ANALISIS DE RIESGOS EN SISTEMAS

Unidad 10: Marco legal, evaluación y certificación

Objetivo específico 10: El alumno conocerá el marco legal en el cual se desenvuelve para la evaluación y certificación en la seguridad, como funciona la firma electrónica, la seguridad en las redes y de información, así también conocerá los criterios comunes de evaluación y la creación de perfiles de protección.

Conceptos a desarrollar en la unidad: Marco legal, de evaluación y certificación, Seguridad en el ámbito de la Administración electrónica, Protección de datos de carácter personal, Firma electrónica, Información clasificada, Seguridad de las redes y de la información, Sistemas de gestión de la seguridad de la información (SGSI), La certificación, La acreditación de la entidad certificadora, Criterios comunes de evaluación (CC), Beneficiarios, Requisitos de seguridad, Creación de perfiles de protección y Uso de productos certificados

Introducción

En este tema se apunta cierta normativa legal, nacional e internacional, relevante al caso del análisis y gestión de riesgos, bien por exigirlo, bien por sustentarlo, bien por ser de utilidad en el Proceso de Gestión de Riesgos. La relación no pretende ser exhaustiva, amén de estar sujeta a un proceso legislativo activo, por lo que es obligación del responsable prestar atención a las novedades que vayan apareciendo..

Se han incluido algunas referencias a acuerdos de carácter político o de otra naturaleza a los cuales conviene también prestar atención. Por ejemplo, las Guías de la OCDE.

10.1 Seguridad en el ámbito de la Administración electrónica

En la actualidad se a incrementado la seguridad en el ámbito de la administración electrónica al realizar operaciones en los diferentes tipos de servicios que se pagan vía electrónica y de los impuestos más cotidianos como el IVA, ISR, IEPS, o de impuestos aduanales, licitaciones, así como de los servicios otorgados por los gobiernos locales o federales.

Con el establecimiento de la firma electrónica avanzada (FIEL), nos permite realizar ante el SAT las declaraciones de impuestos de una manera segura y la seguridad bancaria cuando realizamos operaciones para el pago de impuestos, servicios, proveedores, etc. nos permite una mayor certidumbre para realizar las operaciones electronicas

.

10.2 Protección de datos de carácter personal

Con la Ley de Protección de Datos en la cual todas las empresas están obligadas a realizarlas, le permite a los usuarios permanecer con sus datos de manera confidencial y la empresa que les solicita la información mantenerla de manera confidencial y segura, siendo de carácter obligatorio el no publicar la información de los usuarios.

10.3 Firma electrónica

Con el establecimiento de la firma electrónica, le permite a la autoridad administrativa el poder certificar que la persona que realiza alguna operación ya sea de pagos de impuestos, de solicitud de información de algún servicio o trámite, dándole una gran certidumbre y apoyo a los usuarios de estos servicio de firma electrónica.

Las medidas Fiscales, Administrativas y del Orden Social, en materia de prestación de servicios de seguridad en las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos, con las Administraciones Públicas es cada día más utilizada

.

10.4 Información clasificada

El Instituto federal de acceso a la información y protección de datos (IFAI), este organismo es encargado, fundamentalmente, de:

1. Garantizar el derecho de acceso de las personas a la información pública gubernamental.
2. Proteger los datos personales que están en manos tanto del gobierno federal, como de los particulares.
3. Resolver sobre las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado.

A partir de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, el 12 de junio de 2003, más de 240 dependencias y entidades del gobierno federal tienen la obligación de responder a solicitudes de información bajo la vigilancia del IFAI. El IFAI promovió la recepción de estas solicitudes a través de internet, mediante el sistema INFOMEX [www.infomex.mx].

10.5 Seguridad de las redes y de la información

La seguridad de las redes electrónicas y de los sistemas de información suscita cada ve más preocupación, en paralelo al rápido aumento del número de usuarios y del valor de sus transacciones. La seguridad ha cobrado ahora una importancia crítica, hasta el punto de que constituye un requisito previo para el crecimiento del comercio electrónico y el funcionamiento de la economía en su conjunto.

La combinación de varios factores explica que la seguridad de la información y de las comunicaciones se encuentre en la actualidad a la cabeza de las prioridades políticas en las organizaciones:

Las administraciones públicas se han dado cuenta de hasta qué punto la economía y los ciudadanos dependen del funcionamiento eficaz de las redes de comunicación y varias de ellas han comenzado a revisar sus disposiciones en materia de seguridad.

Internet ha creado una conectividad mundial que pone en contacto millones de redes, grandes y pequeñas, y cientos de millones de ordenadores individuales y, cada vez más, otros aparatos como los teléfonos móviles. Ello ha llevado consigo una reducción considerable del coste del acceso ilegal y a distancia a valiosa información económica.

Es bien conocida la difusión a través de Internet de virus que han causado importantes daños por destrucción de información o denegación de acceso a la red.

La seguridad se ha convertido en uno de los principales desafíos a que se enfrentan los responsables políticos y el estudio de una respuesta adecuada a este problema constituye una tarea cada vez más compleja. Hace tan solo unos años, la seguridad de la red era fundamentalmente un problema para los monopolios de Estado que ofrecían servicios especializados basados en redes públicas, fundamentalmente la red telefónica.

La seguridad de los sistemas informáticos se limitaba a las grandes organizaciones y a los controles de acceso. La elaboración de una política de seguridad constituía una tarea relativamente fácil. La situación ha cambiado radicalmente debido a una serie de transformaciones producidas en el mercado mundial, entre las que cabe citar la liberalización, la convergencia y la mundialización.

Las redes y los sistemas de información están en un proceso de convergencia. Cada vez están más interconectados, ofrecen el mismo tipo de servicio sin descontinuidad y personalizado y comparten en cierta medida la misma infraestructura. Los equipos terminales (PC, teléfonos móviles,

etc.) se han convertido en un elemento activo de la arquitectura de la red y pueden conectarse a distintas redes.

Las redes son internacionales. Una parte significativa de la comunicación actual es transfronteriza y transita por terceros países (a veces sin que el usuario final sea consciente de ello), por lo que cualquier solución a los problemas de seguridad habrá de tener en cuenta este factor. La mayoría de las redes están formadas por productos comerciales procedentes de proveedores internacionales. Los productos de seguridad deberán ser compatibles con las normas internacionales.

La política propuesta debe verse como parte integrante del marco existente para los servicios de comunicación electrónica, la protección de los datos y, más recientemente, la política en materia de *ciberdelincuencia.*

Marco de evaluación y certificación

La complejidad de los sistemas de información conlleva un gran esfuerzo para determinar la calidad de las medidas de seguridad de que se ha dotado y la confianza que merecen. Es frecuente la aparición de terceras partes que de forma independiente emiten juicios sobre dichos aspectos, juicios que se emiten tras una evaluación rigurosa y que se plasman en un documento reconocido.

En este capítulo se repasan someramente dos marcos en los que se ha formalizado el proceso de evaluación y certificación (o registro):

- en los sistemas de gestión de la seguridad de la información
- en los productos de seguridad

Para cada uno de estos marcos se indica su oportunidad, la forma de organizarse para alcanzar la certificación y el marco administrativo y normativo en el que se desarrolla la actividad.

10.6 Sistemas de gestión de la seguridad de la información (SGSI)

Se define “sistema de gestión” como lo que la Organización hace para gestionar sus procesos o actividades, de forma que los productos que fabrica o los servicios que presta satisfagan los objetivos que la propia organización de ha marcado, típicamente

- satisfacer la calidad demandada por los clientes
- cumplir con las obligaciones legales, regulatorias y contractuales

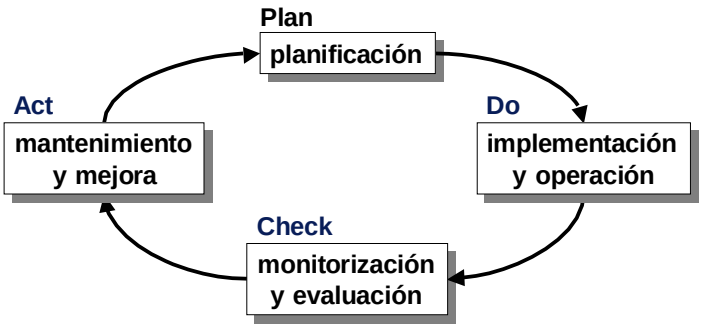
Dentro del sistema de gestión de una Organización, se entiende por “sistema de gestión de la seguridad de la información” (SGSI) la parte relacionada con la seguridad de la información. Es habitual entender que los sistemas de gestión deben ajustarse al llamado ciclo de Denning (PDCA), habitual en sistemas de gestión de la calidad:

P – Plan – Se establecen objetivos y se preparan planes para alcanzarlos. Esto incluye analizar la situación de la Organización: dónde estamos y dónde queremos estar.

D – Do – Se ejecutan los planes.

C – Check – Se evalúan los resultados obtenidos para determinar en qué medida se han alcanzado los objetivos propuestos.

A – Act – A fin de estar cada día mejor (mejora continua), se actualizan los planes y su implantación.



Ciclo PDCA

La planificación (P de *Plan*) debe incluir una política de seguridad que marque objetivos y un análisis de riesgos que modele el valor del sistema, su exposición a amenazas, y lo que se tiene (o se necesita) para mantener el riesgo bajo control. Es natural que con estas bases se genere un plan de seguridad razonado para la gestión de riesgos.

La acción (D de *Do*) es la ejecución del plan, en sus aspectos técnicos y de organización, involucrando a las personas que se hacen cargo del sistema o están relacionadas con éste. Un plan tiene éxito cuando lleva a una operación diaria sin sorpresas.

La monitorización (C de *Check*) de la operación del sistema parte del hecho de que no se puede confiar ciegamente en la eficacia de las medidas, sino que continuamente hay que evaluar si responden a lo esperado con la eficacia deseada. Hay que medir tanto lo que ocurre como lo que ocurriría si no se hubieran tomado medidas. A veces se habla del "coste de la inseguridad" como justificación de que el gasto de dinero y esfuerzo tiene fundamento. Y hay que atender a las novedades que se produzcan, tanto en cuanto a modificaciones del propio sistema de información, como a nuevas amenazas.

La reacción (A de *Act*) es saber derivar consecuencias de la experiencia, propia y de sistemas similares, repitiendo el ciclo PDCA.

La evaluación de un sistema de gestión de la seguridad parte del supuesto de que el esquema anterior vertebra las actuaciones de la Organización en materia de seguridad, y juzga la eficacia de los controles implantados para alcanzar asegurarnos de que se alcanzan los objetivos propuestos.

Nótese que un sistema de gestión maduro debe estar documentado en todos sus aspectos. Es típico de organizaciones inmaduras que las actividades se realizan siguiendo normas y procedimientos que se sobreentienden o están en la cabeza de las personas. Sólo cuando todo figura por escrito podemos hablar de un sistema de gestión que puede ser objeto de una certificación.

10.6.1 La certificación

Certificar un sistema de gestión de la seguridad consiste en que alguien, externo a la Organización y acreditado para la tarea, afirma que ha auditado el sistema y lo considera ajustado a la norma correspondiente.

El que certifica compromete en ello su palabra (por escrito). Con todas las cautelas de alcance y tiempo que se consideren oportunas (y se recojan explícitamente). Y sabiendo que lo que se asegura hoy, hay que revisarlo a medio plazo pues todo evoluciona.

Para obtener un certificado hay que seguir una serie de formalismos. Sin entrar en excesivo detalle nos centraremos en qué evalúa el equipo que envía el organismo de certificación a juzgar a la Organización.

Lo primero que hay que hacer es delimitar el alcance de lo que se va a evaluar como "Sistema de Gestión de la Seguridad de la Información". Esta es una delimitación propia de cada Organización, que refleja su misión y su organización interna. Es importante delimitar con claridad. Si el

perímetro es difuso no quedará claro qué hay que hacer en los pasos siguientes; en particular, no se sabrá muy bien a qué personas y departamentos hay que dirigirse para reclamar la información pertinente. Nótese que esto puede no ser evidente. Actualmente es raro encontrar una organización cerrada desde el punto de vista de sus sistemas de información: la externalización de servicios, la administración electrónica y el comercio electrónico han diluido las fronteras. Por otra parte, el organigrama interno rara vez responde a las responsabilidades en seguridad.

Lo siguiente que hay que tener claro, escrito y mantenido es la política de seguridad corporativa. A menudo la política de seguridad incluye la relación de la legislación que afecta. Es absolutamente necesario delimitar el marco legislativo y regulatorio al que hay que atenerse.

Todo debe estar escrito. Y bien escrito: se entiende, es coherente, se divulga, es conocido por los involucrados y se mantiene al día. Un proceso de certificación siempre tiene un fuerte componente de revisión de documentación.

Antes de que venga el equipo evaluador, hay que tener una foto del estado de riesgo de la Organización. Es decir, que hay que hacer un análisis de riesgos identificando activos, valorándolos, identificando y valorando las amenazas significativas. En este proceso se determina qué salvaguardas requiere el sistema y con qué calidad. Cada caso es un mundo aparte: ni todo el mundo tiene los mismos activos, ni valen lo mismo, ni están igualmente interconectados, ni todo el mundo está sujeto a las mismas amenazas, ni todo el mundo adopta la misma estrategia para protegerse.

El análisis de riesgos es una herramienta (imprescindible) de gestión. Por hacer o dejar de hacer un análisis de riesgos no se está ni más ni menos seguro: simplemente, se sabe dónde se está. A partir de este conocimiento podemos tomar decisiones de tratamiento y ejecutarlas.

Los resultados del análisis de riesgos permiten justificar las decisiones de tratamiento del riesgo. Todo esto deberá ser verificado por el equipo evaluador que, de quedar satisfecho, avalará la concesión del certificado.

El equipo evaluador inspecciona el sistema de información que se desea certificar contrastándolo con una referencia reconocida que permita objetivar la evaluación a fin de evitar cualquier tipo de arbitrariedad o subjetividad y permitir la utilización universal de las certificaciones emitidas. Se utiliza un “esquema de certificación”

La norma 27001 tiene por objeto la especificación de “los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información con independencia de su tipo, tamaño o área de actividad.”

La acreditación de la entidad certificadora

La credibilidad del certificado es la confianza que merezca el certificador. ¿Cómo se construye esta confianza?

Un componente esencial es la credibilidad del esquema de certificación. Un segundo componente es la credibilidad de la organización que emite los certificados. Esta organización es responsable de la competencia del equipo evaluador y de la ejecución del proceso de evaluación. Para certificar que estas responsabilidades se cumplen se procede al llamado “proceso de acreditación” donde una nueva organización evalúa al evaluador. En España, la organización encargada de acreditar organismos certificadores es ENAC, que se acoge a la normativa internacional de reconocimiento mutuo de certificados emitidos por diferentes certificadores en diferentes países.

10.7 Criterios comunes de evaluación (CC)

La necesidad de evaluar la seguridad de un sistema de información aparece muy temprano de la mano de los procesos de adquisición de equipos del Departamento de Defensa de los EEUU que, en 1983, publica el llamado “Libro Naranja” (TCSEC – *Trusted Computer System Evaluation Criteria*). El objetivo es especificar sin ambigüedad qué se necesita por parte del comprador y qué se ofrece por parte del vendedor, de forma que no haya malentendidos sino un esquema transparente de evaluación, garantizando la objetividad de las adquisiciones.

La misma necesidad lleva a la aparición de iniciativas europeas como ITSEC *(Information Technology Security Evaluation Criteria).* A mediados de los años 90, existe en el mundo una proliferación de criterios de evaluación que dificulta enormemente el comercio internacional, llegándose a un acuerdo de convergencia que recibe el nombre de *"Common Criteria for Information Technology Security Evaluation",* normalmente conocidos como "Criterios Comunes" o por sus siglas, CC.

Los CC, además de la necesidad de un entendimiento universal, capturan la naturaleza cambiante de las tecnologías de la información que, en el periodo desde 1980, han pasado de estar centradas en los equipos de computación, a englobar sistemas de información mucho más complejos.

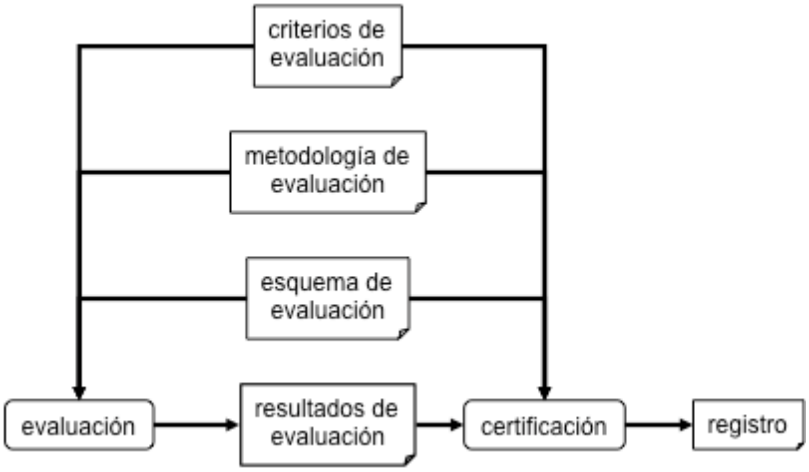
Los CC permiten

1. definir las funciones de seguridad de los productos y sistemas (en tecnologías de la información) y
2. determinar los criterios para evaluar [la calidad] de dichas funciones.

Es esencial la posibilidad que los CC abren para que la evaluación sea objetiva y pueda realizarse por una tercera parte (ni por el proveedor, ni por el usuario) de forma que la elección de salvaguardas adecuadas se vea notablemente simplificada para las organizaciones que necesitan mitigar sus riesgos.

La evaluación de un sistema es la base para su certificación. Para certificar es necesario disponer de

1. unos criterios, que definen el significado de los elementos que se van a evaluar
2. una metodología, que marque cómo se lleva a cabo la evaluación
3. un esquema de certificación[37] que fije el marco administrativo y regulatorio bajo el que se realiza la certificación



Proceso de certificación

De esta forma se puede garantizar la objetividad del proceso; es decir, construir la confianza en que los resultados de un proceso de certificación son válidos universalmente, independientemente de dónde se realice la certificación.

Dado que [la calidad de] la seguridad requerida de un sistema no es siempre la misma, sino que depende de para qué se quiera emplear, CC establece una escala de niveles de aseguramiento:

EAL0: sin garantías

EAL1: probado funcionalmente

EAL2: probado estructuralmente

EAL3: probado y chequeado metódicamente

EAL4: diseñado, probado y revisado metódicamente

EAL5: diseñado y probado semiformalmente

EAL6: diseñado, probado y verificado semiformalmente

EAL7: diseñado, probado y verificado formalmente

Los niveles superiores requieren un mayor esfuerzo de desarrollo y de evaluación, ofreciendo a cambio unas grandes garantías a los usuarios.

10.7.1 Beneficiarios

Los CC se dirigen a una amplia audiencia de potenciales beneficiarios de la formalización de los conceptos y elementos de evaluación: los consumidores (usuarios de productos de seguridad), los desarrolladores y los evaluadores. Un lenguaje común entre todos ellos se traduce en ventajas apreciables:

Para los consumidores

- que pueden expresar sus necesidades, antes de adquirir los servicios o productos que las satisfagan; esta caracterización puede resultar útil tanto en adquisiciones individuales, como en la identificación de necesidades de grupos de usuarios
- que pueden analizar las características de los servicios o productos que ofrece el mercado
- que pueden comparar diferentes ofertas

Para los desarrolladores

- que saben qué se les va a exigir y cómo se van a evaluar sus desarrollos
- que saben, objetivamente, qué requieren los usuarios
- que pueden expresar sin ambigüedad lo que hacen sus desarrollos

Para los evaluadores

- que disponen de un marco formalizado para saber qué tienen que evaluar y cómo tienen que calificarlo

Para todo el mundo

- que dispone de unos criterios objetivos que permiten aceptar las certificaciones realizadas en cualquier parte

Todos estos participantes convergen sobre un objeto a evaluar denominado **TOE** *(Target Of Evaluation*)**,** que es el servicio o producto (de seguridad) cuyas características (de seguridad) se quieren evaluar.

Cuando un análisis de riesgos expone la relación de salvaguardas adecuadas, estas pueden venir expresadas en terminología CC, lo que permite engarzar con las ventajas citadas, convirtiéndose en una especificación normalizada.

10.7.2 Requisitos de seguridad

Dado un sistema se pueden determinar, a través de un análisis de riesgos, qué salvaguardas se requieren y con qué calidad. Este análisis puede hacerse sobre un sistema genérico o sobre un sistema concreto. En CC, el conjunto de requisitos que se le exigen a un sistema genérico se denomina **perfil de protec ción** (**PP** – *Protection Profile*). Si no se está hablando de un sistema ge- nérico, sino de un sistema concreto, el conjunto de requisitos se conoce como **declaración de seguridad** (**ST** – *Security Target*).

Los PP, dado su carácter genérico, cubren diferentes productos concretos. Suelen ser preparados por grupos de usuarios u organismos internacionales que quieren modelar el mercado.

Los ST, dado su carácter específico, cubren un producto concreto. Suelen ser preparados por los propios fabricantes que de esta manera formalizan su oferta[41].

CC determina los apartados en que debe estructurarse un PP o un ST. El índice de estos documentos es un buen indicador de su alcance:

PP- perfil de protección	*ST – declaración de seguridad*
— Introduction — TOE description — Security environment • assumptions • threats • organizational security policies — Security objectives • for the TOE • for the environment — Security requirements • for the environment • TOE functional requirements • TOE assurance requirements — Application notes — Rationale	— Introduction — TOE description — Security environment • assumptions • threats • organizational security policies — Security objectives • for the TOE • for the environment — Security requirements • for the environment • TOE functional requirements • TOE assurance requirements — TOE summary specification — PP claims • PP reference • PP tailoring • PP additions — Rationale

Perfiles de protección y Declaraciones de seguridad

Los PP y los ST pueden ser a su vez sometidos a una evaluación formal que verifique su completitud e integridad. Los PP así evaluados pueden pasar a registros públicos para ser compartidos por diferentes usuarios.

En la elaboración de un ST se hace referencia a los PP a los que se acoge.

10.7.3 Creación de perfiles de protección

La generación de un PP o un ST es básicamente un proceso de análisis de riesgos donde el analista, habiendo determinado el dominio del análisis (el TOE en terminología de CC), identifica amenazas y determina, a través de los indicadores de impacto y riesgo, las salvaguardas que se requieren. En la terminología de CC, las salvaguardas requeridas se denominan **requisitos de seguridad** y se subdividen en dos grandes grupos

requisitos funcionales de seguridad *(functional requirements)*

- ¿qué hay que hacer?
- definen el comportamiento funcional del TOE

requisitos de garantía de la funcionalidad de la seguridad *(assurance requirements)*

- ¿está el TOE bien construido?
- ¿es eficaz? ¿satisface el objetivo para el que se requiere?
- ¿es eficiente? ¿alcanza sus objetivos con un consumo razonable de recursos?

Es importante destacar que CC establece un lenguaje común para expresar los objetivos funcionales y de aseguramiento. Es necesario pues que el análisis de riesgos utilice esta terminología en la selección de salvaguardas. La norma CC nos proporciona en su parte 2 el catálogo estandarizado de objetivos funcionales, mientras que en su parte 3 nos proporciona el catálogo estandarizado de objetivos de aseguramiento.

Parte 2: Requisitos funcionales	*Parte 3: Requisitos de garantía*
FAU: Security audit	ACM: Configuration management
FCO: Communication	ADO: Delivery and operation
FCS: Cryptographic support	ADV: Development
FDP: User data protection	AGD: Guidance documents
FIA: Identification and authentication	ALC: Life cycle support
FMT: Security management	ATE: Tests
FPR: Privacy	AVA: Vulnerability assessment
FPT: Protection of the TOE security functions	APE: PP evaluation
FRU: Resource utilisation	ASE: ST evaluation
FTA: TOE access	
FTP: Trusted path / channels	

Requisitos funcionales y de aseguramiento de la función

10.7.4 Uso de productos certificados

Cuando un TOE ha sido certificado de acuerdo a un PP o un ST, según convenga en cada caso, se puede tener la certeza de que dicho TOE satisface las necesidades y además las satisface con la calidad requerida.

La certificación de un sistema o producto no es garantía ciega de idoneidad: es necesario cerciorarse de que el PP o ST respecto del que se han certificado satisface los requisitos de nuestro sistema. El análisis de riesgos nos ha permitido elaborar el PP o el ST o, en ocasiones, seleccionar un conjunto apropiado a nuestro mapa de riesgos. Pero lo esencial es que de análisis de riesgos se han obtenido unos requisitos de seguridad cuya satisfacción permitirá mantener impacto y riesgo residuales bajo control.

En la medida en que un producto certificado se ajusta a un PP o ST que satisface nuestras necesidades, la gestión de riesgos se reduce a adquirir el producto, instalarlo y operarlo en las condiciones adecuadas.

Es importante destacar que tanto los PP como los ST incluyen una sección denominada “hipótesis” en la que se establecen una serie de prerrequisitos que debe satisfacer el entorno operacional en el que se instala TOE. No se hace sino reconocer que el mejor producto, inadecuadamente instalado u operado, es incapaz de garantizar la satisfacción de los objetivos globales. Por ello, los productos certificados son componentes muy sólidos de un sistema; pero además hay que garantizar su entorno para asegurar el sistema completo.