las medidas de seguridad, en función del objeto protegido, se pueden clasificar en:

— **TRANSEC.** Aseguran los canales de transmisión (seguridad de las transmisiones).

— **COMPUSEC.** Protegen el proceso automático de datos (seguridad de equipos).

— **EMSEC.** Protegen frente a emisión de radiaciones no deseadas (seguridad de las emisiones).

— **NETSEC.** Protegen los elementos de red (seguridad de las redes).

— **CRYPTOSEC.** Protegen la información con criptografía (seguridad criptológica).

Conviene señalar que el término NETSEC está relacionado con la protección de las redes contra la modificación, destrucción o revelación de la información mientras circula por ellas, diferenciándose así del término TRANSEC, vinculado este último con la prevención contra la obtención de información por medio de la interceptación, radiolocalización y análisis de las señales electromagnéticas.

2. Conceptos de seguridad de los sistemas de información

La seguridad de los sistemas de información podría definirse como su capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas que comprometan la confidencialidad, integridad, disponibilidad y autenticidad de la información y servicios que se gestionan.

La confianza es la esperanza que se tiene en alguien o algo. Por tanto confiar es dar esperanza a alguien de que conseguirá lo que desea.

La seguridad entonces puede entenderse como las acciones orientadas a eliminar los riesgos o sus consecuencias, el impacto. Se establecen tres planos de actuación, la defensa, orientada a disminuir la probabilidad de incidentes, el aseguramiento, que pretende disminuir las consecuencias al producirse un incidente y la denuncia o identificación de causas o causantes de los daños.

Como se observa, la definición de seguridad tiene sus matices, pero como idea general, puede resumirse en garantizar la confidencialidad, la integridad, disponibilidad y no repudio de la información (autenticidad).

Las tres primeras características se conocen en conjunto como medidas CIA, por sus siglas inglesas, *Confidentialy, Integrity, Availability.*

— **Confidencialidad.** Se refiere a la situación en que solo aquellos entes autorizados tengan acceso a la información que necesiten. Su fundamento es claro, por ejemplo en el caso de un secreto industrial, ya que no es deseable que la competencia tenga acceso a cierta información.

— **Integridad.** Es el aspecto de seguridad que intenta garantizar que determinada información no sea modificada. Sea una transferencia bancaria. Si un intruso, sin conocer la información que se intercambia, es capaz de modificarla puede generar un riesgo, ya que no es lo mismo realizar una transferencia por un importe, que por otro, por ejemplo, muy elevado. La disponibilidad es la característica que garantiza que la información estará presente siempre que se requiera.

— **Disponibilidad.** Esta característica garantiza que la información se encuentre disponible cuando se requiere y en la forma requerida por los usuarios que estén autorizados.

— **Autenticidad (o No-Repudio).** Característica que asegura la identidad u origen, es decir, la garantía que demuestra que alguien que genera una información, no podrá retractarse de su acción. El ejemplo típico, es el de una transacción en que se compran acciones en bolsa. Si las acciones se desploman, debe garantizarse que el emisor de la información no niegue la orden de compra.

Puede decirse que son tres los componentes a proteger: hardware, software e información. El acceso a la información se realiza a través del hardware, lo que implica al mundo físico, objeto de estudio de la seguridad física, y a través del software, eje de la seguridad lógica. Con la protección del hardware y el software, se persigue la protección de la información, aunque esta incluye otros aspectos.

La información, como intangible, en general no es directamente valorable. Si falla el hardware, por ejemplo, puede estimarse casi instantáneamente qué pérdida se sufre. De igual forma con el software, con matices. Pero la pérdida de información, no siempre es cuantificable, y menos si atiende a la dignidad de las personas.

Teniendo en cuenta los activos a proteger y los tipos de amenazas que existen se concluye que la seguridad no es un producto que pueda comprarse e instalarse a modo de antivirus. Debe ser entendida como un proceso continuo que requiere una monitorización y actualización permanente. Esta filosofía desemboca en la definición de unas políticas de seguridad, que se basará en una serie de normas y prácticas que los responsables de seguridad de la empresa deberán implementar y cuidar de su operación diaria, estableciendo los procedimientos y rutinas que se consideren necesarios.

Para dotar a un sistema de cierto grado de seguridad, deben implementarse servicios orientados a garantizar ciertas condiciones. Estos servicios se condensan en el modelo CIA. Pero, hay que tener en cuenta otros servicios de seguridad, como son los siguientes.

— **Trazabilidad.** Asegura que se podrá determinar quién hizo qué y en qué momento.

— **Autenticación.** Garantiza que la identidad (persona o sistema) del origen es legítima.

— **Autorización.** Es el servicio que controla el acceso de un ente a un servicio.

— **Anonimato.** Puede requerirse en algún servicio. No entrará en conflicto con otros.

— **Referencia temporal.** Provee características de seguridad con marcas temporales.

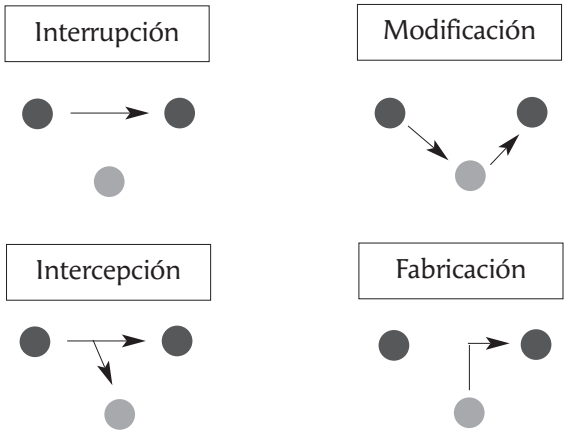
— **Terceros de confianza.** Para garantizar la identidad de las partes puede recurrirse a un tercero de confianza, que las avala mediante certificados.

En cualquier caso, se puede convenir que los cuatro servicios de seguridad que de algún modo engloban al resto son los de confidencialidad, integridad, disponibilidad y autenticidad. Los servicios pueden clasificarse según se refieran al dominio interno o externo de una organización.

Así, los servicios de seguridad en el dominio interno deben proveer control de acceso físico y lógico. Este último incluye la gestión de los sistemas de autenticación y autorización y sistemas de defensa perimetral.

Los servicios de seguridad para la protección de activos en un dominio externo, se refiere a la protección de la información en tránsito.

Para su estudio, se distinguen 4 tipos de ataque: interrupción, interceptación, modificación y fabricación.



Un ataque de interrupción es el que se materializa en la pérdida de una parte del sistema. Un ataque de interceptación es en el que un intruso consigue acceso a un elemento del sistema, al que lógicamente no estaba autorizado. Un ataque de modificación es el que consigue modificar un elemento del sistema y un ataque de fabricación sería una modificación no destructiva en que se persigue que el sistema trabaje de forma similar o sin levantar sospechas, pero habiéndose cambiado alguna parte del objeto final del mismo.

Los métodos de defensa incluyen contramedidas, teniendo en cuenta que no se pueden implantar salvaguardas para disminuir la vulnerabilidad, ya que es imposible asegurar físicamente los medios de transmisión y es necesario asumir que toda comunicación puede ser manipulada. La única salvaguarda posible es disminuir el impacto. Por un lado, debe garantizarse que aunque escuche la comunicación, el atacante no la entiende y que si cambia algo, el autor legítimo se percate de ello.

Los métodos de defensa se basan en algoritmos criptográficos aplicados a las comunicaciones. Cubren dos aspectos, el cifrado, para asegurar la confidencialidad y la firma, para asegurar la integridad.

En definitiva, la seguridad de los sistemas de información es un reto. Destaca el aspecto de la conectividad a redes públicas, como Internet, fuera del control de una organización. La seguridad absoluta, del 100%, ha de definirse como imposible de alcanzar. Por tanto, resulta que la seguridad es proporcional al coste de las medidas de protección y, por tanto, se opone a los sistemas abiertos, sin ningún tipo de protección, que pretenden facilitar el acceso a cualquier usuario.

Así, la implementación de seguridad se convierte en un problema de ingeniería, un compromiso entre costes, funcionalidad y protección. Es más que conveniente implantar la seguridad por niveles. Por tanto, hay que planificar y tener en cuenta aspectos como el análisis de riesgos (estudio y valoración del impacto), su gestión (valoración de los controles que reducen el riesgo), establecer una política de seguridad (adaptación de la operativa habitual a medidas de seguridad), mantenimiento (control continuo de la eficiencia de las medidas) y establecer planes de contingencia (respuesta ante incidentes de seguridad).

2.1. Planificación de la seguridad

Al enfrentarse a un problema suele ser bueno establecer una estrategia. Y, en general, la estrategia comienza con la planificación.

La planificación de la seguridad debe evaluar el nivel de riesgo tolerable para la información para establecer el compromiso coste/beneficio que supone su impacto. Hay que considerar:

— Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).

— Identificar las aplicaciones de alto riesgo.

— Cuantificar el impacto en el caso de suspensión del servicio en las aplicaciones de alto riesgo.

— Formular las medidas de seguridad necesarias para el nivel de seguridad requerido.

La justificación del costo de implantar las medidas de seguridad para clasificar el riesgo debe responder a las preguntas de qué ocurriría en caso de caída del sistema. Si un riesgo implica la paralización total de la actividad, es indicativo de estar ante un sistema de alto riego.

La siguiente pregunta sería qué tiempo máximo podría aguantar la organización sin el sistema en estudio, qué alternativas se contemplan y qué problemas implican y qué procesos se establecen en caso de emergencia.

Una vez definido el grado de riesgo, hay que elaborar una lista de sistemas con las medidas preventivas a tomar y las correctivas en caso de materializarse, según prioridad. Para clasificar una instalación en términos de riesgo se debe:

— **Clasificar la información.** Y los programas que manejan información estratégica de la organización, así como la de difícil recuperación.

— **Valorar la información que contiene.** En particular si la organización podría sobrevivir a una gran pérdida de esa información.

Para cuantificar el riesgo es necesario efectuar entrevistas con la alta dirección afectada directamente por un riesgo y evaluar el impacto de la situación potencial. Para evaluar las medidas de seguridad se debe especificar la aplicación, programas y archivos; las medidas de mitigación en caso de desastre, pérdida total, abuso y los planes necesarios; y las prioridades de las acciones a corto y largo plazo.

En cuanto a la división del trabajo, al menos se deben evaluar precauciones que dependerán del riesgo que suponga la información y del tipo y tamaño de la organización. Así, en principio, el personal que prepara la información no debe tener acceso a la operación; los analistas y programadores no deben tener acceso al área de operaciones y viceversa y los operadores no debieran tener acceso sin restricciones a bibliotecas ni código fuente o ubicaciones en que residan los archivos almacenados. Es importante separar las bibliotecas de las funciones de operación.

Los operadores no deben ser los únicos que tengan control sobre los trabajos procesados y no deben hacer las correcciones de los errores detectados. Al implantar sistemas de seguridad puede reducirse la flexibilidad en el trabajo, pero no debe reducirse la eficiencia.

En todas las actividades existe un riesgo aceptable. Es necesario analizar y entender los factores de riesgo para establecer procedimientos que permitan en caso de materializarse, reparar o minimizar el impacto reanudando las operaciones lo antes posible.

2.2. Elaboración de planes

La normativa ISO define el riesgo tecnológico como la probabilidad de que ocurra una amenaza utilizando vulnerabilidades existentes en los sistemas

o información de una organización generando daños. Existen numerosas formas de enfrentarse al riesgo. Una de ellas se basa en el Plan de Prevención de Riesgos Laborales que contiene los siguientes puntos:

— **Prevención**, el objetivo es identificar qué se desea proteger así como las soluciones para protegerlo. El Plan de Prevención se realiza a través de un Análisis de Riesgos. Este trata de cuantificar la probabilidad de que sucedan hechos problemáticos, la valoración económica de su impacto y contrastará el coste de la protección con el coste de volver a crear o adquirir los activos perdidos.

— **Seguridad**, es la fase de implementación, aquí lo importante es cómo se protege. El Plan de Seguridad debe contemplar toda la infraestructura *TIC* y la información de la organización. El responsable de su elaboración es el director de informática o el perfil equivalente. Este plan contendrá protocolos y mecanismo de actuación, herramientas, tecnología, asignación de tareas y responsabilidades, etcétera. Es vital que todas estas actuaciones se basen y cumplan el marco jurídico vigente (Código penal, *LOPD, LSSICE*, etcétera).

— **Contingencia**, una vez asumido que los sistemas pueden fallar o ser atacados, es imprescindible contar con los protocolos de actuación ante este tipo de situaciones. En este punto se trata de qué hacer cuando falla la seguridad. El Plan de Contingencias es una consecuencia del Análisis de Riesgos. Prevé las acciones y actuaciones a realizar en estos casos. El Plan de Contingencias incluye un Plan de Recuperación de Desastres (en inglés, *Disaster Recovery*), cuyo objetivo es la recuperación inmediata del servicio minimizando daños y costes a la organización.

Existen otras formas para nombrar a estos planes, cada organización puede contar con su propia nomenclatura: Planes de Emergencias, Planes de Prevención y Evacuación, etcétera.

Las organizaciones cuentan con la ayuda de metodologías que les permitirán aproximarse a la evaluación de las medidas necesarias para proteger los activos TIC. Algunos ejemplos son:

— **Metodología de análisis de riesgo BAA**. Realiza una clasificación de los datos en función de las variables **B**eneficio, **A**ccesibilidad y **A**nonimidad para el atacante. Esta metodología pondera el riesgo e identifica la información que por orden de prioridad requiera más protección.

— **Metodología de análisis de riesgo por colores**. Determina el nivel de riesgo a través de la utilización de códigos de colores. Es una metodología cualitativa y puede ser utilizada en organizaciones, industrias y todo tipo de instalaciones.

— **Metodología *MAGERIT*** (Metodología formal de Análisis y Gestión de Riesgos de los Sistemas de Información). En líneas generales, se encarga del análisis de riesgos que pueden comprometer un sistema de información y la recomendación de las medidas apropiadas para reducir y

controlar los riesgos obtenidos, de forma que se reduzcan al mínimo los posibles perjuicios. Cuenta con una herramienta que realiza la implantación, *PILAR* (Procedimiento Informático Lógico para el Análisis de Riesgos). La herramienta calcula los riesgos e incorpora salvaguardas para reducir el riesgo a valores aceptables.

3. Seguridad física

La seguridad física abarca el conjunto de medidas para proteger personas e instalaciones frente a daños eventuales. Las instalaciones incluyen edificios y equipos. Entre los daños se consideran los desastres naturales (incendios, etc.), la presencia de intrusos, accidentes y similares.

La ubicación y la protección física de los sistemas de información son tareas que conviene planificar cuidadosamente teniendo en cuenta aspectos como sus características, su importancia y su valor. El análisis de estos factores determinará su ubicación. Lo más común es agruparlos en un lugar especialmente acondicionado, el Centro de Proceso de Datos, CPD.

Una adecuada seguridad física debe proteger el entorno con medidas como personal de seguridad, dependencias seguras, etc. que suelen agruparse en la llamada seguridad perimetral. Es habitual que el personal encargado de la seguridad establezca guardias que permitan el control e identificación de personas o de vehículos.

Algunas precauciones relativas a la seguridad física que se deben tener en cuenta y revisar en una organización son:

— Comprobar que no sea posible el acceso a dependencias críticas a personas no autorizadas.

— En las instalaciones críticas se debe disponer de equipos de alimentación ininterrumpida (*SAI* o *UPS, Uninterruptible Power Supply*, en inglés), para servidores y equipos de red.

— Se dispondrá de detectores de humo que indiquen la posible presencia de fuego.

— Los conductos de aire acondicionado deben estar limpios, ya que el polvo es causa frecuente de averías.

— En cuanto a los extintores, se debe revisar el número de estos, su capacidad, fácil acceso, peso y tipo de agente extintor. Es frecuente disponer de extintores, pero no estar revisados, según la periodicidad prevista. O tengan un acceso difícil o mala señalización.

— El agente usado en los extintores debe ser tal que no cause un perjuicio mayor a las máquinas (extintores líquidos) o que provoquen gases tóxicos. Es decir, debe ser adecuado a la incidencia para la que se dispone.

— Se debe verificar que el personal sabe usar los equipos contra incendio y que haya prácticas o simulacros de uso y comportamiento.

— Por fin, comprobar también que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos a través de las mismas.

3.1. La identificación personal

La seguridad de las dependencias de los equipos críticos de la organización suele incluir controles de acceso físico. En todo proceso de identificación de acceso personal siempre habrá que establecer un equilibrio entre el valor de lo protegido, las posibles amenazas a las que se expone, la respuesta de las personas y el coste económico de su implantación y mantenimiento.

El modelo de identificación personal se basa en los siguientes indicadores de identidad:

— **Conocimiento**, todo elemento del que una persona tiene noción, por ejemplo un nombre de usuario o una contraseña de acceso.

— **Posesión**, todo elemento de lo que dispone una persona para lograr una acceso, por ejemplo una tarjeta.

— **Característica**, toda cualidad que tiene una persona y que puede ser verificada, por ejemplo su huella dactilar.

Cada indicador permitirá el establecimiento de estrategias para realizar un proceso de identificación personal

3.2. Técnicas biométricas

El diccionario de la Real Academia Española (RAE) define la biometría como el estudio mensurativo o estadístico de los fenómenos o procesos biológicos.

Las técnicas biométricas hacen uso de características biológicas, propias de un individuo como lo es la voz o la huella dactilar. Cuando ese estudio utiliza técnicas matemáticas y tecnologías de la información y comunicación (TIC), hablamos de biometría informática.

Las características biológicas se comparan con un patrón conocido y guardado en una base de datos y si coinciden con el candidato a acceder, se estima que es quien dice ser.

Existen dos tipos de biometría:

— **Fisiológica**. Basada en la obtención de datos y medidas de partes del cuerpo humano, por ejemplo la mano, las huellas dactilares, el rostro, el iris, la retina o la voz.

— **Conductual**, basada en las medidas y datos de las acciones de una persona, por ejemplo la firma o el uso de un teclado.

Todos los sistemas biométricos tienen en común que realizan procesos de:

— Captura, leyendo los datos presentados.

— Extracción, determinando las características relevantes en función del tipo de sistema.

— Comparación de los datos obtenidos los almacenados previamente en bases de datos.

— Decisión, el sistema ha de ser capaz de afirmar que el usuario es quien dice ser.

Algunas de las técnicas biométricas que se emplean actualmente son:

— **Reconocimiento de huellas dactilares.** Se base en el hecho de que no existen dos huellas dactilares iguales. Cada huella posee un conjunto de características (ángulos, arcos, remolinos, bucles, etcétera) denominadas minucias. Está comúnmente aceptado que cada persona posee más de treinta minucias y que dos personas no tienen más de ocho minucias iguales, de ahí que el sistema se considere como muy seguro. Los dispositivos que se utilizan para el reconocimiento analizan cada minucia y su posición relativa para realizar la comprobación. Similar al reconocimiento de la palma de la mano.

— **Reconocimiento de voz.** El usuario pronuncia una información prefijada o una frase propuesta por el sistema para que el usuario la repita. El sistema grabará su voz y analizando sus características (como la entonación o el timbre) será capaz de reconocerla en el caso de petición de acceso.

  La tecnología de reconocimiento lo puede hacer de las siguientes formas:

  - Dependencia, el sistema siempre solicita que se repita la misma frase.
  - Texto aleatorio, el sistema solicita textos diferentes de forma aleatoria.
  - Independencia del texto, el sistema acepta cualquier frase pronunciada.

  Puede deducirse que un problema de este sistema es la gran influencia de factores externos como el ruido o propios de la persona que puedan provocar un cambio en su voz (una afonía, el estado de ánimo, envejecimiento, etcétera). Suele utilizarse para accesos remotos.

— **Reconocimiento facial.** Se analiza el rostro del usuario con técnicas gráficas. Es común el uso de cámaras de baja resolución para la obtención de las características del rostro. Este sistema se enfrenta al problema de las condiciones de luz o a la del cambio de fisionomía de la persona (por barba, joyas, maquillaje, etcétera). Suele utilizarse en entornos de seguridad no muy estricta o combinado con otros métodos.

— **Reconocimiento de firma.** El usuario firma sobre una superficie, se analiza y se establece el patrón de reconocimiento. Se graban las características de la firma (presión, orientación, inclinación, etcétera) sobre un papel o tableta. Se analiza el movimiento, no la imagen de la firma. Está comúnmente aceptado en transacciones financieras y firma de comprobantes de compras.

— **Reconocimiento de patrones oculares.** El sistema obtiene una imagen y la compara con un patrón almacenado. Son muy seguros puesto que la posibilidad de coincidencia entre dos cientos millones de iris es prácticamente cero.

  Suelen existir dos posibles formas de reconocimiento:

  • Reconocimiento del iris, el sistema mide el patrón de las venas en el fondo del ojo. Se realiza proyectando una luz infrarroja a través de la pupila.

  • Reconocimiento de la retina. Mediante el uso de una videocámara, se examinan los patrones únicos de los surcos de la parte coloreada de los ojos.

    Una de las dificultades de este sistema puede ser la negativa de las personas a ser objeto de un examen de iris, pues es posible descubrir enfermedades que los afectados deseen mantener en privado. Suele utilizarse en entornos de máxima seguridad.

— **Reconocimiento vascular.** La piel humana es también un signo que identifica a un individuo. Se toma con una cámara una imagen infrarroja de las venas y se fabrica un mapa de su distribución. Presenta un 99% de éxito en un tiempo muy rápido. Actualmente se utiliza en cajeros automáticos de Japón.

Es común el empleo de varias de estas técnicas combinadas para alcanzar mejores resultados. Es lo que se denominada biometría multimodal.

La aparición de nuevos sistemas biométricos es continua. Se trabaja con las venas de las manos, con cicatrices o con tatuajes para mejorar las capacidades de identificación de las personas.

La aplicación de técnicas biométricas permite la eliminación de las más ampliamente extendidas tarjetas de acceso, ahorrando los costes que produce su fabricación, control, software de gestión y mantenimiento. No hay que olvidar circunstancias como olvidos, pérdidas o falsificación y robo de dispositivos como las tarjetas de acceso. Estas situaciones, en principio, son más difíciles de reproducirse con los dispositivos biométricos.

4. Seguridad Lógica

La información es uno de los recursos más valiosos de una organización. La seguridad lógica se centra en la protección de la información almacenada o en tránsito. Es absolutamente necesario controlar los accesos físicos, pero sería del todo inútil sin una política de seguridad que evite los accesos lógicos, por ejemplo el acceso remoto desde un equipo portátil a los activos de la organización.

4.1. Subestados de la seguridad de la información

En la seguridad lógica conviene destacar los atributos de la seguridad de la información, frecuentemente denominados requisitos ACID (Autentificación, Confidencialidad, Integridad y Disponibilidad). Su definición sería:

— **Autentificación**, característica que garantiza que quien dice ser alguien, realmente lo es.

— **Confidencialidad**, garantiza que la información únicamente se revela a usuarios realmente autorizados. De esta forma, se evita el acceso no autorizado, sea accidental o intencionado.

— **Integridad**, garantiza que la información sea exacta y completa. Además, únicamente podrá ser modificada por el personal autorizado.

— **Disponibilidad**, garantiza que la información se encuentre disponible cuando se requiere y en la forma requerida por los usuarios que estén autorizados.

Es posible añadir dos requisitos adicionales:

— **No repudio**, garantiza que no sea posible que alguna de las partes involucradas pueda negar su participación.

— **Trazabilidad**, esta característica permite asociar acciones con los usuarios o sistemas que las realizaron y, además, en qué momento ocurrieron.

Por tanto, los aspectos que debe cubrir la seguridad lógica son el acceso a la información (políticas de contraseñas, gestión de usuarios, etc.), protección ante "software" malicioso, cifrado de datos, etc. La seguridad lógica aplica mecanismos que permitan mantener a salvo la información de la organización. Alguno de los controles que podrían establecerse serían:

— Limitar el acceso a ciertos programas, aplicaciones o archivos. Pueden emplearse claves o, incluso, criptografía.

— Aplicar el principio del mínimo privilegio a los usuarios de un sistema. Únicamente se otorgarán los permisos exclusivamente necesarios para realizar una tarea.

— Control de las aplicaciones y programas que se utilizan en la organización. Con cierta frecuencia, los desarrollos no cumplen las medidas de seguridad más básicas y son fuente de problemas cuando un atacante explota sus vulnerabilidades.

— Controlar la integridad de la información que fluye en la organización y que únicamente esté disponible para los usuarios autorizados.

El componente más débil de un sistema de información, es el "humanware", las personas. Sus ataques podrán ser conscientes o inconscientes. Es muy importante ejercer una labor de concienciación, muchas veces en los

propios administradores de los sistemas. Junto a esta labor es preciso implementar medidas de prevención, detección y recuperación ante toda la gama de amenazas. Como posibles labores de concienciación estarían:

— No ejecutar software de procedencia desconocida.

— Ejecutar de forma periódica software actualizado que permita detectar programas maliciosos. La norma ISO/IEC 27002 recomienda el uso de, al menos, dos tipos de programas distintos para mejorar las posibilidades de detección de ataques.

— No abrir correos personales desde los sistemas de la organización.

— Establecer de forma periódica comprobaciones en los correos recibidos.

— No utilizar software no aprobado por la organización.

Por tanto, y debido a la enorme variedad de problemas que pueden surgir, la seguridad física no puede existir sin la lógica, son complementarias y deben coordinarse.

4.2. Métodos de protección

Cuando una organización ha sufrido un ataque pueden darse los siguientes supuestos:

— **El ataque ha fallado**. La consecuencia es la de estudiar la tipología del ataque para conocer si los controles han funcionado o el ataqué falló por causa del azar.

— **El ataque tuvo un éxito parcial**. El atacante pudo sortear alguno de los mecanismos de seguridad pero no pudo con todos. La organización debe revisar aquellos mecanismos que fallaron.

— **El ataque tuvo éxito total**. La organización debe contar con sistemas que avisen de que se ha producido un incidente de seguridad y poner en marcha los distintos planes (contención, contingencia, etcétera).

Las medidas de protección pueden ser de muy amplia gama y profundidad, en función de factores como importancia de los activos que hay que proteger o de los recursos económicos y humanos de la organización destinados a seguridad. En todo caso, resulta impensable que una organización no cuente con un sistema de antivirus, un sistema de protección perimetral y un sistema de copias de seguridad.

4.2.1. Antivirus

Se trata de herramientas encargadas de prevenir la infección de los sistemas. Detectan y eliminan virus y otras amenazas lógicas de los equipos que protegen.

Las **funciones principales** de un antivirus son:

— La **vacuna**. Es el motor del antivirus. Es un programa que analiza en tiempo real si existe algún archivo o programa que pueda infectar un equipo al ejecutarse.

— El **detector**. Es un programa que escanea unidades, archivos y directorios con el objetivo de detectar códigos maliciosos y detenerlos.

— El **desinfectador**. Es un programa que elimina el virus y puede reparar el daño que provocó al sistema infectado. Existe la posibilidad de que no pueda eliminarse el virus; en ese caso el programa puede mantenerlo en cuarentena hasta la creación de la solución.

Una **clasificación** típica de antivirus sería:

— **Basados en firmas**, la solución antivirus cuenta con una base de datos con las firmas (o huellas) de los virus conocidos. Obviamente, la actualización de la base de datos representa el éxito de este tipo de soluciones.

— **Basados en detección heurística**. Para la búsqueda de código malicioso se basan en reglas que comparan el contenido de los archivos con criterios preestablecidos.

4.2.2. Sistemas de protección perimetral

Existen varios dispositivos que pueden ubicarse en el perímetro de la red de una organización para protegerla. El más conocido y utilizado es el **cortafuegos**.

Un cortafuegos funciona como filtro entre redes, permitiendo accesos autorizados y bloqueando los accesos no autorizados. Aunque existen distintas configuraciones, se suele colocar entre la red interna de la organización e Internet.

La existencia de un cortafuegos hace más difícil una intromisión en la red de la organización pero no protegen completamente todos los activos. Por ejemplo, no podría proteger de ataques que no se produzcan a través del propio cortafuegos, como la instalación de un virus por parte de un empleado.

4.2.3. Copias de seguridad

Ha quedado claro que la pérdida de información debido a un fallo o a una catástrofe natural, por ejemplo, puede repercutir gravemente en el futuro de una organización.

Las copias de seguridad (en inglés *backup*) permiten la recuperación de la información. La realización de estas copias es vital para la continuidad del negocio. Habitualmente las copias se almacenan en dispositivos de almacenamiento que se depositan en un lugar seguro. Conviene almacenar las copias en lugares lo más alejados posibles de la información respaldada. De nada sirve tener copias de seguridad actualizadas en un armario de las instalaciones donde se encuentra la información si un incendio puede destruir el edificio y acabar con ellas.

A partir de la información almacenada se puede restaurar el sistema en el caso de que se produzca un fallo. Los **fallos** en el sistema pueden ser de varios tipos:

— **Físicos**: se originan fallos en el hardware.

— **De diseño**: se producen fallos en los programas.

— **De operación**: causados por la intervención humana.

— **De entorno**: producidos por desastres naturales o del entorno.

Existen varios **tipos de *backups***:

— **Copias de seguridad completas**: se realizan copias del fichero completo sin tener en cuenta que la información ya hubiera sido copiada.

— **Copias de seguridad incrementales**: copia los archivos que tienen activado el atributo de modificado, es decir, solo se copia la información actualizada. Cuando se realiza la copia de seguridad el atributo de modificado se desactiva. Se realiza una copia completa del fichero únicamente la primera vez que se copia. Ahorra espacio pero para recuperar un fichero es necesario recurrir a la última copia completa y a todas las copias incrementales realizadas hasta el momento.

— **Copias de seguridad diferenciales**: es muy similar a las copias de seguridad incrementales. La diferencia reside en que el atributo de modificado no se desactiva hasta que no se realiza un *backup* completo o incremental. Para recupera un fichero se utiliza la última copia completa y la última diferencial. Por este motivo, la recuperación de archivos es más rápida que con copias incrementales aunque necesitan más dispositivos de almacenamiento.

Es posible combinar copias completas e incrementales o *backups* completos y diferenciales pero nunca combinar copias de seguridad incrementales y diferenciales ya que se podrían perder información desde la última copia de seguridad completa.

Los dispositivos que se utilizan para llevar a cabo las copias de seguridad son diversos, desde discos, cintas magnéticas, CDs, DVDs, subsistemas especializados de almacenamiento, etcétera. Las organizaciones con más medios cuentan con centros de respaldo, propios o alquilados, donde almacenan las copias de sus datos.

También es posible que algunas organizaciones utilicen la posibilidad de guardar datos en la nube utilizando Internet como vía para transferirlos.

Las copias de seguridad se suelen realizar de forma automática cuando se trata de grandes sistemas, utilizando aplicaciones software específicas para ese fin.

Es importante conocer el tiempo con el que se dispone para realizar el *backup*. Dependerá, en gran medida, de la cantidad de información que haya que respaldar, el tipo de copia y el dispositivo utilizado.

Mientras se efectúa la copia, es oportuno no realizar modificaciones sobre los ficheros que se estén respaldando. Por este motivo, una correcta planificación del tiempo del que se dispone para realizar las copias redundará en la eficiencia del sistema de *backup* y, sobre todo, en la de una eventual restauración.

5. Amenazas y vulnerabilidades

Como se ha expuesto en la introducción, una amenaza se entiende como aquello que puede causar un mal. Una vulnerabilidad es algo sobre lo que se puede proyectar un daño, que puede dañarse. Si la amenaza impacta en una vulnerabilidad existe un riesgo. Estructurando las ideas como sujeto, verbo y complemento, el sujeto sería la amenaza, el verbo impactar y el complemento (directo) la vulnerabilidad.

La idea de impacto implica una posibilidad, que se expresa con la palabra riesgo, que se entiende como la contingencia o proximidad de un daño. Siguiendo con el esquema, el conjunto que se presenta amenaza + impacto + vulnerabilidad sería un riesgo.

Las amenazas y vulnerabilidades, por tanto se tratan en conjunto, en lo que se da en llamar la gestión de riesgos. Lo que implica identificarlas. En principio son muy variadas, en particular las amenazas lógicas y de software. Por eso, es más fácil identificar las amenazas físicas, por su notoriedad y frecuencia. Y ser de las primeras que están presentes en los planes de contingencia.

Es posible establecer los siguientes grupos que puedan dañar los sistemas de información de una organización:

— **Amenazas físicas**. Fundamentalmente las personas, desde personal propio de la organización hasta antiguos empleados. También en esa categoría entrarían piratas, ciberterroristas e intrusos, sean curiosos o remunerados.

— **Amenazas lógicas**, aquí entran los efectos de virus, gusanos, caballos de Troya, etcétera.

— **Catástrofes**, aquí entrarían los desastres naturales o del entorno.

5.1. Amenazas y vulnerabilidades físicas

Según la actitud del atacante, suelen distinguirse dos grandes grupos:

— **Atacantes activos**. Realizan ataques que cambian el estado de los sistemas de información o de la propia información.

— **Atacantes pasivos**. Curiosean en los sistemas pero no lo modifican, aunque atentan contra la confidencialidad.

5.1.1. Empleados

Se considera que son responsables de entre el 60% y el 80% de los ataques producidos en las organizaciones. Pueden causar daños de forma intencionada o inconsciente:

— **Inconsciente**. Son incidentes producidos de forma involuntaria. La falta de conciencia o cultura de seguridad provoca muchos de estos daños. Algunos ejemplos de estas malas prácticas podrían ser:

  • Sistemas que no bloquean el acceso y permiten que cualquiera pueda acceder a una sesión activa.

  • Contraseñas de acceso a la vista de todos o conocidas por todos.

  • Consulta del correo electrónico personal -sobre todo la descarga de archivos potencialmente peligrosos- desde los sistemas de la organización.

  • Conexión de equipos personales a la red de la organización.

  • Conversaciones confidenciales sobre aspectos críticos de la organización. en lugares públicos.

— **Intencionada**. Cada empleado tendrá sus razones para cometer actos que pueden perjudicar a su organización. La realidad es que estos ataques existen y son complicados de detectar, pues el empleado conoce la organización, los puntos débiles, tiene acceso de las instalaciones e incluso puede conocer contraseñas de acceso. Las actividades intencionadas más habituales son:

  • Daños informáticos. Pueden producirse por la eliminación de datos o de software utilizado en la organización. También es común que el empleado introduzca virus o realice actividades de sabotaje contra los sistemas.

  • Acceso a información confidencial. El objetivo suele ser el de apropiarse de datos de la organización. Existe una gran casuística: desde quedarse con los datos para uso propio hasta tratar de obtener una compensación económica vendiéndoselos a organizaciones competidoras o incluso, chantajear a la propia organización.

  • Creación de empresas competidoras. Un empleado o empleados pueden aprovechar la información de la organización en la que estaban para crear su propia empresa. Es habitual la copia de proyectos, de listas de clientes y contactos, etcétera.

  • Calumnias, injurias y amenazas. Los empleados pueden intentar dañar la imagen de la organización utilizando, incluso, los recursos de la propia organización, como las cuentas de correo electrónico, perfiles de redes sociales, etc.

  • Uso inapropiado de los recursos de la organización. Un empleado puede utilizar las unidades de almacenamiento para guardar programas, copias ilegales de películas, música, etcétera.

5.1.2. Terceros

Se trata de personas ajenas a la organización que cometen robos o fraudes, habitualmente con fines económicos. Aunque la lista podría ser amplia, los perfiles más usuales son:

— **Curiosos**, personas interesadas en las *TIC* y en demostrar sus aptitudes. No suelen buscar hacer daño, más bien buscan notoriedad.

— **Antiguos empleados**, aquí pueden darse motivos de venganza o de obtención de datos que le servirán en su nuevo puesto en otra organización.

— **Crackers**, personas con amplios conocimientos que buscan realizar acciones delictivas, desde la copia ilegal de software, música o películas (pirateo), el robo de números de tarjetas bancarias (*carding*), la utilización ilegal de redes (*Phreaking* y *Foning*) hasta la destrucción de sistemas por el simple placer de destruir.

— **Intrusos remunerados**, personas con amplísimos conocimientos y potencial económico que les permite una infraestructura tecnológica muy importante. Pueden actuar bajo demanda de otro agente externo.

— **Ciberterroristas**. Podrían ser incluido en la categoría de intrusos remunerados pero también entran aquí los distintos gobiernos que utilizan sus recursos para realizar actividades de espionaje o contraespionaje e, incluso, de ataques contra instalaciones de otros gobiernos.

Los ataques provocados por terceros son mínimamente denunciados y por tanto casi pasar desapercibidos. Los motivos suelen ser:

— Desconocimiento de la legislación que trata estos incidentes

— Miedo al descrédito, mala publicidad, pérdida de competitividad si la competencia es conocedora del incidente o pérdida de confianza en la organización por parte de clientes o accionistas

— La organización prefiere resolver los incidentes de forma interna

5.2. Amenazas y vulnerabilidades lógicas

Por código malicioso se entiende cualquier software que pueda causar daño a un sistema de información. El aumento en el número y complejidad de estos sistemas ha supuesto, además, la aparición de nuevas formas de comprometer su seguridad. Asimismo, existen factores clave en el incremento es su propagación, cada vez más rápida consecuencia directa de la mayor velocidad de las redes de datos así como de que la comunidad de intrusos no deja de aumentar.

Al código malicioso se le conoce habitualmente con el término inglés malware. Este hace referencia a programas que se instalan en un sistema, habitualmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de dicho sistema, de aplicaciones, de datos o, simplemente, para molestar o perjudicar a un sistema víctima.

Desde el punto de vista del creador de malware, a día de hoy le resulta mucho más atractivo un sistema Windows frente a otro Unix/Linux por ser mucho más común -especialmente en el ámbito de equipos de escritorio-, contar con más usuarios y ser casi omnipresente en todo tipo de organizaciones.

El creciente uso de Linux, de las aplicaciones para dispositivos móviles en formato de código libre y el reciente fenómeno Internet de las cosas (en inglés *Internet of Things,* IoT), que ha incrementado el número de dispositivos con conectividad a Internet y que implementan mucho software libre basado en Linux, hacen que se cree un gran terreno por explotar para los creadores de malware.

No todo el software malicioso es igual; se trata de programas creados por todo tipo de personas con intereses e ideas diferentes.

Cada individuo dispondrá de sus propios medios técnicos, grados de conocimiento así como de una motivación o finalidad. Además, es necesaria la oportunidad, esto es, se tiene que dar la ocasión que facilite el desarrollo del ataque (por ejemplo, la aparición de una vulnerabilidad en un sistema o aplicación que permitiera la creación de un código malicioso que la aprovechase).

En función de estos intereses suelen provocarse las siguientes situaciones:

— Ataques a objetivos claros y específicamente definidos (un usuario, una organización determinada, un sistema o servicio de esa organización, etc.).

— Ataques a un público objetivo definido atendiendo al grupo de interés. Sería el caso de ataques a los usuarios de un sistema operativo concreto, ataques a las bases de datos de un tipo concreto, etc.

— Ataques aleatorios sin objetivos definidos y sin razonamiento previo.

Asimismo, las motivaciones de los atacantes pueden ser de lo más diverso:

— Lucrativas. Consistirán en robar para, posteriormente, vender información de valor. En esta categoría también estarán los ataques a bases de datos con el objetivo de conseguir datos personales a los que, posteriormente, se enviará publicidad por parte de empresas que habrán pagado a los que se hicieron con los datos.

— Ideológicas. Son ataques que se basan en la difusión de ideologías políticas fundamentalmente, aunque también éticas o religiosas. También entraría en esta categoría la apología del terrorismo.

— Entretenimiento. Los intrusos pueden realizar ataques simplemente como diversión o para probar sus habilidades.

Existe una gran variedad de amenazas en forma de software malicioso. Esto, unido a que cada día se descubren nuevos programas de este tipo, dificulta el establecimiento de una clasificación. Pese a ello, podrían distinguirse tres criterios:

1. **Según el impacto producido sobre la víctima.**

   Para evaluar el grado de peligrosidad se estudia la gravedad de las acciones que el código produce sobre el sistema infectado, su velocidad y facilidad de propagación así como la cantidad de infecciones producidas.

   De acuerdo a este criterio, podrían establecerse los siguientes niveles de peligrosidad:

   — Bajo.

   — Medio.

   — Alto.

2. **Según su forma de propagación.**

   Atendiendo a este criterio, los tipos de malware más conocidos son:

   — **Virus**. Se trata de software malicioso de muy distinta naturaleza cuya finalidad es alterar el funcionamiento de un sistema sin el conocimiento previo de su usuario, corrompiendo o destruyendo sus archivos. Pueden aprovecharse de vulnerabilidades en aplicaciones (navegador, programas de correo electrónico, etc.), sistemas, redes, etc.

     La principal característica está en su capacidad de propagación. Para ello, precisa de la intervención humana, que ayudará en su ejecución.

     Su funcionamiento es bastante simple. Cuando se ejecuta el código, el virus se instala en el sistema (memoria RAM, sector de arranque, etc.), infecta archivos ejecutables y guarda los archivos infectados en disco. Esta forma de proceder permite que cada vez que utilice el fichero infectado se ejecute el virus.

     Los efectos de los virus pueden ser de múltiples tipos, desde completamente inofensivas aunque molestas (por ejemplo, cambiar la ubicación de algunas carpetas), hasta de consecuencias gravísimas (por ejemplo, modificar el registro de Windows con el objetivo de evitar un cortafuegos y permitir que un atacante controle el sistema).

     La forma de propagación también es variada: reproducción al ejecutar un fichero, al visitar una página web que enlaza con otra que contiene código malicioso, etc.

   — **Gusanos**. Es un tipo de malware que se propaga automáticamente sin necesidad de infectar otros archivos, pues puede duplicarse a sí mismo y extenderse sin necesidad de intervención de los usuarios de los sistemas infectados.

     Su finalidad no es destruir archivos o sistemas sino que están pensados para consumir recursos de un sistema o redes, logrando su saturación, y provocar una denegación de servicio (DoS).

Sus principales formas de difusión son las siguientes:

- A través de programas de mensajería instantánea o canales de chat.
- Utilizando los recursos compartidos de una red local.
- A través de las redes *peer to peer (P2P).* Es una de las vías preferidas de infección. Los gusanos se camuflan como archivos con nombres atractivos para los usuarios, adoptando nombres de películas de actualidad, vídeos humorísticos, etc. En estas redes un equipo puede descargarse archivos de cualquier otro equipo de la red y a su vez compartir archivos con los demás, lo que hace que el riesgo de infección sea increíblemente alto.
- Correo electrónico. Pueden ir adjuntos al mensaje o bien camuflados dentro del código *HTML* de los mensajes, por lo que bastaría con una visualización previa del mismo para activarlos. En todos estos casos, los mensajes que los incluyen suelen tener un asunto interesante para captar la atención del destinatario y así lograr que abra el mensaje (por ejemplo, el famoso gusano *I love you*, llamado así porque ese era el asunto del mensaje que lo incluía).

— **Troyanos**. Se trata de un software malicioso que se instala en un sistema aparentando ser un programa inofensivo. Su finalidad es permitir a un usuario no autorizado adquirir el control del sistema infectado.

A diferencia de los virus, los troyanos ni infectan o corrompen archivos o programas y se diferencian de los gusanos en que no cuentan con capacidad para propagarse automáticamente, únicamente buscan permitir la administración remota del equipo a usuarios ilegítimos.

Las infecciones con este tipo de malware se suelen producir cuando el usuario ejecuta un programa infectado. El programa, aparentemente, funciona correctamente, pero en un segundo plano, de forma inadvertida, se instala el troyano. Una vez que se instalan, pasan desapercibidos para el usuario del sistema infectado llevando a cabo diversas acciones, fundamentalmente con el objetivo de controlar ese equipo.

Un troyano, habitualmente, está constituido por dos programas: un cliente en el equipo atacante, que es el que envía las órdenes, y un servidor que se instala en el sistema infectado y es el que recibe las órdenes del intruso y las ejecuta, enviando la información solicitada. La conexión entre estos dos programas se lleva a cabo de dos formas diferentes:

- Conexión directa. El cliente se conecta al servidor para enviarle órdenes. Es la más habitual.
- Conexión inversa. El servidor envía directamente la información al cliente. Es mucho más efectiva, pues muchos cortafuegos no analizan la información saliente del sistema.

Los tipos más habituales de troyanos son:

- **Puertas traseras** (en inglés *Backdoors*). Son muy peligrosos. Permiten el acceso remoto a un atacante sobre una aplicación, una página web, un recurso o, incluso, sobre el sistema operativo.

  Un sistema infectado con este tipo de troyanos será controlador por un atacante sin necesidad de iniciar sesión y tendrá acceso total al equipo. Podrá copiar, modificar, robar o destruir toda la información. Además, podría utilizar el sistema controlado para otras finalidades, por ejemplo, para hacerlo parte de una red de sistemas *zombies* o *Botnets*.

- ***Keyloggers*** .Capturan las pulsaciones de teclado en el sistema de la víctima proporcionándoselas al atacante. El peligro de esta posibilidad es evidente: desde obtener claves de otros sistemas o de cuentas bancarias hasta hacerse con conversaciones escritas.

  Las entidades que utilizan sistemas de autenticación basados en la introducción de caracteres vía un teclado han tenido que proporcionar a sus usuarios mecanismos de seguridad adicionales, como por ejemplo, el uso de un teclado virtual para introducir ciertos datos.

- ***Downloaders***. Su peligro radica en la descarga de archivos con código malicioso y su ejecución en el sistema infectado.

- ***Proxies***. Los intrusos los utilizan para encubrir su identidad pues consiguen que el sistema infectado actúe como un servidor proxy, que le posibilitará el acceso a Internet y que toda la actividad que realice apunte al sistema infectado.

Este tipo de malware es especialmente dañino por las consecuencias que puede ocasionar para los usuarios infectados.

3. **Según las acciones que realiza.**

De acuerdo a este criterio, podrá diferenciarse entre aquel código malicioso que provoca acciones dañinas logrando un impacto medio o alto el que produce acciones no dañinas permitiendo disponer de los sistemas.

— **Software malicioso no dañino.**

Se consideran no dañinas acciones como mostrar publicidad, mostrar información falsa, la realización de bromas. Suele denominarse grayware. Los principales tipos son:

- ***Spyware*** (***Spy Software***, software espía). Es un tipo de software que trata de conseguir información del usuario. Algunos sitios web intentan conocer cuánto tiempo permanece en ellos un visitante. Habitualmente se trata de

motivos estadísticos pero cuando esta actividad se realiza para conseguir información de cara a realizar una acción dañina se trataría de malware.

- ***Adware*** (***Adv****ertisement Soft****ware***, software publicitario). Este software muestra publicidad de forma intrusiva, en forma de ventanas emergentes. No suele representar una amenaza de ataque pero tampoco puede descartarse que no esté ocultando la acción de otro tipo de malware. Es muy habitual la combinación del adware con el spyware para lograr información y transmitirla a terceros.

- ***Cookies***. Son pequeños archivos de texto que el navegador almacena y clasifica. Almacenan información sobre una página web. Se convierten en un riesgo en el momento en que son utilizadas como elementos de rastreo por parte de empresas de publicidad.

- ***Hijacking*** (apropiación, secuestro). Son ataques que intentan modificar configuraciones de programas (por ejemplo el navegador) para obtener un beneficio como el de lograr más visitas a una web que, habitualmente, contendrá publicidad.

- ***Jokes*** (bromas). Es un malware que se limita a asustar al usuario. Utiliza mensajes que advierten del borrado del disco duro o que se enviará información personal a través de Internet, por ejemplo. No realizan acciones dañinas sobre los sistemas infectados.

- ***Hoaxes*** (bulos). Mediante técnicas de ingeniería social, este software consigue engañar a los usuarios sobre amenazas no reales: una estafa, virus, una amenaza de seguridad, etc.

— **Software malicioso dañino.**

Este tipo de software representa una amenaza real contra la seguridad de los sistemas de información. Acciones como la obtención de información, modificación o eliminación de información almacenada y amenazas a los usuarios con el fin de lograr un beneficio económico son escenarios habituales. Algunas variedades de este tipo de malware son:

- ***Ransomware*** (***Ransom*** *soft****ware***, software con rescate). Este tipo de malware cifra archivos importantes del disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos.

  Un ejemplo reciente es *Cryptolocker*, que se camufla en un correo electrónico procedente de una compañía conocida y con la que es más que posible tener relación (por ejemplo Correos). Una vez infectado el sistema de archivos, que también puede ser el de la red local de una empresa, el atacante exige un pago para proporcionar la clave de desbloqueo.

- ***Rogueware*** (***Rogue** soft**ware***, falso software). Esta variedad de malware consigue hace creer al usuario, de forma errónea, que su sistema está infectado por algún virus y que la única forma de desinfectarlo es adquiriendo una solución antivirus por la que habrá que pagar una cantidad de dinero. En ocasiones, se indica al usuario que la única forma de eliminar el virus ficticio del equipo es descargar una solución antivirus entrando en un enlace que se visualiza por pantalla. Al descargar ese supuesto antivirus, se podría estar dando el control total a un atacante remoto, que podría ver todo lo que visualiza por pantalla la víctima o darle acceso a su disco duro o a la red empresarial.

- ***Password stealer*** (Ladrón de contraseñas). Los navegadores son la herramienta más utilizada para casi todo tipo de operaciones relacionadas con Internet, por ejemplo la creación de cuentas de correo web o cuentas de redes sociales. Existen algunos tipos de malware que se aprovechan de esta situación y modifican el navegador para que capture y envíe las contraseñas cuando la víctima las introduce, obteniendo los datos de sesión.

- Bombas lógicas. Este tipo de malware se ejecuta cuando se cumple alguna condición, como que una fecha concreta, que se cambie algún dato en una base de datos o que se modifique un archivo del disco.

- ***Rootkits***. Se trata de herramientas cuya principal misión es la de ocultar la actividad de un atacante, tanto a los usuarios como a los administradores de seguridad o de los sistemas afectados. Además, pueden ir acompañadas de otras funcionalidades como puertas traseras o keylogger.

  Comprender el funcionamiento de un rootkit puede aportar conocimiento de gran utilidad para detectar la presencia de elementos indeseados en una organización.

- ***Keyloggers*** y puertas traseras. Tipo de malware enormemente peligroso. Han sido explicados en el apartado de los troyanos.

- Inyección de código. Este tipo de malware trata de inyectar código en aplicaciones web, sobre todo a través de formularios. Algunos ejemplos son:

  - Inyección de LDAP. El código malicioso intentará modificar cadenas de entrada en lenguaje de filtros LDAP para manipular el funcionamiento de la aplicación web.

  - Inyección de SQL. Exactamente como en el caso anterior pero modificando cadenas de entrada en consultas realizadas en lenguaje SQL.

- Cross Site Scripting (XSS). Este ataque intentará inyectar código malicioso Javascript o Visual Basic Script en foros, chats, redes sociales, etc. Cualquier usuario de esos canales podrá ser infectado a través del navegador.

Hay que destacar la aparición en los últimos años de una nueva categoría de amenazas: las amenazas persistentes y avanzadas (en inglés *Advanced Persistent Threats,* APT).

Se caracterizan por ser amenazas reales, sofisticadas -en la gran mayoría de los casos- y por contar con tal premeditación y persistencia como para ser completamente eficaces contra las contramedidas establecidas en los sistemas de información o en los sistemas de seguridad que constituyen su objetivo.

Los afectados rara vez son conocedores de que son el objetivo de un ataque. Además, desconocen el origen, el alcance o la autoría del mismo.

Una vez definido el objetivo, los atacantes iniciarán una ofensiva en la que no importa el tiempo que se invierta. No suelen esperar un beneficio a corto plazo sino que prefieren pasar desapercibidos mientras dura el ataque hasta que logran su objetivo.

Nuevamente, los objetivos suelen ser económicos (aunque en este caso suelen decantarse por el espionaje, fundamentalmente industrial), militares (revelación de información de seguridad, búsqueda de debilidades, etc.), técnicos (hacerse con credenciales, con código fuente, etc.) o políticos (desestabilización geopolítica, debilitar misiones diplomáticas, etc.). Como puede deducirse, se trata de ataques que pueden afectar a sectores tan críticos como el gubernamental, el industrial, el financiero, el tecnológico, etc.

Tabla que muestra los ataques APT más conocidos en los últimos años

2009	***Operación Aurora***. En ella, más de 30 multinacionales (entre ellas *Google, Adobe Systems o Juniper Networks*) sufrieron robos de información confidencial.
	Operación GhostNet. En ella se vieron implicados unos 1.300 equipos en 103 países. Su objetivo era el espionaje de países del sur de Asia así como al Dalai Lama.
2010	***Stuxnet***. Malware avanzado que afecta a sistemas de monitorización y control de procesos. Inicialmente diseñado para atacar infraestructuras iraníes, su uso se extendió a EE.UU., Indonesia o India.
	Operación Night Dragon. Diseñada para robar información confidencial en multinacionales relacionadas con el petróleo, la química y el sector energético.
2011	***Operación Shady RAT***, orientada al robo de información por la que se vieron afectadas más de 70 organizaciones entre las que se incluían Naciones Unidas, gobiernos y diversas empresas en todo el mundo.
	Nitro, orientada al ciberespionaje industrial y enfocada al robo de información (patentes, fórmulas, procesos de manufactura) de grandes empresas químicas y del sector defensa.
2012	***Flame***, malware avanzado diseñado para llevar a cabo ataques de ciberespionaje en países de oriente medio, viéndose principalmente afectados países como Irán, Israel, Sudán, Siria, Líbano, Arabia Saudí o Egipto.
	Duqu, malware orientado a sistemas industriales. Encontrado en instalaciones europeas y enfocado a la recolección de información.
	Gauss, malware detectado en oriente medio (sobre todo en Líbano, Israel y territorios palestinos) dirigido al robo de credenciales y espionaje de transacciones bancarias viéndose afectadas grandes entidades bancarias.
	Operación Medre, red de espionaje industrial cuyo objetivo es robar ficheros de tipo AutoCAD (diseños y planos). Se centra en países de habla hispana, España incluida.
2013	***APT1***, unidad militar del ejército chino encargada de ciberinteligencia a nivel mundial, especialmente en países de habla inglesa.
	Red October, utilizada para el robo de información de instituciones gubernamentales de distintos países. Similar a Flame.

Pese a las clasificaciones, existe toda una gama de acciones transversales que son válidas para varias de las categorías expuestas: la ingeniería social y las redes sociales.

La primera consiste en la manipulación de las personas para que, de forma voluntaria, realicen actos que pueden suponer un problema a su organización. La tipología es amplia, desde un correo electrónico que insta a descargarse una solución antivirus cuando lo que se adjunta es el propio virus hasta una llamada telefónica de un supuesto componente del servicio de soporte solicitando la contraseña de acceso a un sistema, son ejemplos conocidos.

Es común que los atacantes tomen ventaja de la confianza de los usuarios o una predisposición a ayudar mal entendida.

En el caso de las redes sociales, un fenómeno más reciente, la amenaza puede ser tanto física como lógica. La publicación de mensajes que indican dónde nos encontramos, quiénes son nuestros contactos, familia o amigos y lo que hacemos en cada momento puede colocarnos ante un ataque.

Aún más, un atacante podría crearse un perfil social haciéndose pasar por un tercero. Un conocido que confiara en ese falso perfil pensando que es real, podría facilitarle información requerida a través de técnicas de ingeniería social.

Por último, las redes sociales están siendo grandes propagadoras de malware debido a que pueden intercambiarse programas desarrollados por los programadores de la propia red. Los atacantes podrían aprovechar vulnerabilidades para acceder a un gran número de cuentas de usuario y hacerse con información.

5.3. Catástrofes

La protección de los sistemas de información ante los daños causados por agentes físicos no es, a veces, muy tenida en cuenta en comparación a los causados por agentes lógicos. Sin embargo, un incendio, un terremoto o una inundación pueden acabar no sólo con los activos tecnológicos de una organización, sino con la propia organización.

Es cierto que en estos casos hay que contar con el factor de probabilidad. Si es bajo, la gran mayoría de las veces se aceptará el riesgo, pues la implementación de las medidas que pudieran mitigarlo sería imposible de abordar.

Existen dos grandes grupos de catástrofes:

— **Desastres naturales.**

- **Incendios y humo**. Un cortocircuito, el uso inadecuado de combustibles, una colilla o la ubicación errónea del papel pueden provocar un fuego en alguna dependencia de la organización. El uso de materiales ignífugos, la instalación de detectores de humo e incendios y de extintores ayudará a su detección y extinción.

- **Terremotos**. Difíciles de prevenir, la construcción de edificios antisísmicos para albergar las instalaciones TIC de la organización o la propia organización suele ser la medida más apropiada para mitigar sus efectos.

- **Inundaciones**. También son difíciles de prevenir. La correcta planificación de la ubicación de las instalaciones TIC es fundamental, así como la existencia de sistemas de evacuación de agua. Una inundación también puede producirse al intentar sofocar un incendio.

- **Humedad**. Es preciso contar con un cierto nivel de humedad que evite la electricidad estática pero niveles altos de humedad podrían dañar las instalaciones TIC de una organización. El uso de sensores informará de los niveles de humedad existentes.

Es casi imposible el control de los fenómenos naturales pero sí es posible anticiparse. Por ejemplo, no ubicar los sistemas de información en lugares con alta probabilidad de terremotos. Las organizaciones con más capacidad económica cuentan con un centro de respaldo, instalación que es capaz de retomar la actividad TIC de la organización ante una pérdida de servicio de toda o parte de la instalación principal.

También es posible delegar la ubicación de la infraestructura TIC a empresas que ofrecen instalaciones diseñadas con las mejores técnicas para minimizar los efectos de una catástrofe.

— **Desastres del entorno.**

- **Temperaturas extremas**. Pueden dañar gravemente a los sistemas. Es preciso respetar las especificaciones del fabricante y disponer de sistemas de climatización y ventilación adecuados.

- **Incidencias de carácter eléctrico**. Subidas y caídas de tensión pueden afectar a los sistemas. El uso de estabilizadores de tensión ayudan a prevenir problemas. También pueden originarse cortes eléctricos. En estos casos el uso de sistemas de alimentación auxiliares e ininterrumpidos solventa temporalmente esa circunstancia. Es preciso considerar el riesgo de cables en mal estado o cortados pues pueden provocar interferencias. Resulta muy conveniente realizar revisiones periódicas del suelo técnico.

6. Infraestructura física de un CPD: acondicionamiento y equipamiento

Los Centros de Proceso de Datos (CPD) son los lugares donde se aloja el equipamiento informático principal que soporta el sistema de información de una organización. El CPD ha de garantizar tanto la continuidad como la disponibilidad de los servicios de la organización.

Esta disposición implica la responsabilidad de prevenir incidencias y desastres en el CPD, desde la protección de sistemas de información y de comunicaciones hasta la protección de los de almacenamiento. Es obligatorio que se identifiquen riesgos y establezcan salvaguardas. Todo con el objetivo de la continuidad funcional, así como de la disponibilidad de servicios y sistemas.

De otra forma, que la información pueda recuperarse con un nivel de confianza (fiabilidad e integridad) al que, estando autorizado, la solicite (acceso y confidencialidad).

Las organizaciones son conscientes de la importancia estratégica de sus activos tecnológicos y de información, que suelen ubicar en el CPD. Por ello, cada vez más, invierten en la consecución de un CPD que garantice la disponibilidad y la seguridad de sus activos más valiosos.

El valor de negocio de una organización suele basarse en incrementar los ingresos, reducir costes y utilizar mejor los activos. El cálculo del valor de la infraestructura del CPD se realiza relacionando el coste inicial y la disponibilidad. El dinamismo de las TIC ha influido en la aparición de dos criterios más: la flexibilidad y el coste total de la propiedad (en inglés *Total Cost of Ownership,* TCO). La flexibilidad pone a prueba la capacidad de la infraestructura para adaptarse a los cambios. El cálculo del coste total del CPD es obligatorio para realizar posteriores análisis de retorno de inversión (en inglés *Return of Investment,* ROI).

El diseño clásico de los CPDs valoraba el rendimiento, la disponibilidad y la seguridad. La consecuencia fue el sobredimensionamiento de todos sus componentes, lo que terminó por establecer un uso ineficiente de los equipos TIC, un aumento de los costes y un impacto medioambiental que todos padecemos. Desde hace unos años, se aplica un enfoque más energético, reduciendo las emisiones tóxicas al medioambiente. Los principales fabricantes han considerado que la mejor forma de hacerlo es mediante un redimensionamiento de todas las infraestructuras y una reducción del número de sistemas, utilizando, por ejemplo, técnicas de virtualización que consoliden servidores y servicios.

Pero no solo se consideran los factores energéticos en la creación de los CPDs. La aparición de nuevas tecnologías (Internet de las cosas (*IoT*) o de la Informática en la nube o *Cloud Computing*) o una creciente preocupación en seguridad están haciendo que aparezcan nuevos **modelos de CPDs** basados en:

— **La fortaleza de los datos**. Debido a los crecientes ataques que son, además, cada vez más sofisticados y con consecuencias más graves, las organizaciones están demandando la existencia de CPDs que prioricen la seguridad. Se trabaja en separar los datos muy confidenciales del resto, aislándolos de la red y protegiéndolos con sistemas eléctricos y de refrigeración también separados.

— **Uso real de la nube**. Algunos informes han constatado que la infrautilización de los servidores es muy grande: estiman que únicamente utilizan entre el 5% y el 15% de su capacidad de proceso y eso que las técnicas de virtualización mejoraron las prestaciones de los sistemas y liberaron mucho espacio en los CPDs. Las organizaciones prevén la existencia de CPDs compartidos, aprovechando ese excedente de espacio y estando cada vez más presentes en la nube.

— **Informática "en la niebla"**. Este concepto, creado por la compañía Cisco para dar visibilidad al exponencial aumento de datos consecuencia del fenómeno Internet de las Cosas (IoT), consiste en conectar redes pequeñas en una más grande utilizando aplicaciones distribuidas, con dispositivos y sistemas que mejoren su rendimiento y concentrando los datos más cerca de los dispositivos y redes.

— **Cumplimiento de la responsabilidad social corporativa**. Cada vez más organizaciones son conscientes del impacto de la huella de carbono de los CPDs y de que la sociedad valora esfuerzos en sostenibilidad. El sector está respondiendo con el uso de energías alternativas para reducir las emisiones de carbono.

Existen numerosas posibilidades para una organización a la hora de afrontar dónde y cómo protege sus sistemas de información. Puede alquilar el espacio a empresas que ya cuentan con CPDs con todas las prestaciones o puede construirlo en sus instalaciones. La gran diferencia entre ambos modelos estará en la propiedad, acceso, responsabilidad y, por supuesto, costes.

6.1. Diseño de un CPD

Es habitual que se enumeren las siguientes características a la hora de diseñar un CPD:

— **Robustez**, el objetivo es mantener operativo el CPD en todo momento.

— **Modularidad**, conviene diseñarlo en partes intercambiables para favorecer su escalabilidad y simplicidad.

— **Flexibilidad**, la adaptación a los cambios tiene mucho valor para las organizaciones. Por ello se valora la construcción con materiales de fácil movilidad.

— **Estándar**. El diseño debería mantener una misma apariencia, etiquetado, señalización, etcétera. Estas medidas facilitarán la resolución de problemas.

— **Buenas prácticas**. Facilitar información a los usuarios y establecer guías de actuación entendibles son acciones imprescindibles.

Queda claro que el CPD no está formado exclusivamente por los sistemas TIC que almacenan la información de la organización. Es necesario contemplar todas las infraestructuras que garantizarán el buen estado de dicha información.

— **Infraestructura de obra**. Es el espacio que ocupa el CPD y las áreas asociadas: salas de almacenamiento, cuartos de electricidad, suelo técnico, paredes, techos, etcétera.

— **Infraestructura energética**. Constituida por el suministro eléctrico, los sistemas de alimentación ininterrumpida, grupos electrógenos, tomas de tierra y luminarias. El suministro suele ser proporcionado por una empresa externa a la organización.

— **Infraestructura de climatización**. Su misión es la de extraer el calor del CPD. Compuesta por las unidades que absorben y liberan el calor, por los compresores y sistemas de válvulas.

— **Infraestructura de protección contra incendios**. Está formada por los sistemas de detección y extinción. Aunque la gran mayoría de incendios suceden fuera del CPD, este ha de estar preparado tanto para

resistir la propagación como para detectar y extinguir un fuego que se origine en la propia sala.

— **Infraestructura de racks**. Son las estructuras modulares donde se instalan los sistemas.

— **Infraestructura de cableado**. Cableado estructurado que conecta los sistemas. Es habitual la presencia de cobre y fibra.

— **Infraestructura de seguridad**. Está compuesta por controles de acceso, cámaras de seguridad y sistemas de monitorización.

6.1.1. Infraestructura de obra: edificio e instalaciones

El elemento principal de la infraestructura del CPD es el lugar físico, es decir, el edificio. Entre los requisitos exigibles a los edificios se encuentran los de "protección medioambiental", relativos a su ubicación, para protegerlo frente a desastres naturales (inundaciones, terremotos y similares). Es posible que la circunstancias de las distintas organizaciones sean muy diferentes y así lo reflejarán en el diseño y la construcción del CPD. Piénsese en el caso de Japón y la frecuencia de sus terremotos.

Asimismo, son importantes los requisitos contra "interferencias internas", centrados en el diseño arquitectónico interno para ubicar y dimensionar dependencias. Su objetivo es anticipar los efectos de accidentes como inundaciones, problemas eléctricos u otros, buscando el mayor aislamiento del CPD en caso de incidencias.

Se considera parte de la infraestructura las instalaciones que aportan y complementan la funcionalidad de las actividades propias del CPD y las que aseguran unos niveles de confort y seguridad a las personas que trabajen en el CPD, como son las instalaciones de aire acondicionado o de refrigeración por agua.

La instalación de alimentación eléctrica debe asegurar la potencia necesaria estabilizada y sin interrupciones para la activación de equipos y el resto de las instalaciones que lo requieran, como la iluminación. Las redes de suministro eléctrico deben ser independientes para reducir riesgos al aislar posibles problemas.

Debido a que el suministrador eléctrico puede fallar, podría preverse la situación contratando un doble suministro con otro proveedor. Si la importancia del CPD lo requiriese, se podría dotar al con equipos electrógenos u otras alternativas. Una primera solución a la falta de suministro eléctrico se consigue con sistemas de alimentación ininterrumpida, SAI o UPS en inglés, que funcionan con baterías.

El resto del equipamiento de un CPD tiene como objetivo mejorar el nivel de seguridad ante riesgos del edificio y sus ocupantes. Así, las instalaciones de seguridad y control de accesos pretenden evitar la invasión de personas no autorizadas. Las instalaciones de detección y extinción de incendios mantendrán controlado el riesgo o, en caso de ocurrencia, limitarán sus efectos.

El coste que supone la caída de un CPD es una de las mayores preocupaciones de las organizaciones. No solo es el económico, que puede llegar a ser muy elevado en función del tipo de negocio, sino que también puede estar en juego el prestigio o incluso repercusiones de carácter legal. Es muy común en estos entornos hablar de disponibilidad.

La disponibilidad suele medirse como un porcentaje de tiempo y se representa con varios "nueves". A mayor número de nueves, mayor porcentaje de disponibilidad, puesto que más se acercará el valor al 100% de tiempo activo. La siguiente tabla muestra los niveles de disponibilidad de un CPD:

Nivel de disponibilidad	Porcentaje	Tiempo de caída anual
Seis nueves	99,9999	32 segundos
Cinco nueves	99,999	5 minutos y 15 segundos
Cuatro nueves	99,99	52 minutos y 36 segundos
Tres nueves	99,9	8 horas y 46 minutos
Dos nueves	99	3 días, 15 horas y 40 minutos

Si se desea alcanzar un alto grado de disponibilidad, será necesario establecer un número de niveles en la infraestructura del CPD. En terminología inglesa se denominan *Tiers*.

Un nivel o tier mostrará la disponibilidad del *CPD* atendiendo a cuatro niveles:

1. ***Tier I***, es el nivel básico. Proporciona un 99,671% de disponibilidad. Los CPDs con esta clasificación disponen de líneas dedicadas de distribución de potencia y refrigeración. Sin embargo, no cuentan con redundancia en los componentes. Al menos una vez al año es preciso realizar una parada completa para realizar tareas de mantenimiento. Se estima que su tiempo de inactividad anual alcanza las 28,8 horas.

2. ***Tier II***. Proporcionan un 99,741% de disponibilidad. Incluyen redundancia en los componentes. Pueden requerir alguna interrupción para realizar mantenimientos parciales. Se estima que su tiempo de inactividad anual es de 22 horas.

3. ***Tier III***. Proporcionan un 99,982% de disponibilidad. Permiten la realización de mantenimientos simultáneos programados que provoquen interrupciones sin alterar el funcionamiento del servicio. En el caso de las tareas no programadas sí pueden provocar paradas. Se estima que su tiempo de inactividad anual es de 1,6 horas.

4. *Tier IV*. Proporcionan un 99,995 de disponibilidad. Se los conoce como a prueba de fallos. Las interrupciones programadas no afectan al servicio y, al menos, deben resistir una interrupción no programada sin que afecte a los servicios críticos. Se estima que su tiempo de inactividad anual es de 0,4 horas.

Además de la disponibilidad, existen otros valores que pueden medir la fiabilidad de un CPD:

— El tiempo medio entre fallos (en inglés *Mean Time Between Failures,* MTBF). Muestra el tiempo de funcionamiento de un sistema de alimentación ininterrumpida entre dos fallos producidos de forma consecutiva.

— El tiempo medio de reparación (en inglés *Mean Time To Repair,* MTTR). Muestra el tiempo que el sistema de alimentación ininterrumpida estará fuera de servicio debido a reparaciones.

Hay que considerar que, pese a que aumente la protección, también aumenta la posibilidad de error debido al aumento de la complejidad: en tiempo de instalación, durante emergencias, cuando actúen los sistemas de respaldo, etc.

6.1.2. Infraestructura de protección contra incendios

A) Detección de incendios

Un sistema de detección de incendios permite localizar un incendio y activar la alarma. Puede darse el caso de que la central de incendios esté gestionada por personal o se encuentre programada para realizar acciones de forma automática.

Los principales componentes de un sistema de detección de incendios podrían ser:

— Detectores.

— Pulsadores.

— Centrales de señalización.

— Líneas.

— Sistemas auxiliares. Entre otros estarían: alarmas generales, megafonía, accionamiento de los sistemas de extinción, etcétera.

• Detectores

Existen diversos tipos de detectores de incendios:

— **Iónicos**. Detectan gases de combustión, tanto visibles como invisibles. Funcionan con cámaras ionizadas por un elemento radiactivo. La irrupción del gas provoca la interrupción de la corriente de iones y genera una señal de alarma.

— **Ópticos**. Gestionan sensores ópticos que toman medidas de luz que envían a una central. Su análisis compara los resultados con los valores programados y su resultado podrá provocar una señal de alarma.

— **Termovelocimétricos**. Son detectores de calor que comprueban dos parámetros de temperatura. También envían los valores a una central, se analizan y generan señales de alarma en función de las diferencias con los valores programados.

— **Detectores por aspiración**. Son sistemas muy sensibles que no esperan a que el humo alcance a los detectores tradicionales. Succionando y analizando el aire de forma continua consiguen detectar la presencia de humo.

• **Pulsadores manuales**

Son mecanismos de protección que pueden agruparse en:

— Pulsadores de alarma de extinción.

— Pulsadores de activación manual de extinción.

— Pulsadores de bloqueo manual de extinción.

Suelen contar con control de acceso para evitar pulsaciones accidentales o intencionadas.

• **Centrales de señalización**

Son sistemas que controlan a los equipos de detección de incendios. Cuentan con puertos de comunicaciones para conectarse con el puesto de control cuando detectan alguna circunstancia que obliga a provocar una alarma. Esta puede mostrarse mediante indicadores luminosos, acústicos, desconexiones, activación de evacuaciones, cierre de puertas, etcétera.

B) Extinción de incendios

La extinción de un incendio suele realizarse mediante gas o mediante agua. En el caso concreto de los CPDs, se emplean gas y agua nebulizada.

• **Extinción mediante el uso de gas**

Cuenta con varias características:

— Actúa de forma muy rápida en el foco del incendio y llega también a zonas muy poco accesibles.

— No deja residuos.

— El gas no conduce la electricidad.

— No provoca tantos daños como el uso del agua.

— Es posible reanudar la actividad tras la descarga del gas.

Para lograr un correcto funcionamiento son obligatorios unos requisitos de diseño e instalación pues el gas es sensible tanto al sistema de refrigeración como a la estanqueidad. La existencia de corrientes de aire en el CPD puede provocar que no se active el sistema de extinción o que se active pero no extinga el incendio.

Una descarga indeseada puede provocar accidentes que afecten a las personas, en función de la toxicidad del gas utilizado.

Los gases que pueden emplearse en la extinción de incendios en un CPD pueden ser:

— Halón.

— Co2.

— Novec 1230.

— Halocarburos (HFCs).

— Inertes.

• **Extinción mediante el uso de agua nebulizada**

Es agua formada por microgotas impulsadas a alta presión mediante el uso de boquillas especiales y descargada a mucha velocidad. Esta técnica alcanza una superficie de refrigeración muy amplia y la vaporización es bastante rápida.

Esta técnica elimina el incendio mediante enfriamiento, bloqueando el calor radiante y eliminando el oxígeno. Sus características principales son:

— Logra la extinción del incendio. Los sistemas tradicionales y el agua pulverizada son considerados sistemas de control y supresión.

— No precisa la estanqueidad del recinto.

— Consumen menos agua que las técnicas similares basadas en agua.

— La descarga no produce daños a los equipos ni a las personas en caso de una descarga indeseada.

6.1.3. Infraestructura de seguridad

Es sabido que es preciso asegurar físicamente el entorno de un CPD pues contiene equipamiento, aplicaciones y los datos de la organización. Conviene, por tanto, garantizar su acceso mediante el uso de restricciones así como su monitorización:

A) Restricciones físicas

El método más utilizado es el de controlar quién puede acceder al CPD. Existen diversas posibilidades:

— Establecer políticas de control de acceso. Resulta fundamental establecer y divulgar políticas de acceso para que todo el personal de una organización conozca si está o no autorizado a entrar en su CPD. Estas políticas suelen basarse en conceder accesos en función del tipo de trabajo que se realizará en el CPD. También existen políticas basadas en accesos a corto y largo plazo.

— Puertas. Casi todas las organizaciones apuestan por un sistema automatizado, habitualmente con tarjetas de acceso. También son frecuentes los sistemas biométricos. Es importante pensar también en la salida, no únicamente en la entrada. Hay que habilitar mecanismos que permitan abandonar el CPD en caso de alguna circunstancia: incendio, descarga inminente de productos de extinción de incendios, etcétera. Resulta conveniente que el sistema de seguridad permita conocer quién está en el CPD en cada momento para ayudar a una posible evacuación.

— Jaulas. Rodear a los servidores con una reja añade un punto más de seguridad física. Puede ser un sistema sustitutivo de algunas paredes en un CPD.

— Cierre de racks. Se considera un añadido en la seguridad física de los servidores. Prácticamente todos los racks cuentan con una cerradura, bien de llave bien de lector de tarjetas.

B) Monitorización

El sistema de monitorización más habitual es el que se basa en la colocación de un conjunto de cámaras de vigilancia, tanto dentro del CPD como en zonas perimetrales. Una correcta distribución permitirá registrar quién intenta entrar o salir y si lo consigue o no. Las cámaras suelen ser gestionadas por el personal de seguridad. Existe la opción de grabar las imágenes tomadas para una visualización posterior.

La monitorización mediante la utilización de cámaras no informa de las condiciones ambientales existentes en el CPD pues únicamente recoge aspectos relacionados con el control de accesos. Es muy conveniente monitorizar condiciones como la humedad, la temperatura, fugas de agua, de humo, caídas de tensión, etcétera. Un adecuado sistema de monitorización detectará estas situaciones y emitirá las alarmas necesarias a los responsables de gestión del CPD, así como a los administradores de los sistemas que puedan verse afectados.

Es absolutamente recomendable la integración de todos los sensores que controlen tanto las circunstancias anteriores como los de detección de humo o fuego, por ejemplo. Esta integración puede permitir a los administradores tomar medidas antes de que se produzca la descarga del sistema de extinción.

Es común el uso del protocolo SNMP para la monitorización de los distintos sensores o componentes. Junto a la utilización de una MIB (*Management Information Base*) permitirán la notificación directa a los sistemas de gestión.

Esta acción puede convertirse en la mejor política de protección. Es casi imposible establecer un conjunto de normas que cubran todas las posibles circunstancias a las que puede verse sometida una infraestructura tecnológica, siempre quedará alguna que no se ha contemplado.

Aspectos como el sentido común y el respeto a la infraestructura se dan por asumidas para todas aquellas personas que tengan acceso a un *CPD*.

Otro de los aspectos que las organizaciones suelen implantar es la Gestión de Cambios. Obviamente, también debería afectar al *CPD* para evitar sorpresas. Establecer un método de planificación, coordinación y comunicación sobre las actividades del *CPD* ayudarán a prever situaciones de emergencia. Una correcta comunicación en casos como modificaciones en las salas a todos los afectados evitará situaciones de pérdida de servicio, anulación de procedimientos establecidos, etcétera. En definitiva, redundará en una mejor productividad.

6.2. Implementación de un CPD

Es un proceso complejo, con muchos elementos implicados. Es habitual confiar en empresas especialistas, tanto para su diseño como para su implantación, pero no es obligatorio que sea la misma. Una implantación suele contar con las siguientes fases:

— **Elaboración del pliego de prescripciones técnicas**. El pliego recoge todos los requisitos que posteriormente se plasmarán en la propuesta técnica.

— **Análisis de situación**. Revelará el estado en que se encuentran las instalaciones, tanto del edificio como de la que será la ubicación del *CPD*. El análisis es la base para la posterior toma de decisiones y adoptar la solución más idónea.

— **Propuesta técnica**. Es la solución que se propone para la consecución del CPD más idóneo para la organización respetando los requisitos establecidos en el pliego de prescripciones técnicas.

— **Conclusiones**. Una vez finalizadas las fases de diseño e implementación, conviene extraer conclusiones, que serán de ayuda a todas las partes y mejorarán el resultado final.

7. Sistemas de gestión de incidencias

La gestión de incidencias hay que entenderla en un marco más amplio, el de la gestión de seguridad de los sistemas de información (*SGSI*), incluida en la norma ISO 27001 desde el año 2005 y revisada en 2013. Esta norma considera a la organización como una totalidad y tiene en cuenta a todos y

cada uno de los aspectos que pueden verse afectados en el caso de la existencia de un incidente. La norma está estructurada en once dominios de control; la gestión de incidencias es uno de ellos.

Entendemos por incidencia en un sistema de información aquellos eventos que causan en los usuarios del mismo la necesidad de comunicarse con los responsables de dicho sistema de información a fin de trasladar algunas de las siguientes circunstancias:

— Pérdida de servicio, equipos o instalaciones.

— Fallos del sistema, sobrecargas, malfuncionamiento (por ejemplo lentitud).

— Errores humanos.

— Fallos en políticas o directrices (por ejemplo fallos en el acceso a recursos compartidos).

— Cambios del sistema no controlados (por ejemplo actualizaciones inesperadas o no informadas debidamente).

— Desconocimiento en el uso del software o del hardware.

— Violaciones de acceso.

— Eventos que afecten a la identificación y autenticación de los usuarios.

— Eventos que afecten a los derechos de acceso a los datos.

— Eventos que afecten a los procedimientos de copias de seguridad y recuperación.

— Sugerencias de los usuarios respecto del sistema de información.

— Cualquier otra situación que afecte al normal funcionamiento del sistema.

La gestión de estas incidencias comenzará por el adecuado registro de las mismas, con indicación de la fecha de registro, descripción detallada del problema, intentos de soluciones, cada incidencia mantendrá un historial de cada cambio.

La gestión de incidencias comúnmente tendrá un único punto de entrada que será un centro de atención de usuarios, bien vía telefónica, vía telemática o ambas. En dicho centro de atención se ofrecerá el servicio de soporte al cliente de la organización para crear, actualizar y resolver incidencias reportadas por los usuarios del sistema de información o incluso incidentes reportados por otros empleados de la organización.

Cada incidencia en el sistema puede tener un nivel de urgencia asignado, basado en la importancia total de ese evento. Los incidentes críticos son los más severos que deben ser resueltos en la forma más expedita posible, tomando precedencia sobre todos los demás incidentes.

7.1. Tipología de incidencias. Niveles de urgencia

Una posible clasificación de incidencias sería la que sigue:

— **Crítica:** una emergencia es un incidente cuya resolución no admite demora. Los incidentes de este tipo se procesarán en paralelo de haber varios, y en su resolución se emplearán todos los recursos disponibles.

— **Alta:** un incidente de alta prioridad es aquel cuyas características requieren que sea atendido antes que otros, aunque sea detectado posteriormente. Para esto se mantiene una cola independiente de incidentes de alta prioridad, y no se procesarán los de prioridad inferior mientras queden de estos. Los incidentes de alta prioridad se procesan en serie.

— **Media:** por defecto, los incidentes se atienden en serie por orden de llegada, mientras no requiera atención uno de prioridad superior. Un incidente de prioridad normal puede adquirir la categoría de alta prioridad si no recibe atención por un tiempo prolongado.

— **Baja:** los incidentes de baja prioridad se atienden en serie por orden de llegada, mientras no requiera atención uno de prioridad superior. Un incidente de baja prioridad será cerrado automáticamente si no recibe atención por un tiempo prolongado.

Asimismo, una categorización típica, de menor a mayor grado de gravedad puede ser la siguiente.

— **Categoría 4**. Incidencias rutinarias o que en un futuro podrían ocasionar problemas.

— **Categoría 3**. Incidencias de fácil solución. En el peor de los casos afectarían a pocos usuarios.

— **Categoría 2**. Incidencias de riesgo grave predecible. En caso de producirse llevan asociado un largo proceso de recuperación o podrían detener un sistema o aplicación.

— **Categoría 1**. Incidencias urgentes. Problema complejo que paraliza la operación y afecta a muchos usuarios. La situación puede no tener vuelta atrás o proceder de la combinación o evolución de incidencias de categorías inferiores.

— **Categoría 0**. Incidencias de emergencia. Situación grave que paraliza todo el servicio.

El seguimiento de incidencias se apoyará en una base de conocimiento que contiene información sobre cada usuario registrado, soluciones a problemas comunes y herramientas para la asignación de técnicos de soporte que ayudarán al seguimiento de errores y fallos del sistema. Las preguntas más frecuentes (FAQs), por ejemplo, serán un producto típico de dicha base de conocimiento.

El registro de cada incidencia otorgará un número de referencia o número de caso, el cual es usado para permitir al cliente o al personal de soporte localizar, añadir o comunicar información de seguimiento al estado del incidente.

La arquitectura más común de sistema de seguimiento de incidencias se basa en una base de datos como repositorio de almacenamiento para los datos que son gestionados por la capa de negocio de la aplicación. Cada vez que se produce un evento el sistema de seguimiento de incidentes registra la acción y quién la hizo, llevando un histórico de las acciones tomadas en la resolución del caso.

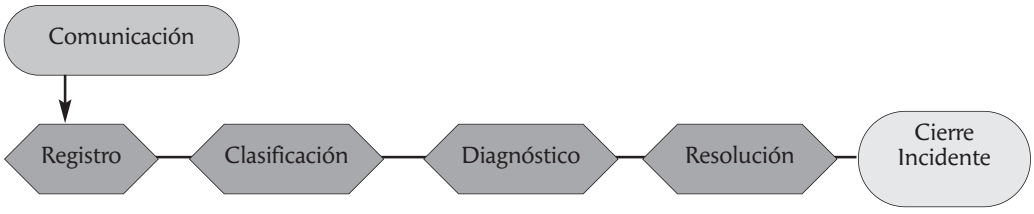
El **proceso de trabajo en la gestión de incidencias** se ilustra como sigue:

— Un técnico del servicio al cliente recibe una llamada telefónica, correo electrónico, o es el usuario quien accede a una web de registro para informar de un problema. Se verifica que el problema es real, que el usuario informante es pertinente y se complementa toda la información posible al respecto.

— Conforme se trabaja en el incidente, el sistema es actualizado por los técnicos de soporte. Cada acción para solventar el problema debe ser anotada en el sistema de incidentes.

— Después de que la incidencia está solucionada, se informa al usuario afectado para verificar su acuerdo o permitirle reclamar y reabrir el caso.

— A veces la cuestión puede finalmente no ser resuelta por deberse a carencias de diseño, incidencias crónicas conocidas sin solución, o tener solo una solución parcial.



En el *argot* de la profesión se emplean los anglicismos “HelpDesk” y “Call Center” para referirse al soporte a usuarios y centro de llamadas respectivamente. Los departamentos TIC y sus centros de llamadas, que atienden con frecuencia peticiones para resolver incidencias, recurren a aplicaciones software para la gestión de dichas incidencias.

7.2. Marco normativo

Es obligado señalar que la gestión de incidencias también cuenta con su marco normativo o forma parte de él. Estándares, normas y leyes condicionan su aplicación y, como no, pueden suponer la diferencia a la hora de decidirse por un sistema u otro o bien externalizar el servicio.

Las normas permiten a la organización asegurar el cumplimiento de los siguientes puntos:

— Identificar y valorar activos.

— Establecer el grado de cumplimiento de los estándares de la organización.

— Gestionar las incidencias.

— Documentar procedimientos, registros, etcétera.

— Medir el grado de avance.

— Formar a los implicados.

Estas normas pueden ser: la LOPDCP (Ley Orgánica de Protección de Datos de Carácter Personal), el ENS (Esquema Nacional de Seguridad, en el caso de las Administraciones Públicas), SGSI (Sistema de Gestión de Seguridad de la Información –ISO 27001) o metodologías como ITIL *(Information Technology Infrastructure Library -ISO 20000).*

7.3. Acuerdos de nivel de servicio

El servicio de soporte a usuarios es uno de los servicios que se externaliza más frecuentemente, esto es, que se confía a empresas externas bien porque la organización no cuenta con los recursos necesarios para realizar la tarea, bien porque prefiere dejar esas tareas en manos de empresas con más experiencia o por motivos económicos.

En estas situaciones suele ser muy habitual, casi imprescindible la firma de los denominados acuerdos de nivel de servicio (en inglés *Service Level Agreement, SLA*).

Un acuerdo de nivel de servicio es un documento escrito entre el proveedor del servicio y la organización contratante.

La empresa a la que se confía el servicio de soporte tendrá que presentar a la organización contratante respuestas a los siguientes puntos:

— Definición de objetivos.

— Identificación de expectativas.

— Planificación temporal.

— Optimización de procesos, realizando modificaciones si es preciso.

Cuando la organización es consciente de lo que necesita está mejor preparada para aceptar un acuerdo de nivel de servicio. Los principales puntos a recoger en este acuerdo podrían ser:

— Tipo de servicio, en este caso servicio de asistencia técnica.

— Tipo de soporte y establecimiento del nivel de incidencias.

— Medios para contactar con el servicio de asistencia técnica.

— Procedimientos de escalado de incidencias.

— Disponibilidad horaria del servicio.

— Provisiones para seguridad y datos.

— Garantías de disponibilidad del sistema.

— Tiempos de respuesta para los distintos escenarios de incidencias.

— Penalizaciones por incumplimiento.

No siempre las organizaciones quedan plenamente satisfechas con un SLA acordado con una empresa externa. Las causas más frecuentes son:

— No existen experiencias previas en la organización, no hay cultura organizativa en la utilización de *SLAs*.

— El acuerdo de nivel de servicio acordado es, o muy extenso, o muy corto.

— El acuerdo de nivel de servicio no está enfocado a las áreas de usuario.

— El acuerdo de nivel de servicio fue acordado con objetivos inalcanzables.

— Existen errores en la definición de prioridades.

Cabe señalar que un mal servicio de gestión de incidencias habitualmente comienza con un mal servicio de atención al cliente, operadores mal entrenados o desconocedores del negocio, con escasa sensibilidad para la priorización de los problemas y que se basan en argumentarios muy "robotizados" o incluso el registro de incidencias basado en locuciones pregrabadas pueden causar sobre los usuarios rechazo, pérdida de confianza e incluso desdén ante nuevas incidencias que no serán informadas para su solución.

Otro factor importante es la capacitación y agilidad de los técnicos de soporte, a veces si la solución de una incidencia está mal enfocada o incorrectamente clasificada se da lugar a múltiples reasignaciones entre los posibles técnicos de soporte (partido de tenis) y el usuario final acaba resultando desatendido.

7.4. Herramientas y soluciones de gestión de incidencias

Pese a los intentos de las organizaciones de establecer sistemas de gestión de incidencias basados en otras plataformas, es muy común aún el uso del teléfono para notificar una incidencia al servicio técnico de una organización. El sistema permitirá abrir, gestionar la asignación de un técnico y cerrar la incidencia.

No obstante el método anterior, existen numerosas soluciones que permiten gestionar las incidencias de una organización, tanto en el modelo de

código abierto como propietarias. Casi todas ellas cuentan con las siguientes características:

— Oferta de interfaz web para usuarios y para técnicos de soporte. Es muy habitual que incluyan la posibilidad de un chat con, al menos, una primera línea de soporte. Es de gran utilidad y es una solución muy rápida que puede agilizar la resolución de cierto tipo de incidencias.

— Integración con el correo electrónico. Es una cualidad muy útil para los usuarios, que están más acostumbrados al uso de ese servicio y plantearán menos resistencia que si se les plantea una nueva plataforma. Para los técnicos no genera mayor problema, pues los correos son automáticamente convertidos en tickets de incidencias.

— Existencia de generador de informes, cuadros de mando y gestor de tiempos para facilitar los *SLAs*.

— Cada vez más son compatibles con plataformas móviles -Android e IOS-.

Entre las plataformas de software libre abierto que permiten la gestión de incidencias estarían *Request Tracker* (RT), GLPI, *Open Ticket Request System* (OTRS) o e-Pulpo (Plataforma de Unificación Lógica de los Procesos Operativos).

En el software propietario se podrían citar Xperta, Remedy o Integria IMS. Finalmente, conviene citar la posibilidad, cada vez más común, de contratar el servicio de gestión de incidencias en la nube. Un ejemplo lo constituye el producto Horizoon.

8. Control remoto de puestos de usuario

Una vez conocida una incidencia, registrada en el sistema gestor correspondiente y realizada la asignación de un técnico de soporte, es bastante común que el soporte de usuarios mediante control remoto se constituya en el primer nivel de atención a clientes desde el "HelpDesk" ya que supone un apoyo inmediato y rápido, y en función del tipo de escenario tecnológico un buen número de incidencias podrían ser resueltas de este modo.

La combinación de la asistencia telefónica y telemática constituye una herramienta muy potente en la resolución de problemas de forma remota sin que sea necesaria la intervención presencial de un técnico de soporte, lo que desde el punto de vista del análisis de costes en tiempo y costes económicos supone un valor añadido a considerar. Obviamente, la asistencia remota ahorra dinero a la empresa y hace más rentables los departamentos de HelpDesk siempre que se sea eficaz en su aplicación, si no el efecto será el de sensación de desatención y frustración en los usuarios.

El punto de equilibrio será determinar en qué caso el cliente requiere un contacto directo con un técnico de soporte que gestione adecuadamente la incidencia y "ponga cara" al servicio de atención al cliente y en qué casos es suficiente con la atención remota.

La sistematización de los protocolos a seguir en la recogida de llamadas, los procedimientos preestablecidos, la clasificación de prioridades y la determinación del canal más adecuado en cada caso son los puntos clave que determinarán el éxito del servicio de soporte.

El acceso remoto no solo ofrece asistencia al usuario, también puede emplearse para realizar mantenimiento preventivo a servidores o equipos de difícil acceso.

Si se carece de las herramientas de acceso remoto, es muy frecuente que el técnico deba guiar al usuario telefónicamente sin ver lo que se está haciendo en tiempo real, lo que puede generar complicaciones y pérdidas de tiempo del técnico y el del usuario, incidencias que suelen requerir finalmente desplazamientos para resolver el problema.

La gran mayoría de herramientas precisan de la autorización del usuario para que el técnico de soporte se haga con el control del equipo. De hecho, los aspectos de seguridad y privacidad son los principales obstáculos para este tipo de software. No suele agradar al usuario que alguien tome control de su equipo y pueda realizar modificaciones, por ejemplo.

La seguridad también es un factor importante. Es frecuente que las herramientas de control remoto sean capaces de evitar los cortafuegos de las organizaciones, anulando gran parte de las medidas de seguridad perimetrales.

Algunas herramientas precisan de la instalación de un cliente en las máquinas de los usuarios. En el caso de producirse vulnerabilidades en el software, los atacantes podrían aprovecharlas y tomar control remoto de dichas máquinas.

Además, con la externalización y globalización de todo tipo de servicios, en muchas ocasiones los de soporte no se encuentran en la misma ubicación de la organización, esto es, se proporcionarán utilizando Internet como red de comunicaciones. Es común que los fabricantes de hardware y software propongan sesiones de control remoto cuando se requiere asistencia técnica en caso de incidencias. Por ello, se hace necesario garantizar altos estándares de seguridad en situaciones de conexiones remotas que tomarán el control de equipos.

Como consecuencia, se desarrollaron técnicas que permiten conexiones más seguras, como el empleo de Redes Privadas Virtuales (*Virtual Private Networks, VPNs*), que restringen las conexiones en función de perfiles utilizando, además, cifrado en las comunicaciones.

Existe un gran número de herramientas que permite el control remoto de los puestos de usuario, tanto en la modalidad de software libre como propietario.

En esta última y para entornos Microsoft Windows, la propia Microsoft ha incluido en sus sistemas operativos de usuario el asistente de ayuda y soporte técnico.
De hecho, existe una cuenta predefinida en el sistema que se activa cuando se requiere soporte y se elimina cuando no se precisa.

Otras herramientas son WebEx de Cisco, Tivoli, de IBM o *System Center Configuration Manager (*SCCM*),* también de Microsoft.

De entre las herramientas más comunes empleadas en el acceso remoto para ofrecer soporte en la gestión de incidencias a los puestos de usuario se encuentran RemoteVNC y TightVNC, ambas basadas en el software VNC (en inglés *Virtual Network Computing*). VNC es un programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente.

Otras herramientas gratuitas, si su uso no es comercial, son TeamViewer, JoinMe, ShowMyPc, etcétera.

Por último, es interesante conocer algunas funcionalidades que ofrece el navegador Google Chrome en materia de control remoto. La funcionalidad se denomina Chrome Remote Desktop. Funciona con los principales sistemas operativos, Microsoft Windows, Linux y Mac OS X y también para facilitar soporte a equipos con el sistema operativo de Google, Chrome OS. Es muy cómodo de utilizar. Exige instalar la extensión para el navegador o la aplicación para Android y puede combinarse con Google Talk para que los usuarios conectados puedan mantener conversaciones en paralelo.