Introducción a la Seguridad Informática

Índice

1. Información y seguridad.
2. Un ejemplo trivial.
3. Evolución de la seguridad de los sistemas de información.
4. Los marcos de seguridad europeo y mundial.
5. Situación en España.

1. Información y seguridad

Significado de la palabra información

Si buscamos en un diccionario el significado del término información podemos encontrar lo siguiente:

---

información

nombre femenino

1. Acción de informar.
"cualquier país democrático tiene leyes que garantizan la libertad de información"
2. Noticia o dato que informa acerca de algo.
"el gobierno israelí recibió información acerca de dos de sus siete soldados desaparecidos; el periódico dispone de corresponsales distribuidos por todos los países que recogen las informaciones y las transmiten con la mayor rapidez"
3. Lugar, establecimiento o departamento donde se informa sobre algo a la persona que lo solicita.
"trabaja en información; para saber qué avión debe tomar diríjase a información"
4. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.
"editaron un catálogo con informaciones acerca de los productos que venden"

- **información privilegiada**
  Información a la que, por sus características, tienen acceso pocas personas, o lo tienen antes que otras muchas a las que también debe llegar.
- **información reservada**
  Información secreta.

5. Investigación de los antecedentes genealógicos de una persona, que se lleva a cabo con determinado fin, como el hecho de ocupar un empleo.

Etimología de la palabra información

La palabra *información* deriva del sustantivo latino *informatio(-nis)* (del verbo *informare*, con el significado de "dar forma a la mente", "disciplinar", "istruir", "enseñar"). Ya en latín la palabra *informationis* era usada para indicar un "concepto" o una "idea", pero no está claro si tal palabra pudiera haber influido en el desarrollo moderno de la palabra *información*.

Por otra parte la palabra griega correspondiente era "μορφή" (*morfè*, de la que por metatesis surgió la palabra latina *forma*), o si no "εἶδος" (*éidos*, de la cual deriva la latina *idea*), esto es: "idea", "concepto" o "forma", "imagen"; la segunda palabra fue notoriamente usada técnicamente en el ámbito filosófico por Platón y Aristóteles

para indicar la identidad ideal o esencia de algo (véase Teoría de las ideas). *Eidos* se puede también asociar a "pensamiento", "aserción" o "concepto".

Principales características de la información

En general la información tiene una estructura interna y puede ser calificada según varias características:

- **Significado** (semántica): Del significado extraído de una información, cada individuo evalúa las consecuencias posibles y adecúa sus actitudes y acciones de manera acorde a las consecuencias previsibles que se deducen del significado de la información. Esto se refiere a qué reglas debe seguir el individuo o el sistema experto para modificar sus expectativas futuras sobre cada posible alternativa.

- **Importancia** (relativa al receptor): Es decir, si trata sobre alguna cuestión importante. La importancia de la información para un receptor se referirá a en qué grado cambia la actitud o la conducta de los individuos. En las modernas sociedades, los individuos obtienen de los medios de comunicación masiva gran cantidad de información, una gran parte de la misma es poco importante para ellos, porque altera de manera muy poco significativa la conducta de los mismos. Esto se refiere a en qué grado cuantitativo deben alterarse las expectativas futuras. A veces se sabe que un hecho hace menos probables algunas cosas y más otras, la importancia tiene que ver con cuanto menos probables serán unas alternativas respecto a las otras.

- **Vigencia** (en la dimensión espacio-tiempo): Se refiere a si está actualizada o desfasada. En la práctica la vigencia de una información es difícil de evaluar, ya que en general acceder a una información no permite conocer de inmediato si dicha información tiene o no vigencia.

- **Validez** (relativa al emisor): Se evalúa si el emisor es fiable o puede proporcionar información no válida (falsa). Tiene que ver si los indicios deben ser considerados en la revaluación de expectativas o deben ser ignorados por no ser indicios fiables.

- **Valor** (activo intangible volátil): La utilidad que tiene dicha información para el destinatario.

Historia de la información

La historia de la información está asociada a su producción, tratamiento y transmisión. Una cronología de esa historia detallada, según la Wikipedia, puede ser:

- Siglos V a X - Alta Edad Media. El almacenamiento, acceso y uso limitado de la información se realiza en las bibliotecas de los monasterios de forma amanuense o manual.
- Siglo XII. Los Incas (Perú) usan un sistema de cuerdas para el registro de información numérica llamada Quipu, usado principalmente para contar ganado.
- Siglo XV - Edad Moderna. Con el nacimiento de la imprenta en Europa (Gutenberg), los libros comienzan a fabricarse en serie. Surgen los primeros periódicos.

- Siglo XX. 1926. Se inicia la primera retransmisión de televisión que afectará al manejo y tratamiento de la información con gran impacto en los métodos de comunicación social durante todo el siglo.
- Siglo XX. 1940. Jeremy Campbell, definió el término información desde una perspectiva científica, en el contexto de la era de la comunicación electrónica.
- Siglo XX. 1943. El austro-húngaro Nikola Tesla es considerado como inventor de la radio, aunque dicho invento se atribuyó en 1904 al italiano Guglielmo Marconi (premio Nobel de física junto con Ferdinand Braun, en 1909) y la patente no se reconoce a su autor hasta los años 1960 (patente de EE.UU. No. 645576, presentada en 1897 y aprobada el 20 de marzo de 1900) .
- Siglo XX. 1947. En diciembre John Bardeen (premio Nobel de física en 1956 y 1972), Walter Houser Brattain y William Bradford Shockley (premios Nobel de física en 1956), inventan el transistor. Acaban de sentar sin saberlo la

primera de las dos bases para una nueva revolución tecnológica y económica, actuando como detonante de un aumento exponencial de la capacidad de integración microeletrónica, de la popularización y la potencia de cálculo del ordenador.

- Siglo XX. 1948. Claude E. Shannon, elabora las bases matemáticas de la Teoría de la Información. Acaba de dar la segunda base de la revolución de las tecnologías de la información y la comunicación: la aplicación del Álgebra de Boole será el fundamento matemático para industrializar el procesamiento de la información. Nace así la Ciencia de la Computación o Ingeniería informática. La nueva revolución económica está servida. La humanidad entra en la **Era Digital** usando el transistor y la numeración binaria para simbolizar, transmitir y compartir la información.
- Siglo XX. 1948. Norbert Wiener, elabora la idea de cibernética en su famosa obra *Cibernética o el control y comunicación en animales y máquinas* (*Cybernetics or Control and Communication in the Animal and the Machine*) (1948) donde se encargó de "mantener el orden" en cualquier sistema natural o artificial de información.
- Siglo XX. 1951-1953. James Watson y Francis Crick descubren los principios de los códigos de ADN, que forman un sistema de información a partir de la doble espiral de ADN y la forma en que trabajan los genes.
- Siglo XX. 1969. En el contexto de la guerra fría, en la década de 1960, nace la embrionaria internet cuando se establece la primera conexión de ordenadores, conocida como ARPANET, entre tres universidades en California y una en Utah, (EE.UU.). Su expansión y popularización, y la democratización del conocimiento que facilita, transformará radicalmente las relaciones económicas, sociales y culturales en un mundo más y más interdependiente.
- Actualmente, ya en el siglo XXI, en un corto período de tiempo, el mundo desarrollado se ha propuesto lograr la globalización del acceso a los enormes volúmenes de información existentes en medios cada vez más complejos, con capacidades exponencialmente crecientes de almacenamiento y en soportes cada vez más reducidos. A pesar de ello todavía existen muchas fuentes de información en formato no digital o inaccesibles digitalmente por diversas causas. En este marco la proliferación de redes de transmisión de datos e información, de bases de datos con acceso en línea, ubicadas en cualquier lugar, localizables mediante internet, permiten el hallazgo de otras redes y centros de información de diferentes tipos en cualquier momento desde cualquier lugar. Es el resultado de datos gestionados a través de aplicaciones informáticas donde los datos son procesados y transformados en información que posteriormente es manejada como signo integrador y característico de progreso económico del siglo XXI.

Características de la información en internet

En internet hay gran cantidad de información a la que se puede acceder de manera casi instantánea. Las características de esta información son:

- Es **casi instantánea**, podemos acceder a ella de forma rápida y eficaz. La rapidez de acceso es un parámetro de gran importancia para el usuario, las páginas web que tardan en descargarse más de 20 segundos suelen ser consideradas lentas por los usuarios y es posible que no las vuelvan a visitar.

- Es **dinámica**. Los contenidos que se encuentran en internet se amplían con mucha frecuencia. Además, bastantes páginas son dinámicas cambiando su contenido regularmente. De forma que una de los criterios de calidad de la información en internet es la mayor o menor actualización.

- La información en internet es '**temporal**' de modo que aquella dirección electrónica que nos permitía acceder a un documento, en otro momento nos puede presentar otra información o producir un error.

- No toda la información que ofrece internet es de libre acceso. Hay muchas revistas que muestran resúmenes de los artículos y **se precisa de suscripción** o pago para la consulta del documento completo.

- Por último, es habitual encontrar **información en internet falsa**. Se puede encontrar tanto información veraz y de calidad como 'pseudoinformación' que bajo la apariencia de información de calidad oculta la finalidad de la misma que puede hacer que la información no sea totalmente veraz o esté sesgada hacia una dirección determinada, **caso típico de las pseudociencias**. En consecuencia, es imprescindible contrastar la información obtenida con otros documentos y con el propio criterio del profesional.

La siguiente imagen (tomada del blog Magonia) muestra cómo saber si una información es falsa.

Como ejemplo de que no nos debemos de fiar de cualquier información, se puede ver el siguiente artículo publicado en la revista de ARP-SAPC, Burundanga: nunca dejes que la verdad arruine una buena noticia" También es interesante La Medicina, la magia y la posverdad, publicado en el periódico Redacción Médica.

Posverdad y la difusión de información falsa

Internet ha contribuido a poner de moda palabras como **posverdad,** el término se atribuye al bloguero británico David Roberts, quien lo usó por vez primera en 2010. (el Diccionario Oxford incorporó la palabra *post-truth* a su listado y la denominó "palabra del año 2016", y el término se ha incluido en España en el diccionario de la RAE en diciembre de 2017), la mayor parte de los que leen de nuevas la palabra posverdad se sienten obligados a darle inmediatamente un significado. Y razonan (más o menos) así: si la posverdad está claro que no es la verdad, y lo contrario de la verdad es la mentira, concluimos que posverdad no es sino un nuevo rótulo para las mentiras de toda la vida, que a saber por qué oscuros motivos no reciben ya ese nombre de siempre. Yerran, sin embargo, lo cierto es que no, la posverdad no es lo mismo que la mentira. Mientras que a un mentiroso le interesa la verdad, para transmitir la idea contraria (su mentira), en tiempos de posverdad lo que le ocurre a la verdad es que simplemente ha dejado de interesar. No importa que lo que digas sea verdadero. Tampoco, como al mentiroso, te interesa convencer de algo falso (y beneficioso para ti). Simplemente interesa hablar con una total indiferencia hacia

cómo son las cosas en realidad. Y que a la audiencia, naturalmente, también le dé igual qué sea o no sea verdad.

Según el profesor de la UNAM (México) Arnoldo Kraus, "estudios recientes han demostrado que el 70 % de los internautas tienen dificultades para distinguir entre una noticia falsa y una verdadera. Esa es una de las razones por las cuales Trump obtuvo más de sesenta millones de votos. Nada bueno auguran los tiempos donde lo fatuo y estúpido se viraliza. Televisión, internet y el mundo, bastante imbécil, de los tuits, suman mucho. Si a ese conglomerado agregamos miedo, inseguridad e inestabilidad económica, el caldo de cultivo queda servido: la posverdad cuenta con suficientes nutrientes".

La comunidad científica de EE.UU. está preocupada porque el presidente Trump ha manifestado su propósito de tomar decisiones ajenas a los hechos contrastados y porque creen que su política se opondrá al progreso del conocimiento. Y los científicos del Reino Unido creen que la salida de la Unión Europea debilitará de forma significativa a la ciencia británica. De confirmarse esos temores, el avance del conocimiento se vería frenado en dos de los países con mayor tradición y potencia científica del mundo. Dejarían así un mayor espacio al avance de la sinrazón. Habría comenzado a formarse de ese modo un círculo vicioso de imprevisibles consecuencias.

Teoría de la información

La teoría de la **comunicación se refiere a los medios para transmitir información de una fuente a un usuario**. La naturaleza de la fuente puede ser muy variada, podría ser voz, una señal electromagnética o una secuencia de símbolos binarios. El canal puede ser una línea telefónica, un radioenlace o un medio magnético u óptico: cinta magnética o disco compacto. El canal generalmente será perturbado por el ruido que dependerá del entorno y de la naturaleza del canal: perturbaciones eléctricas, arañazos, etc. . . . Un codificador realiza operaciones en la salida de la fuente antes de la transmisión. Estas operaciones pueden ser, por ejemplo, la modulación, la compresión o la adición de redundancia para combatir el ruido en las redes de comunicación. Generan una salida de la fuente compatible con el canal. En, el decodificador se podrá, a partir de la salida del canal, transmitir de manera aceptable la información facilitada por la fuente.

“La información contenida en este libro", "La información que tienes sobre el problema", "La información codificada en el genoma", "La poca información proporcionada por su larga intervención"... estos son sólo algunos ejemplos de las diversas frases y contextos en los que la palabra información es comúnmente utilizada. Cuando hablamos de información, a menudo insinuamos "información de algún valor", o "información que puede ser usada para un propósito", o "contenido de información". En el contexto mismo de la investigación informática, la palabra información, tal como se emplea en la expresión “tecnologías de la información y la comunicación”, tiene varios significados. Se trata de técnicas diseñadas para proteger la información, como la criptografía, y en un campo muy diferente, el de las bases de datos, la creación de sistemas de información.

En la década de 1940, el ingeniero Claude E. Shannon (biografía en: http://centenaire-shannon.cnrs.fr/) desarrolló una teoría matemática llamada **teoría de la información** que describe los aspectos más fundamentales de los sistemas de comunicación. Esta teoría se refiere a la construcción y estudio de modelos matemáticos utilizando esencialmente la teoría de probabilidades. Desde este primer trabajo publicado en 1948, la teoría de la información se ha vuelto cada vez más precisa y se ha convertido en una parte esencial de cualquier sistema de comunicación, en el sentido más amplio del término.

Es una teoría matemática que formaliza la información y su transmisión de manera probabilística. Sin embargo, cuando se quiso hablar específicamente sobre la información genética en los años setenta, se trataron de establecer vínculos con esta teoría matemática; los resultados no fueron proporcionales a las esperanzas y ambiciones anunciadas. De manera similar, mientras que en un momento dado la teoría de la información de Shannon pudo haber sido pensada como "teoría informática", pronto se descubrió que este no era el caso. De hecho, la teoría de Shannon es una **teoría del contenido de la información relativa a objetivos como comprimir o transmitir información a través de un canal**. Es relativa a las distribuciones de probabilidad; en última instancia, es independiente de los propios datos. No dice nada sobre un conjunto de datos en particular, sino sobre el promedio de un conjunto de datos.

Otra teoría de la información, llamada "teoría algorítmica de la información" o "teoría de la información de Kolmogorov", fue propuesta por Andrei Kolmogorov en 1965. Veremos cómo estas dos teorías se relacionan entre sí, y cuáles son las limitaciones de ambas.

Problema general de las teorías de la información

Supongamos que tenemos una secuencia de símbolos s, que forman una cadena de caracteres. Podemos mostrar poco o mucho interés en estos símbolos, encontrar significado o no en su secuenciación. Independientemente de estos elementos externos, ¿a qué nos referimos cuando hablamos de su contenido o valor informativo?

He aquí algunos ejemplos muy concretos de una serie de símbolos a los que reconocemos el contenido y el valor informativo:

- Relación de caracteres que componen el libro “El Mundo y sus Demonios (Carl Sagan);
- Lista mecanografiada de los emplazamientos de lanzamisiles estadounidenses en todo el mundo;
- Una tabla de logaritmos;
- El genoma completo de un virus del VIH (SIDA);
- Un CD con conciertos de piano de Chopin interpretados por Samson François;
- El programa de procesamiento de textos utilizado para escribir este texto;
- El programa de este mismo procesador de textos antes de que haya sido compilado, (programa fuente).

Estos ejemplos corresponden a objetos que tienen, o han tenido en algún momento, un contenido informativo de algún valor para la persona que los ha producido y, con toda seguridad, para otros. Por ejemplo, podemos darle a estos objetos un precio, un valor de mercado.

Aceptamos que hay un contenido “bruto” de información para cada uno de estos objetos. Este contenido bruto se da en dígitos (o bits) y puede definirse como el número de memorias elementales que la cadena s ocupa en la memoria de un ordenador cuando no se somete a ningún tratamiento en particular, salvo ponerlo en un formato compatible con el sistema informático.

El contenido “bruto” de información de una cadena de caracteres s de longitud n está dado por n si n tiene solo ceros (0) y unos (1) y n log(m)/log(2) si la cadena tiene caracteres tomados de entre m, en lugar de entre 2.

Entre nuestros ejemplos, el objeto con mayor contenido de información bruta es el disco compacto, el objeto con menor contenido de información es la lista de ubicaciones de lanzamisiles. El que tiene el valor de mercado más alto es el procesador de texto no compilado. El que menos valor tiene actualmente es la tabla de logaritmos.

De estos ejemplos se desprende claramente que el contenido de la información bruta no determina su valor: el valor de la información es algo más complicado y, sobre todo, adquiere un significado diferente según el contexto. Esto explica por qué hay varias teorías de la información. Dependiendo del significado que le demos a la palabra información, el concepto debe formalizarse de manera diferente.

Adoptaremos el siguiente procedimiento: primero, fijaremos una meta, luego determinaremos el valor de la información en las cadenas para esa meta. Descubriremos así que al especificar el objetivo, obtenemos diferentes teorías, incluyendo la teoría de la información de Shannon y la teoría algorítmica de la información, mencionadas anteriormente.

Teoría algorítmica de la información

Si nos fijamos el objetivo de poder hacer la cadena de caracteres s, y si asumimos que tenemos una máquina M para este propósito, entonces el valor de la información de s es la longitud del programa más pequeño (escrito en binario) que, cuando se da a M, le permite reconstituir la cadena s. El valor en la información es este contenido incomprensible de s. Hablamos de compresión, ya que sustituimos la cadena s por algo más corto, el programa más pequeño que la genera. (Por ejemplo, la cadena "papapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapapa... papapapapapapapapapapapapapa" se comprimirá en "recopia N veces' pa'".

La idea aquí es simple: un mensaje es pobre en información si es generado por un programa de computación rudimentario, y rico en información si se trata de programas sofisticados, por lo tanto, los grandes pueden producir este mensaje.

Resulta que la potencia de computación de las máquinas no es ilimitada. Pueden ir más o menos rápido, pero tan pronto como se trata de máquinas de cierta potencia, lo que pueden calcular es el máximo de lo que cualquier máquina poderosa puede

calcular. Este es el descubrimiento fundamental de Turing en 1936: hay mecanismos computacionales universales y cualquier microordenador es un mecanismo universal. Mientras nos demos un mecanismo de cálculo universal, la noción del programa más pequeño que puede generar s no depende de la máquina universal que usemos. O más precisamente, depende de esta máquina sólo por una constante aditiva, que puede despreciarse en la primera aproximación si se trata de secuencias suficientemente largas. El descubrimiento de este resultado de independencia, o teorema de invariancia, es lo que subyace a la teoría algorítmica de la información.

La noción de valor en la información obtenida es particularmente atractiva. Esta es la noción de complejidad de Kolmogorov o contenido de información de Kolmogorov.

El papel teórico particular desempeñado por la teoría de Kolmogorov, como la teoría óptima del contenido descriptivo de la información, está comenzando a ser reconocido por biólogos y físicos. En física, el concepto de información es difícil de identificar, a pesar de los vínculos a menudo evocados con la termodinámica, relaciones que parecen haber sido objeto de una importante revisión muy recientemente gracias al trabajo de Bennett y Zurek. En cuanto a la biología, combina todas las dificultades, porque obviamente debe atribuirse un sentido pragmático al concepto de información biológica, que hace que las teorías matemáticas de la información sean inadecuadas o incompletas, y la utilidad de las teorías termodinámicas de información. Frente a estos problemas difíciles, la noción de complejidad o contenido de información de Kolmogorov ofrece una nueva herramienta teórica.

Teoría de la información de Shannon

Si el objetivo es transmitir una cadena de caracteres a un receptor con algún conocimiento de la frecuencia de las letras (tomadas en el alfabeto {a1, a2, ..., an}) de la cadena s que queremos transmitir, entonces usaremos otra definición de información, que se deriva de la teoría de la información de Shannon.

Esta formulación proporciona el contenido de información promedio del conjunto de cadenas de caracteres cuando se tienen en cuenta las probabilidades p(i) de las letras utilizadas. El "teorema de la vía sin ruido" indica que no se puede, en promedio, comprimir más las cadenas de caracteres s.

Implícitamente, en este diseño de información, se supone que es probable que el receptor haga ciertos cálculos para reconstruir s a partir de lo que se le transmite. Implícitamente, por lo tanto, asumimos un cierto poder de cálculo del receptor. En última instancia, la máquina M que ejecuta la decodificación se puede tomar como referencia, y a continuación, se descubre que la teoría de Shannon debe ser vista como una versión probabilística de la teoría de la información algorítmica y compatible con élla en el sentido siguiente:

El contenido algorítmico medio de información de Kolmogorov de las cadenas de caracteres de longitud n (ponderados por probabilidades resultantes de las

frecuencias supuestas p(i) para las letras ai) es del mismo orden de magnitud que el contenido de información de Shannon.

Por lo tanto, la teoría de la información de Shannon es también una teoría de la información por compresión, que, en lugar de considerar cualquier secuencia, supone que las secuencias que uno transmite satisfacen ciertas propiedades estadísticas. Finalmente, la teoría de Shannon es una teoría del contenido de información relativa a un propósito de compresión y una cierta distribución estadística de las secuencias. Por lo tanto, no se trata de una teoría de la información limitada porque solo trata el problema de la transmisión, como a veces decimos, es una teoría de la información probabilística compatible con la teoría algorítmica de la información y limitada simplemente porque se relaciona con distribuciones probabilísticas particulares.

Por lo tanto, hablar de la información Shannon del genoma de un ser vivo no tiene sentido, debido a que el genoma es una cadena única: aproximarlo por el contenido incompresible medio del conjunto de cadenas a las que pertenece puede conducir a un error grave. Otro ejemplo, si una cadena de diez millones de 0 y 1 es vista como un elemento particular del conjunto de todas las cadenas de diez millones de 0 y 1 (0 y 1 provistos de igual peso), se le asignará un contenido de información de diez millones de bits, lo cual es absurdo, porque tal secuencia se puede describir con algunos bits (eso es lo que acabo de hacer). Tal conjunto no es un elemento "típico" del conjunto de las diez millones de secuencias de 0 y 1.

La teoría de la información de Shannon es consistente con la de Kolmogorov. Cada una tiene su papel a jugar, por ejemplo, en una teoría de medición o toma de información. Es el juego complementario de las dos teorías que deben considerarse. Una situación en la que tenemos pocos elementos solo puede asimilarse a la situación típica de todas las situaciones compatibles con lo que conocemos, entonces usamos la teoría de Shannon. A medida que se adquieren los detalles, es la teoría de Kolmogorov la que debe convertirse en preponderante.

Todas las teorías que acabamos de presentar son teorías de información "compresionales" (o "descriptivas"). La compresión de datos es ciertamente importante para almacenarlos a bajo costo o para transmitirlos lo más rápido posible, pero está bastante claro que esto no es lo único que constituye el valor de la información. Sabemos, por ejemplo, que una secuencia aleatoriamente dibujada de 0 y 1 es habitualmente incompresible, pero eso no significa, por supuesto, que cada secuencia de 0 y 1 tenga valor, ni que cada secuencia de 0 o 1 es incompresible.

Teorías pragmáticas de la información

Entre nuestros ejemplos, consideramos un programa de procesamiento de textos. Está claro que la compilación de un programa fuente en un programa ejecutable crea información valiosa.

Aquí el objetivo es mixto: tener una forma compacta de un algoritmo bastante rápido realizando una familia de cálculos. Se destaca que:

- Cuanto más rápido sea el código, más valiosa será la compilación;
- Cuanto más compacto es el código compilado, más valioso es (hoy en día, contrariamente a lo que ocurrió hace 30 años, preferimos la velocidad a costa del espacio, porque el precio de las memorias ha bajado);
- Cuantos más problemas maneje el programa compilado, mayor será su valor.

El valor de la información contenida en un programa compilado es una mezcla de estas tres cualidades (rapidez, compacidad, campo de problemas tratados), y otras más como la originalidad, portabilidad, etcétera. El valor informativo de un programa compilado (y muchas cadenas) no puede reducirse a un solo aspecto: el contenido informativo de un programa compilado no es la información algorítmica de Kolmogorov, ni la teoría de Shannon o la información de profundidad de Bennett.

Si consideramos que el objetivo perseguido es de naturaleza práctica, como sobrevivir en un entorno determinado o ganar el máximo de dinero posible en la bolsa de Madrid, entonces el valor de la información en una cadena se medirá en función de este objetivo. La información de gran valor será el lugar a donde ir para obtener un alimento en particular, o el nombre de la acción que subirá. Una vez más, las teorías descriptivas de la información serán de poca utilidad.

Estas teorías matemáticas de la información, ya sea que estén disponibles o aún se están desarrollando, tienen pretensiones de universalidad y aplicabilidad. Pero debemos tener cuidado. A veces se entienden mal: la de Shannon ha dado lugar a mucha retórica, que ahora se entiende que no ha sido suficientemente cautelosa; la retórica de Kolmogorov a veces también parece engañar. Sin embargo, la actitud de prudencia que hay que tomar frente a estas teorías no implica infertilidad: recordemos al premio Nobel Jacques Monod que, sin duda sintiendo que no todo estaba claro por el lado de las teorías físicas de la información, hablaba de lo que se les hacía decir "de generalizaciones y asimilaciones imprudentes". Monod, el gran científico que descubrió el ARN mensajero y revolucionó la biología molecular, fue cauteloso. Por instinto, sospechaba de la especulación demasiado precipitada, y sin embargo su trabajo no era estéril. En estas zonas de riesgo, si queremos ir demasiado rápido, corremos el riesgo de no verlo todo; en los últimos años se han propuesto muchas ideas muy interesantes, sería una pena que nos las perdiéramos porque estamos conduciendo nuestras cabezas en la oscuridad.

Usos de la información

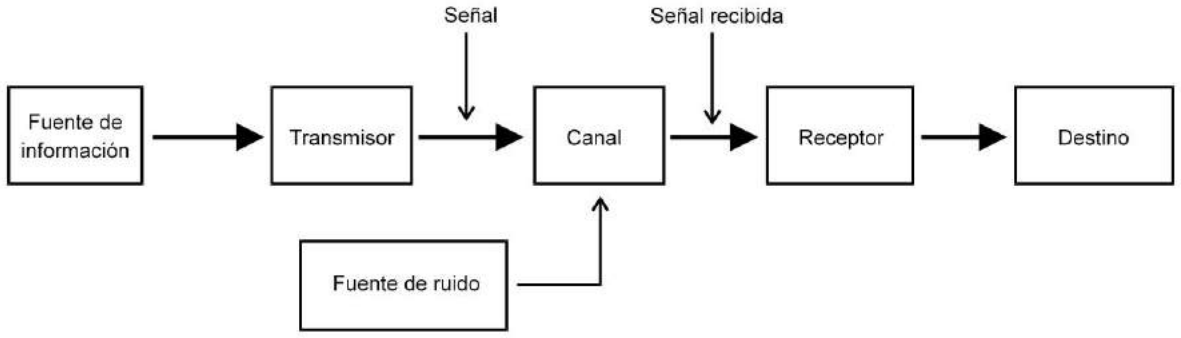
Se considera que la generación y/o obtención de información persigue estos objetivos:

- Aumentar/mejorar el conocimiento del usuario, o dicho de otra manera reducir la incertidumbre existente sobre un conjunto de alternativas lógicamente posibles.
- Proporcionar a quien toma decisiones la materia prima fundamental para el desarrollo de soluciones y la elección.
- Proporcionar una serie de reglas de evaluación y reglas de decisión para fines de control.

En relación con el tercer punto, la información como vía para llegar al conocimiento, debe ser elaborada para hacerla utilizable o disponible (este proceso empírico se llama Documentación y tiene métodos y herramientas propios), pero también es imposible que la información por sí sola dote al individuo de más conocimiento, es él quien valora lo significativo de la información, la organiza y la convierte en conocimiento. El dato, por así llamarlo, es en sí un "prefijo" de la información, es decir, es un elemento previo necesario para poder obtener la información.

Daños a la información

La información que circula entre una fuente y un receptor en el destino es habitual que resulte dañada, siendo las diversas fuentes de ruido que afectan al medio de transmisión las responsables más importantes, siendo muchas veces físicamente inevitables.



Las diversas situaciones respecto al flujo de la información son las siguientes:

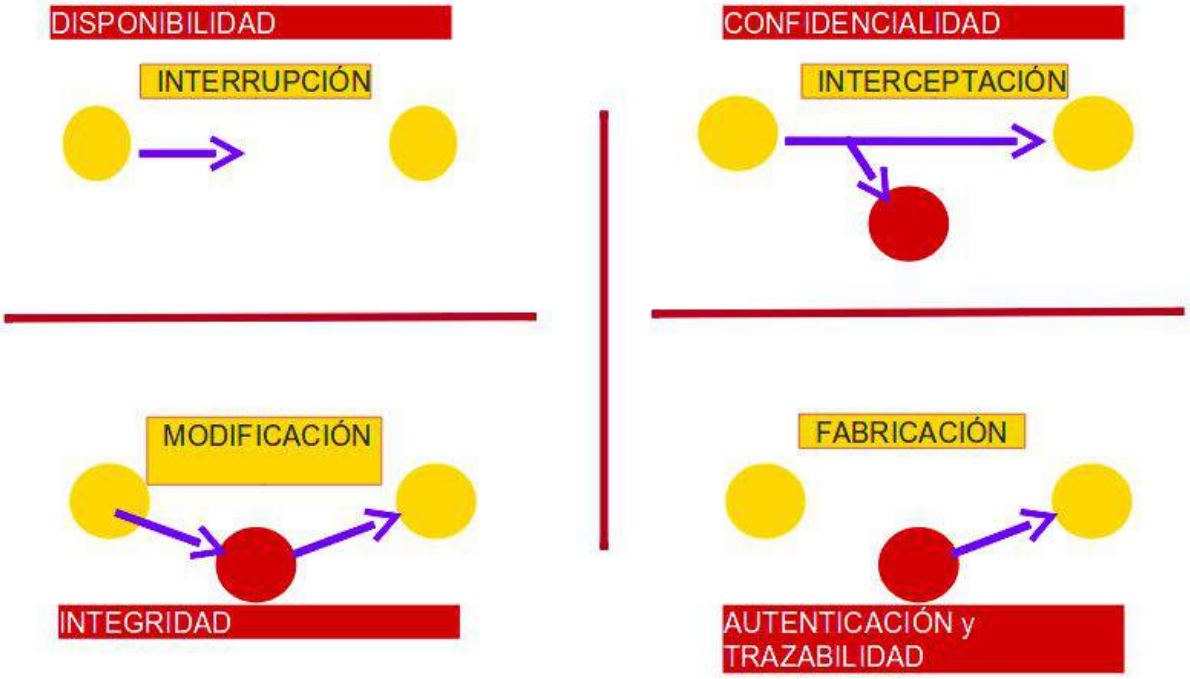
FLUJO NORMAL: Los mensajes en una red se envían a partir de un emisor a uno o varios receptores El atacante es un tercer elemento; en la realidad existen millones de elementos atacantes, intencionales o accidentales.

INTERRUPCIÓN: El mensaje no puede llegar a su destino, un recurso del sistema es destruido o temporalmente inutilizado. Este es un ataque contra la Disponibilidad Ejemplos: Destrucción de una pieza de hardware, cortar los medios de comunicación o deshabilitar los sistemas de administración de archivos.

INTERCEPTACIÓN: Una persona, ordenador o programa sin autorización logra el acceso a un recurso controlado. Es un ataque contra la Confidencialidad. Ejemplos: Escuchas electrónicos, copias ilícitas de programas o datos, escalamiento de privilegios.

MODIFICACIÓN: La persona sin autorización, además de lograr el acceso, modifica el mensaje. Este es un ataque contra la Integridad. Ejemplos: Alterar la información que se transmite desde una base de datos, modificar los mensajes entre programas para que se comporten diferente.

FABRICACIÓN: Una persona sin autorización inserta objetos falsos en el sistema. Es un ataque contra la Autenticidad. Ejemplos: Suplantación de identidades, robo de sesiones, robo de contraseñas, robo de direcciones IP, etc… Es muy difícil estar seguro de quién está al otro lado de la línea.



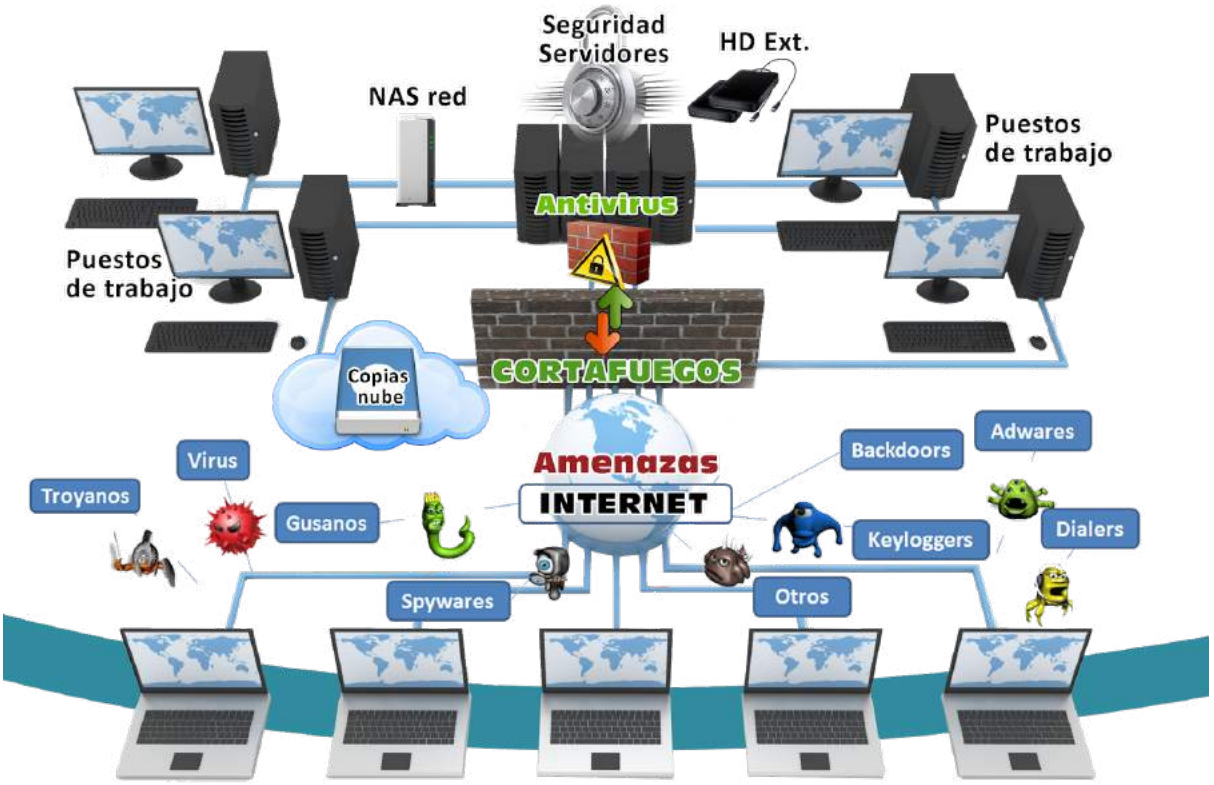
Seguridad

Según la Wikipedia, **seguridad** (del latín *securitas*) cotidianamente se puede referir a la ausencia de riesgo o a la confianza en algo o en alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo de conocimiento a la que haga referencia en la seguridad. En términos generales, la seguridad se define como "el estado de bienestar que percibe y disfruta el ser humano".

Una definición de la seguridad es "**Ciencia interdisciplinaria que está encargada de evaluar, estudiar y gestionar los riesgos que se encuentra sometido una persona, un bien o el ambiente**". Se debe diferenciar la seguridad sobre las

personas (seguridad física), la seguridad sobre el ambiente (seguridad ambiental), la seguridad en ambiente laboral (seguridad e higiene), etc.

Con el desarrollo del uso de internet, cada vez más empresas están abriendo sus sistemas de información a sus socios o proveedores, por lo que es imprescindible conocer los recursos que dispone la empresa para proteger y controlar el acceso y los derechos de los usuarios de los sistemas informáticos. Además, con el nomadismo, que consiste en permitir al personal conectarse desde cualquier lugar, el personal es impulsado a "transportar" parte del sistema de información fuera de la infraestructura segura de la empresa.



El aspecto que nos interesa es la seguridad Informática, que se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

- **Confidencialidad**: Los datos solo pueden ser legibles y modificados por personas autorizadas, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

- **Integridad**: Los datos están completos, sin modificar y todos los cambios son reproducibles (se conoce el autor y el momento del cambio).

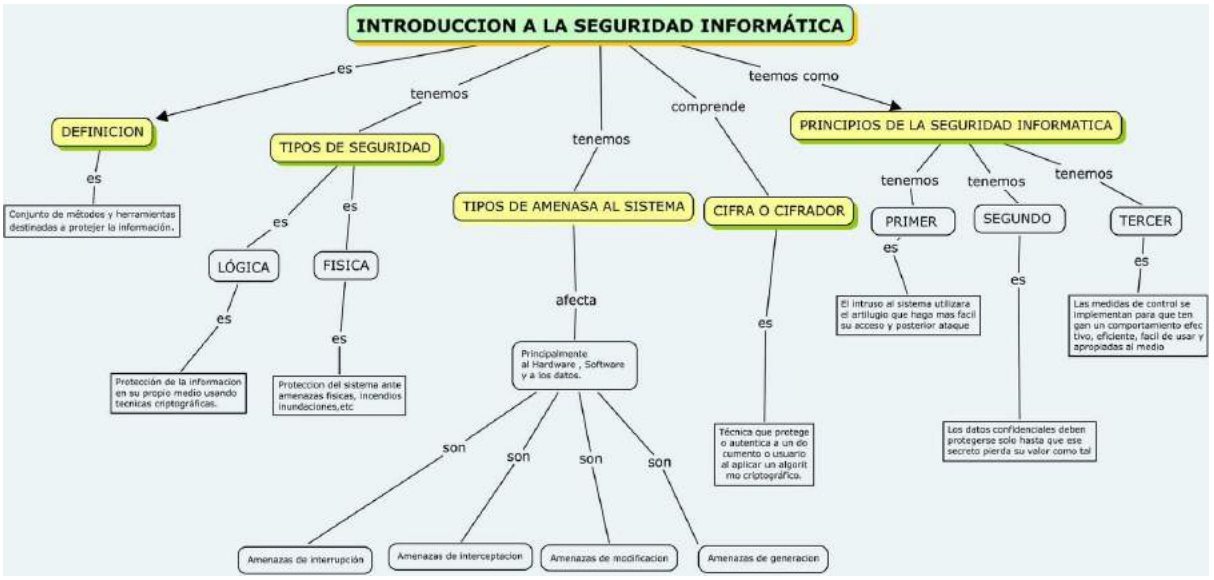
- **Disponibilidad**: El acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallos del sistema y proveer el acceso adecuado.

Otros dos aspectos que se consideran habitualmente son:

- **No repudio**: Garantiza que una transacción no puede ser negada.
- **Autenticación**: Asegurando que solo las personas autorizadas tengan acceso a los recursos.

Necesidad de un enfoque global de seguridad

La seguridad de un sistema informático suele estar sujeta a metáforas. De hecho, se compara regularmente con una cadena, explicando que el nivel de seguridad de un sistema se caracteriza por el nivel de seguridad del eslabón más débil. Por ejemplo, una puerta reforzada es inútil en un edificio si las ventanas están abiertas y accesibles desde la calle.



Esto significa que la seguridad debe abordarse en un contexto global y, en particular, tener en cuenta los siguientes aspectos:

- **Sensibilizar** a los usuarios sobre los problemas de seguridad.
- **Seguridad lógica**, es decir, seguridad a nivel de datos, incluyendo datos empresariales, aplicaciones o sistemas operativos.
- **Seguridad de las telecomunicaciones**: tecnologías de red, servidores corporativos, redes de acceso, etc.
- **Seguridad física**, es decir, seguridad a nivel de infraestructuras físicas: salas seguras, lugares abiertos al público, zonas comunes de la empresa, puestos de trabajo para el personal, etc.

Aplicación de una política de seguridad

La seguridad de los sistemas informáticos se limita, en general, a garantizar los derechos de acceso a los datos y recursos de un sistema mediante el establecimiento de mecanismos de autenticación y control que garanticen que los usuarios de dichos recursos solo tienen los derechos que se les conceden.

Sin embargo, los mecanismos de seguridad establecidos pueden causar molestias a los usuarios y las normas y reglamentos se complican cada vez más a medida que la red se amplía. Por lo tanto, la seguridad informática debe estudiarse de manera que no impida a los usuarios desarrollar los usos necesarios para ellos y que puedan utilizar el sistema de información con confianza.

Por este motivo, es necesario definir una política de seguridad en primera instancia, que se desarrolla en las cuatro etapas siguientes:

- Identificar las necesidades de seguridad, los riesgos informáticos y sus posibles consecuencias;
- Desarrollar reglas y procedimientos a implementar en los distintos departamentos de la organización para los riesgos identificados;
- Supervisar y detectar las vulnerabilidades del sistema de información y mantenerse al tanto de los fallos de la aplicación y del hardware;
- Definir las acciones a tomar y con quién contactar si se detecta una amenaza.

Por lo tanto, la política de seguridad es el conjunto de orientaciones seguidas por una organización (en el sentido más amplio) en términos de seguridad. Como tal, debe desarrollarse a nivel de gestión de la organización interesada, ya que afecta a todos los usuarios del sistema.

A este respecto, no corresponde exclusivamente a los administradores de TI definir los derechos de acceso de los usuarios, sino más bien a sus gestores jerárquicos. El rol del administrador de TI es, por lo tanto, asegurar que los recursos de TI y los derechos de acceso sean consistentes con la política de seguridad de la organización.

Además, dado que es el único que conoce perfectamente el sistema, es responsable de transmitir la información de seguridad a la dirección, posiblemente asesorando a los responsables de la toma de decisiones sobre las estrategias a implementar, además de ser el punto de entrada para la comunicación con los usuarios sobre cuestiones y recomendaciones de seguridad.

La seguridad informática de la empresa se basa en un buen conocimiento de las normas por parte de los empleados, gracias a campañas de formación y sensibilización dirigidas a los usuarios, pero debe ir más allá y cubrir, en particular, los siguientes ámbitos:

- Un sistema de seguridad físico y lógico adaptado a las necesidades de la empresa y de los usuarios;
- Un procedimiento de gestión de actualizaciones;
- Una estrategia de copias de seguridad correctamente planificada;
- Plan de recuperación de incidentes;
- Un sistema documentado y actualizado;

Situación real en muchos casos

Muchas organizaciones dedican demasiado tiempo y dinero a una amplia gama de soluciones que no funcionan bien como un todo y no proporcionan una visión completa e integrada de los riesgos ambientales. Esta situación se ve agravada por la falta de recursos para la ciberseguridad, que ha sido objeto de mucho debate. Además, el uso simultáneo de soluciones y plataformas de muchos vendedores crea vacíos a los que pueden dirigirse los *hackers*. La clave es establecer lo que llamamos un enfoque de seguridad por capas, basado en controles de seguridad reconocidos como la base de un alto nivel de seguridad en toda la organización.

En concreto, ¿cuáles son las causas profundas del problema al que nos enfrentamos? No es muy difícil convertirse en un cibercriminal. Los kits operativos están disponibles en línea, lo que simplifica el proceso de ciberataque incluso para los *hackers* más inexpertos. Estos kits incluyen un código operativo preescrito, y los delincuentes a menudo tendrán acceso a soporte y actualizaciones para estos kits, al igual que el software legal comercial. Añadiendo a esas sofisticadas herramientas, originalmente diseñadas para el espionaje cibernético y ahora fácilmente accesibles, tenemos una caja de juego llena de “armas letales”.

Si se aplicaran parches con regularidad y la seguridad de todos se mantuviera en un nivel aceptable, los ataques podrían contenerse. Sin embargo.....

- **El software es inherentemente vulnerable**: Cientos de miles de líneas de código han sido escritas por humanos. Pero los humanos cometemos errores, nadie escribe software que esté completamente libre de errores e inmune a posibles atacantes.

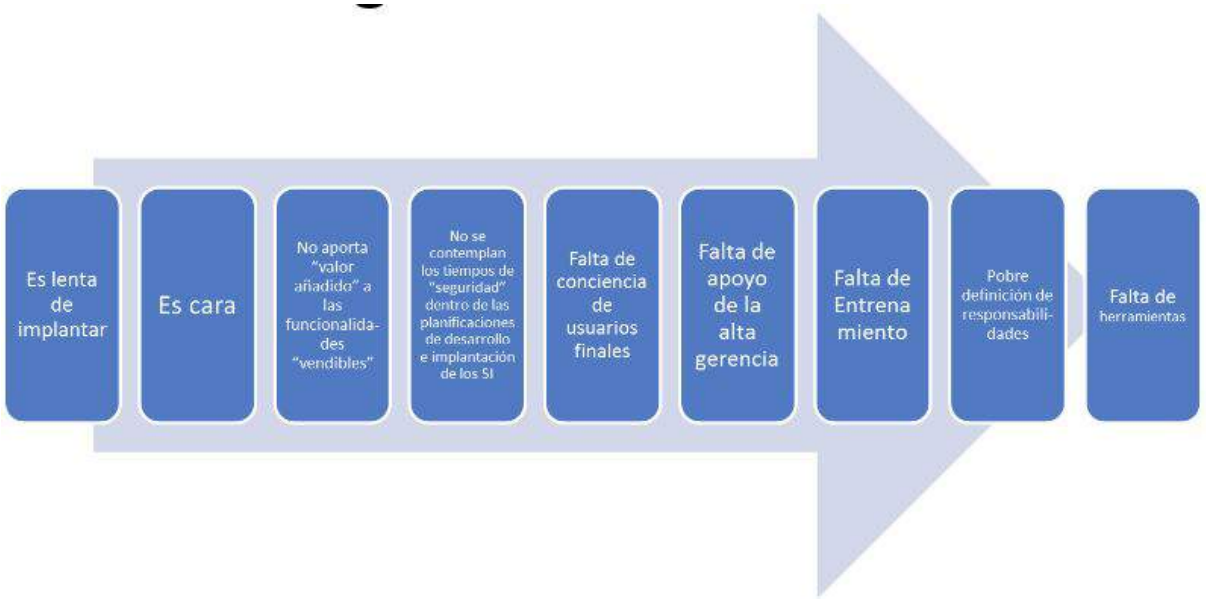
- El software más antiguo tiene más vulnerabilidades expuestas y el software heredado no se corrige, por lo que **cuanto más antiguo es el software, más se descubren, exponen y explotan sus vulnerabilidades**. Además, en los programas de ordenador ya no se corrigen sus fallos después de cierto tiempo. Esta no es una regla universal pero, en general, el software heredado no recibe las actualizaciones que necesita.

- **El software más reciente no está correctamente actualizado**: Por ejemplo, los parches estaban disponibles para los sistemas operativos Windows antes de WannaCry. Sin embargo, incluso con estos parches disponibles, las organizaciones fueron víctimas de NotPetya un mes después de WannaCry. Tal vez no tenían las herramientas para reparar su entorno o tenían recursos

limitados. Cualquiera que sea la razón, la disponibilidad de parches no significa que se apliquen correctamente.

Una vez establecidos los fundamentos de la seguridad a nivel de software, se debe considerar el aspecto humano. La educación del usuario es vital para evitar que los correos electrónicos de *phishing* potencialmente maliciosos se infiltren, mientras que las copias de seguridad regulares (incluyendo copias de seguridad fuera de la red para proteger contra *ransomware*) reducirán el riesgo de pérdida de datos. La configuración adecuada de los cortafuegos también puede ayudar a detener la propagación de los programas de rescate dentro de la empresa. Sin embargo, el parcheo y el control de aplicaciones deben estar en la parte superior de la lista para todas las organizaciones que buscan fortalecer su estrategia contra los ataques y pueden ayudar a reducir significativamente el tamaño de su ataque, haciendo más fácil apoyar los ataques que pasan, incluso con recursos limitados.

Los ataques de envergadura tienen un impacto mundial y mediático, pero luego las organizaciones vuelven a un estado de ceguera ante los problemas de ciberseguridad. Es probable que corrijan las vulnerabilidades señaladas, pero no siempre tienen en cuenta seriamente cómo actualizarán sus máquinas en el futuro, y no ponen en marcha un plan proactivo de respuesta a incidentes y seguridad que pueda simplificar y acelerar el retorno a la normalidad después de un ataque, y reducir significativamente las posibilidades de infectarse en primer lugar. La base de un enfoque de "retorno a lo básico" es el establecimiento de un programa de seguridad de una manera estratégica en lugar de reactiva o táctica.



Riesgo

Del ant. *riesco* 'risco', por el peligro que suponen.
1. m. Contingencia o proximidad de un daño.
2. m. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

riesgo de crédito
1. m. Econ. riesgo que sufre una entidad financiera derivado de la no devolución en plazo de los créditos concedidos a sus clientes.

riesgo de interés
1. m. Econ. riesgo de que disminuya el valor de un título, especialmente de renta fija, como consecuencia de una subida de los tipos de interés.

riesgo de mercado
1. m. Econ. Incertidumbre para un inversor o entidad financiera, derivada de que los cambios que se producen en los mercados, p. ej., en los tipos de interés, de cambio, etc., alteren el precio de sus activos.

riesgo de reinversión
1. m. Econ. riesgo de que los rendimientos futuros de una inversión no puedan ser reinvertidos al tipo de interés vigente en la actualidad.

riesgo específico
1. m. Econ. riesgo que puede ser reducido mediante la diversificación.

riesgo operativo
1. m. Econ. riesgo que sufre una empresa derivado de la posibilidad de fallos en su propio funcionamiento.

riesgo país
1. m. Econ. riesgo total de una operación financiera asociado a los factores políticos y estructurales del país en el que se realiza.

riesgo sistémico
1. m. Econ. riesgo asociado con el mercado total de activos y que no puede reducirse mediante la diversificación.

riesgo soberano
1. m. Econ. riesgo de que el Gobierno de un país no cumpla sus obligaciones.

a riesgo y ventura
1. loc. adv. Dicho de acometer una empresa o de celebrar un contrato: Sometiéndose a influjo de suerte o evento, sin poder reclamar por la acción de estos.

correr riesgo algo
1. loc. verb. Estar expuesto a perderse o a no verificarse.

El término riesgo tuvo su origen en el siglo XVII con las matemáticas asociadas a los juego de azar, actualmente se refiere a la **combinación de la probabilidad y la magnitud de potenciales pérdidas y ganancias**. Durante el siglo XVIII, el riesgo, fue visto como un concepto neutral, considerando las pérdidas y ganancias y fue empleado en la marina. En el siglo XIX, el riesgo se extendió al estudio de la economía. En el siglo XX tomó una connotación negativa al referirse a los peligros en la ciencia y tecnología.

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización". (ISO/Guide73:2009(en). Disponible: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en)

Medición del riesgo

Es importante medir los riesgos, no solo por la probabilidad o frecuencia de su aparición, sino también por la medición de sus efectos potenciales, que

dependiendo de las circunstancias y cuando ocurren, pueden tener consecuencias insignificantes o catastróficas. A veces cuando falla un programa informático, basta con reiniciarlo, pero a veces el incidente se agrava y hay que realizar una reparación o corrección antes de continuar el trabajo emprendido. Pero estos mismos incidentes pueden tener consecuencias mucho más graves:

- Datos irreparablemente perdidos o alterados, haciéndolos inutilizables;
- Datos o tratamientos que no estén disponibles de forma permanente, lo que puede dar lugar a la interrupción de una producción o servicio;
- Divulgación de información confidencial o errónea que pueda beneficiar a las empresas competidoras o dañar la imagen de la empresa;
- Acciones que pueden causar accidentes físicos o tragedias humanas.

En la época en que vivimos, de procesamiento e intercambio masivo generalizado, el impacto de eventos importantes como un corte de suministro de energía a gran escala o la saturación de la red de internet durante varias horas darían lugar a consecuencias graves.

Aparte de estos casos excepcionales, se pueden anticipar muchos riesgos y hay casos para la mayoría de ellos. Un ejemplo son las precauciones tomadas poco antes del año 2000, que, aunque la realidad del riesgo era (y sigue siendo) a veces controvertida, puede haber evitado graves inconvenientes.

Cada organización, pero también cada usuario, tiene un interés personal en evaluar, aunque sea a grandes rasgos, los riesgos a los que se enfrentan y las salvaguardias razonables que pueden implementar. En el mundo profesional, los riesgos y los medios de prevención se evalúan principalmente por sus costes. Es obvio, por ejemplo, que un fallo que resultara en el cierre de una planta por un día merece realizar un gasto económico para evitar que ocurra a una fracción del valor de su producción diaria; esta fracción será aún más importante cuando la probabilidad y frecuencia de tal fallo sea alta.

Riesgos técnicos

Los riesgos técnicos son simplemente los relacionados con fallos y averías “inevitables” en todos los sistemas de hardware y software. Estos incidentes son obviamente más o menos frecuentes dependiendo del cuidado que se tenga durante la fabricación y las verificaciones antes de poner en servicio los sistemas informáticos. Sin embargo, las averías a veces tienen causas indirectas o incluso muy indirectas, por lo que son difíciles de predecir.

- **Incidentes relacionados con el hardware**: Si bien la probabilidad de que un procesador cometa un error en tiempo de ejecución se puede pasar por alto la mayoría de las veces (aunque hubo una excepción famosa con una de las primeras generaciones del procesador Pentium de Intel que podría producir, en determinadas circunstancias, errores computacionales, y actualmente la vulnerabilidad con la mayoría de las CPU de diversas marcas: Meltdown y

Spectre), la mayoría de los componentes electrónicos, producidos en grandes series, pueden tener defectos y finalmente fallar. Algunas de estos fallos son bastante difíciles de detectar porque son intermitentes o raros.

- **Incidentes relacionados con el software**: son con diferencia los más frecuentes; la creciente complejidad de los sistemas operativos y programas requiere el esfuerzo combinado de decenas, cientos o incluso miles de programadores. Individual o colectivamente, inevitablemente cometen errores que los mejores métodos de trabajo y herramientas de control o testeo no pueden eliminar en su totalidad. Las fisuras que le permiten tomar el control total o parcial de un ordenador se hacen regularmente públicas y se enumeran en sitios como SecurityFocus o Secunia. Algunos errores no son corregidos rápidamente por sus autores. Algunos programas están diseñados para comunicarse con internet y por lo tanto no es deseable bloquearlos completamente con un *firewall* (por ejemplo, un navegador web).

- **Incidencias ambientales**: Las máquinas electrónicas y las redes de comunicación son sensibles a los cambios de temperatura o humedad (especialmente en caso de incendio o inundación), así como al campo electromagnético. Es frecuente que los ordenadores experimenten averías permanentes o intermitentes debido a condiciones climáticas inusuales o a la influencia de las instalaciones eléctricas, en particular las instalaciones industriales.

Estándares y gestión del riesgo

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "**la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización**".

La gestión del riesgo consiste en los siguientes procesos: establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación de riesgos, comunicación y consulta de riesgos, y revisión y seguimiento del riesgo. Ver figura 1.

- **Establecimiento del contexto**
  El proceso de establecimiento de contexto recibe como entrada toda la información relevante acerca de la organización, determinando el alcance y los límites del proceso. La salida del proceso es la especificación de estos parámetros.

- **Evaluación del riesgo**
  Este proceso consta de tres subprocesos: **identificación de riesgos, análisis de riesgo y evaluación de riesgos.** El proceso recibe como entrada la salida del proceso de establecimiento de contexto. Identifica de forma cuantitativa o cualitativa los riesgos y les da prioridad a los criterios de evaluación que dependen de los objetivos de la organización. Al identificar los

riesgos se busca determinar lo que podría causar una pérdida potencial y comprender cómo, dónde y por qué puede ocurrir dicha pérdida; identificando los activos, amenazas, medidas de seguridad, vulnerabilidades y sus consecuencias.

Por último, el proceso de evaluación de riesgos recibe como entrada la salida del proceso de análisis de riesgos. Se comparan los niveles de riesgo con los criterios de evaluación de riesgos y los criterios de aceptación del riesgo. El resultado del proceso es una lista de los riesgos priorizados de acuerdo a los criterios de evaluación de riesgo.

- **Tratamiento del riesgo**
  Tiene como objetivo seleccionar las medidas de seguridad para reducir o evitar los riesgos y definir un plan de tratamiento de riesgo. El proceso recibe como entrada la salida del proceso de evaluación de riesgos y produce como salida el plan de tratamiento de riesgos.

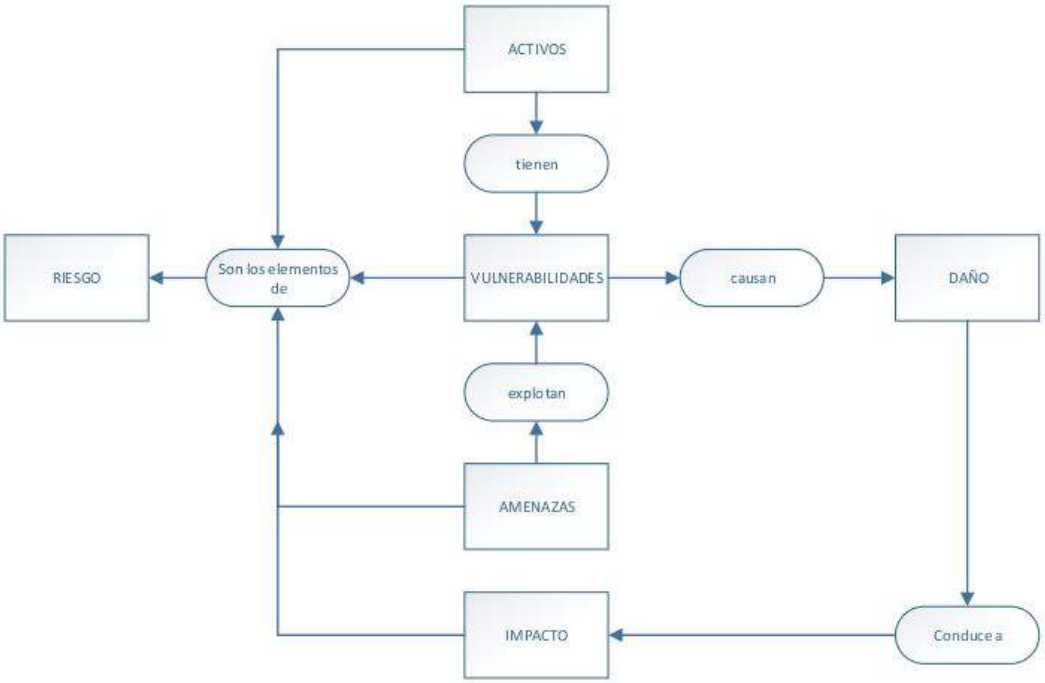
  Después de que se han tomado las decisiones del tratamiento de riesgos, siempre habrá riesgo restante, llamados riesgos residuales. Estos riesgos pueden ser difíciles de evaluar, pero por lo menos se debe hacer una estimación para asegurar la suficiente protección. Si el riesgo residual es inaceptable, el proceso del tratamiento del riesgo se debe repetir. En el tratamiento del riesgo debe identificarse los factores limitantes y dependientes, prioridades, plazos, recursos, incluyendo las aprobaciones necesarias para su asignación.

- **Consulta y comunicación del riesgo**
  Es un proceso horizontal que interactúa de forma bidireccional con todos los demás procesos de gestión de riesgos. Su propósito es establecer un entendimiento común de todos los aspectos de riesgo entre todas las parte interesadas de la organización.

- **Monitoreo y revisión del riesgo**
  La gestión de riesgos es un proceso continuo, donde las medidas de seguridad implementadas son monitoreadas y revisadas para asegurar que funcionan correctamente de forma efectiva. El mantenimiento de las medidas de seguridad debe ser planeado y realizado sobre una base programada regularmente. Por último, se deben realizar auditorías internas de forma regular por parte de un tercero y tener una documentación completa, accesible y con procesos controlados para apoyar al SGSI.

Conceptos relacionados al riesgo

El riesgo se genera por la interrelación de algunos elementos como se visualiza en el siguiente esquema, y que a continuación se explican en detalle.



- **Activo**
  Es cualquier cosa que tenga valor en la organización, sus operaciones comerciales y su continuidad, incluido los recursos de información que apoyan la misión de la organización.

  Se pueden distinguir dos clases de activos: los activos primarios que incluyen a los procesos del negocio, actividades e información; y los activos de apoyo, que incluyen hardware (equipos de procesamiento de datos, periféricos y medios de comunicación), software (sistema operativo, servicio, software de aplicación), red, personal (directores, usuarios, personal de operación y desarrolladores), lugar y estructura de la organización (proveedores y fabricantes).

  La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente. La seguridad informática protege la información de un amplio rango de amenazas con el objetivo de asegurar la continuidad de los negocios, minimizar el daño comercial y maximizar el reembolso de las inversiones y oportunidades comerciales.

  La información puede existir en muchas formas; puede ser de forma escrita, impresa, electrónica, transmitida por correo o usando medios electrónicos o hablado en una conversación.

  La seguridad de la información es evaluada bajo tres aspectos fundamentales: disponibilidad, integridad y confidencialidad.

- Confidencialidad: asegura que solo los usuarios con acceso autorizado puedan acceder a la información.
- Integridad: proteger la exactitud, totalidad de los datos y métodos de procesamiento de la información que los usuarios autorizados gestionan.
- Disponibilidad: los recursos deben estar disponibles cuando sean requeridos en cualquier instante de tiempo.

- **Amenaza**
  Es una vulnerabilidad de un activo que puede ser explotada por una o más causas potenciales de un incidente, que puede resultar en daño al sistema u organización. Las amenazas pueden ser de varios tipos:

  - **De origen natural.** Incendio, inundación, tormenta eléctrica, terremoto, siniestros mayores que afectan la disponibilidad de los activos como son los equipos informáticos, infraestructura física y medios de soporte de información.
  - **Del entorno.** Incendio, inundación, polvo, sobrecarga eléctrica, corte de suministro eléctrico, condiciones inadecuadas de temperatura o humedad afectan la disponibilidad de los activos como son los equipos informáticos, infraestructura física y medios de soporte de información.

    - El fallo de los servicios de comunicaciones afecta la disponibilidad de las redes de comunicaciones.
    - La degradación de los soportes de almacenamiento de la información afecta la disponibilidad de los medios de soporte de información como son las cintas de respaldo.
    - Las emanaciones electromagnéticas afectan la confidencialidad de los equipos informáticos, medios de soporte de información.

- **Defecto de aplicaciones**
  Aquellos problemas que se producen en el equipo por defectos de fábrica o en la implementación, se denominan vulnerabilidades técnicas. Por lo general, la recuperación de este tipo de problemas se logra por parte del proveedor o siguiendo una guía de configuración; para ello se debe tener respaldada la información para restaurarla caso de ser necesario.

- **Causadas por las personas de forma accidental**
  - Los errores de los usuarios que acceden al servicio afectan la integridad, confidencialidad y disponibilidad de los datos, servicios, claves criptográficas, soportes de información y aplicaciones.
  - Los errores del administrador responsable de la instalación y operación afectan la disponibilidad, integridad y confidencialidad de los datos, claves criptográficas, servicios, aplicaciones,

equipos informáticos, redes de comunicación y soportes de información.
    - Los errores de monitorización afectan la trazabilidad de los registros de actividad, por la falta de registros, registros incompletos, registros incorrectamente fechados o registros incorrectamente atribuidos.
    - Los errores de configuración afectan la integridad de los datos de configuración.
    - Los errores de encaminamiento afectan la confidencialidad de los servicios, aplicaciones y las redes de comunicaciones.

- **Causadas por las personas de formas deliberada**
    - La manipulación de los registros de actividad afectan la integridad y por lo tanto a su trazabilidad.
    - La manipulación de la configuración afecta la integridad, confidencialidad y disponibilidad de los registros de actividad.
    - La suplantación de la identidad del usuario, abuso de privilegios de acceso y acceso no autorizado afectan la confidencialidad, autenticidad e integridad de la información, claves criptográficas, servicios, aplicaciones y redes de comunicaciones.
    - La monitorización no autorizada del tráfico y la intercepción de información afecta la confidencialidad de las redes de comunicaciones.
    - El robo y ataque destructivo de los activos afectan la disponibilidad y confidencialidad.
    - La propagación de virus, *spyware*, gusanos, troyanos... afectan la disponibilidad, integridad y confidencialidad de las aplicaciones.

- **Vulnerabilidad**
  Los activos se ven influidos por una serie de amenazas; la probabilidad de que se materialice una de dichas amenazas y la degradación que le supone a un activo es lo que se conoce como vulnerabilidad según MAGERIT.

  Se clasifican de acuerdo a la clase de activos, es decir: hardware (susceptibilidad a la humedad, polvo, suciedad, almacenamiento sin protección), software (sin pruebas de software, falta de seguimiento de auditoría), red (líneas inadecuadas, falta de seguridad), sitio (ubicación en un área susceptible a inundaciones, red de energía inestable), y organización (falta de auditorías periódicas, falta de planes de continuidad).

- **Impacto**
  Es un indicador de qué puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando se materializa sobre un activo. El impacto se estima, conociendo el valor de los activos y la degradación causa por las amenazas.

Impacto = Valor * Degradación

Análisis del riesgo

El análisis de riesgos es conocido como el **proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización**. Permite determinar cómo es, cuánto vale y cómo de protegido se encuentra un sistema, siguiendo los objetivos, estrategia y política de la organización para elaborar un plan de seguridad. Al implantar y operar este plan debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la dirección de la organización. Al conjunto de estas actividades se le denomina “Proceso de Gestión de Riesgos”.

El análisis de riesgo se realiza ya sea cuantitativa o cualitativamente. El análisis cualitativo es recomendable hacerlo en primer lugar, utiliza una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales ya sea bajo, medio o alto; y la probabilidad de que se produzcan estas consecuencias. Un análisis cualitativo permite:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos, aquellos sujetos a un riesgo máximo.

El análisis cuantitativo es más detallado y utiliza una escala con valores numéricos para las consecuencias y probabilidad, (*"Si puedes medir aquello de lo que estás hablando y expresarlo con números, entonces sabes algo sobre ello. Pero si no puedes medirlo, si no puedes expresarlo en números, tu conocimiento es bien magro e insatisfactorio."* Lord Kelvin) permitiendo:

- Detallar las consecuencias económicas de la materialización de una amenaza en un activo.
- Estimar la tasa anual de ocurrencia de amenazas.
- Detallar el coste de despliegue y mantenimiento de las salvaguardas.
- Permitir ser más precisos en la planificación de gastos de cara a un plan de mejora de seguridad.

Los sistemas de gestión de la seguridad de la información formalizan cuatro etapas cíclicas donde el análisis de riesgos es parte de las actividades de planificación, se toman decisiones de tratamiento, estas decisiones se materializan en la etapa de implantación, en el cual se despliegan elementos que permiten la monitorización de las medidas tomadas para poder evaluar la efectividad de las mismas y actuar dependiendo a éstas, dentro de un círculo de excelencia o mejora continua, como se muestra en la figura.

El riesgo es una función de la probabilidad y el impacto.

Riesgo = Probabilidad * Impacto

Existen varios estándares reconocidos a nivel mundial como por ejemplo la serie ISO 27000 que trata sobre la gestión de riesgos en seguridad de la información proporcionando recomendaciones, lineamientos de métodos y técnicas de evaluación de riesgos de la seguridad en la información que conllevan a medir los niveles de riesgo por su impacto y probabilidad; también hay metodologías y herramientas que ayudan a manipular grandes volúmenes de información generados para realizar un análisis completo en un mediana o grande empresa.

Estándares y metodologías de gestión del riesgo

- **Estándares de gestión del riesgo**

Las normas internacionales más importantes son:

BS 7799 publicada por el British Standard Institute (Reino Unido) que tiene como objetivo dar seguridad efectiva a la información a través de un programa permanente de actividades de gestión de riesgos, además incluye la identificación y evaluación del riesgo mediante la implementación y mejora continua del sistema basado en el control del riesgo.

Serie ISO/IEC 27000, familia de estándares sobre gestión de la seguridad de la información derivados de la norma BS 7799, varias normas dentro de las series ya han sido publicadas; otros se encuentran en desarrollo. Dentro de esta serie están:

ISO/IEC 27001:2013 - Requisitos de la Gestión de la Seguridad de la Información", estándar diseñado para asegurar la selección de las medidas adecuadas de seguridad que protegen los activos de información y brindan confianza a las partes interesadas. La norma abarca todo tipo de organizaciones como pueden ser: empresas comerciales, agencias gubernamentales y organizaciones sin fines de lucro; y especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información en el contexto de la organización. Además se especifican los requisitos para la aplicación de medidas de seguridad adaptados a las necesidades de las organizaciones.

ISO/IEC 27002:2013 define qué debe hacerse en términos de controles de seguridad de la información, proporciona las directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo en la seguridad de la información.

ISO/IEC 27005:2011 - Gestión de riesgos en seguridad de la información, esta norma proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñado para guiar en la implementación de seguridad de la información basado en el enfoque de gestión de riesgos.

ISO/IEC 31000:2009 – Principios y directrices de gestión de riesgos, se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, tanto si tiene consecuencias positivas o negativas. Esta norma no es específicamente sobre la seguridad de la información o para los riesgos de TIC. Proporciona un enfoque común en apoyo a las normas de control de riesgos.

Guía ISO 73:2009 proporciona las definiciones de los términos relaciones con la gestión de riesgos. Su objetivo es fomentar una comprensión y enfoque coherente, la descripción de las actividades relacionadas con la gestión del riesgo y el uso de la terminología uniforme a los procesos y marcos que se ocupan de esta gestión.

"Guía de gestión de riesgos para los sistemas de tecnología de la información" de EE.UU., SP 800-53 proporciona una base común para personas con y sin experiencia, técnicos y no técnicos que usan el proceso de gestión de riesgos en sus sistemas TIC. Las directrices de NIST son para las organizaciones federales que procesan información sensible, pero también puede ser utilizado por empresas no gubernamentales.

Metodologías en riesgos

Un método es un procedimiento o proceso sistemático y ordenado para alcanzar algún objetivo. Una metodología se materializa por un conjunto de métodos, técnicas y herramientas. No contiene métodos específicos, sin embargo, lo especifica por procesos que conforman el marco de gestión de riesgo.

La metodología cualitativa es el método más utilizado para el análisis de riesgos y cumple con los requisitos ISO 27001. El nivel de riesgo se basa en niveles de probabilidad e impacto:

Nivel de riesgo:

Nivel de Riesgo	Acción requerida para el tratamiento del riesgo
Muy alto	Inaceptable: acciones deben tomarse inmediatamente
Alto	Inaceptable: acciones deben tomarse lo antes posible
Medio	Acciones requeridas y que deben tomarse en plazo razonable
Bajo	Aceptable: no se requieren acciones como resultado de la evaluación de riesgos
Muy bajo	Aceptable: ninguna acción requerida

La salida de la ecuación del riesgo se puede representar mediante una escala de tres niveles refiriéndose al impacto de un evento producido a una probabilidad de ocurrencia.

Matriz de tres niveles de riesgo

Probabilidad	ALTA	Riesgo medio	Riesgo alto	Riesgo muy alto
	MEDIA	Riesgo bajo	Riesgo medio	Riesgo alto
	BAJA	Riesgo muy bajo	Riesgo bajo	Riesgo medio
		BAJO	MEDIO	ALTO
		Impacto		

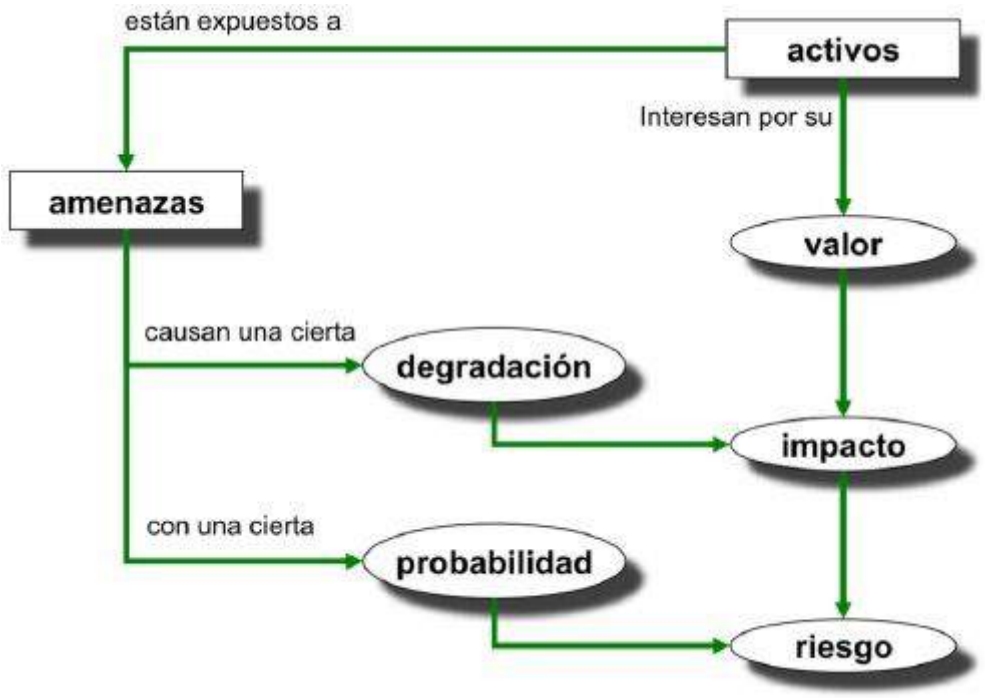
Seguidamente se comentan las metodologías más reconocidas:

- **MAGERIT**
  Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los sistemas de información; fue creada en España por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000. En el año 2012 se actualizó a la versión 3.

  Los objetivos que busca alcanzar son:
  - Hacer que los responsables de los sistemas de información sean conscientes de la existencia de riesgos y de la necesidad de tratarlos a tiempo.

- Ofrecer un método sistemático para el análisis de riesgos.
- Ayudar en la descripción y planificación de las medidas adecuadas para mantener los riesgos bajo control.
- De forma indirecta, preparar la organización de los procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La metodología se puede resumir en el siguiente gráfico.



1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

MAGERIT consiste en tres libros en versiones inglés, español e italiano:

Libro I: Método
Libro II: Catálogo de Elementos
Libro III: Guía de Técnicas

- **OCTAVE**

OCTAVE es la metodología de “Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades” para agilizar y optimizar el proceso de evaluación de riesgos de seguridad de la información alineados a los objetivos y metas de la organización.

Existen tres metodologías publicadas: OCTAVE aplicable en organizaciones con más de 300 empleados, OCTAVE-S aplicable en organizaciones de hasta 100 empleados y OCTAVE Allegro que permite una amplia evaluación del entorno del riesgo operativo sin la necesidad de un amplio conocimiento de evaluación de riesgos y requiere menos tiempo de implementación.

Los dos objetivos específicos de OCTAVE son:

- Desmitificar la falsa creencia: la seguridad informática es un solamente un asunto técnico.
- Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos.

OCTAVE divide los activos en dos tipos: sistemas y personas. En el primer grupo se consideran el hardware, software y los datos.

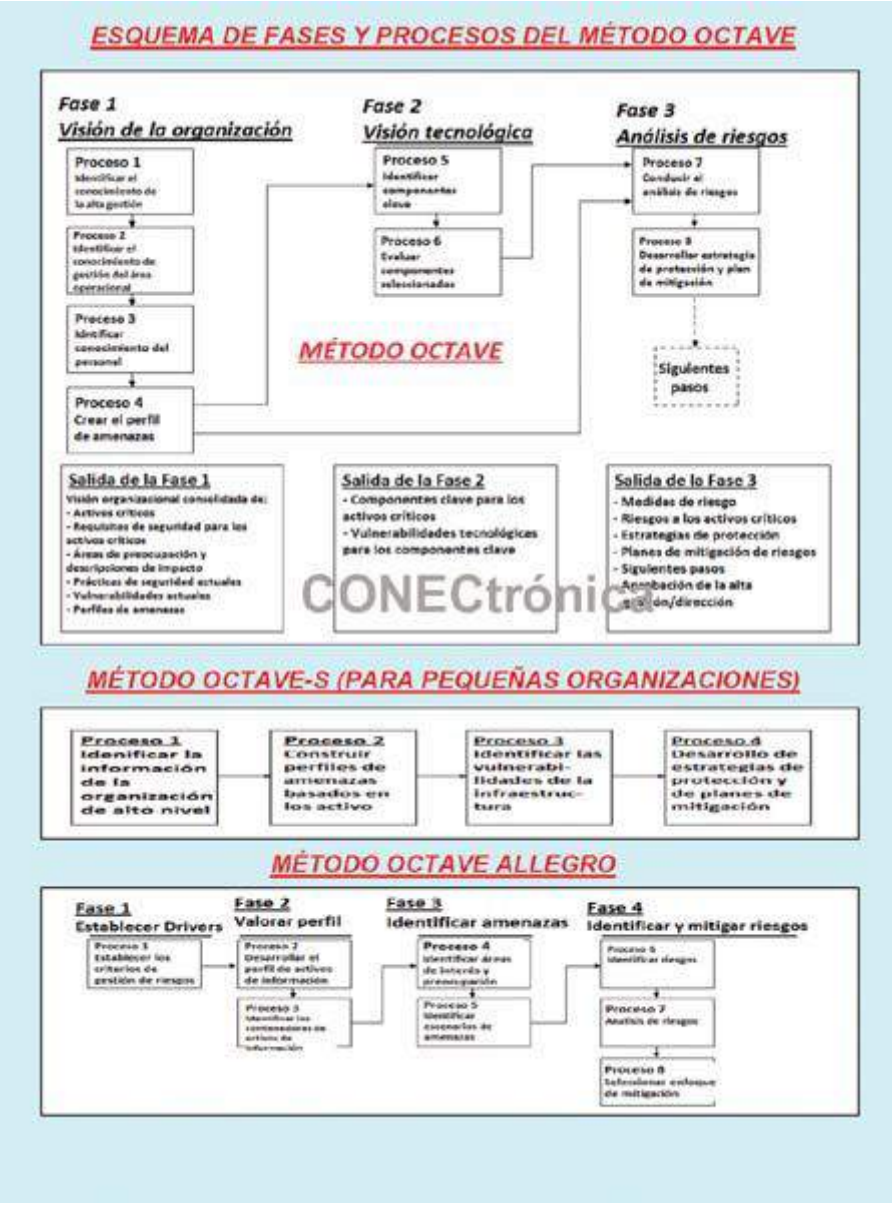
La metodología OCTAVE está compuesta por tres fases:

1. Visión de la organización: donde se definen los elementos como los activos, vulnerabilidad de la organización, amenazas, exigencias de seguridad y normas existentes.
2. Visión tecnológica: se clasifican en dos componentes, las claves y vulnerabilidades técnicas.
3. Planificación de las medidas y reducción de riesgos: se clasifican los elementos como la evaluación de riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de riesgos.

El método OCTAVE ofrece un proceso simplificado enfocado en los activos de la información, que pretende ayudar a una organización a:

- Desarrollar criterios de evaluación de riesgos cualitativos que describen el riesgo operacional de la organización.
- Identificar los activos que son importantes para la misión de la organización.
- Identificar las vulnerabilidades y amenazas de los activos.
- Determinar y evaluar las consecuencias potenciales para la organización tras una amenaza.

La metodología de OCTAVE Allegro consiste en ocho pasos organizados en cuatro etapas, como se indica en el siguiente diagrama



- Establecer manejadores, donde la organización desarrolla los criterios de medición de riesgos que sean coherentes con los manejadores de la organización.
- Perfil de activos, donde los activos que son el foco de evaluación de riesgos se identifican y se perfilan.
- Identificar las amenazas, donde las amenazas de los activos, dentro del contexto de los contenedores, son identificadas y documentadas a través de un proceso estructurado.
- Identificar y mitigar riesgos, donde se identifican y analizan los riesgos que se basan en la información sobre amenazas, y se desarrollan las estrategias de mitigación para manejar los riesgos.

Las salidas de cada paso en el proceso son documentadas en una serie de hojas de trabajos que son usadas como entradas del siguiente paso en el proceso.

- **Metodología NIST SP 800-30**
  El Instituto Nacional de Estándares y Tecnología (NIST) fundado en 1901 es parte del Ministerio de Comercio de Estados Unidos. Los estándares de NIST deben ser cumplidos por todos los productos y servicios que de alguna forma dependen de alguna tecnología, desde los dispositivos creados a nanoescala hasta por una red eléctrica inteligente.

  La Ley de Gestión de la Seguridad de la Información Federal (FISMA) requiere a las agencias federales seguir un conjunto de estándares de seguridad. Estos estándares son provistos por NIST y son conocidos como Estándares Federales de Procesamiento de Información (FIPS).

  FIPS es una serie de publicaciones especiales de la serie SP 800 sobre la seguridad de la información. Esta serie incluye una metodología para el análisis y gestión de riesgos de la seguridad de la información, alineada y complementaria con el resto de documentos de la serie.

  La metodología NIST SP 800-30 está compuesta por nueve pasos básicos para el análisis de riesgo, según se muestra en los siguientes diagramas

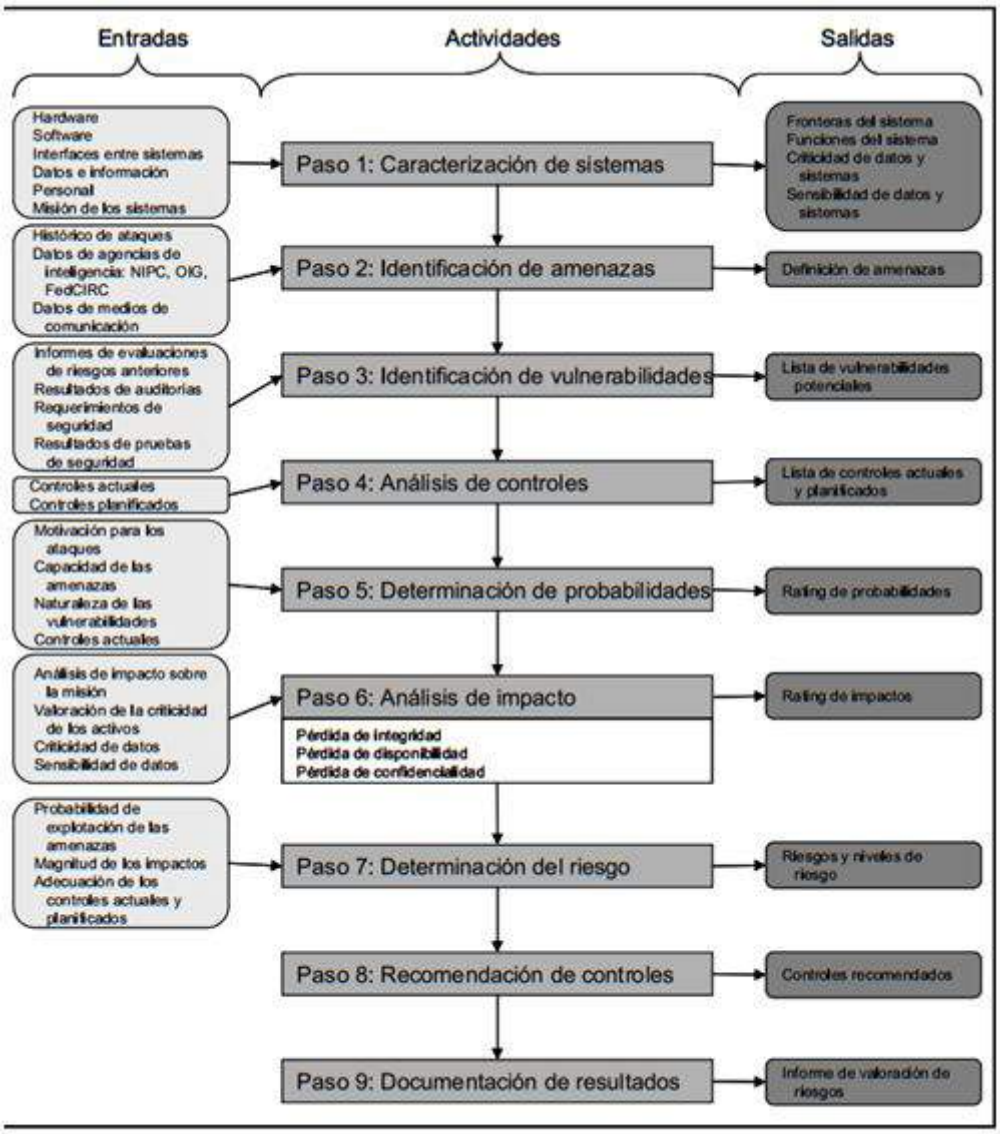


Figura 13: Proceso de análisis de riesgos de NIST SP 800-30

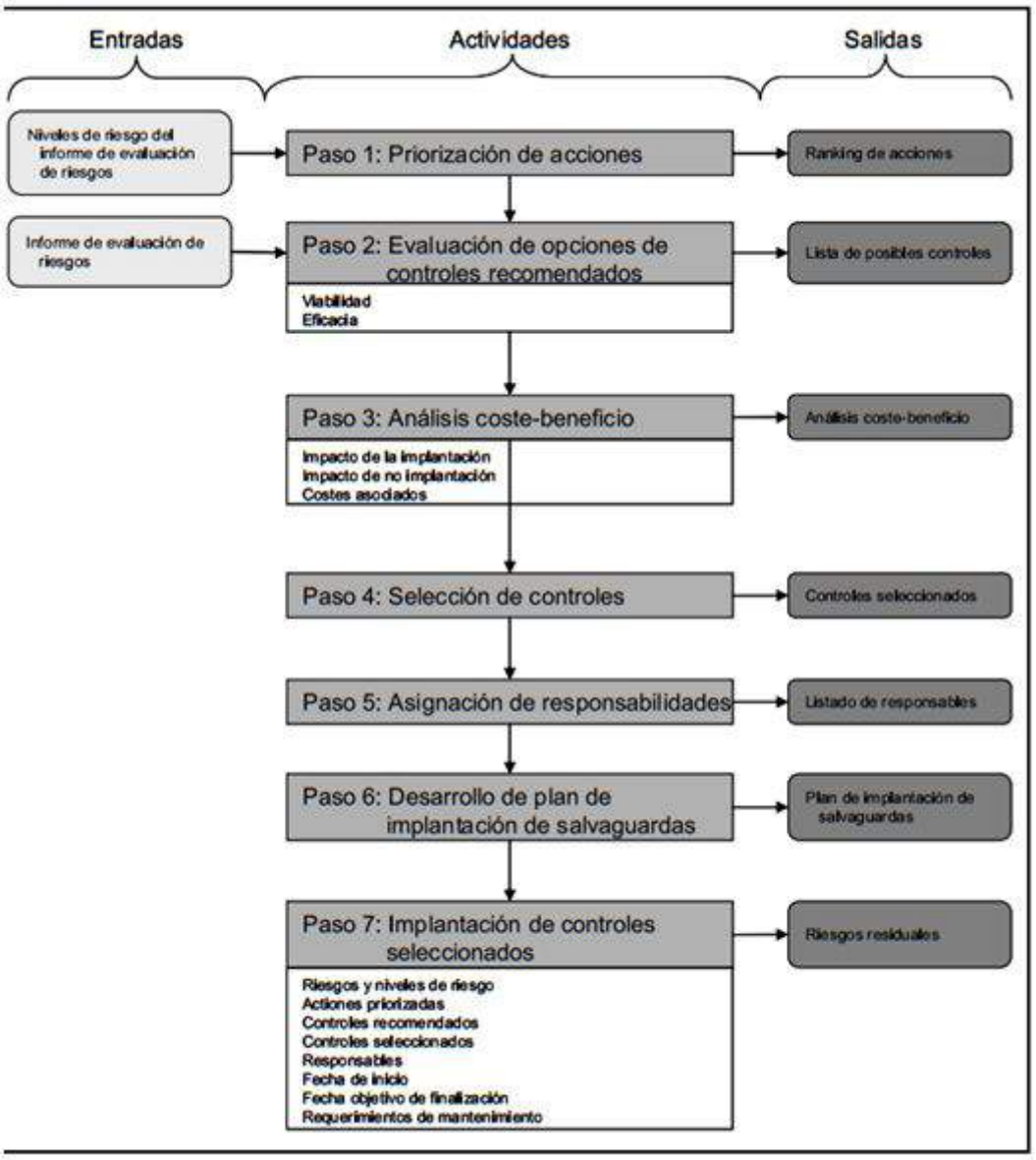


Figura 14: Proceso de gestión de riesgos de NIST SP 800-30

- **CRAMM**
  Es una metodología desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Es el método de análisis de riesgo preferido en los organismos de administración pública. Se compone de tres etapas, cada una apoyada por cuestionarios, objetivos y directrices. Las dos primeras se encargan de identificar y analizar los riesgos para el sistema, y la tercera recomienda la manera en que estos riesgos deben ser gestionados. CRAMM sigue el proceso:

  - Utiliza reuniones, entrevistas y cuestionarios para la recolección de datos.
  - Identifica y clasifica los activos de TI en tres categorías; datos, software y activos físicos.

- Requiere que se consideren el impacto de la pérdida de confidencialidad, integridad y disponibilidad del activo.
- Mide la vulnerabilidad por niveles: muy alto, alto, medio, bajo o muy bajo.
- Mide el riesgo por niveles: alta, media o baja.

- **MEHARI**
  Es una metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (CLUb de la Sécurité de l'Information Français) en 1995 y se deriva de las metodologías previas Melissa y Marion.

  El primer objetivo de MEHARI es proporcionar un método para la evaluación y gestión de los riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005, proporcionando el conjunto de herramientas y elementos necesarios para su implementación.

  Otros objetivos adicionales son:
  - Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios.
  - Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, medio y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

- **CORAS**
  Desarrollado a partir de 2001 por SINTEF, un grupo de investigación noruego financiado por organizaciones del sector público y privado. Se desarrolló en el marco del Proyecto CORAS financiado por la Unión Europea. El método CORAS proporciona:

  - Una metodología de análisis de riesgos basado en la elaboración de modelos, que consta de siete pasos, basados fundamentalmente en entrevistas con los expertos.
  - Un lenguaje gráfico basado en UML para la definición de los modelos (activos, amenazas, riesgos y salvaguardas), y guías para su utilización a lo largo del proceso. El lenguaje se ha definido como un perfil UML.
  - Un editor gráfico para soportar la elaboración de los modelos, basado en Microsoft Visio.
  - Una biblioteca de casos reutilizables.
  - Una herramienta de gestión de casos, que permite su gestión y reutilización.
  - Representación textual basada en XML del lenguaje gráfico.
  - Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

Herramientas de gestión de riesgos

Por lo general los análisis de riesgos conllevan considerar una gran cantidad de activos, y a cada uno de estos les corresponde un sinnúmero de amenazas y salvaguardas, por ello resulta un arduo trabajo manipular tal magnitud de información y es por esta razón que se han desarrollado herramientas de apoyo de análisis de riesgos que cumplen ciertos requisitos:

- Permiten trabajar con un conjunto amplio de activos, amenazas y salvaguardas.
- Permiten un tratamiento flexible del conjunto de activos para asemejar al modelo real de la organización.
- Demostrar resultados cercanos a la realidad.

Las herramientas más útiles para el análisis, son: MSAT, RISICARE y PILAR.

- **PILAR**
  PILAR es la herramienta que se usará en las prácticas de la asignatura, desarrollada para soportar el análisis y la gestión de riesgos de sistemas de información siguiendo la metodología MAGERIT. Las siglas de PILAR provienen de “Procedimiento Informático Lógico para el Análisis de Riesgos” creado por el Centro Nacional de Inteligencia, actualmente se encuentra disponible la versión 6.2.6.

  Analiza los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Para tratar el riesgo se proponen: salvaguarda o contramedidas, normas y procedimientos de seguridad.

Esta herramienta soporta las fases del método MAGERIT:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

Evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

PILAR presenta los resultados en varias formas, ya sea en informes RTF, gráficas o tablas que se pueden agregar a una hoja de cálculo, logrando elaborar diferentes tipos de informes y presentaciones de los resultados.

Finalmente, la herramienta calcula calificaciones de seguridad respecto a normas ampliamente conocidas, como son UNE-ISO/IEC 27002:2009: sistemas de gestión de seguridad, RD 1720/2007: datos de carácter personal y RD 3/2010: Esquema Nacional de Seguridad.

Cabe destacar que esta herramienta incorpora tanto los modelos cualitativos como cuantitativos, logrando alternarse entre estos para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos.

Algunos datos relacionados con la seguridad

Planta de tratamiento de aguas en Maroochy Shire (Australia)

Evento 2000. Vertido de dos millones de litros de aguas no tratadas en ríos, parques, etc. en el paraje natural de Maroochy.

Impacto: Pérdida de vida salvaje, peligro para habitantes de la zona y costes económicos y naturales millonarios.

Descripción: Producido por un ex empleado de forma remota. Utilizó medios inalámbricos comerciales y el aplicativo SCADA para hacerse con las comunicaciones de tipo OPC, DNP3 y ModBus. Suplantó una de las 142 estaciones de bombeo que conforman el sistema SCADA. Causó más de 46 incidentes premeditados en menos de tres meses.

Lecciones Aprendidas:
Eliminar todos los accesos al terminar la relación laboral.

Utilizar transmisiones inalámbricas y de radio seguras**.**

Central nuclear Davis Besse (Ohio, EE. UU.)

Evento 2003. Parada de diversos sistemas de monitorización del funcionamiento de la planta debido al gusano Slammer.

Impacto: Caída completa de los sistemas de visualización de parámetros de seguridad (casi cinco horas) y el ordenador de procesos de planta (más de seis horas).

Descripción: El gusano Slammer accedió a la central a través del enlace directo de un contratista a la red corporativa. El gusano se transfirió por diferentes redes, desde la red corporativa hasta la red de control, donde encuentra un servidor vulnerable (parche disponible desde seis meses antes del ataque).

Lecciones Aprendidas:
Uso de accesos remotos seguros.
Aplicar parches de seguridad.
Utilizar una estrategia de defensa en profundidad.

Central nuclear Natanz (Irán)

Evento 2010. Primer *malware* orientado directamente a los sistemas de control.

Impacto: Sabotaje a la central nuclear. Afectó a varias centrales más en la zona

Descripción: Stuxnet aprovechaba varias vulnerabilidades *0-day* en los PLC de Siemens. Era capaz de modificar la programación de los PLC afectados. Stuxnet sirvió de base para otros malware posteriores como Flame o DuQu.

Lecciones Aprendidas:
Necesidad de un programa de gestión de parches.
Air Gap no es una solución válida de seguridad.
Usar soluciones antivirus o listas blancas.

Control de tráfico en Italia

Evento 2009. Autoridades italianas analizan cambios no autorizados en los sistemas de regulación del tráfico

Impacto: Incremento del número de multas al saltarse semáforos en rojo hasta las 1400 multas en dos meses

Descripción: Un desarrollador del sistema de multas T-Redspeed y otras 100 personas más (agentes, policías y gerentes de empresas) fueron investigadas por

manipular y reducir el tiempo de la luz ámbar en los semáforos con el fin de imponer más multas. Los beneficios de las multas son repartidos entre las empresas y las autoridades.

Lecciones aprendidas:
No desestimar las amenazas provenientes desde la propia empresa.
Garantizar la separación de tareas.

Sistema ferroviario de Lodz (Polonia)

Evento 2008. Descarrilamiento de trenes.

Impacto: Daños materiales y personales (Hubo 12 heridos).

Descripción: Un joven fue capaz de hacerse con el control del centro de tráfico ferroviario. Utilizó un dispositivo que emitía en la misma frecuencia que los sistemas de cambio de vía y pudo modificar las agujas de los trenes. Realizó un estudio previo de los trenes y sus rutas antes de realizar su ataque.

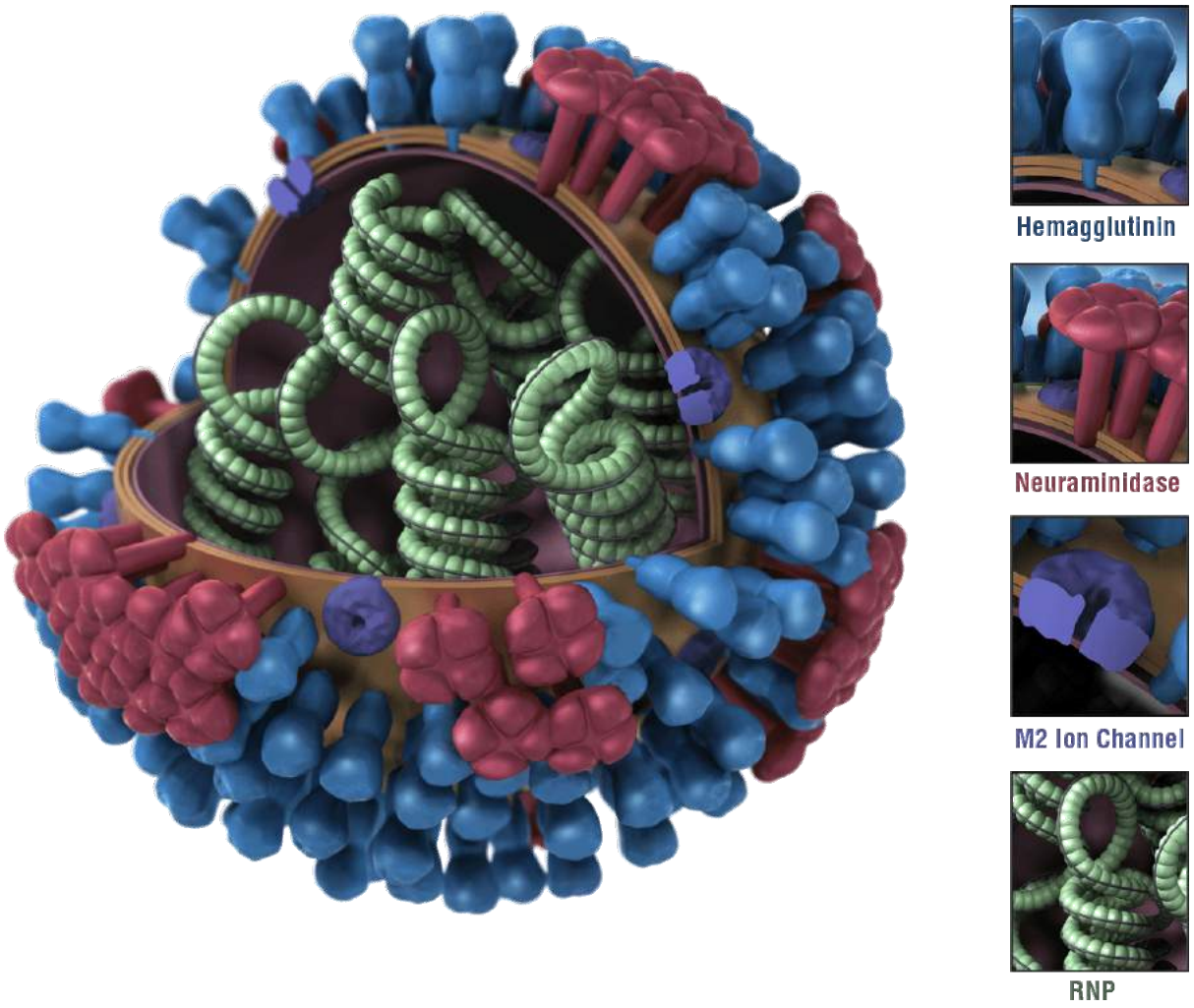
Lecciones Aprendidas:
No confiar en la seguridad por oscuridad de los protocolos.
Uso adecuado de control de accesos a los dispositivos de campo.

2. Un ejemplo trivial

Los mecanismos de SGSI pueden hacerse visibles a cualquier persona sin necesidad de tener conocimientos informáticos poniendo como ejemplo la seguridad de otro ‘sistema’, por ejemplo nuestro cuerpo y su estado de salud.

En ese caso el cuerpo es el dominio compuesto por distintos activos (los órganos susceptibles de ser atacados), y las amenazas son los distintos agentes infecciosos que habitualmente se encuentran en el entorno.

Por ejemplo la amenaza se materializa como agresión de un agente vírico, en forma de afección gripal provocada por los tan conocidos virus de la influenza (A y B), que dan lugar a epidemias anuales.



La **hemaglutinina (HA)** es una proteína que causa la aglutinación de los hematíes o glóbulos rojos de la sangre. Este proceso recibe el nombre de hemaglutinación. La hemaglutinación se define como la capacidad que tienen ciertos virus y bacterias para unir entre sí los glóbulos rojos, gracias a las proteínas que poseen en su capa externa.

La **neuraminidasa (NA)** es una enzima presente en la envoltura de la cápside del virus de la gripe. Es un tetrámero con forma como de "champiñón" proyectado. Su cabeza consiste en cuatro subunidades coplanares y esféricas y una región hidrofóbica (está dentro del interior de la membrana del virus). Está formado por una única cadena polipeptídica que está orientada en la dirección opuesta a la del antígeno HA. La composición del polipéptido es una cadena simple de seis aminoácidos conservados polares seguidos por aminoácidos hidrofílicos variables.

Los **canales iónicos** son proteínas transmembrana que contienen poros acuosos que cuando se abren permiten el paso selectivo de iones específicos a través de las membranas celulares. Así, los canales iónicos son proteínas que controlan el paso de iones, y por tanto el gradiente electroquímico, a través de la membrana de toda célula viva. Estos canales actúan como compuertas que se abren o se cierran en función de los estímulos externos, aunque algunas sustancias tóxicas pueden desactivar su función natural.

Una **ribonucleoproteína (RNP)** es una nucleoproteína que contiene ARN, es decir, es un compuesto que combina tanto ácido ribonucleico como proteína. Es uno de los componentes principales del nucleoplasma.

Las personas adoptamos habitualmente salvaguardas elementales que pueden llamarse organizativas, tales como:

- Abrigarse si baja la temperatura.
- Lavarse las manos antes de comer.
- Evitar corrientes de aire.

Siempre hay que poseer pensamiento crítico, pues muchas veces se realizan acciones basadas en mitos o creencias, y sin evidencia científica,

Ante posibles problemas se suele realizar un ‘análisis de riesgos’:

- Este indica que la vulnerabilidad aumenta al avanzar la epidemia gripal de todos los otoños y que el impacto previsible va desde simples molestias a secuelas importantes para su salud, e incluso la muerte.
- Los factores, vulnerabilidad e impacto, permiten evaluar el riesgo de contagiarse de la gripe y sus secuelas.

Si la persona considera importante el nivel de riesgo evaluado, prepara una batería de salvaguardas para ‘gestionar’ ese riesgo (no para anularlo, pues sería realista erradicar el virus de la influenza del entorno o no ir al trabajo varios meses para evitar contagios).

Por tanto, como no puede evitar totalmente los ambientes contagiosos (el lugar de trabajo o el transporte público), la persona puede vacunarse como salvaguarda preventiva para reducir la vulnerabilidad (la probabilidad de coger la gripe). La vacuna es también una salvaguarda curativa pues reduce en parte el impacto sobre la salud (la virulencia del ataque).

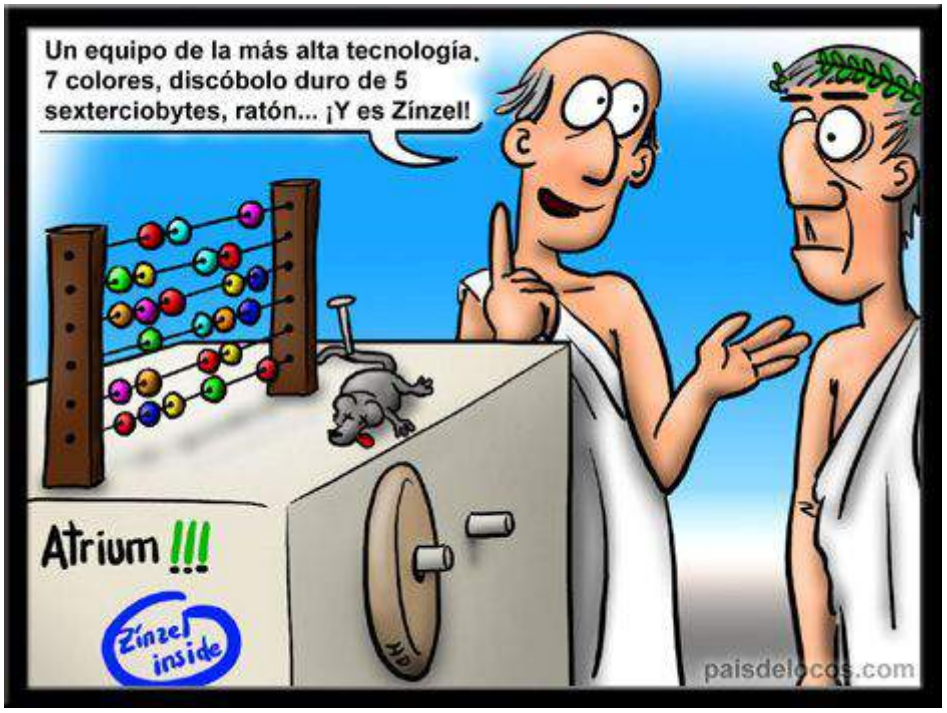
MAGERIT y otros métodos avanzados de Análisis y Gestión de Riesgos para Sistemas de Información y Telecomunicaciones trabajan:

- Con los mismos conceptos (dominio, activo, amenaza, vulnerabilidad, impacto, riesgo, salvaguarda).

- Con objetivos de optimización parecidos (mejorar la relación coste-beneficio de las salvaguardas frente a los riesgos).
- Con un encadenamiento semejante de situaciones y eventos.

3. Evolución de la Seguridad de los Sistemas de Información

Se suele recurrir a considerar las generaciones para situar la evolución de la informática y también para relacionar la evolución de los SI con respecto a la seguridad.



Primera generación
Esta generación de métodos para analizar los riesgos de los SI, consiste básicamente en:

- Listas de chequeo (*checklists*).
- Modelos rudimentarios, pero efectivos, de relacionar causas y efectos relacionados con la seguridad.

Segunda generación
Desde mediados de la década de 1980, una segunda generación de métodos más formalizados irrumpe sobre todo en el ámbito europeo:

- CRAMM, CCTA Risk Analysis and Management Method (CCTA es la Agencia ministerial británica de informática)

Tercera generación

A finales de la década de 1990, se crea una tercera generación de métodos, como MAGERIT, específico de las administraciones públicas españolas; métodos paralelos a la creciente sensibilidad legislativa y normativa en la materia:

- Basados en el análisis de riesgos.
- Establecen los estados inicial y final de seguridad (estado de arranque del proceso de aseguramiento hasta el estado final deseado o realmente alcanzado).
- Debe haber un plan de entregas o actuaciones para pasar del EI al EF (filosofía del marco europeo EUROMÉTODO de desarrollo de contratos sobre proyectos de SI basados en el riesgo).

Cuarta generación

Preocupada por un cuarto nivel de seguridad certificable de los componentes de la "cadena" que asegure una confianza previsible en el sistema compuesto:

- Los SI actuales se encontrarían, en general, pasando al tercer nivel o generación.
- La 'madurez' de la SSI estaría 'un paso atrás', con una generación atrasada respecto a su madurez tecnológica.

	G1	G2	G3
Tecnología	*host*	cliente/servidor	en red
Sistema	manejable	complejo	incierto
Objetivo técnico	eficiencia	eficacia del sistema	eficacia para los usuarios
Calidad	funciona	predecible	controlable
Objetivo de negocio	manejar volumen	organizar	mejorar la productividad
Información	herramienta	estrategia	recurso
Amenazas	naturales	accidentales	deliberadas

Comparaciones con otras ingenierías

El equipo de ingenieros que diseñan una obra de ingeniería civil, por ejemplo un puente:

– Conoce perfectamente el significado del concepto “puente seguro”
– Nunca solicitan un equipo “separado” que una vez finalizado el diseño “securicen el puente”.
– “Firma” que el puente es seguro bajo determinadas condiciones de utilización
– No se le ocurriría indicar que se puede comenzar a utilizar el puente “mientras se encuentran los fondos o el momento para realizar las pruebas de carga”

4. Los marcos de seguridad europeo y mundial

Directrices de la OCDE

Directrices para la seguridad de sistemas y redes de información “**Hacia una cultura de la seguridad**” de la Organización para la Cooperación y el Desarrollo Económico OCDE (junio 2002):

1) Concienciación
Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

2) Responsabilidad
Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

3) Respuesta
Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.

4) Ética
Los participantes deben respetar los intereses legítimos de terceros.

5) Democracia
La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

6) Evaluación del riesgo
Los participantes deben llevar a cabo evaluaciones de riesgo.

7) Diseño y realización de la seguridad
Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

8) Gestión de la Seguridad
Los participantes deben adoptar una visión integral de la administración de la seguridad.

9) Reevaluación
Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

Directiva NIS de la Unión Europea

El 19 de julio de 2016 se publicó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS (*Network and Information Security*).

En su Artículo 1, la Directiva fija su objeto y ámbito de aplicación en los siguientes puntos:

a) establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;

b) crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;

c) crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «*computer security incident response teams*») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;

d) establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;

e) establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

La Directiva entró en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. A partir de ese momento, los Estados miembros adoptarán y publicarán, a más tardar el nueve de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Del mismo modo, los Estados tendrán seis meses más para identificar a los operadores de servicios esenciales.

Algunos aspectos de la directiva NIS

Directiva de la Unión Europea 2016/1148, de 6 de julio de 2016 relativa a las medidas destinadas a **garantizar un elevado nivel común de seguridad de las redes y sistemas de información** en la Unión.

Según la directiva , el objeto y ámbito de aplicación es:

1. La presente Directiva establece medidas con el objeto de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior.

2. A tal fin, la presente Directiva:

    a. establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;
    b. crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;
    c. crea una red de equipos de respuesta a incidentes de seguridad informática (en lo sucesivo, «red de CSIRT», por sus siglas en inglés de «*computer security incident response teams*») con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;
    d. establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;
    e. establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y

CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información.

3. Los requisitos de seguridad y notificación previstos en la presente Directiva no serán aplicables a las empresas que están sujetas a los requisitos de los artículos 13 bis y 13 ter de la Directiva 2002/21/CE ni a los proveedores de servicios de confianza sujetos a los requisitos del artículo 19 del Reglamento (UE) n.o 910/2014.

4. La presente Directiva se entenderá sin perjuicio de la Directiva 2008/114/CE del Consejo ([1]) y las Directivas 2011/93/UE ([2]) y 2013/40/UE ([3]) del Parlamento Europeo y del Consejo.

5. Sin perjuicio de lo dispuesto en el artículo 346 del TFUE, la información que se considere confidencial de acuerdo con las normas de la Unión y nacionales, como las normas sobre confidencialidad empresarial, se intercambiará con la Comisión y otras autoridades competentes únicamente cuando tal intercambio sea necesario a efectos de la aplicación de la presente Directiva. La información que se intercambie se limitará a aquella que resulte pertinente y proporcionada para la finalidad del intercambio. Dicho intercambio de información preservará la confidencialidad de esta y protegerá los intereses de seguridad y comerciales de los operadores de servicios esenciales y de los proveedores de servicios digitales.

6. La presente Directiva se entenderá sin perjuicio de las acciones emprendidas por los Estados miembros para salvaguardar sus funciones estatales esenciales, en particular para salvaguardar la seguridad nacional, incluidas las acciones que protejan la información cuya revelación los Estados miembros consideren contraria a los intereses esenciales de su seguridad, y para mantener el orden público, en particular para permitir la investigación, la detección y el enjuiciamiento de infracciones penales.

7. Se aplicará lo dispuesto en un acto jurídico sectorial de la Unión, cuando este requiera que los operadores de servicios esenciales o los proveedores de servicios digitales garanticen la seguridad de sus redes y sistemas de información o notifiquen incidentes, siempre que dichos requisitos tengan al menos un efecto equivalente al de las obligaciones establecidas en la presente Directiva.

Esta directiva establece “Equipos de respuesta a incidentes de seguridad informática” (CSIRT):

1. Cada Estado miembro designará uno o varios CSIRT que cumplan los requisitos establecidos en el anexo I, punto 1, que cubran al menos los sectores que figuran en el anexo II y los tipos de servicios digitales que figuran en el anexo III, responsables de la gestión de incidentes y riesgos de conformidad con un procedimiento claramente definido. Podrá crearse un CSIRT en el marco de una autoridad competente.

2. Los Estados miembros velarán por que los CSIRT designados dispongan de recursos adecuados para ejercer eficazmente sus funciones, tal como se establece en el anexo I, punto 2. Los Estados miembros garantizarán una cooperación efectiva, eficiente y segura de sus CSIRT en la red de CSIRT a que hace referencia el artículo 12.

3. Los Estados miembros velarán por que sus CSIRT designados tengan acceso a una infraestructura de comunicación e información apropiada, segura y resiliente a escala nacional.

4. Los Estados miembros informarán a la Comisión del mandato y de los elementos principales del proceso de gestión de incidentes de sus CSIRT.

5. Los Estados miembros podrán solicitar la asistencia de la ENISA a la hora de crear CSIRT nacionales.

El **artículo 12** de la directiva trata sobre la **red de CSIRT**

1. A fin de contribuir a desarrollar la confianza y la seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz, se establece una red de CSIRT nacionales.

2. La red de CSIRT estará formada por representantes de los CSIRT de los Estados miembros. La Comisión participará en la red de CSIRT en calidad de observador. La ENISA se hará cargo de la secretaría y apoyará activamente la cooperación entre los CSIRT.

3. La red de CSIRT desempeñará los siguientes cometidos:

    a. intercambiar información sobre servicios, operaciones y capacidades de cooperación de los CSIRT;

    b. a instancias de un representante de un CSIRT de un Estado miembro que pueda verse afectado por un incidente, intercambiar y discutir

sobre información sensible de carácter no comercial relacionada con ese incidente y los riesgos asociados; no obstante, todo Estado miembro podrá negarse a contribuir a dicha discusión si existe riesgo de perjuicio para la investigación del incidente;

c. intercambiar y proporcionar voluntariamente información no confidencial sobre incidentes concretos;

d. a instancias de un representante de un CSIRT de un Estado miembro, discutir y, cuando sea posible, determinar una respuesta coordinada a un incidente que se haya identificado dentro del ámbito de competencias de ese Estado miembro;

e. prestar apoyo a los Estados miembros a la hora de abordar los incidentes transfronterizos sobre la base de su asistencia mutua voluntaria;

f. discutir, explorar e identificar más formas de cooperación operativa, incluidas las relacionadas con:

   i. categorías de riesgos e incidentes,
   ii. alertas tempranas,
   iii. asistencia mutua,
   iv. principios y modalidades de coordinación, cuando los Estados miembros respondan ante incidentes y riesgos transfronterizos de seguridad de las redes y sistemas de información;

g. informar al Grupo de cooperación sobre sus actividades y sobre las formas adicionales de cooperación operativa sobre las que se haya discutido conforme a la letra f), y solicitar directrices a este respecto;

h. discutir sobre la experiencia adquirida a partir de los ejercicios relativos a la seguridad de las redes y sistemas de información, entre ellas las organizadas por la ENISA;

i. a instancias de un CSIRT determinado, analizar las capacidades y la preparación de ese mismo CSIRT;

j. publicar directrices para facilitar la convergencia de prácticas operativas con respecto a la aplicación de lo dispuesto en el presente artículo en lo que atañe a la cooperación operativa.

4. A efectos de la revisión que contempla el artículo 23, a más tardar el nueve de agosto de 2018, y cada año y medio a partir de entonces, la red de CSIRT elaborará un informe en el que se examine la experiencia adquirida a través de la cooperación operativa, en particular las conclusiones y recomendaciones, practicada con arreglo al presente artículo. Dicho informe también se enviará al Grupo de cooperación.

5. La red de CSIRT establecerá su reglamento interno.

5. Situación en España

Seguidamente se indican los organismos involucrados en la seguridad informática en el ámbito nacional.

Consejo Superior de Administración Electrónica (CSAE antes CSI) tiene entre sus competencias la colaboración con el Centro Criptológico Nacional del Centro Nacional de Inteligencia en la elaboración de medidas de seguridad de las tecnologías de la información y comunicaciones

Centro Criptológico Nacional (CCN), es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifrado, garantizar la seguridad de las Tecnologías de la Información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo.

CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI).

Instituto Nacional de Ciberseguridad (INCIBE), es una Sociedad Estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Su misión es reforzar la ciberseguridad, la privacidad y la confianza en los servicios de la Sociedad de la Información, aportando valor a los ciudadanos, empresas, administraciones públicas. y al sector TIC, coordinando esfuerzos con los organismos nacionales e internacionales que trabajan en esta materia.

Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), es el órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas. Fue

creado en el año 2007, mediante Acuerdo de Consejo de Ministros de dos de noviembre, siendo sus competencias reguladas por la **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y por el **Real Decreto 704/2011**, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Su objetivo principal es impulsar y coordinar los mecanismos necesarios para garantizar la seguridad de las infraestructuras que proporcionan los servicios esenciales a nuestra sociedad, fomentando para ello la participación de todos y cada uno de los agentes del sistema en sus correspondientes ámbitos competenciales.

Mediante la integración de todos estos esfuerzos, se pretende fomentar un modelo de seguridad basado en la confianza mutua, creando una asociación público-privada que permita minimizar las vulnerabilidades de las infraestructuras críticas ubicadas en el territorio nacional.

¿Qué es un CERT?

Se denomina CERT (*Computer Emergency Response Team*, Equipo de respuesta ante emergencias informáticas) a un conjunto de medios y personas responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

En este sentido, el secretario de Estado de Seguridad, y el secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, firmaron un Convenio suscrito el cuatro de octubre de 2012 entre ambos departamentos en materia de Ciberseguridad para la creación del **Centro de Respuesta a Incidentes de Seguridad TIC** (CERT) conjunto de los Ministerios del Interior e Industria, Energía y Turismo.

El CERT de Seguridad e Industria da respuesta a la primera línea estratégica de acción: incrementar la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas en materia de seguridad pública y protección de infraestructuras críticas.

Asimismo, con el objetivo de reforzar las capacidades en ciberseguridad y mejorar la coordinación de las acciones de los Fuerzas y Cuerpos de Seguridad del Estado en este ámbito, se creó una **Oficina de Coordinación Cibernética** (OCC), integrada dentro del CNPIC, que sirve de punto de contacto del Ministerio de Interior para todo lo relativo a la ciberseguridad.

¿Qué es una Infraestructura Crítica?

El **Plan Nacional de Protección de Infraestructuras Críticas** las define como: *"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".* Esta definición fue establecida por la Directiva de la Unión Europea: 2008/114/CE del ocho de diciembre de 2008, destacando la importancia de *"la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección".*

Las sociedades actuales se caracterizan por la complejidad e interdependencia de los sistemas de prestación de servicios, suministros y comunicaciones sobre las que se sustenta su estilo de vida y su progreso.

Estos servicios esenciales están basados en un conjunto de infraestructuras de gestión pública y/o privada, que son consideradas críticas porque la interrupción o perturbación severa de su funcionamiento, ocasionaría efectos significativos sobre el desarrollo habitual de las actividades básicas de la sociedad.

Uno de los ámbitos prioritarios de actuación de la **Estrategia de Seguridad Nacional** son las Infraestructuras Críticas, con el objetivo de "Robustecer las infraestructuras que proporcionan los servicios esenciales para la Sociedad".

En este sentido se establecen siete Líneas de Acción Estratégicas, que son:

1. Responsabilidad compartida y cooperación público-privada. Es imprescindible que tanto las Administraciones Públicas como los operadores privados asuman la responsabilidad correspondiente y trabajen de forma coordinada en la protección de las infraestructuras críticas en todo momento. El Gobierno

promoverá la creación de un sistema que comprenda a todos los agentes responsables y facilitará los canales y procedimientos de comunicación seguros, que hagan posible la cooperación mutua y el intercambio de información de interés para todas las partes.

2. Planificación escalonada. Se impulsará un sistema de planificación escalonada, que permita identificar, evaluar, prevenir y mitigar los riesgos a los que nos enfrentamos, desde la perspectiva más global y estratégica, hasta aquellos activos que se encuentren bajo la responsabilidad de un operador u organización. Este sistema se abordará a partir de un enfoque integral multirriesgo y homogeneizador.
3. Equilibrio y eficiencia. El Gobierno aplicará una metodología homogénea que permitirá concentrar los esfuerzos sobre las áreas más vitales: catalogará las infraestructuras de manera priorizada y permitirá una racionalización en la asignación de recursos.
4. Resiliencia. Más allá de las medidas que doten a los activos críticos de una mayor seguridad, las políticas en materia de protección de infraestructuras críticas deberán promover las acciones necesarias con el fin de lograr un incremento de la capacidad de los sistemas que les permita seguir operando, pese a estar sometidos a un ataque o incidente, aun cuando sea en un estado degradado o debilitado. En este sentido, se debe contemplar la existencia de sistemas redundantes o aislados y la adecuada dotación de elementos de reposición.
5. Coordinación. La gestión de crisis a nivel gubernamental organizará todas las tareas, responsabilidades y recursos existentes teniendo en cuenta las infraestructuras críticas como parte integrante en las fases de preparación, respuesta y recuperación. Resulta esencial la existencia de una adecuada coordinación operativa entre las organizaciones responsables de la gestión de riesgos y la gestión de crisis.
6. Cooperación internacional. Se impulsará el cumplimiento del Programa Europeo de Protección de Infraestructuras Críticas (EPCIP) y de la Directiva Europea 2008/114/CE del Consejo, sobre la Identificación y Designación de Infraestructuras Críticas Europeas y Evaluación de la Necesidad de Mejorar su Protección. Ambos instrumentos se entienden como los mejores medios para lograr la consecución de la cooperación de los países europeos y la protección de nuestros intereses nacionales. De la misma manera, se favorecerá la existencia de canales internacionales de información, alerta temprana y respuesta, así como la participación activa en foros internacionales.
7. Garantía en la seguridad de las infraestructuras críticas conforme a lo expuesto en el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC). Se dotará a estas instalaciones de sistemas redundantes e

independientes de otras tecnologías y operadores, dado que sobre ellas descansa el funcionamiento de los servicios esenciales

La legislación vigente establece el liderazgo en esta materia del Ministerio del Interior, a través de la Secretaría de Estado de Seguridad (órgano responsable del Sistema de Protección de Infraestructuras Críticas), asistida por el Centro Nacional para la Protección de las Infraestructuras Críticas.

Se consideran infraestructuras críticas las siguientes: Administración (servicios básicos, instalaciones, redes de información, y principales activos y monumentos del patrimonio nacional); Instalaciones del Espacio; Industria Química y Nuclear (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.); Agua (embalses, almacenamiento, tratamiento y redes); Centrales y Redes de energía (producción y distribución); Tecnologías de la Información y las Comunicaciones (TIC); Salud (sector e infraestructura sanitaria); Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.); Alimentación (producción, almacenamiento y distribución); y Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones).

¿Qué beneficios supone para el operador de estas infraestructuras?

La puesta a disposición de un equipo de estas características tiene varios beneficios directos para el operador, entre los que destacan:

- Acceso a un equipo técnico especializado.

- Contar con un servicio de notificación de alerta temprana de riesgos, amenazas o incidentes que puedan afectar a los sistemas de información del operador.

- Aumentar la capacidad de mitigación del incidente a través de la coordinación con los diferentes agentes implicados, como proveedores de servicios en internet, Fuerzas y Cuerpos de Seguridad del Estado u otros CERTs, incluso en el ámbito internacional en el caso de incidentes originados fuera de la jurisdicción española.

- Acceso a servicios de carácter preventivo orientados a proteger de una manera más eficiente las infraestructuras nacionales.

- Contar con un soporte jurídico y legal en todo el ciclo de vida del incidente.

- El seguimiento de los incidentes en base a un protocolo de actuación común

Esquema Nacional de Seguridad (ENS)

En el ámbito de la Administración Electrónica española, el Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho esquema se regula en Real Decreto 3/2010, de ocho de enero, y es establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

El ámbito de aplicación del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007:

- A la Administración General del Estado, Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

Sus elementos principales son:

- Los **principios básicos** a ser tenidos en cuenta en las decisiones en materia de seguridad.
- Los **requisitos mínimos** que permitan una protección adecuada de la información.
- La **categorización de los sistemas**, en nivel Alto Medio o Bajo, para la adopción de medidas de seguridad proporcionales a la naturaleza de la información, del sistema y de los servicios a proteger y a los riesgos a que están expuestos.
- Las **medidas de seguridad** (75) organizadas en: **Marco Organizativo** (4), **Marco Operacional** (31) y **Medidas de protección** (40)
- La **auditoría de la seguridad** que verifique el cumplimiento del Esquema Nacional de Seguridad

Actualización de ENS:

El 23 de octubre de 2015, el Consejo de Ministros aprobó un Real Decreto que modifica otro Real Decreto, el del ocho de enero de 2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Se introducen en el Esquema Nacional de Seguridad, entre otras, las siguientes medidas adicionales:

- Introduce la gestión continuada de la seguridad en los servicios disponibles, por medios electrónicos veinticuatro horas al día.
- Especifica la necesidad de utilizar productos que tengan certificada la funcionalidad de seguridad que se corresponda con la categoría y nivel de seguridad del sistema afectado.
- Introduce los procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información precisando el concepto de incidente de seguridad.

- Clarifica el papel del Centro Criptológico Nacional y del CCN-CERT, especificando que será necesaria la notificación a ellos de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.
- Explicita y relaciona las instrucciones técnicas de seguridad, que serán de obligado
- cumplimiento por las Administraciones Públicas y que regularán el estado de seguridad, la auditoría de seguridad, la gestión de incidentes, la criptología, la interconexión y los requisitos de seguridad en entornos externalizados, entre otras.

MAGERIT

MAGERIT (**Metodología de Análisis y Gestión de Riesgos** de los **Sistemas de Información** de la Administraciones) es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno. Se han publicado tres versiones, en los años 1997, 2005 y 2012, algunas disponibles también en inglés e italiano. MAGERIT versión 3 se ha estructurado en tres libros: "Método", "Catálogo de Elementos" y "Guía de Técnicas".

> MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.- Edita: © Ministerio de Hacienda y Administraciones Públicas, octubre 2012.- NIPO: 630-12-171-8
>
> Libro I : Método (PDF - 1,47 MB)
>
> Libro II: Catálogo de Elementos (PDF - 3,37 MB)
>
> Libro III: : Guía de Técnicas (PDF - 1,28 MB)

MAGERIT persigue los siguientes objetivos directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Las herramientas informáticas que acompañan a MAGERIT son:

PILAR (Procedimiento Informático Lógico para el Análisis de Riesgos)

EAR (Entorno de análisis de riesgos)

Disponibles en:

https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html

CISM (*Certified Information Security Management*)

Es una certificación para administradores de seguridad de la información respaldada por ISACA (Information Systems Audit and Control Association). Está enfocada en la gerencia y ha sido obtenida por varios miles de personas desde su introducción, en el año 2004.

A diferencia de otras certificaciones de seguridad, CISM define los principales estándares de competencias y desarrollo profesionales que un director de seguridad de la información debe poseer, competencias necesarias para dirigir, diseñar, revisar y asesorar un programa de seguridad de la información.

La certificación precisa acreditar conocimientos en los dominios de la seguridad de la información, el examen consiste de 200 preguntas de opción múltiple que deben ser contestadas en cuatro horas. El examen está dividido en cuatro áreas:

- Gobierno de la seguridad de la información
- Gestión del riesgo de la información y cumplimiento
- Desarrollo y gestión del programa de seguridad de la información
- Gestión de incidentes de seguridad de la información.

Certificación de ENS

las normas de ENS establecen la obligatoriedad de realizar una auditoría de certificación de la conformidad por una entidad de certificación acreditada por ENAC (por ejemplo AENOR) en todos los sistemas de información de categoría Media y Alta; es decir, aquellos sobre los que un posible incidente tendría un impacto que afectaría a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad. En el caso de los sistemas de categoría Básica la certificación no será obligatoria, aunque sí recomendable.

Los sistemas de información de los servicios electrónicos de las AA.PP. deberían de estar adecuados al ENS antes del cuatro de noviembre de 2017.