Niveles de Gestión de la Seguridad

Índice

1. Introducción.
2. Nivel 0: el sentido común.
3. Nivel 1: salvaguardas preventivas mínimas. Cumplimiento de la legislación obligatoria.
4. Nivel 1,5: salvaguardas adicionales mínimas. Legislación administraciones públicas. Esquema Nacional de Seguridad.
5. Nivel 2: gestión del proceso de seguridad. Estándares y normas europeas y españolas. Certificación.
6. Nivel 3. gestión global de la seguridad.
7. Nivel 4. certificación de componentes y de sistemas.

1. Introducción

¿Cómo se puede determinar en una organización si se encuentra segura?

Las organizaciones necesitan responder a las siguientes cuestiones:

- ¿Cómo puede justificarse el coste de nuevas medidas de seguridad?
- ¿Recibe la organización algo a cambio de su inversión?
- ¿Cuándo sabe la organización que está "segura"?
- ¿Cuántos recursos son necesarios para estar "seguro"?
- ¿Cómo puede comparar la organización su estado con otras del sector y con los estándares de buenas prácticas?

La respuesta tradicional a estas preguntas se relaciona con la **evaluación del riesgo y el riesgo residual** que la organización está dispuesta a asumir en función de sus necesidades de negocio y limitaciones de presupuesto.

La gestión del riesgo puede darse por sentada, aunque no conduce necesariamente a un estado de mayor seguridad. Hay una tendencia a disponer de grandes cantidades de herramientas de seguridad y evitar los controles más caros y menos glamurosos.

Los controles más complicados tienden a ser de naturaleza organizativa, requiriendo cambios culturales (tales como un plan de recuperación de desastres), más que soluciones llave en mano (tales como cortafuegos y sistemas de detección de intrusos, IDS). La dirección piensa que está comprando más seguridad por menos dinero.

Sin embargo, podemos hacer algunas preguntas:

- ¿En una organización quién dice que se compre más seguridad?
- ¿Cómo puede medir la organización la protección relativa obtenida con cada adquisición?

- ¿Está comprando la organización las salvaguardas de seguridad en el orden correcto?

- ¿Está exponiéndose la organización a más riesgo debido al enfoque no sistemático de la implantación?

Crear programas de seguridad desde el inicio permite abordar estos problemas tradicionales de métricas de seguridad de otra forma.

Una mirada renovada a dichos problemas facilita el desarrollo de una solución exhaustiva para cualquier sector.

Este enfoque nuevo, más sistemático, de las métricas de seguridad permitirá:

- Generar mediciones reproducibles y justificables.

- Medir algo que tenga valor para la organización.

- Determinar el progreso real en el estado de la seguridad.

- Ser aplicable a un amplio espectro de organizaciones, al tiempo que produce resultados similares.

- Determinar el orden en que deberían aplicarse los controles de seguridad.

- Determinar los recursos que necesitan ser destinados al programa de seguridad.

Métrica	Supuesta Medición	Peligros
Número de virus o códigos malignos detectados	Eficacia de los controles antivirus automáticos	¿Por qué pasan tantos virus en primer lugar? ¿Cuántos pasaron y nunca se detectaron?
Número de incidentes e investigaciones de seguridad	Nivel de actividad de la monitorización de eventos de seguridad	¿Qué umbral desencadena un incidente o una investigación? ¿Se desencadenan incidentes por defectos en los procedimientos organizativos?
Coste de las brechas de seguridad	Pérdidas económicas reales debidas a fallos de seguridad	¿Qué riesgos residuales eligió asumir la empresa? ¿Es una medida de la respuesta ante crisis o desastres, pero no necesariamente función de las salvaguardas sensatas implantadas?
Recursos asignados a las funciones de seguridad	Coste económico real de utilizar un programa de seguridad	¿Son ineficientes las herramientas, tareas asignadas o procedimientos, llevando al personal a perder tiempo?
Cumplimiento de las reglas de seguridad	Nivel de cumplimiento de los objetivos del programa de seguridad	¿Cómo se relaciona el cumplimento con la eficacia? ¿Cuál es el orden de cumplimiento? Una vez logrado el cumplimiento, ¿se "acaba" el programa de seguridad?

La **clave de las métricas de seguridad** está en obtener medidas que tengan las siguientes características ideales:

- Deberían medir entes **significativos** para la organización.
- Deberían ser **reproducibles**.
- Deberían ser **objetivas e imparciales**.
- Deberían ser capaces de medir algún tipo de **progresión a lo largo del tiempo**.

En la práctica, casi todas las métricas de seguridad publicadas no incorporan todas estas características.

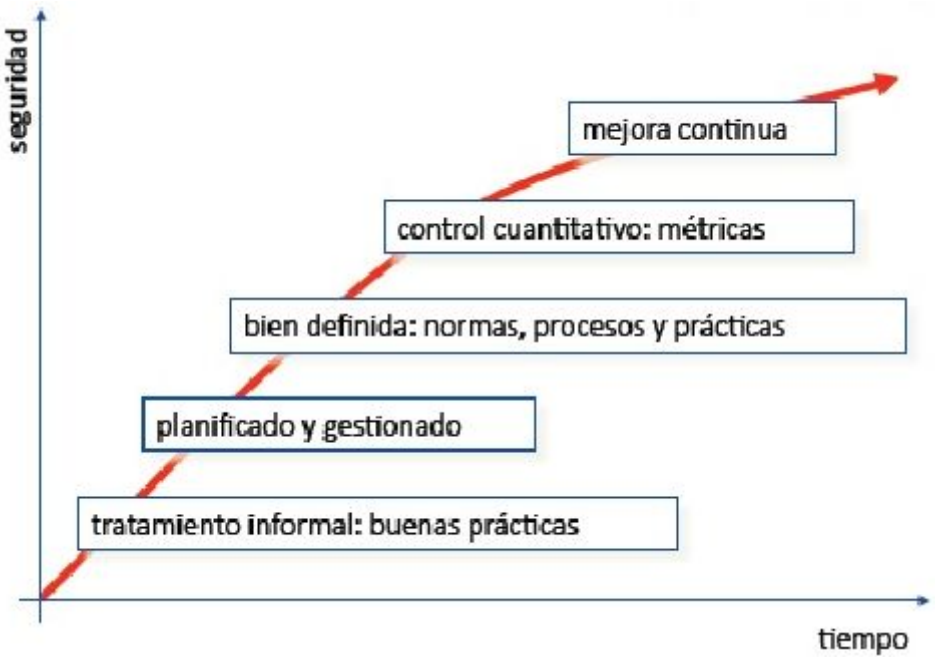
Las métricas de seguridad tradicionales eran un asunto de "toma todo lo que puedas", es decir, cualquier métrica que estuviese disponible se tomaba y reportaba.

Esta forma de pensar debería cambiar. Se necesita un enfoque más sistemático para el desarrollo de métricas que encajen directamente en las características mencionadas anteriormente.

Madurez del Programa de Seguridad

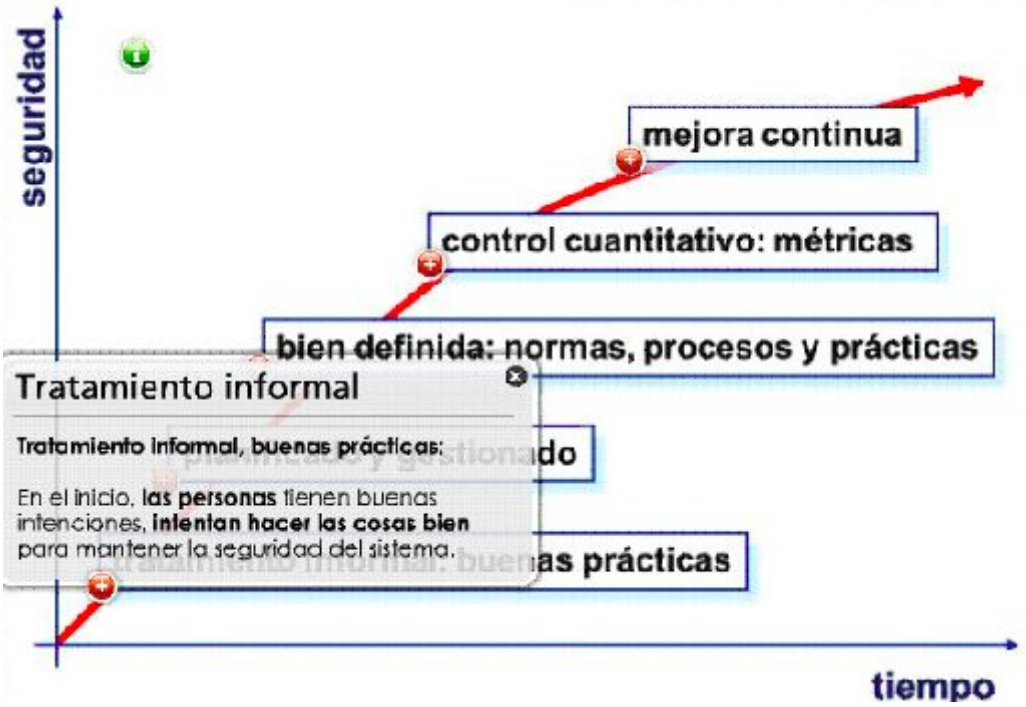
Una pieza del puzzle de métricas de seguridad es la medida del progreso del programa de seguridad frente a un modelo de madurez. Este enfoque apunta directamente al menos a dos de las cuatro características mencionadas previamente:

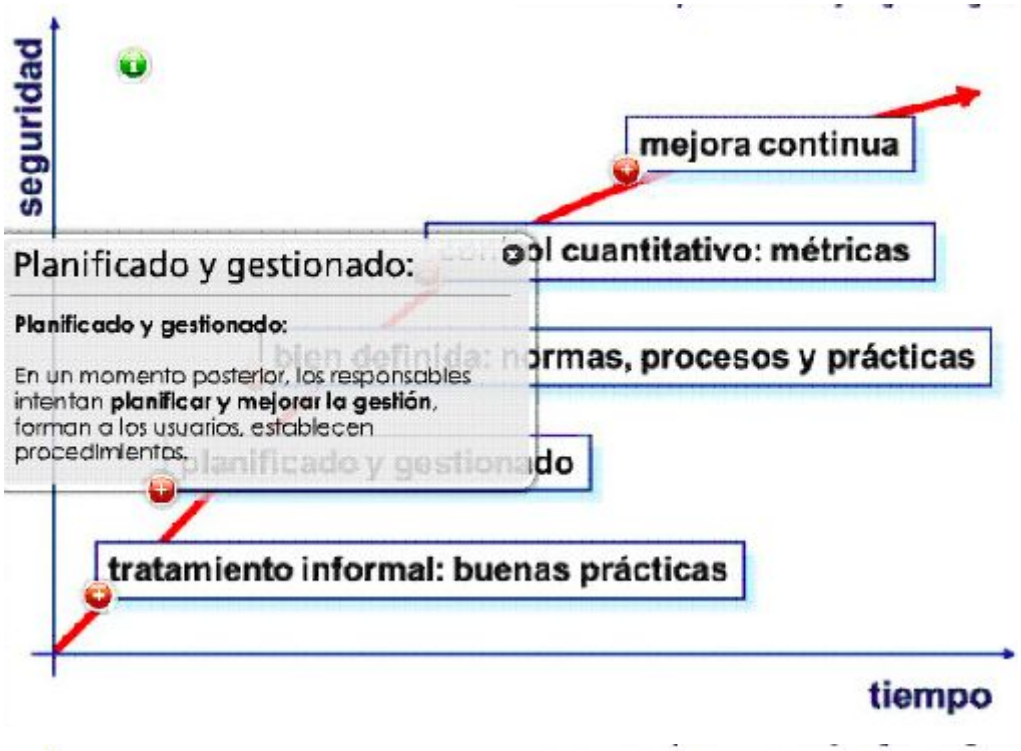
- Mide entes significativos para la organización
- Progresión hacia un objetivo.

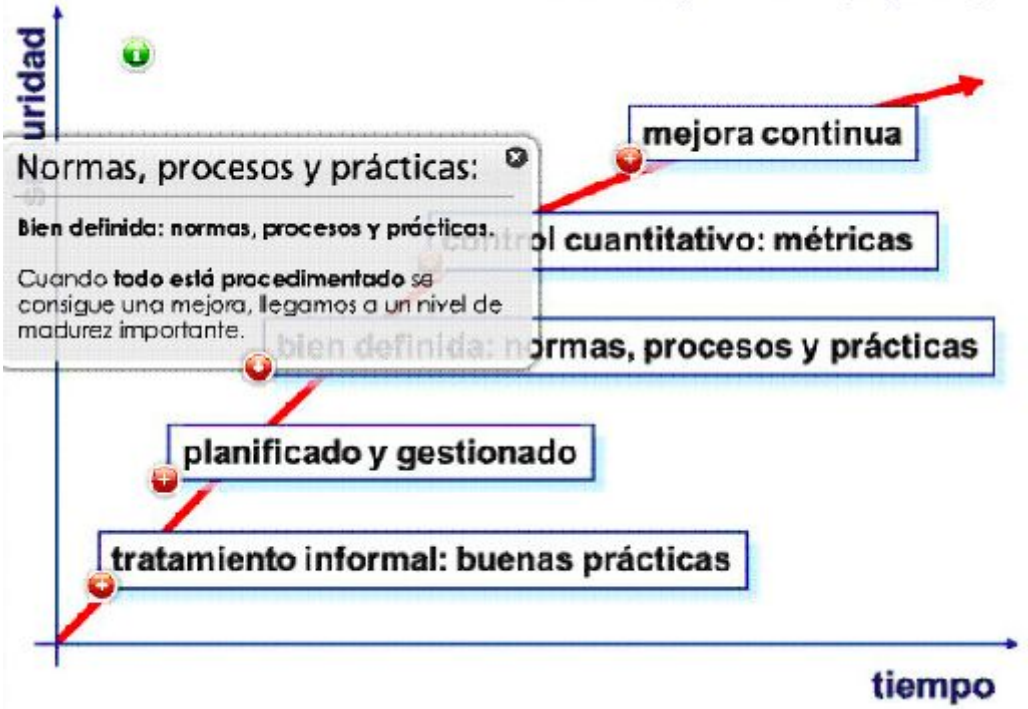


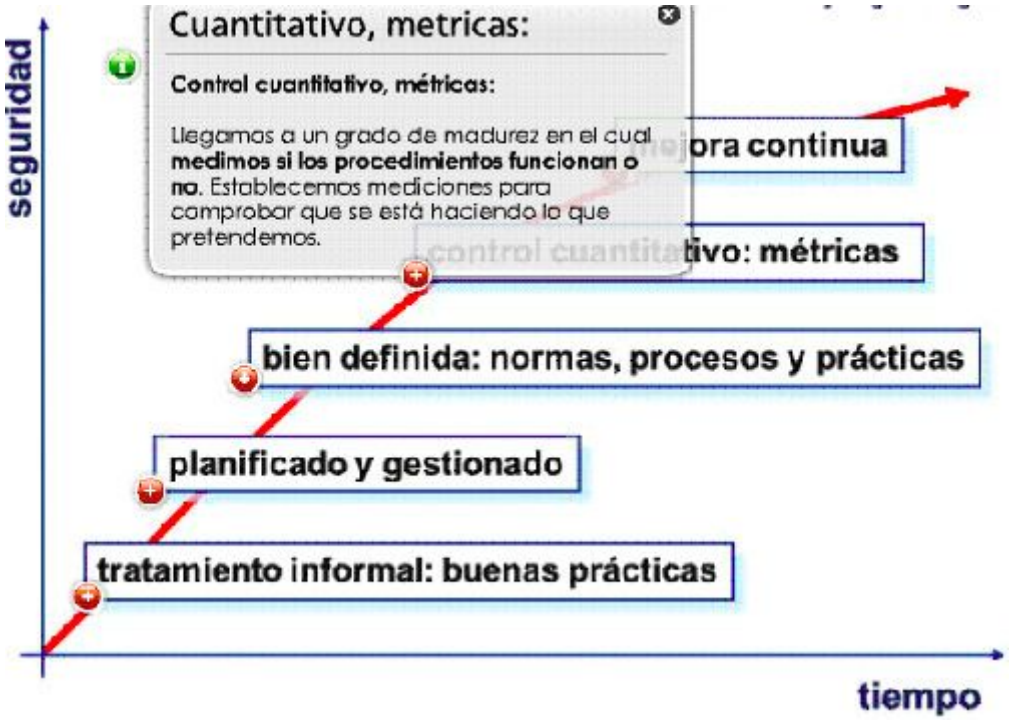
Madurez del manejo de un sistema de información


Madurez
La seguridad del sistema evoluciona con el tiempo:
mejora continua
cuantitativo: métricas
rmas, procesos y prácticas
do
as prácticas
tiempo


seguridad
mejora continua
control cuantitativo: métricas
bien definida: normas, procesos y prácticas
Tratamiento informal
Tratamiento informal, buenas prácticas:
En el inicio, las personas tienen buenas intenciones, intentan hacer las cosas bien para mantener la seguridad del sistema.
do
as prácticas
tiempo


seguridad
mejora continua
cuantitativo: métricas
Planificado y gestionado:
Planificado y gestionado:
En un momento posterior, los responsables intentan planificar y mejorar la gestión, forman a los usuarios, establecen procedimientos.
rmas, procesos y prácticas
tratamiento informal: buenas prácticas
tiempo


mejora continua
Normas, procesos y prácticas:
Bien definida: normas, procesos y prácticas.
Cuando todo está procedimentado se consigue una mejora, llegamos a un nivel de madurez importante.
cuantitativo: métricas
rmas, procesos y prácticas
planificado y gestionado
tratamiento informal: buenas prácticas
tiempo


Cuantitativo, metricas:
Control cuantitativo, métricas:
Llegamos a un grado de madurez en el cual medimos si los procedimientos funcionan o no. Establecemos mediciones para comprobar que se está haciendo lo que pretendemos.
seguridad
mejora continua
control cuantitativo: métricas
bien definida: normas, procesos y prácticas
planificado y gestionado
tratamiento informal: buenas prácticas
tiempo

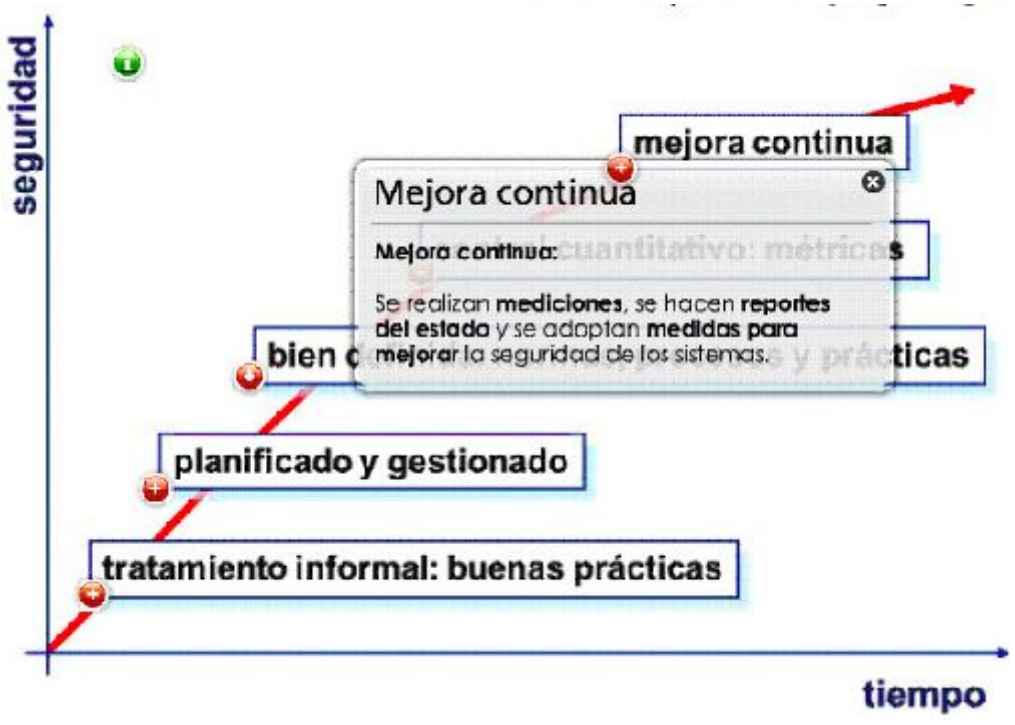

seguridad
mejora continua
Mejora continua
Mejora continua:
Se realizan mediciones, se hacen reportes del estado y se adoptan medidas para mejorar la seguridad de los sistemas.
planificado y gestionado
tratamiento informal: buenas prácticas
tiempo

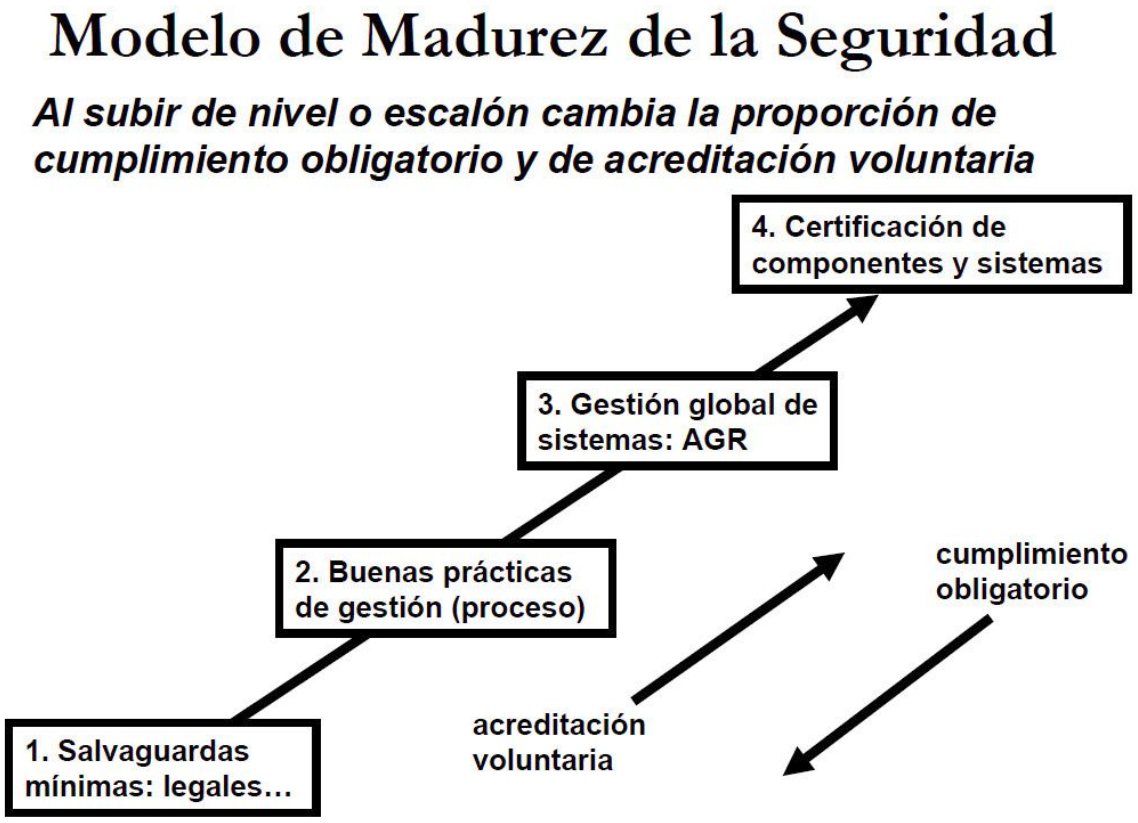
Figura 3 - Modelos de Madurez de Seguridad Publicados

Modelo	Descripción	Comentarios
Modelo de Madurez de Seguridad TI de NIST CSEAT[2]	Cinco niveles de madurez progresiva: 1. Política 2. Procedimiento 3. Implantación 4. Prueba 5. Integración	Centrado en niveles de documentación
Modelo de Evaluación de la Seguridad de la Información de Citigroup (CITI-ISEM)[3]	Cinco niveles de madurez progresiva: 1. Autocomplacencia 2. Reconocimiento 3. Integración 4. Prácticas comunes 5. Mejora continua	Centrado en concienciación y adopción por parte de la organización
Modelo de madurez de COBIT® [4]	Cinco niveles de madurez progresiva: 1. Inicial / *ad hoc* 2. Repetible pero intuitivo 3. Proceso definido 4. Gestionado y medible 5. Optimizado	Centrado en procedimientos específicos de auditoría
Modelo SSE-CMM[5]	Cinco niveles de madurez progresiva: 1. Realizado informalmente 2. Planificado y perseguido 3. Bien definido 4. Controlado cuantitativamente 5. Continuamente mejorado	Centrado en ingeniería de seguridad y diseño de software
Evaluación de la Capacidad de Seguridad de CERT/CSO[6]	Cinco niveles de madurez progresiva: 1. Existente 2. Repetible 3. Persona designada 4. Documentado 5. Revisado y actualizado Mide usando cuatro niveles: 1. Inicial 2. En desarrollo 3. Establecido 4. Gestionado	Centrado en la medición de la calidad relativa a niveles de documentación

Las entidades pueden organizar su estrategia y política de seguridad en forma escalonada para mejorar su nivel progresivamente.:

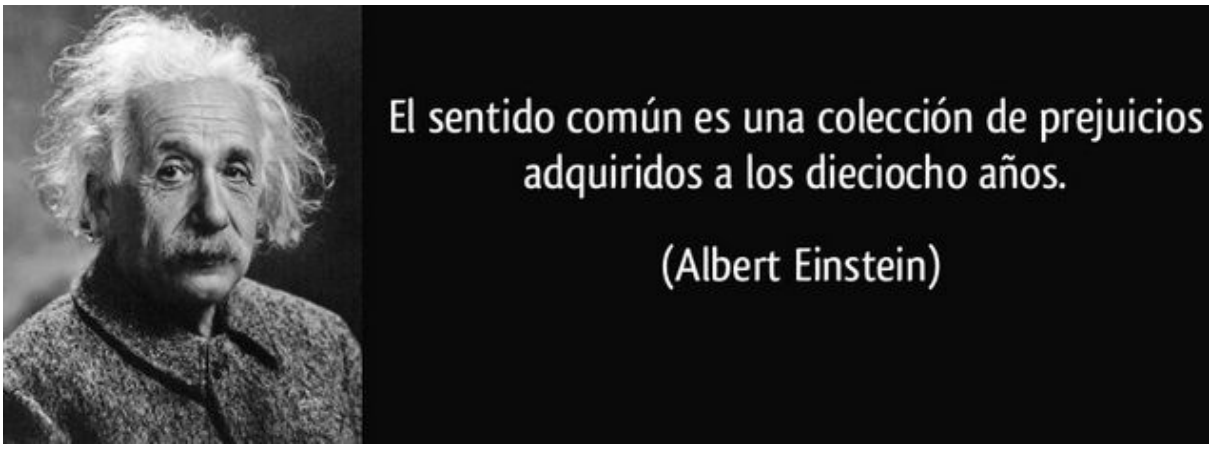
- Nivel 0: el “sentido común”
- Nivel 1: el cumplimiento de la legislación obligatoria (ej. Reglamento de seguridad)
- Nivel 2: la evaluación del Proceso de Gestión de Seguridad, con algún Código de Buenas Prácticas
- Nivel 3: el análisis de riesgos y la gestión de su resolución, con un método como MAGERIT

- Nivel 4: la adquisición de productos y la integración de componentes en sistemas compuestos, certificados siguiendo criterios de evaluación de seguridad homologables (Criterios Comunes u otros)



A continuación se tratan en detalle los distintos niveles.

2. Nivel 0: El sentido común



El sentido común aplicado a la Seguridad de los Sistemas de Información (SSI) puede resumirse en algunos principios sencillos (aunque no siempre tenidos en cuenta como demuestra la experiencia):

- Simplicidad: la primera salvaguarda es prestar atención para detectar el peligro y usar el sentido común para abortarlo.

- Adecuación: más vale ‘tiritas’ en la herida que vendaje ‘momia’ fuera de ella.

- Cadena: siempre se rompe por el eslabón más débil (pero hay que conocer toda la cadena del riesgo para centrarse en los puntos débiles).

- Economía: “que no cueste más el remedio que la enfermedad”

- Leer los manuales, porque parte del trabajo está hecho: los sistemas comportan muchas salvaguardas (a menudo no hay más que reforzar y sistematizar este tipo de salvaguardas para neutralizar muchos riesgos).

Peligros:

- Infravalorar los costes de los riesgos (o no atenderlos adecuadamente)

- Sobrevalorar los costes de las salvaguardas (y de su instalación)

En conclusión:

Problema de:	Termina con el uso e instalación de:
Sistemas de información	Mecanismos informacionales
Seguridad	Mecanismos de salvaguarda

Decálogo esencial para el diseño de seguridad de Saltzer y Shroeder (1973)	
Economía de Mecanismo	Diseño lo más simple y pequeño posible.
Seguro por defecto	Todo lo no permitido explícitamente está prohibido.
Mediación completa	El acceso a todo recurso debe ser explícitamente autorizado.
Diseño abierto	La seguridad no depende de mantener en secreto el diseño.
Separación de privilegios	Descomponer capacidades de acceso en partes que deberán concurrir simultáneamente (ejemplo: los tradicionales tres claveros de la administración local).
Mínimo privilegio	Si fallan los controles, que se cause el menor daño posible.
Mínimos mecanismos comunes	Para evitar que las interacciones entre subsistemas que se diseñaron por separado acaben dando lugar, al combinarlos, a vulnerabilidades no presentes en cada uno de ellos.
Aceptabilidad psicológica	La falta de facilidad de uso equivale a no-uso. Alineación entre la interfaz y el modelo mental del usuario y del diseñador.
Factor de trabajo	Aunque difícil de evaluar, para diseñar un control de seguridad, hay que comparar el coste de evitar un control de seguridad, con los recursos del hipotético atacante.
Registro de la brecha	Establecer mecanismos para detectar y caracterizar brechas producidas en el sistema. Hay que detectar los fallos.

3. Nivel 1: Salvaguardas preventivas mínimas

- LOPDP: Obligación de inscripción
- INSCRIBIR TODOS LOS FICHEROS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL
- Inscripción previa a la creación del fichero:
    - Inscripción lo más amplia posible
    - Notificación de cambios en la finalidad del fichero responsable y ubicación
    - En el plazo de un mes, se entiende inscrito a todos los efectos

El reglamento de desarrollo de la LOPDP, se encuentra en el Real Decreto 1720/2007 (21 diciembre) que desarrolla la Ley 15/99 de Protección de Datos de Carácter Personal.

Las medidas de seguridad a implantar, exigibles a los ficheros y tratamientos (Título VIII), se clasifican en tres niveles de seguridad:

- **Nivel básico:** todos los ficheros con datos personales.

- **Nivel medio**: datos relativos a solvencia patrimonial y crédito y los que permitan evaluar la personalidad.

- **Nivel alto**: datos de ideología, religión, creencias, origen racial, salud, sexualidad.

Según el reglamento de desarrollo de la LOPD, las medidas de seguridad a tomar obligatoriamente (todos los niveles, reforzadas en el medio y/o en el alto), se consideran en un documento de seguridad, que contenga al menos:

- Ámbito de aplicación con especificación detallada de los recursos protegidos.

- Medidas, normas, procedimientos, reglas y estándares.

- Funciones y obligaciones del personal.

- Estructura de los ficheros y descripción de los SI que los tratan.

- Procedimiento de notificación, gestión y respuesta ante las incidencias.

- Procedimientos de realización de copias de respaldo y recuperación de datos.

- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Medidas adicionales si hay datos de protección media:

- Designación de responsables de seguridad

- Control de acceso físico

- Identificación de acceso de usuarios

- Control de acceso de usuarios

- Gestión de soportes (identificar contenido y autorizar salida)

- Medidas en caso de reutilización o de desecho de soportes

- Copias de respaldo y recuperación (semanales)

- Procedimientos de recuperación de los datos

- Auditoría (cumplimiento del Reglamento, los procedimientos e instrucciones, al menos, cada dos años)

Medidas adicionales si hay datos de protección alta:

- Registro de accesos (usuario, hora, fichero, tipo de acceso, autorizado o no)

- Conservación de copia de respaldo y de los procedimientos de recuperación de los datos en un lugar distinto

- Distribución de soportes (cifrado)

- Telecomunicaciones (cifrado)

- Prohibición de pruebas con datos reales

El Cumplimiento riguroso del Reglamento de Seguridad (Real Decreto 1720/2007) implica evaluar y alcanzar un grado 1º de certificación del proceso por medio de las auditorías periódicas exigidas para los niveles de protección medio y alto.

Una de las innovaciones más destacables en su momento fue que la norma (RDLOPD) incluye expresamente en su ámbito de aplicación a los ficheros y tratamientos de **datos no automatizados** (en papel) y fija criterios específicos sobre medidas de seguridad de los mismos, según se indican a continuación:

- Aplicación de unos criterios de archivo que garanticen la conservación y el ejercicio de derechos.

- Los armarios, archivadores y demás elementos de almacenamiento, deberán disponer de mecanismos adecuados de cierre (llave) que impidan el acceso a la documentación por personas no autorizadas.

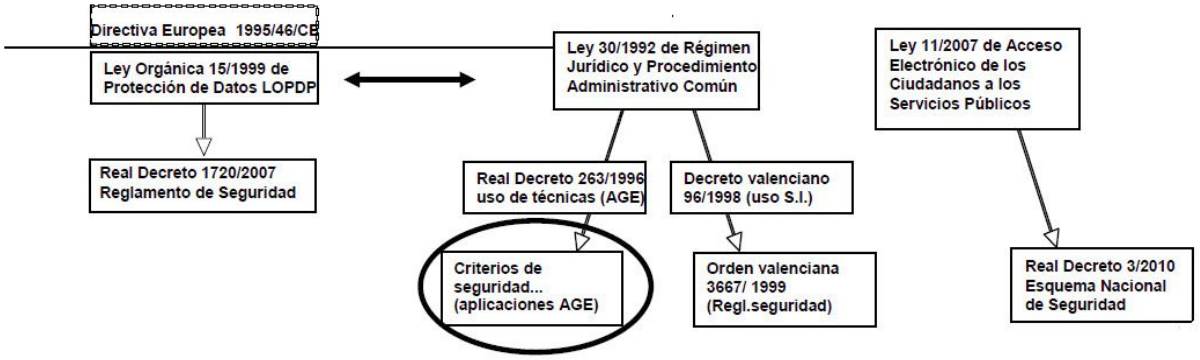
- Cuando estos ficheros contengan datos incluidos en un nivel de seguridad alto, deberán estar en áreas cerradas con el dispositivo de seguridad pertinente (puertas con llave).

4. Nivel 1.5: Salvaguardas adicionales mínimas

El nivel 1 de la seguridad de los sistemas de información y de su proceso de gestión en las Administraciones Públicas se obtiene por el obligatorio cumplimiento de la legislación vigente, según dos ramas relacionadas pero distintas:

- Rama de la intimidad (LOPDP y RD 1720/2007), aplicable a todos los sectores público y privado;

- Rama de la validez de documentos y aplicaciones de las Administraciones Públicas (LRJPAC 30/1992), aplicable sólo a éstas y dividida por su aplicación en la Administración General del Estado (RD 263/1996, Criterios de seguridad) o en una Administración autonómica (por ejemplo D 96/1998, Orden 3667/1999 en la autonomía valenciana).

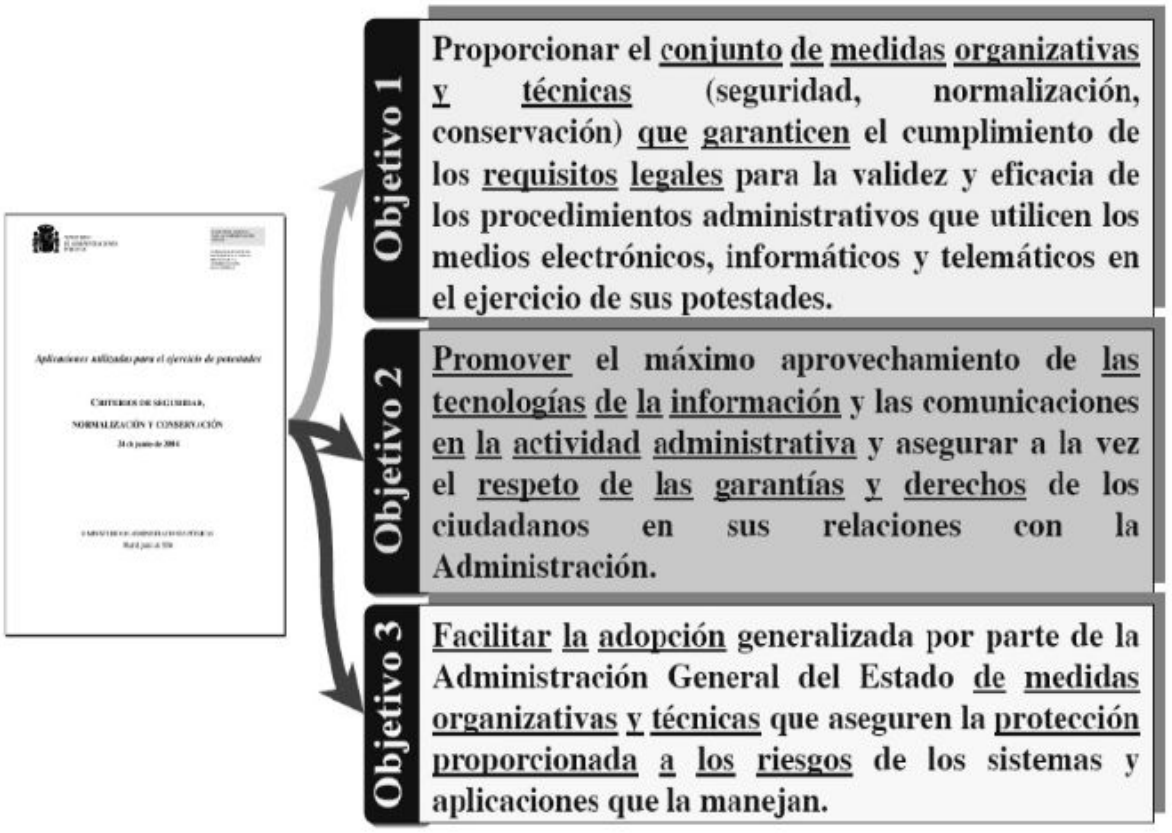


El Real Decreto 263/1996 regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado (validadas en la LRJPAC 30/1992) y prevé la difusión de los criterios de seguridad, normalización y conservación de las aplicaciones cuyo resultado se use por los órganos y entidades de la AGE para el ejercicio de las potestades que tienen atribuidas. Los criterios a considerar son:

- Criterios de seguridad: requisitos, criterios y recomendaciones para implantar las medidas de seguridad organizativas y técnicas en el diseño, desarrollo, implantación y explotación de las aplicaciones para ejercicio de potestades.

- Criterios de normalización: pautas para normalizar dichas aplicaciones y facilitar así la compatibilidad técnica, disponibilidad, interoperabilidad y conformidad con las normas nacionales e internacionales.

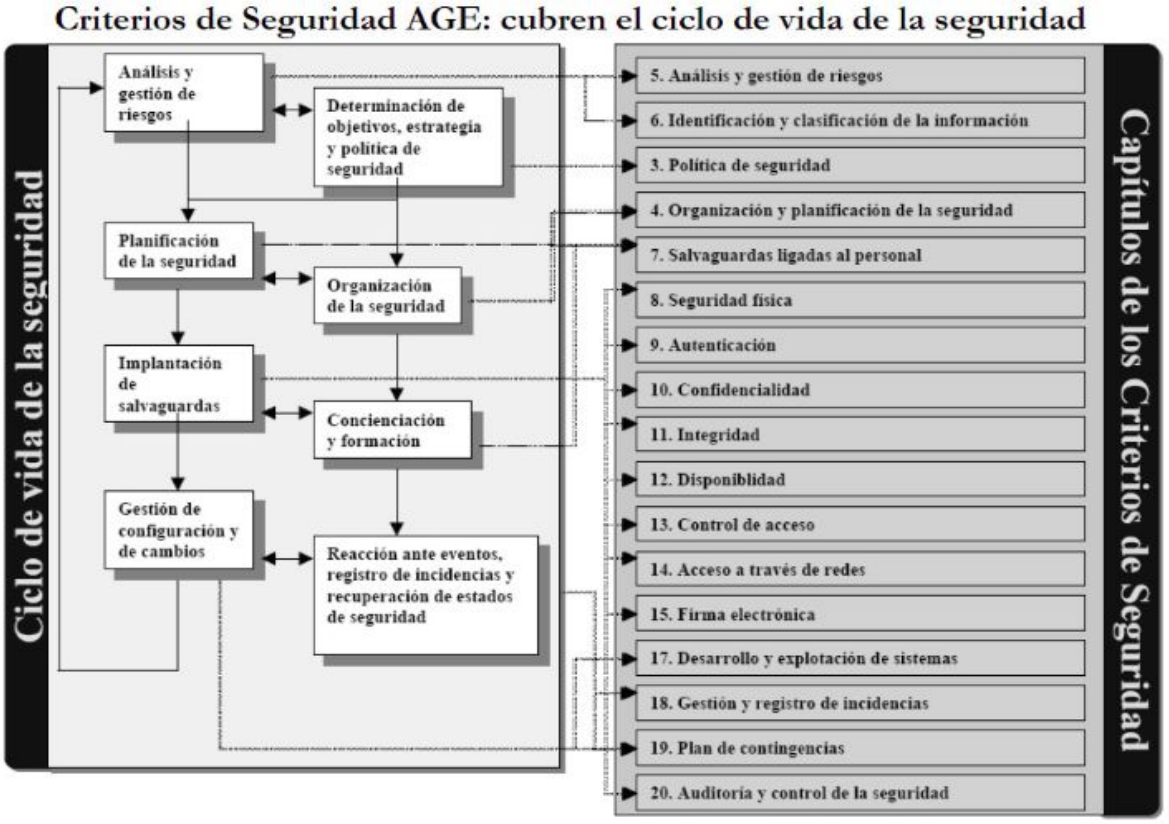
- Criterios de conservación: requisitos, criterios y recomendaciones para la conservación de la información en soporte electrónico en dichas aplicaciones.



Criterios de seguridad AGE: cubren el ciclo de vida de la seguridad.

Gestión global de la seguridad de la información	Integridad
Política de seguridad	Disponibilidad
Organización y planificación de la seguridad	Control de acceso
Análisis y gestión de riesgos	Acceso a través de redes
Identificación y clasificación de activos a proteger	Firma electrónica
Aspectos de seguridad ligados al personal	Protección de soportes de información y copias de respaldo
Seguridad física	Desarrollo y explotación de sistemas
Autenticación	Gestión y registro de incidencias

Confidencialidad	Plan de contingencias
	Auditoría y control de seguridad

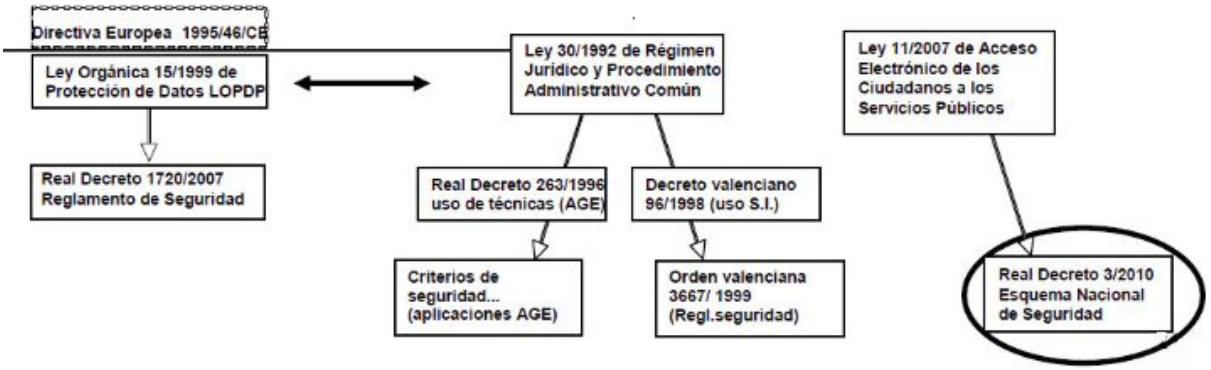


Salvaguardas adicionales mínimas

El nivel 1 de los sistemas de seguridad de los sistemas de información y de su proceso de gestión en las Administraciones Públicas se obtiene por el cumplimiento obligatorio de la legislación vigente, según dos ramas relacionadas pero distintas:

La rama de la intimidad (LOPD y RD 1720/2007), aplicable a todos los sctores públicos y privados.

La rama de la validez de documentos y aplicaciones de las Administraciones Públicas (LRJPAC 30/1992), aplicable solo a éstas y dividida por su aplicación en la Administración General del Estado (RD 263/1996, Criterios de seguridad) o en una Administración Autonómica (por ejemplo D 96/1998 Orden 367/1999 en la autonomía de Valencia)



Esquema Nacional de Seguridad

El Real Decreto 3/2010, de ocho de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica regula el citado esquema previsto en el artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Su objetivo es 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.

La finalidad del Esquema Nacional de Seguridad es:

- Crear las condiciones necesarias para la confianza en el uso de los medios electrónicos.

- Establecer medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

- Permitir el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Respecto a los principios básicos de seguridad, el objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información.

En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- Seguridad integral
- Gestión de riesgos

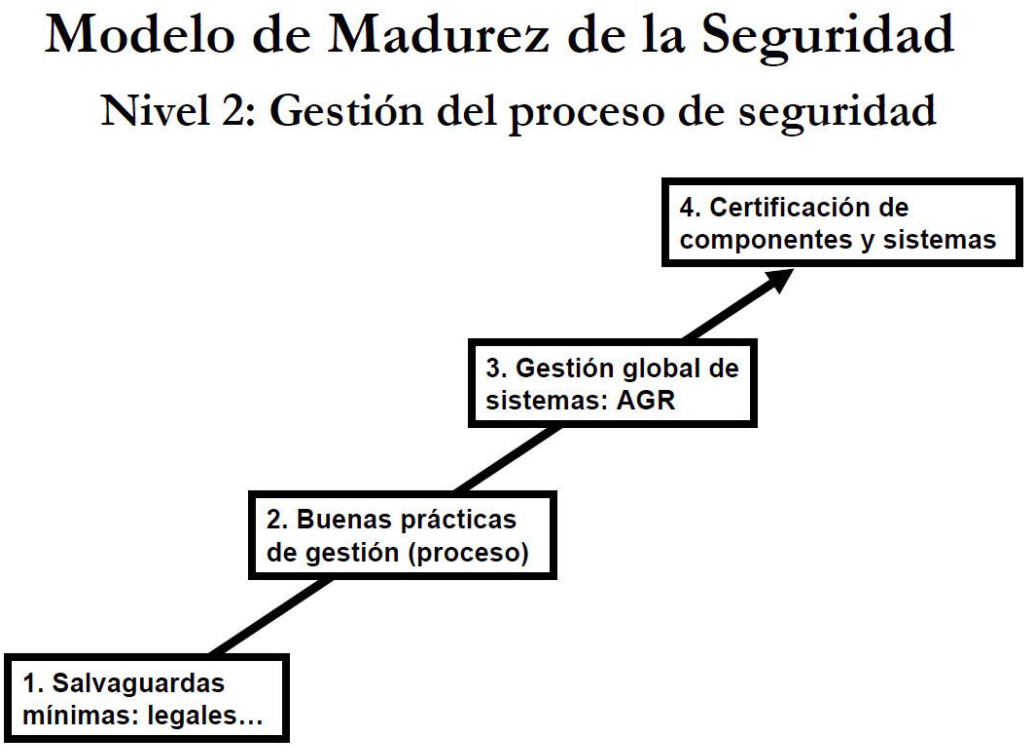
- Prevención, reacción y recuperación
- Líneas de defensa
- Reevaluación periódica
- Función diferenciada

Las Medidas de Seguridad en el Esquema Nacional de Seguridad, se clasifican en:

- Medidas Organizativas: Política de Seguridad, Normativas, Procedimientos de Seguridad, Procesos de autorizaciones…
- Medidas Operacionales: Análisis de Seguridad, Arquitectura de seguridad, adquisición de componentes, inventario de activos…
- Medidas de Protección sobre los Activos: gestión de personal, soportes de información, …

Las categorías de la seguridad en el Esquema Nacional de Seguridad son: bajo, medio o alto, de acuerdo al impacto de un posible incidente en cada una de las dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad).

5. Nivel 2: Gestión del proceso de seguridad



Buenas prácticas de gestión de seguridad

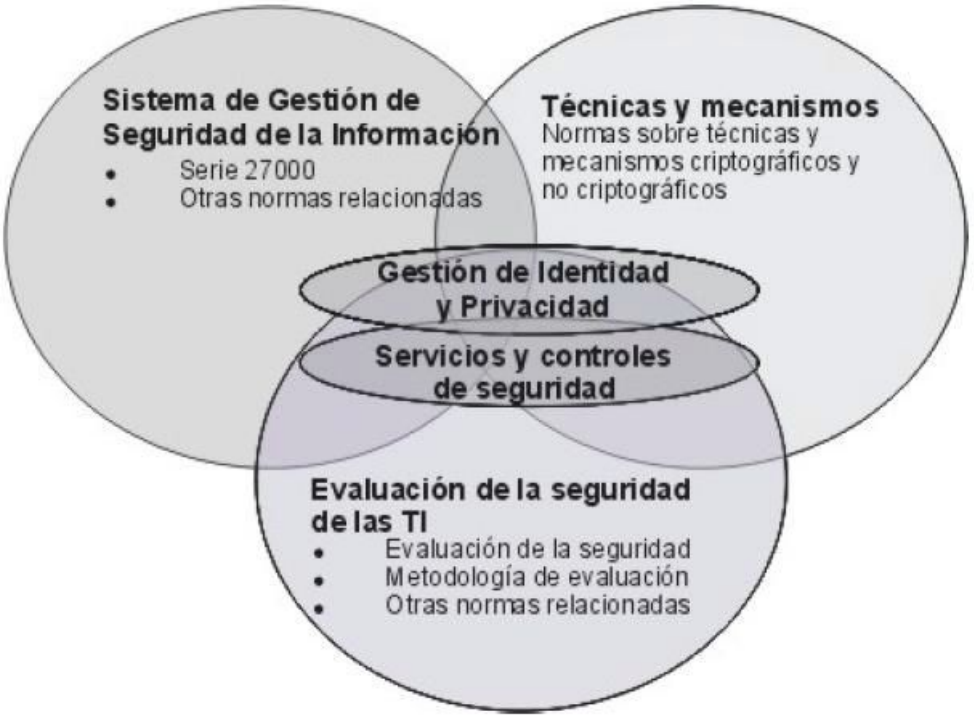
Las normas estándares internacionales y nacionales son la referencia para evaluar y alcanzar un grado 2 de certificación de procesos de una entidad. Estas normas son **especificaciones técnicas, de carácter voluntario, consensuadas, elaboradas con la participación de las partes interesadas** (fabricantes, usuarios y consumidores, laboratorios, administración, centros de investigación, etc.) y **aprobadas por un organismo reconocido**. Sus características principales son:

- Tienen el carácter de acuerdos documentados
- Contienen las especificaciones técnicas o criterios precisos
- Contribuye a simplificar y a incrementar la fiabilidad y eficiencia de los bienes y servicios
- Son documentos de aplicación voluntaria, elaborados por las partes interesadas, por consenso y aprobados por un organismo reconocido.

Organismos de normalización

- Ámbito internacional:
    - ISO (Organización Internacional de Normalización)
    - Órganos de trabajo técnicos de ISO:
        - Comités Técnicos (CT)
        - Subcomités (SC)
        - Grupos de Trabajo (GT)
    - IEC (Comisión Electrotécnica Internacional)
- Ámbito europeo:
    - CEN (Comité Europeo de Normalización). Emite principalmente:
        - Normas europeas (EN, European Standards),
        - Especificaciones técnicas (TS, Technical Specifications)
        - Informes técnicos (TR, Technical Reports).
    - En 1997 se creó CEN/ISSS (Comité Europeen de Normalisation / Information Society Standardization System) para centralizar las actividades de normalización europea en materia de tecnologías de la información y las comunicaciones
- Ámbito nacional:

- AENOR, Asociación Española de Normalización y Certificación es el comité miembro que representa los intereses españoles en el campo de la normalización y quien distribuye los productos de ISO/IEC, CEN/CENELEC, así como las normas UNE.
- De la normalización en materia de seguridad de las tecnologías de la información se ocupan:
  - En el ámbito internacional de ISO/IEC el subcomité ISO/IEC JTC 1/SC 27
  - En el ámbito europeo de CEN el órgano CEN/ISSS
  - En el ámbito nacional de AENOR el subcomité espejo AEN/CTN 71/SC 27



Panorámica general de ámbitos de normalización en ISO/IEC SC27

Normas de gestión de seguridad de la información

En 2004 se crea la serie 27000, con los objetivos de:

- Contribuir a la mejor identificación y ordenación de las normas de gestión de seguridad de la información.

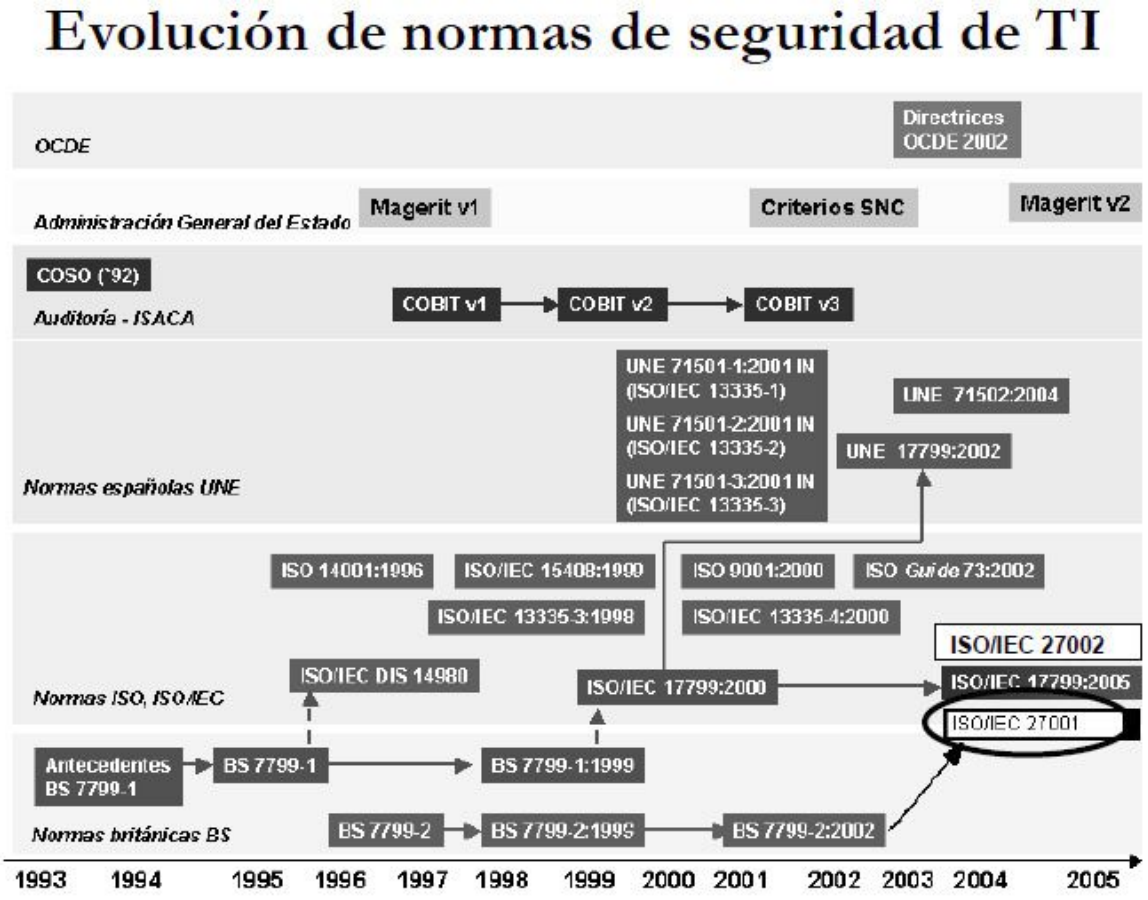
- Proporcionar un marco homogéneo de normas y directrices.

- Proporcionar requisitos, metodologías y técnicas de valoración.
- Evitar el solapamiento de las normas y favorecer la armonización.
- Alinearse con los principios generalmente aceptados relativos al gobierno de las organizaciones.
- Ser consistente con las Directrices de Seguridad de la OCDE.
- Usar lenguaje y métodos comunes.
- Facilitar la flexibilidad en la selección e implantación de controles.
- Ser consistente con otras normas y directivas de ISO.

Ampliación de información en:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306www.iso27000.es

Antecedentes de las normas de seguridad de TI

- En 1995 el British Standard Institute publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.
- En 1998, también el BSI publica la norma BS77992, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.
- Tras una revisión de ambas partes de BS7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799.
- En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS77992.
- En 2005 se revisa la norma ISO/IEC 17799: 2005 a la que se debe adaptar la UNE 17799: 2002
- En enero de 2006 se convierte la ISO BS7799-2: 2002 en la norma ISO 27001 y desde 2008 está disponible la ISO 27002 idéntica a la ISO/IEC 17799: 2005.
- Sistemas de Gestión de la Seguridad de la Información: Normativas de la serie ISO/IEC 27k.



Norma ISO/IEC 27001

- Norma principal de la serie ISO/IEC 27k
- Contiene los requisitos del sistema de gestión de seguridad de la información
- Tiene su origen en la BS 7799-2:2002
- Es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones
- En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002 para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI

- A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados

Norma ISO/IEC 27001

Define sistema de gestión de seguridad de la información como: “parte del sistema global de gestión, que sobre la base de un enfoque basado en los riesgos, se ocupa de establecer, implantar, operar, seguir, revisar, mantener y mejorar la seguridad de la información”.

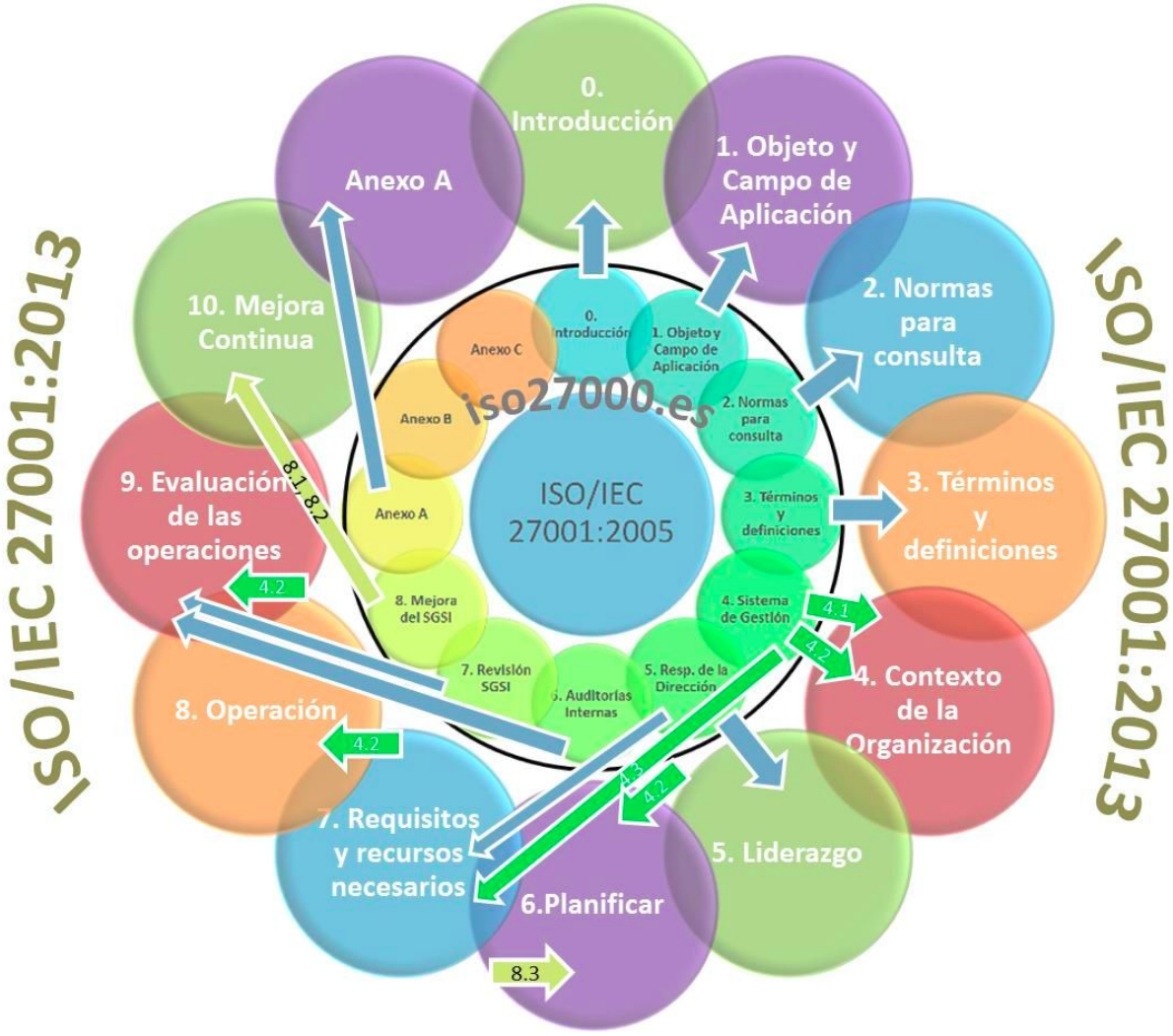
Nota: El sistema de gestión incluye estructuras organizativas, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.”

La implantación de un SGSI permite a una organización:

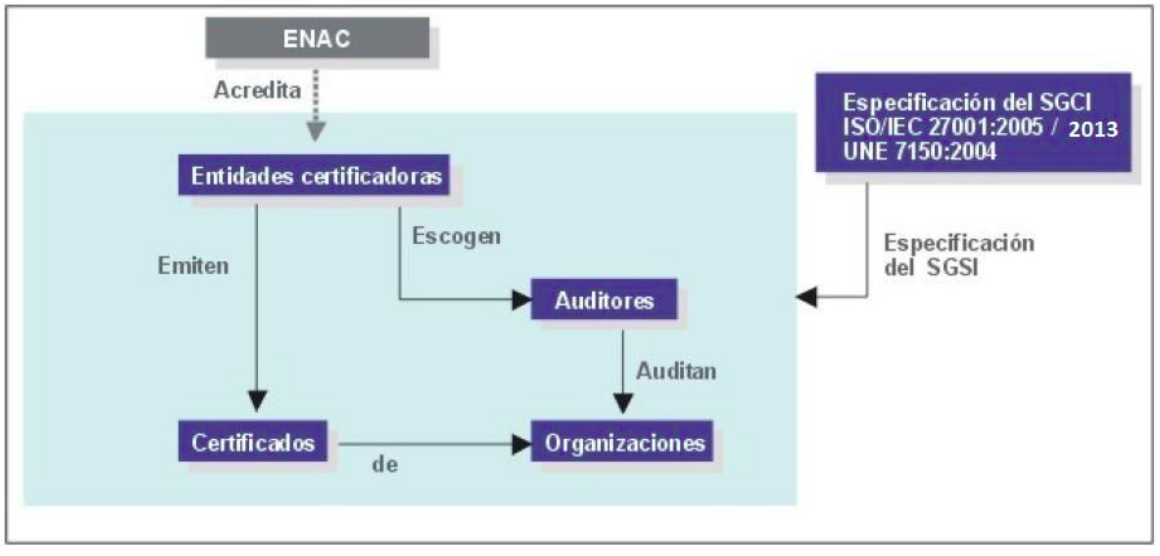
- Conocer los riesgos.

- Prevenir, reducir, eliminar o controlar los riesgos mediante la adopción de los controles adecuados.

- Asegurar el cumplimiento de la legislación en materias tales como la protección de los datos de carácter personal, los servicios de la sociedad de la información o la propiedad intelectual, entre otras.



- Cumplimiento de las normas de “buenas prácticas” Implementación efectiva de un entorno controlado y en proceso de mejora continua



- Existencia, uso y conocimiento de Políticas, Normas, Procedimientos e Instrucciones

- operativas relacionadas con la Seguridad de la Información

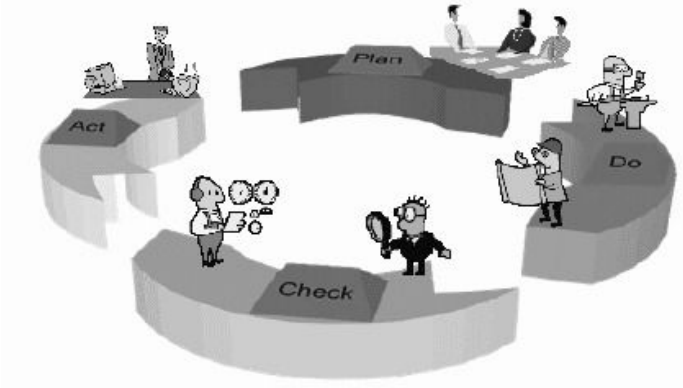
- Concienciación global corporativa sobre la Seguridad de la Información y los sistemas donde ésta reside y/o se procesa

- Implicación de la Alta Dirección de la Organización respecto a la importancia de los Sistemas de Información

Nivel 2: Gestión del proceso de seguridad

Norma ISO/IEC 27001

- Se basa en el ciclo de Demming PDCA (Plan/Do/Check/Act) aplicado en los Sistemas de gestión de la calidad ISO 900x



- ***Plan (planificar):*** establecer el SGSI
- ***Do (hacer):*** implementar y utilizar el SGSI
- ***Check (verificar):*** monitorizar y revisar el SGSI
- ***Act (actuar):*** mantener y mejorar el SGSI

Norma ISO/IEC 27002

Desde el uno de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Sus características más destacadas son:

- Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

- No es certificable.

- Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

- La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 desde el 9 de Diciembre de 2009 (a la venta en AENOR). Otros países donde también está publicada en español son, por ejemplo, Colombia (NTC-ISO-IEC 27002), Venezuela (Fondonorma ISO/IEC 27002), Argentina (IRAM-ISO-IEC 27002), Chile (NCh-ISO27002), Uruguay (UNIT-ISO/IEC 27002) o Perú (como ISO 17799; descarga gratuita)

- El original en inglés y su traducción al francés pueden adquirirse en iso.org.

- Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013. (Fuente: http://www.iso27000.es/iso27000.html#seccion2)

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la informac.
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

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

10. CIFRADO.
10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.
13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.
14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.
18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

La aplicación práctica de la norma UNE ISO/IEC 27002, concede destaca los siguientes aspectos:

- La adopción de los controles proporcionados a los riesgos detectados.
- La documentación de las políticas, los procedimientos y los controles.
- La identificación de las responsabilidades al nivel adecuado.
- La presencia de un control formalizado, en términos de formalización del control y de su periodicidad.
- La generación y conservación de evidencias.
- El tratamiento de los incidentes de seguridad.

En particular, ISO/IEC 27002 otorga al análisis y gestión de riesgos el papel clave para la identificación de los requisitos de seguridad, cuestión esencial, y para la identificación y selección de los controles y sobre su aplicación, en términos de su formalización y su periodicidad, en el marco del principio de proporcionalidad, que relaciona el valor de los activos y los riesgos a los que están expuestos, junto con el estado de la tecnología y los costes de la posible materialización de los riesgos, así como de los controles que los contrarrestan; todo ello de acuerdo con la idea básica de que la seguridad es más barata si se incorpora, cuanto antes, en las fases de análisis y de diseño de los sistemas.

Controles esenciales de la Norma ISO/IEC 27002:

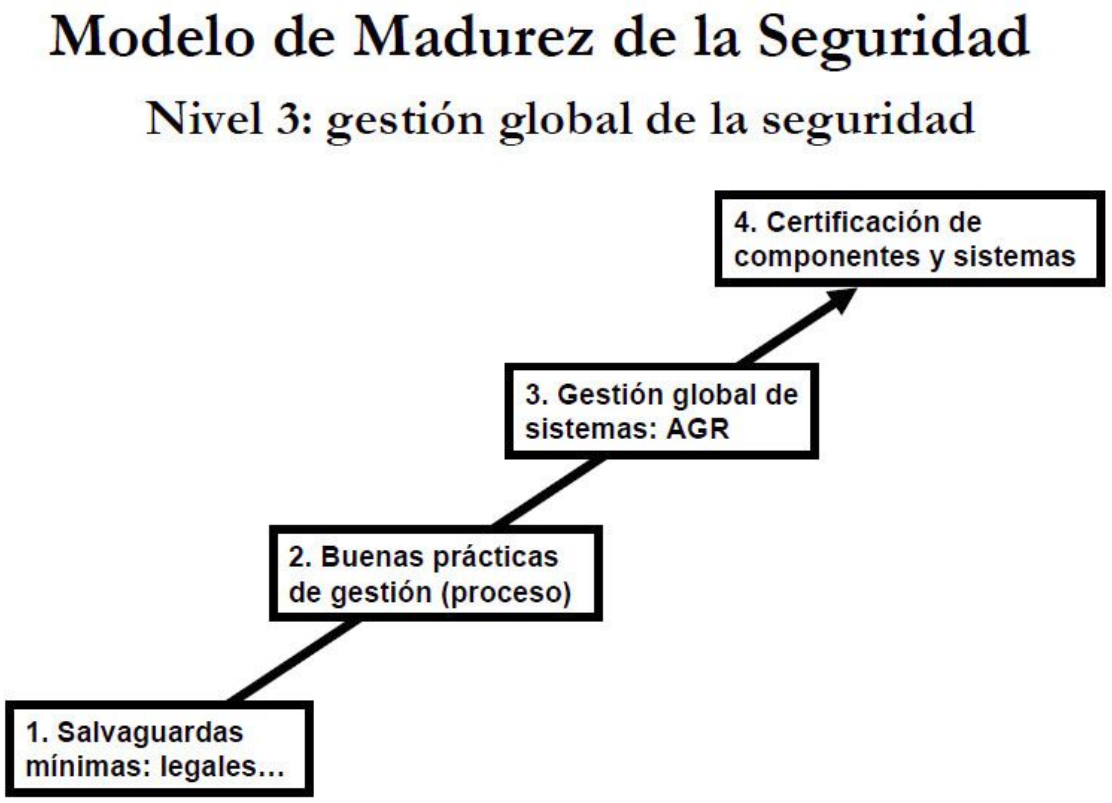
a) la protección de los datos de carácter personal y la intimidad de las personas
b) la salvaguarda de los registros de la organización
c) la documentación de la política de seguridad de la información
d) la asignación de responsabilidades de seguridad de la información
e) la formación y capacitación para la seguridad de la información
f) el procesamiento correcto de las aplicaciones
g) la gestión de la vulnerabilidad
h) la gestión de la continuidad del negocio
i) la gestión de las incidencias de la seguridad de la información y sus mejoras

Certificación, aspectos destacados:

• El proceso general de certificación consta de dos grandes etapas: consultoría y auditoría.

• En la primera de ellas, un equipo de consultores con experiencia en la norma ayuda a la organización a cumplir los requisitos de certificación: política de seguridad, procedimientos, controles…
• Cuando la organización – asesorada por los consultores – considera que cumple los requisitos de la norma, solicita la certificación a un organismo acreditado, como AENOR, que será el encargado de realizar la auditoría.

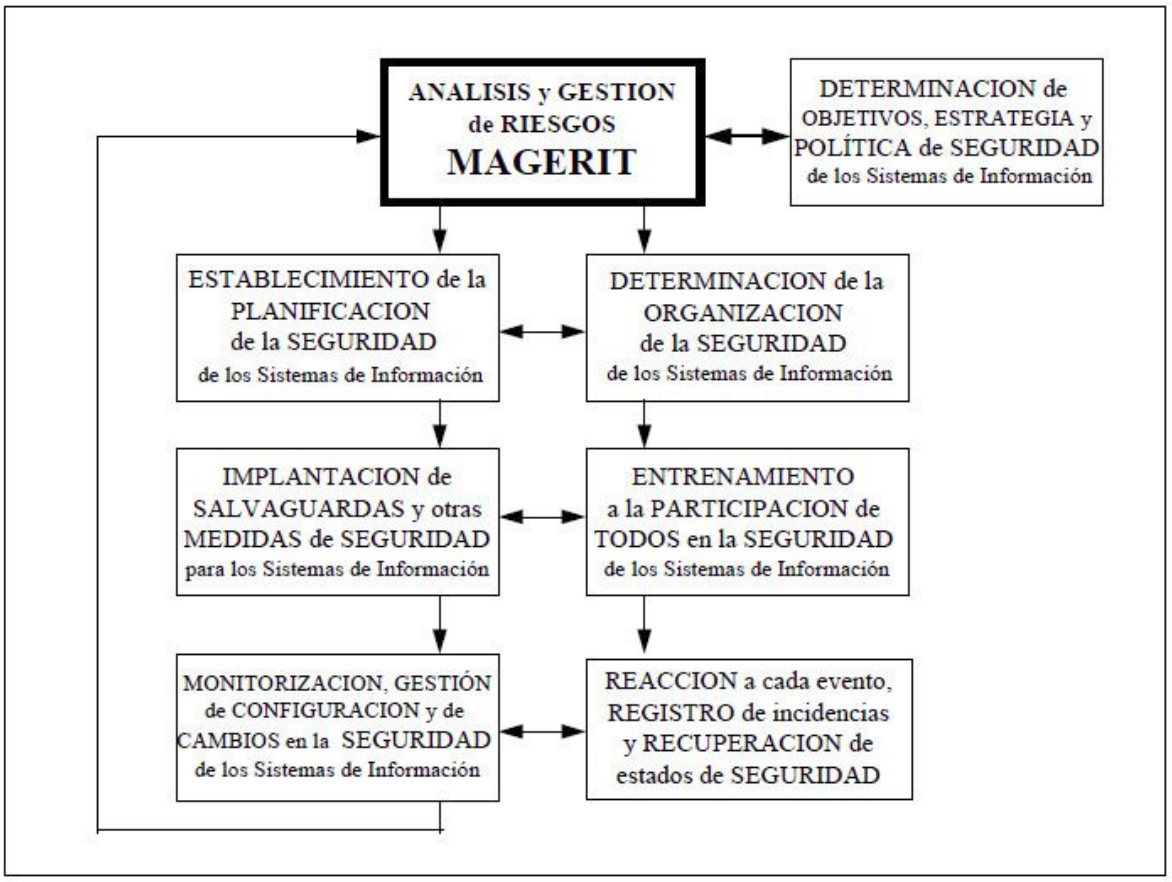
6. Nivel 3: Gestión global de la seguridad



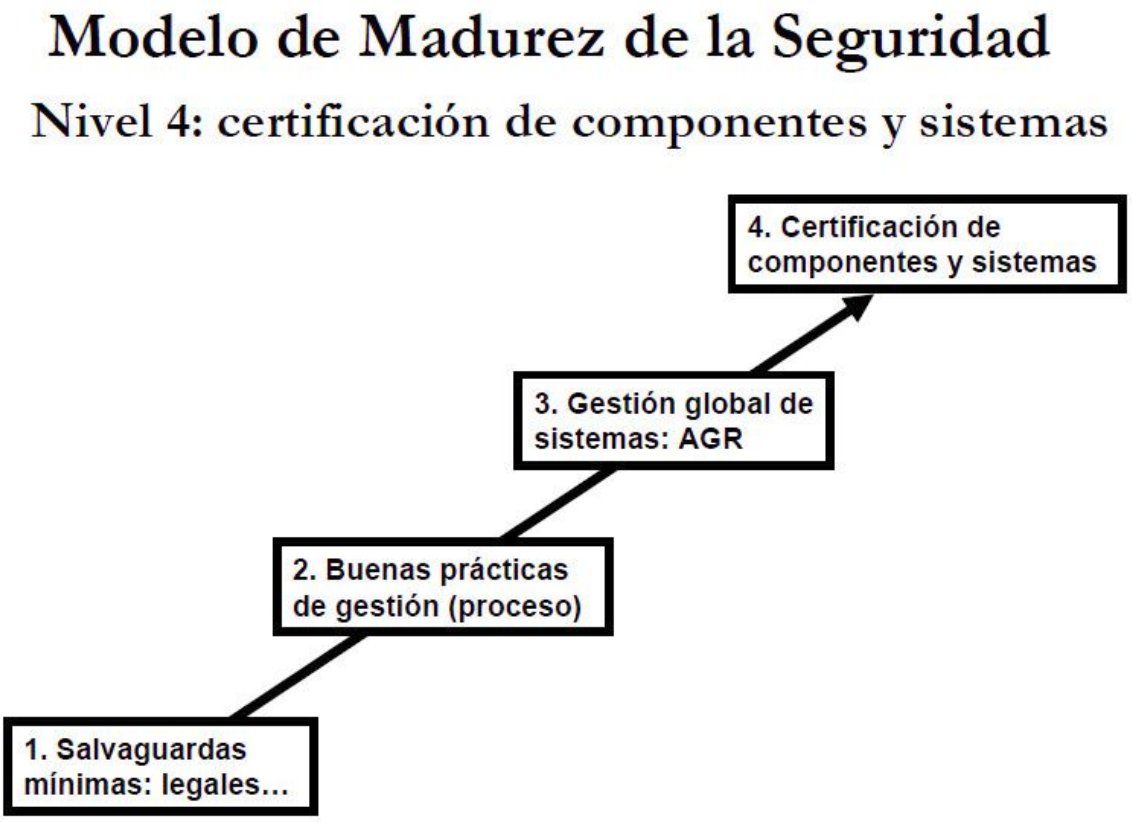
- El cumplimiento del Nivel 2 apoyado en los estándares y referencias normativas (con certificación o sin ella), sustituye con ventaja a las salvaguardas mínimas legales y el uso de Guías de buenas prácticas de Seguridad Informática.

- La gestión de la seguridad en Organizaciones más problemáticas requiere un nivel o escalón 3 de medidas más complejas.

- Se suele requerir la consulta a especialistas de seguridad y un proyecto detallado de Análisis y Gestión de Riesgos para establecer hasta dónde las salvaguardas son necesarias y rentables y para determinar la forma de implementarlas.


ANALISIS y GESTION de RIESGOS MAGERIT
DETERMINACION de OBJETIVOS, ESTRATEGIA y POLÍTICA de SEGURIDAD de los Sistemas de Información
ESTABLECIMIENTO de la PLANIFICACION de la SEGURIDAD de los Sistemas de Información
DETERMINACION de la ORGANIZACION de la SEGURIDAD de los Sistemas de Información
IMPLANTACION de SALVAGUARDAS y otras MEDIDAS de SEGURIDAD para los Sistemas de Información
ENTRENAMIENTO a la PARTICIPACION de TODOS en la SEGURIDAD de los Sistemas de Información
MONITORIZACION, GESTIÓN de CONFIGURACION y de CAMBIOS en la SEGURIDAD de los Sistemas de Información
REACCION a cada evento, REGISTRO de incidencias y RECUPERACION de estados de SEGURIDAD

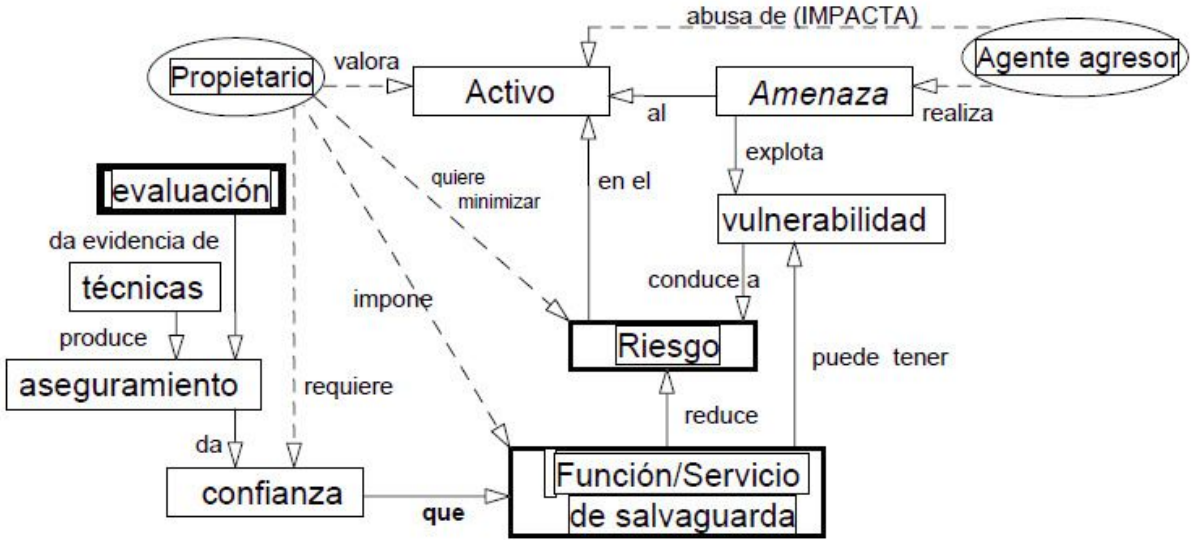
7. Nivel 4: Certificación de componentes y de sistemas



Nivel 4: Certificación de componentes

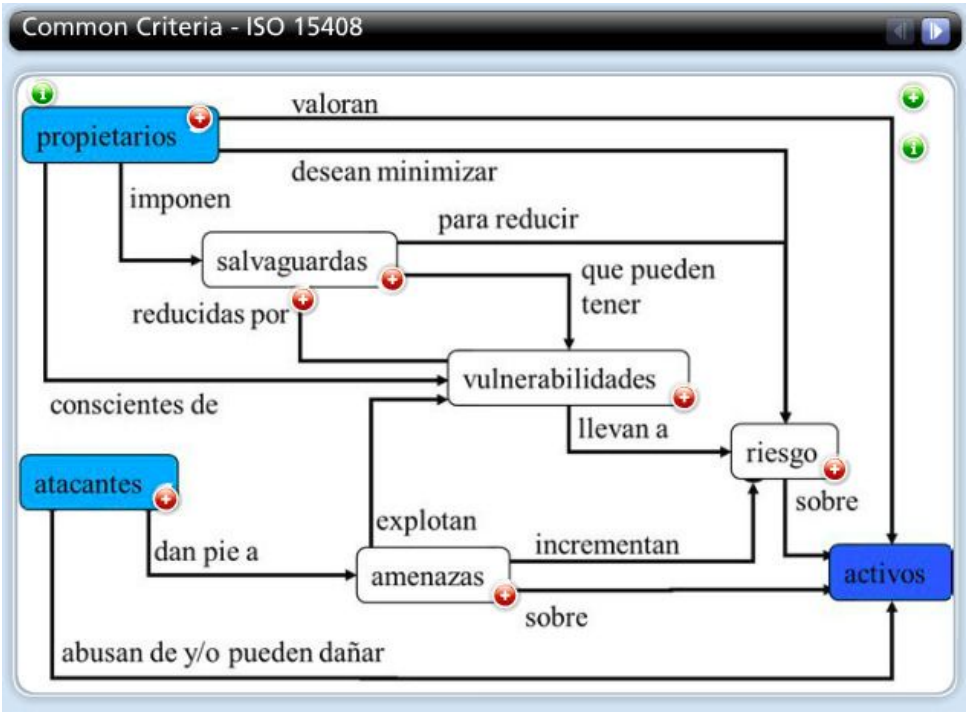
- **ISO/IEC 15408 – Criterios comunes** para evaluación de la seguridad de las tecnologías de la información.

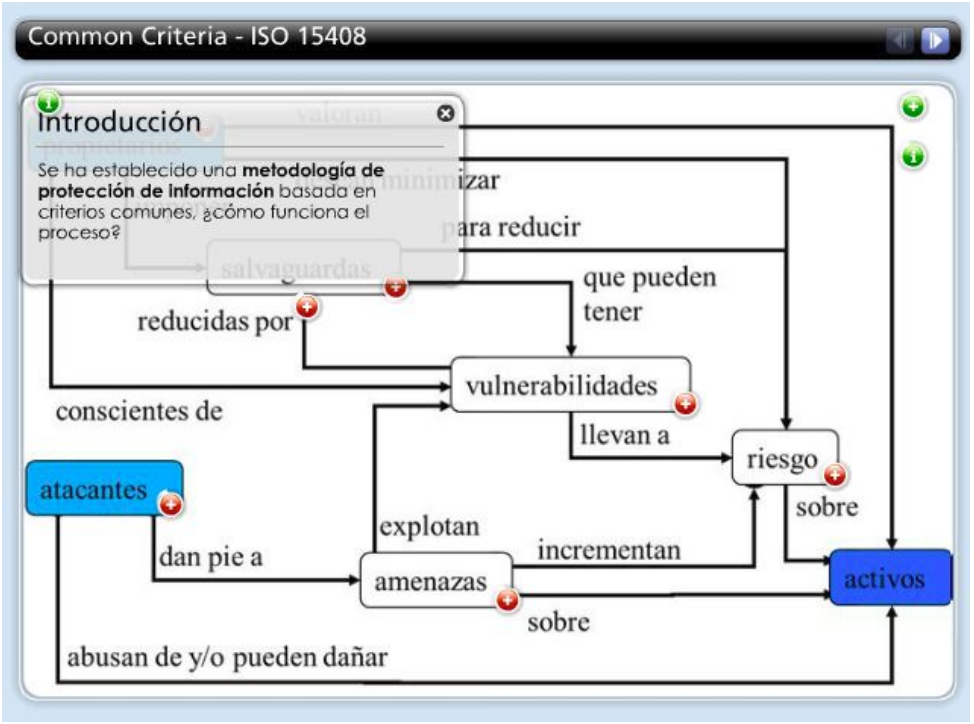
CC se apoyan en este modelo de conceptos y relaciones de seguridad y evaluación (que amplia el modelo MAGERIT)

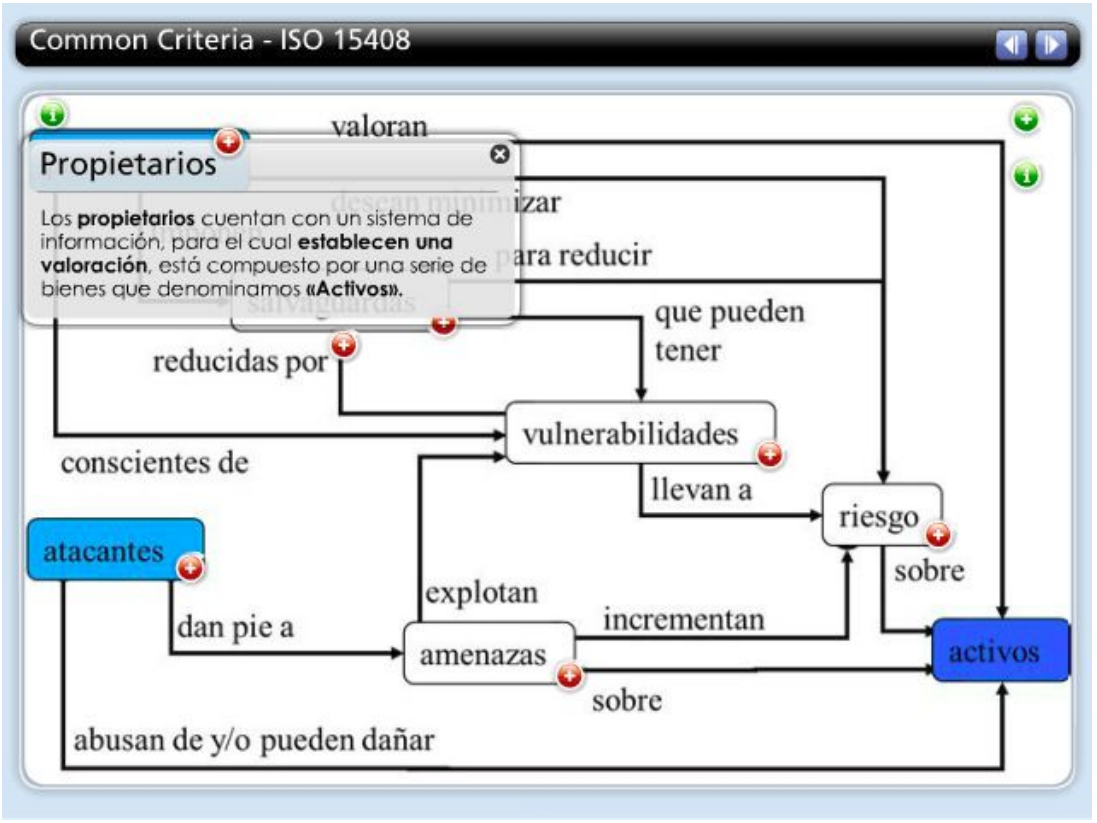


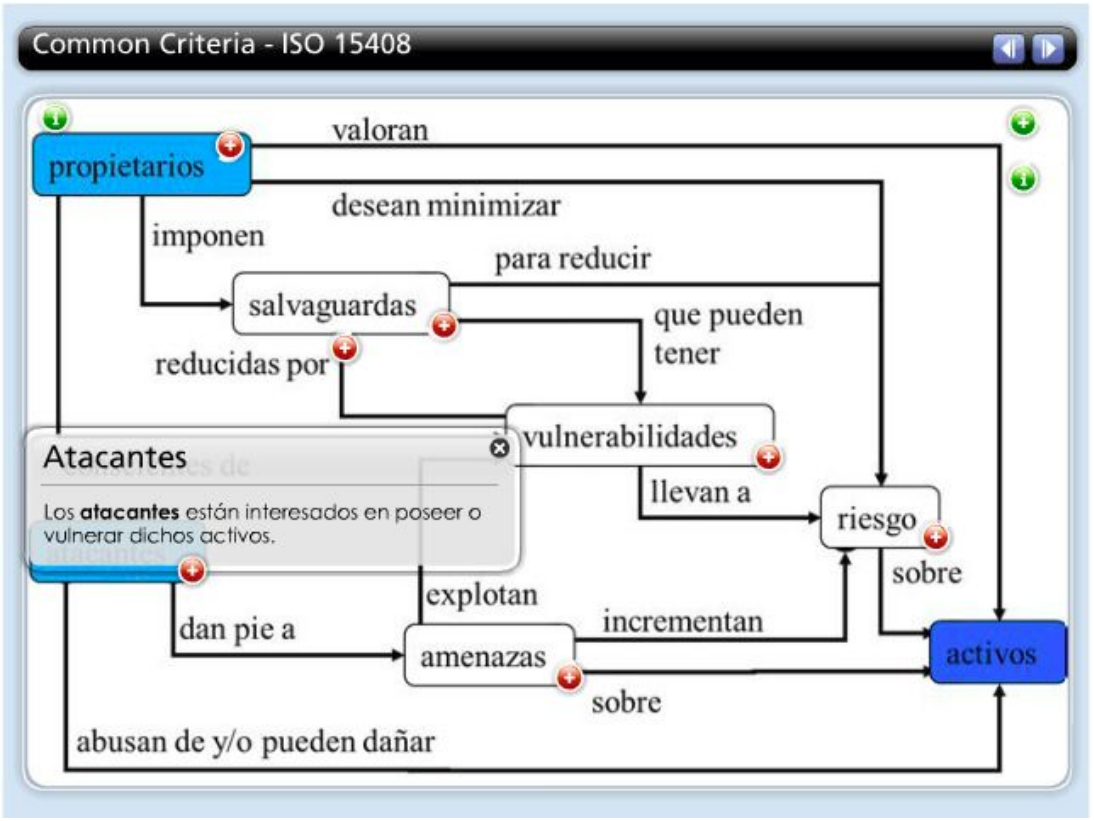
Criterios comunes:

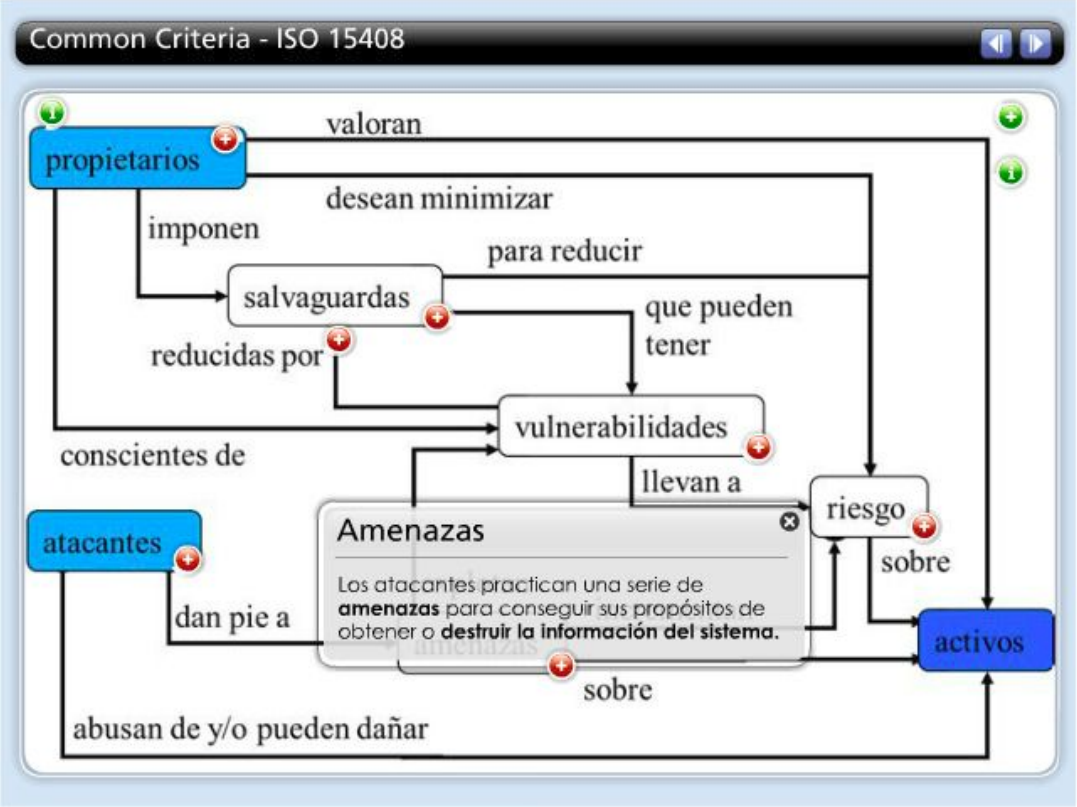
- Definir las funciones de seguridad de los productos y sistemas.
- Determinar los criterios para evaluar (la calidad) de dichas funciones.
- Dentro de ISO 15408-1 se detalla el proceso que se sigue desde que se identifica la necesidad de desarrollo/adquisición de software hasta que se obtiene un conjunto de requisitos tanto funcionales, como de seguridad y finalmente de entorno.

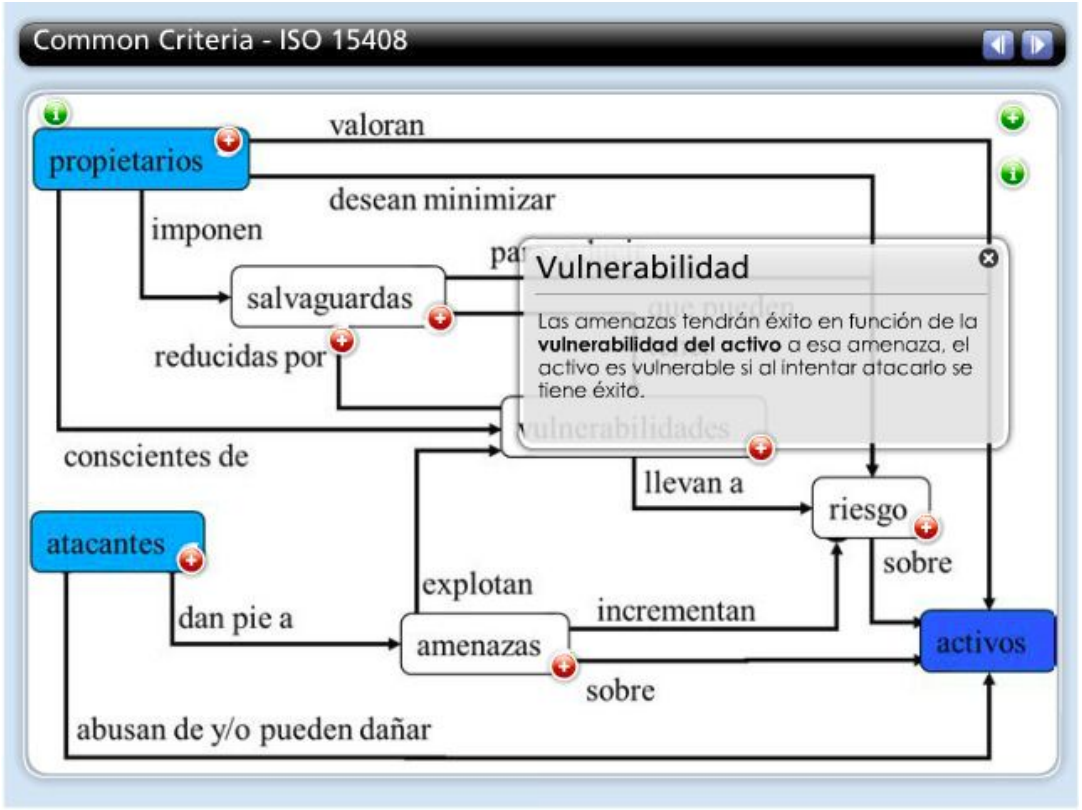

Common Criteria - ISO 15408
propietarios
valoran
desean minimizar
imponen
para reducir
salvaguardas
que pueden
tener
reducidas por
vulnerabilidades
conscientes de
llevan a
riesgo
atacantes
sobre
explotan
dan pie a
incrementan
amenazas
activos
sobre
abusan de y/o pueden dañar

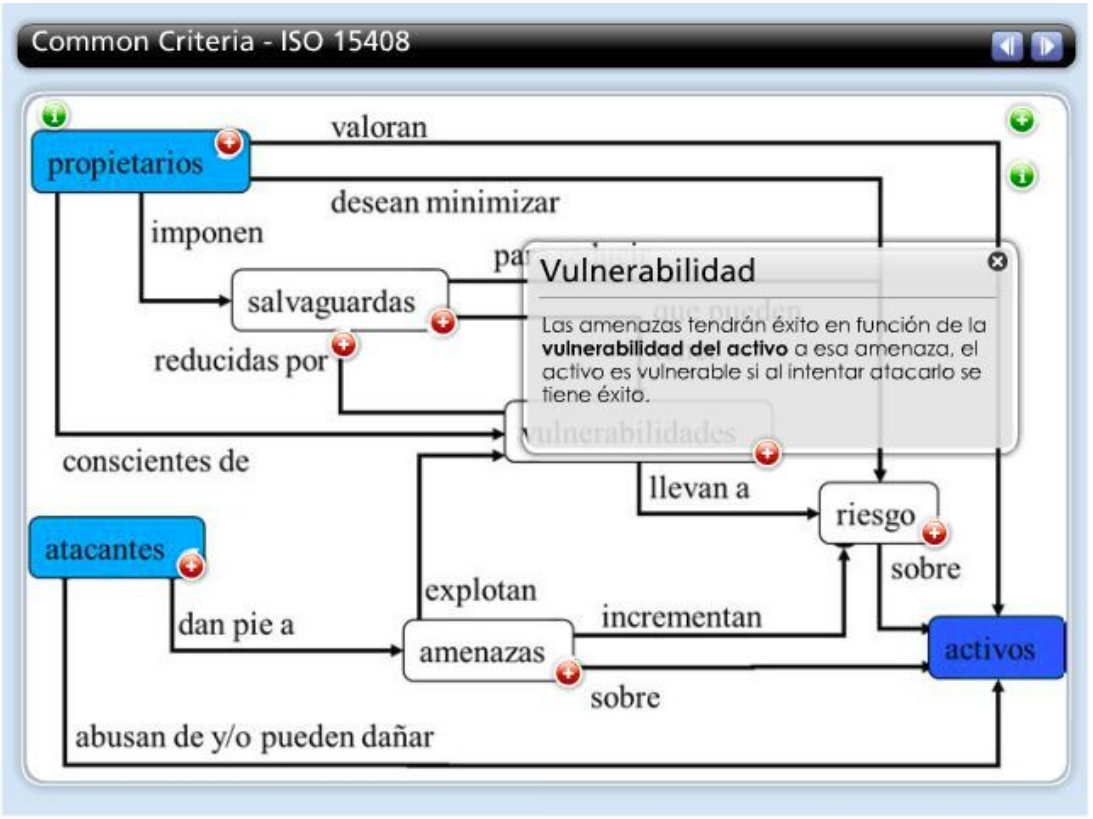

Common Criteria - ISO 15408
Introducción
Se ha establecido una metodología de protección de información basada en criterios comunes, ¿cómo funciona el proceso?
reducidas por
que pueden
tener
vulnerabilidades
conscientes de
llevan a
riesgo
atacantes
sobre
explotan
dan pie a
incrementan
amenazas
activos
sobre
abusan de y/o pueden dañar

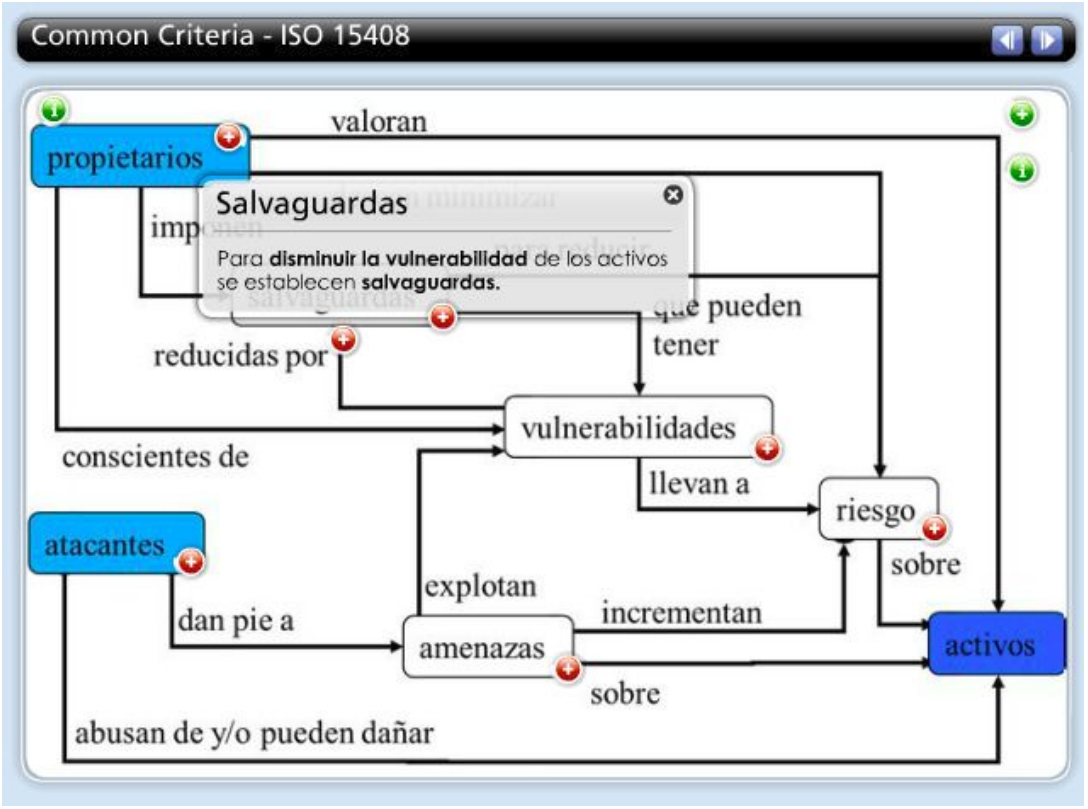

Common Criteria - ISO 15408
Propietarios
Los propietarios cuentan con un sistema de información, para el cual establecen una valoración, está compuesto por una serie de bienes que denominamos «Activos».
valoran
izar
ara reducir
que pueden
tener
reducidas por
vulnerabilidades
conscientes de
llevan a
riesgo
sobre
atacantes
explotan
dan pie a
incrementan
amenazas
activos
sobre
abusan de y/o pueden dañar

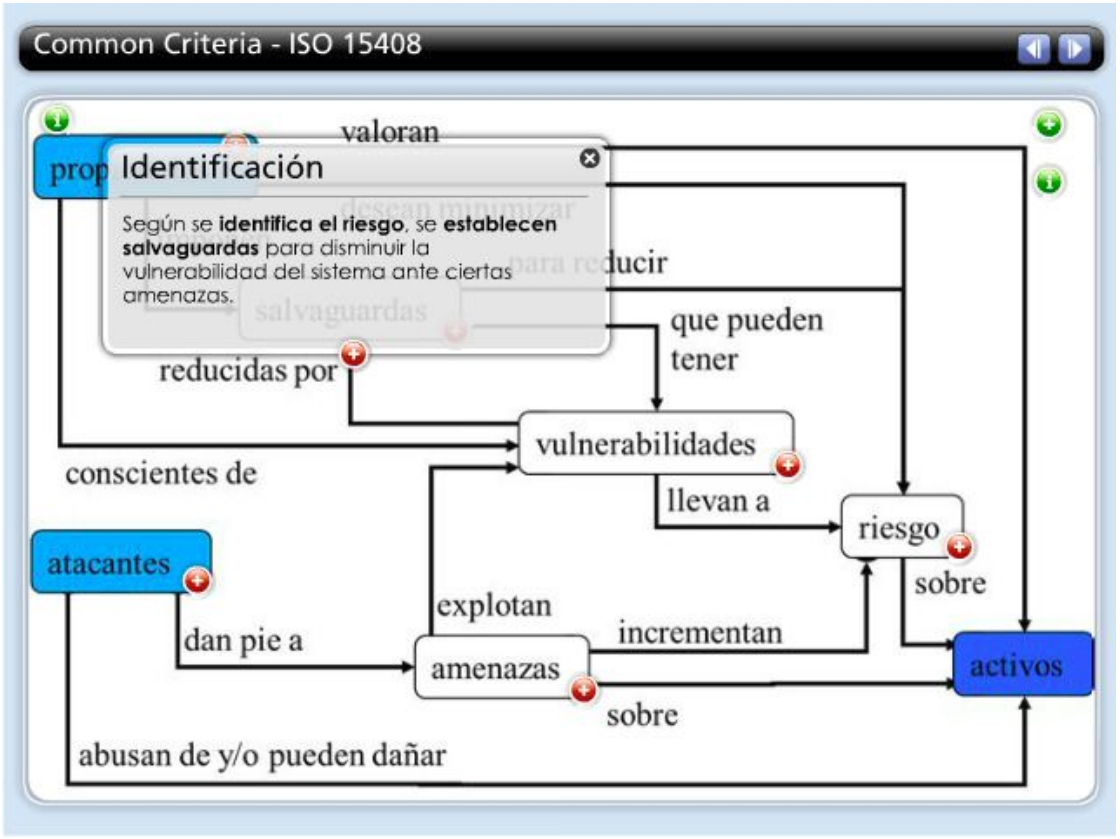

Common Criteria - ISO 15408
propietarios
valoran
desean minimizar
imponen
para reducir
salvaguardas
que pueden
tener
reducidas por
vulnerabilidades
Atacantes
Los atacantes están interesados en poseer o vulnerar dichos activos.
llevan a
riesgo
sobre
explotan
dan pie a
incrementan
amenazas
activos
sobre
abusan de y/o pueden dañar

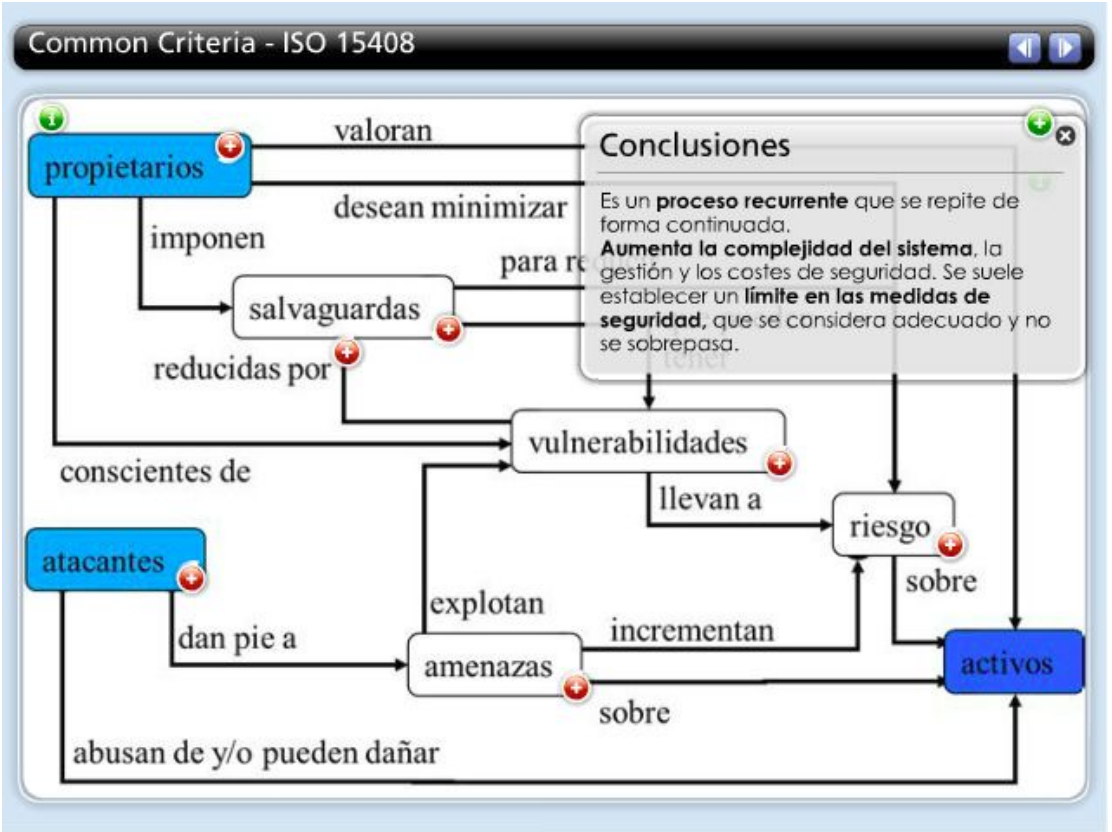

Common Criteria - ISO 15408
propietarios
valoran
desean minimizar
imponen
para reducir
salvaguardas
que pueden
tener
reducidas por
vulnerabilidades
conscientes de
llevan a
riesgo
sobre
atacantes
Amenazas
Los atacantes practican una serie de amenazas para conseguir sus propósitos de obtener o destruir la información del sistema.
dan pie a
activos
sobre
abusan de y/o pueden dañar

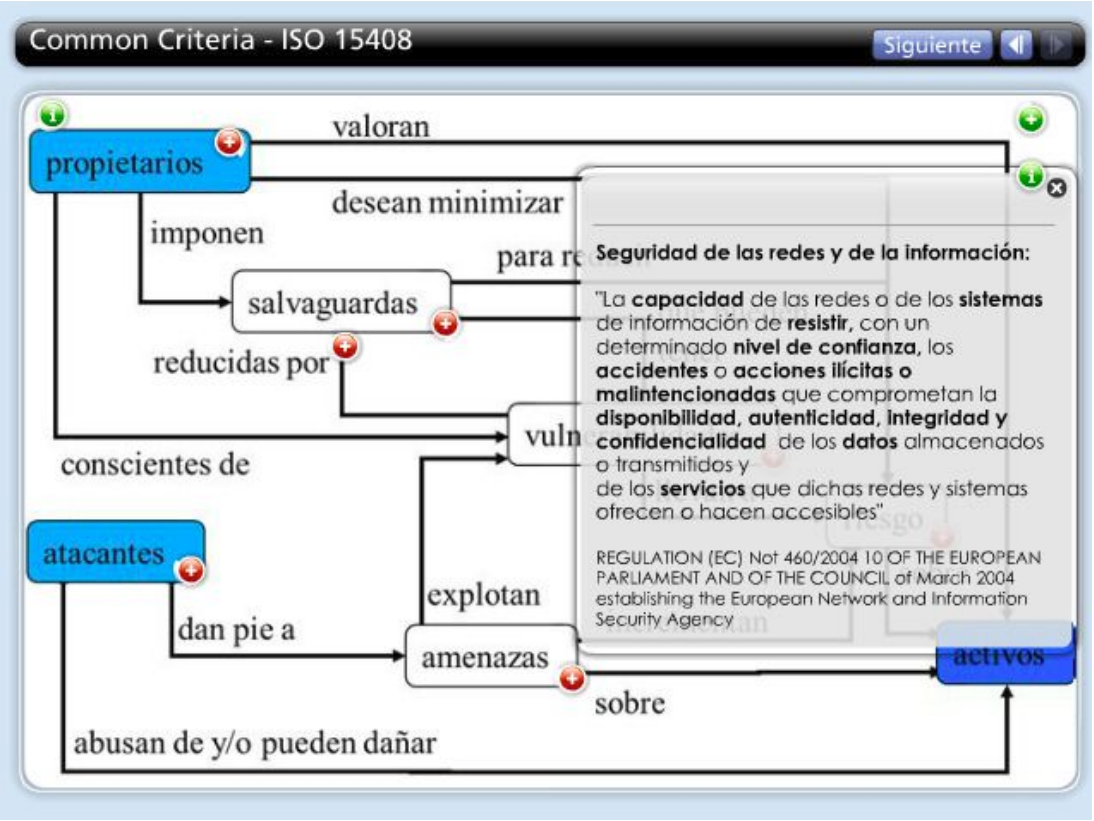

Common Criteria - ISO 15408
propietarios
valoran
desean minimizar
imponen
Vulnerabilidad
Las amenazas tendrán éxito en función de la vulnerabilidad del activo a esa amenaza, el activo es vulnerable si al intentar atacarlo se tiene éxito.
salvaguardas
reducidas por
conscientes de
llevan a
riesgo
sobre
atacantes
explotan
incrementan
dan pie a
amenazas
activos
sobre
abusan de y/o pueden dañar


Common Criteria - ISO 15408
propietarios
valoran
desean minimizar
imponen
salvaguardas
reducidas por
Vulnerabilidad
Las amenazas tendrán éxito en función de la vulnerabilidad del activo a esa amenaza, el activo es vulnerable si al intentar atacarlo se tiene éxito.
conscientes de
llevan a
riesgo
sobre
atacantes
explotan
dan pie a
incrementan
amenazas
activos
sobre
abusan de y/o pueden dañar


Common Criteria - ISO 15408
propietarios
valoran
Salvaguardas
Para disminuir la vulnerabilidad de los activos se establecen salvaguardas.
reducidas por
que pueden
tener
vulnerabilidades
conscientes de
llevan a
riesgo
sobre
atacantes
explotan
dan pie a
incrementan
amenazas
activos
sobre
abusan de y/o pueden dañar


Common Criteria - ISO 15408
valoran
Identificación
Según se **identifica el riesgo**, se **establecen salvaguardas** para disminuir la vulnerabilidad del sistema ante ciertas amenazas.
que pueden tener
reducidas por
vulnerabilidades
conscientes de
llevan a
riesgo
sobre
atacantes
explotan
incrementan
dan pie a
amenazas
activos
sobre
abusan de y/o pueden dañar


Common Criteria - ISO 15408
valoran
propietarios
Conclusiones
Es un **proceso recurrente** que se repite de forma continuada.
Aumenta la complejidad del sistema, la gestión y los costes de seguridad. Se suele establecer un **límite en las medidas de seguridad**, que se considera adecuado y no se sobrepasa.
desean minimizar
imponen
salvaguardas
reducidas por
vulnerabilidades
conscientes de
llevan a
riesgo
sobre
atacantes
explotan
incrementan
dan pie a
amenazas
activos
sobre
abusan de y/o pueden dañar



Nivel 4 Certificación de componentes

'Common Criteria', Criterios Comunes para la SSI

- El Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de la Tecnología de la Información (conocido por sus siglas en inglés CCRA) especifica los requisitos que han de cumplir los Certificados de Criterios Comunes, los Organismos de Certificación y los Centros de Evaluación de la seguridad de las tecnologías de la información.

- Ratificación en mayo de 2000 – ocho países de la Unión Europea (España), Australia/Nueva Zelanda, EE.UU., Canadá del Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las TI.

- A partir del 17 de agosto de 2006, España cambia su estatus en el Arreglo y se convierte en participante acreditado para emitir certificados de seguridad de la tecnología de la información.

Certificación de un 'compuesto'

ISO/IEC 15408 – Criterios comunes para la evaluación de la seguridad de las tecnologías de la información.
• "Un sistema se diseña para satisfacer las necesidades de un grupo particular de utilizadores finales.
• Su entorno es real y puede definirse y observarse detalladamente.
• Las amenazas contra su seguridad son reales y pueden determinarse.
• Un producto debe ser apto para incorporarse a gran número de sistemas, sobre cuyo entorno el diseñador del producto susceptible de ser componente de éstos sólo puede hacer hipótesis generales.

• Quien adquiere el producto y construye el sistema es quien debe asegurarse que esas hipótesis son coherentes con el entorno real del sistema". (Fuente: ITSEC)

Reglamento Europeo de Protección de Datos

El nuevo **Reglamento Europeo de Protección de Datos**, también conocido como Reglamento General de Protección de Datos (RGPD) o General Data Protection Regulation (GDPR), supone el cambio más significativo en los últimos años, a nivel europeo en la legislación de protección de datos.

El 25 de mayo de 2016 entró en vigor, y sustituirá a la actual normativa vigente y que comenzará a aplicarse el 25 de mayo de 2018. Este período de dos años tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones y también las empresas y organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

Todas aquellas empresas que dispongan de información personal de residentes en la Unión Europea (también de Suiza y del Espacio Económico Europeo) deben adaptarse a partir del 25 de mayo de 2018 al cumplimiento de las normas de dicho reglamento. Ignorarlo o no cumplirlo correctamente, puede implicar costes importantes. Una infracción puede dar lugar a sanciones de hasta 20 millones de euros o hasta un 4 % de los ingresos globales de la empresa denunciada.

A partir del 25 de mayo, el usuario **tendrá que dar el consentimiento inequívoco para que las empresas puedan usar sus datos,** aplicable a los ciudadanos europeos. Es más, tendrán que decir qué datos están utilizando, cómo los están tratando, para qué y quién es la persona responsable de los mismos.

Los derechos

Los ciudadanos **podrán solicitar y lograr que sus datos personales sean eliminados** cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita. El derecho al olvido existe desde la sentencia del Tribunal de Justicia de la Unión Europea, pero ahora se recoge en este Reglamento.

El derecho a la portabilidad permite que los datos se están tratando de modo automatizado, se puedan **recuperar en un formato para cederlos a otro responsable**. Estos datos deben estar "en un formato estructurado, de uso común y lectura mecánica (por ejemplo un CSV de hojas de cálculo) para que puedan ser transmitidos fácilmente a otro responsable y facilitar así un cambio de proveedor.

Los tratamientos que estén basados en un consentimiento de los interesados y que se haya obtenido antes de que el GDPR sea aplicable (es decir, del 25 de mayo de 2018), si **ese consentimiento no se obtuvo de forma conforme al reglamento, el consentimiento ya no es válido.**

Respecto a los **incidente de seguridad** las empresas deberán informar en un plazo máximo de 72 horas de que han sufrido un incidente de seguridad. Y no sólo deberán dar parte a las autoridades competentes (en el caso de España, la Agencia de Protección de Datos), sino también a todos los usuarios cuyos datos se hayan podido ver comprometidos.

Aparte de los datos especialmente protegidos que ya preveía la LOPD, que ahora pasan a denominarse "categorías especiales de datos", el Reglamento incluye dos nuevas categorías especiales de datos:

- Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica.

- Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de esta persona (imágenes faciales, datos dactiloscópicos, etc.).

Qué es un Delegado de Protección de Datos

El RGPD configura una serie de "medidas de responsabilidad activa" aplicables a los responsables, y en ocasiones, también a los encargados de tratamiento. En la Guía del Reglamento General de Protección de Datos para responsables de tratamiento se analizan estas medidas distinguiendo las siguientes: análisis de riesgos, registro de actividades de tratamiento, protección de datos desde el diseño y por defecto, medidas de seguridad, notificación de "violaciones de seguridad de los datos", evaluación de impacto sobre la protección de datos, y finalmente, el delegado de protección de datos.

Esta figura, conocida popularmente como DPO (en inglés, *Data Protection Officer*), constituye uno de los elementos claves del RGPD, y es un garante del cumplimiento de la norma de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control.

Al Delegado de Protección de Datos, que deberá contar con conocimientos especializados sobre Derecho, y obviamente en protección de datos, que actuará de forma independiente, se le atribuyen una serie de funciones reguladas en el artículo 39 del RGPD, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado.

Las únicas entidades que pueden certificar en España delegados de protección de datos son aquellas que han sido acreditadas por ENAC conforme a la norma UNE-EN ISO/IEC 17024:2012 y en el ámbito de la aplicación del Esquema de Certificación de Delegados de Protección de Datos.

Herramienta de ayuda RGPD

Con la finalidad de facilitar la adecuación al RGPD a las empresas y profesionales (responsables o encargados de tratamientos) que traten datos personales de escaso riesgo para los derechos y libertades de las personas, la Agencia Española de Protección de Datos pone su disposición la herramienta Facilita_RGPD.

Facilita_RGPD es una herramienta fácil y gratuita. Una vez finalizada su ejecución, los datos aportados durante el desarrollo de la misma se eliminan, por lo que la Agencia Española de Protección de Datos en ningún caso puede conocer la información que haya sido aportada.

Ha sido diseñada como un recurso útil para cualquier empresa o profesional, ya que con tan solo tres pantallas de preguntas muy concretas permite a quien la utiliza valorar su situación respecto del tratamiento de datos personales que lleva a cabo: si se adapta a los requisitos exigidos para utilizar Facilita_RGPD o si debe realizar un análisis de riesgos.

Facilita_RGPD no podrá utilizarse para tratamientos que impliquen un alto riesgo para los derechos y libertades de las personas, como datos de salud o tratamientos masivos de datos, entre otros.

RGPD y el consentimiento de los menores de edad

El **Reglamento General de Protección de Datos (RGPD)** establece nuevas directrices con respecto al consentimiento de los menores de edad en el uso de los datos personales. Estas novedades se añaden con el objetivo de aumentar la privacidad de la información en los niños.

El tratamiento de los datos personales en el ámbito de los servicios de la sociedad de la información en menores de edad, por ejemplo por parte de las redes sociales, será legal siempre y cuando estos tengan más de 16 años. Aunque el reglamento permite rebajar esta edad y que cada estado miembro establezca una propia, siempre con el límite inferior de edad de 13 años.

En el caso de España, está fijada actualmente en 14 años, pero **con la aplicación directa del RGPD se reduce desde los 14 a los 13 años** para adaptar el sistema español al Reglamento General de Protección de Datos.

Para edades por debajo de los 13 años, se necesitará el consentimiento del "titular de la patria potestad", algo que puede resultar complicado en el entorno de internet. El **artículo 8** muestra información, aunque no describe cómo las autoridades responsables del control pueden determinar si se ha cumplido este requisito.

Según la Agencia Española de Protección de Datos (AEPD), a partir del 25 de mayo de 2018, cuando se recopilen datos personales han de tener siempre en cuenta que el consentimiento tiene que ser verificable y que el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan comprender.

Google Analytics y RGPD

Según las condiciones del servicio de Google Analytics, **a los clientes del servicio se les está prohibido enviar información personal a Google**.

Y en lo que se refiere a información personal, **Google se refiere a ella en las condiciones de Analytics como *información personal identificable***, que comprendería, entre otros, los siguientes datos:

- Nombres
- Números de la seguridad social
- DNI
- Direcciones de correo electrónico
- … ...

Google Analytics por defecto no recopila este tipo de información. En cuanto a **las direcciones IP**, que también pueden considerarse información personal identificable, y por este motivo las protege la RGPD, tampoco los informes de Google Analytics incluyen esta información, aunque pueden recopilarla.

Google ha actualizado sus condiciones del servicio **para procesamiento de datos** respecto a la RGPD.

Aceptación de política de privacidad en los comentarios de un blog

Uno de los requisitos principales de la RGPD, es obtener el consentimiento expreso y consciente de los usuarios de los datos que guardarás de ellos en tu sitio. Uno de los integrantes de un sitio, como por ejemplo un blog con Wordpress, que guarda información de los usuarios son los comentarios.

No es suficiente si dentro del menú de configuración del programa que se use para gestionar comentarios, en los ajustes se desmarca la opción de solicitar el correo electrónico y nombre. La razón es que es habitual que este tipo de programas almacene la IP del usuario.

En consecuencia es imprescindible **añadir una opción de selección en la que el usuario dé permiso explícitamente para almacenar la información que se guarde**, y **con un enlace a la política de privacidad** donde se informará de:

- Quién es el depositario de sus datos
- Qué datos se almacenan
- Con quién se comparten
- Cuánto tiempo se mantienen
- Que los datos viajarán y se almacenarán encriptados
- Dónde y cómo borrar sus datos de usuario
- Dónde y cómo solicitar sus datos

Transferencias internacionales de datos

El modelo de transferencias internacionales diseñado por el RGPD sigue los mismos criterios que el establecido por la Directiva 95/46 y por las legislaciones nacionales de trasposición. Según este modelo, los datos sólo podrán ser comunicados fuera del Espacio Económico Europeo:

- A países, territorios o sectores específicos (el RGPD incluye también organizaciones internacionales) sobre los que la Comisión haya adoptado una decisión reconociendo que ofrecen un nivel de protección adecuado.
- Cuando se hayan ofrecido garantías adecuadas sobre la protección que los datos recibirán en su destino.
- Cuando se aplique alguna de las excepciones que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales.

Desde el punto de vista de los responsables y encargados que actualmente realizan transferencias internacionales o que las efectuarán en el marco del RGPD, hay algunas novedades a tener en cuenta:

- Las decisiones de adecuación que la Comisión ha adoptado con anterioridad a la aplicación del RGPD seguirán siendo válidas, y por tanto podrán seguir realizándose transferencias basadas en ellas, en tanto la Comisión no las sustituya o derogue.
- Las decisiones de la Comisión estableciendo cláusulas tipo para los contratos en los que se establecen garantías para las transferencias internacionales seguirán siendo válidas hasta que la Comisión las sustituya o derogue.
- Las autorizaciones de transferencias que las autoridades nacionales de protección de datos hayan otorgado sobre la base de garantías contractuales seguirán siendo válidas en tanto las autoridades no las revoquen.
- Las garantías sobre la protección que recibirán los datos en destino las debe ofrecer el exportador, que podrá ser tanto un responsable como un encargado de tratamiento.
- Se amplía la lista de posibles instrumentos para ofrecer garantías, incluyéndose expresamente, entre otros, las Normas Corporativas Vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación, así como los cláusulas contractuales modelo que puedan aprobar las autoridades de protección de datos.

- En los casos de Normas Corporativas Vinculantes, cláusulas contractuales estándar, códigos de conducta y esquemas de certificación, la transferencia no requerirá la autorización de las autoridades de supervisión.
- Se añade una excepción al listado que en su momento estableció la Directiva 95/46. Se trata de la posibilidad de que el responsable pueda transferir datos a un país sin nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer intereses legítimos imperiosos del responsable y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados y deberá comunicarse a la autoridad de protección de datos.

Vídeo de Oracle Ibérica sobre GDPR