Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Gestión de riesgos

- Introducción
- Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
- Metodologías comúnmente aceptadas de identificación y análisis de riesgos
- Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo
- Resumen

Introducción

Importancia de la Gestión de Riesgos en la Seguridad de la Información

- Garantizar la seguridad de la información: Para asegurar la protección de los datos, es esencial asignar recursos y esfuerzos adecuados, siguiendo los principios de Confidencialidad, Integridad y Disponibilidad (CIA).
- Racionalización de recursos: La aplicación de medidas proporcionales a los riesgos existentes es clave. Esto se logra mediante métodos de Análisis y Gestión de Riesgos (AGR), que permiten evaluar y abordar de manera efectiva las vulnerabilidades y amenazas.

Introducción

Proceso de Análisis y Gestión de Riesgos (AGR)

- Análisis de Riesgos (AR): Es el proceso sistemático para evaluar la magnitud de los riesgos a los que está expuesta una organización. Utilizando el método MAGERIT, se identifican y cuantifican las posibles amenazas a la seguridad de la información.
- Gestión de Riesgos (GR): Consiste en la selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Esta etapa, también definida por MAGERIT, permite tomar decisiones informadas para mitigar los riesgos de manera efectiva.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Importancia del Análisis y Gestión de Riesgos (AGR)

- Realizar un Análisis y Gestión de Riesgos (AGR) es crítico para las empresas que dependen de sistemas de información para cumplir su misión. Esto se debe a que los sistemas de información son vulnerables a una variedad de amenazas que pueden comprometer la seguridad de los datos y la continuidad del negocio.
- Además, llevar a cabo un AGR antes de emprender cambios importantes, como la implementación de nuevos servicios o inversiones en tecnología, permite integrar medidas de seguridad desde el diseño mismo. Esto garantiza que la seguridad sea una consideración central desde el principio, evitando la necesidad de aplicar soluciones de seguridad como una ocurrencia posterior, lo que podría resultar en costos adicionales y esfuerzos innecesarios.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Casos Necesarios para un AGR

- Hay varios casos en los que es indispensable llevar a cabo un AGR. Uno de ellos es cuando una empresa busca obtener certificaciones de cumplimiento de normas, como la ISO 27001, que requieren un enfoque estructurado para la gestión de riesgos de seguridad de la información.
- Asimismo, es crucial realizar un AGR por precepto legal, como lo establece la Ley Orgánica de Protección de Datos, que exige a las organizaciones adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos personales.
- Otros casos incluyen la realización de auditorías de seguridad o la definición de marcos de cumplimiento legal, donde un AGR proporciona una base sólida para abordar los requisitos de seguridad de manera efectiva.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Consideraciones de Costo y Equipo

- Es importante reconocer que realizar un AGR puede ser costoso y requiere la participación de diversas personas en la empresa. Esto puede implicar la asignación de recursos financieros y humanos significativos para llevar a cabo el proceso de manera efectiva.
- Además, es fundamental establecer un criterio homogéneo para valorar los riesgos. Esto asegura que las decisiones sobre qué riesgos abordar primero se basen en una evaluación objetiva y consistente.
- Para ello, se requiere la formación de un equipo diverso que incluya a la dirección de la empresa, responsables de seguridad de la información, propietarios o responsables de procesos críticos, y representantes de usuarios. Esta diversidad de perspectivas garantiza una evaluación integral de los riesgos y una mayor aceptación de las medidas de seguridad propuestas.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Proceso de Análisis de Riesgos (AR)

- La primera fase del AGR, conocida como Análisis de Riesgos (AR), es fundamental para comprender y evaluar los riesgos a los que está expuesta la empresa.
- Durante esta fase, se identifican los activos de información críticos, se analizan las amenazas y vulnerabilidades que podrían afectarlos, y se estima el impacto potencial de un incidente de seguridad, así como la probabilidad de que ocurra.
- Los resultados de este análisis proporcionan una base sólida para el diseño de ampliaciones del sistema o la gestión de cambios importantes, asegurando que se aborden los riesgos más críticos de manera prioritaria.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Proceso de Gestión de Riesgos (GR)

- La segunda fase del AGR, denominada Gestión de Riesgos (GR), implica la selección e implementación de medidas para mitigar los riesgos identificados durante el análisis.
- Durante esta fase, se evalúan diversas acciones para tratar los riesgos, como mitigar, evitar, transferir o aceptar el riesgo, teniendo en cuenta requisitos legales, operacionales, objetivos empresariales y rentabilidad.
- Al adoptar un enfoque estructurado para la gestión de riesgos, las organizaciones pueden minimizar el impacto de los incidentes de seguridad, proteger sus activos de información y garantizar la continuidad del negocio en un entorno cada vez más complejo y dinámico.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Proceso de Gestión de Riesgos (GR)

- La segunda fase del AGR, denominada Gestión de Riesgos (GR), implica la selección e implementación de medidas para mitigar los riesgos identificados durante el análisis.
- Durante esta fase, se evalúan diversas acciones para tratar los riesgos, como mitigar, evitar, transferir o aceptar el riesgo, teniendo en cuenta requisitos legales, operacionales, objetivos empresariales y rentabilidad.
- Al adoptar un enfoque estructurado para la gestión de riesgos, las organizaciones pueden minimizar el impacto de los incidentes de seguridad, proteger sus activos de información y garantizar la continuidad del negocio en un entorno cada vez más complejo y dinámico.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Análisis de Riesgos (AR)

- Identificación de activos y sus relaciones de dependencia.
- Identificación de amenazas y vulnerabilidades.
- Estimación del impacto y probabilidad del riesgo.
- Evaluación del nivel de riesgo y coste de mitigación.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Gestión de Riesgos (GR)

- Identificación de criterios de aceptación de riesgo (regulatorios, normativos, objetivos de la empresa y rentabilidad)
- Determinación de la aceptabilidad del riesgo calculado.
- Identificación y evaluación de medidas de seguridad necesarias.
- Selección e implementación de medidas proactivas o reactivas.
- Evaluación de la efectividad de las medidas.
- Estimación del nivel de riesgo residual.
- Adopción de medidas según sean aceptables o no.
- Ciclo de retroalimentación para mejorar continuamente el proceso.

Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

Ciclo de Gestión de Riesgos

- El proceso de Gestión de Riesgos sigue un ciclo continuo.
- Comienza con el análisis de riesgos para identificar y evaluar los riesgos.
- Luego, se pasa a la gestión de riesgos, donde se seleccionan e implementan medidas para mitigar los riesgos.
- Finalmente, se evalúa la efectividad de las medidas y se retroalimenta el proceso para mejorar la seguridad de manera continua.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos

Inicio del Proceso de Gestión de Riesgos

- El proceso de Gestión de Riesgos comienza con la medición de los riesgos, utilizando modelos de ocurrencia de incidentes de seguridad y considerando activos vulnerables y amenazas.
- Se emplean técnicas para determinar los activos y su valor en términos de seguridad (confidencialidad, integridad y disponibilidad).
- A continuación, se analizan en detalle algunos métodos de análisis de riesgos, comenzando por el análisis de riesgo de la metodología MAGERIT.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Metodología MAGERIT

- El Consejo Superior de Administración Electrónica publicó en 2006 la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).
- Reconoce el desafío de la complejidad en los métodos de análisis de riesgos y la necesidad de una aproximación rigurosa para obtener conclusiones confiables.
- El AGR busca comprender los riesgos para poder enfrentarlos y controlarlos, contrarrestando el temor a lo desconocido con el conocimiento.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Exhaustividad de la Metodología

- MAGERIT se propone como una metodología exhaustiva que abarca todos los aspectos relevantes en el análisis y gestión de riesgos de los sistemas de información, que considera diversos escenarios y situaciones frecuentes, como:
  - Sistemas simples o reducidos, donde puede ser suficiente un enfoque informal para el análisis de riesgos.
  - Análisis específicos requeridos por la legislación, como el estudio de los ficheros afectados por la LOPDGDD (Ley Orgánica de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales).
  - Evaluación de aspectos específicos de seguridad, como la confidencialidad de la información o la disponibilidad de los servicios.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Enfoque de MAGERIT

- Se destaca la importancia de seguir un enfoque constructivo, comenzando con un ámbito reducido y ampliándolo gradualmente según las necesidades y la complejidad del entorno de riesgos. Esto permite una adaptación flexible de la metodología a las particularidades de cada organización y sistema de información.
- MAGERIT busca ofrecer un enfoque metódico y estructurado que evite la improvisación y la arbitrariedad en el análisis de riesgos.
- Su objetivo es proporcionar un marco sólido para la identificación, evaluación y gestión de riesgos en los sistemas de información.
- Al seguir los principios y directrices de MAGERIT, las organizaciones pueden mejorar la confiabilidad y seguridad de sus sistemas de información.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos

Cinco pasos simples para obtener una lista de riesgos del sistema de información:

- Determinar activos y valorar su Confidencialidad (C), Integridad (I) y Disponibilidad (A).
- Identificar amenazas y evaluar su impacto en C, I y A, así como su probabilidad.
- Analizar las salvaguardas existentes y su eficacia para prevenir la degradación de C, I y A.
- Evaluar el impacto potencial de la materialización de una amenaza.
- Calcular el riesgo como el impacto ponderado por la probabilidad de ocurrencia de la amenaza.

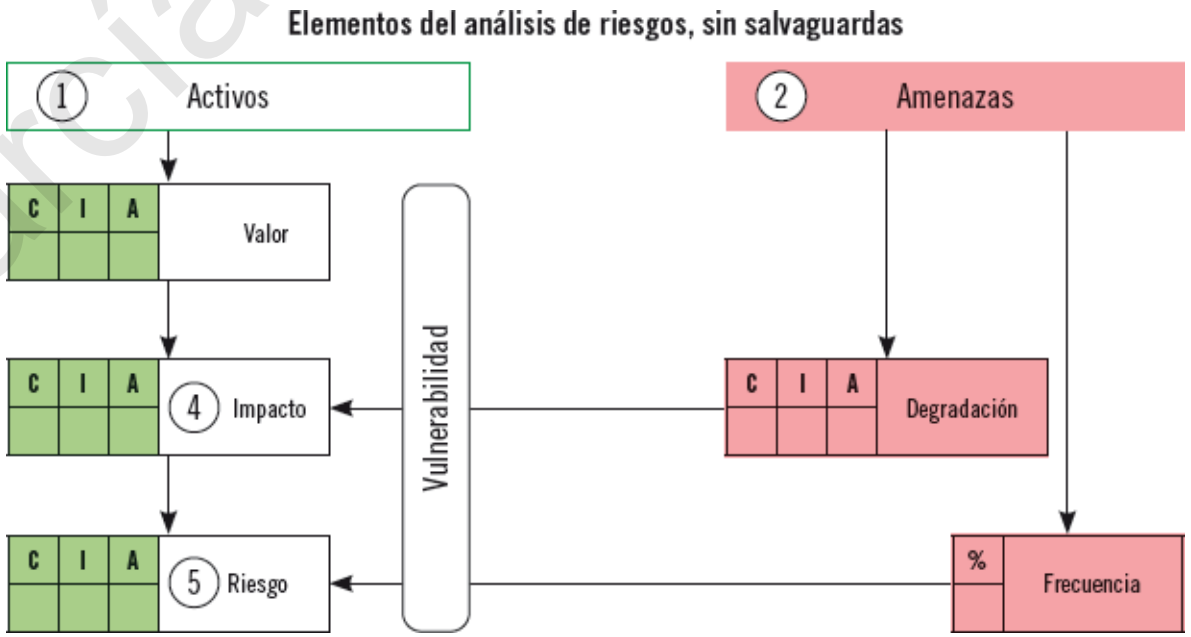
Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos

Se analiza el sistema sin salvaguardas para obtener el riesgo potencial.

Esto incluye los pasos 1, 2, 4 y 5 del proceso de análisis de riesgos.

Luego, se añaden las salvaguardas (paso 3) para obtener el riesgo real.



Los "activos" tienen un "valor", y unas "vulnerabilidades", que permiten que las "amenazas" produzcan una "degradación", cuantificada en un daño o "impacto", que se producirá con cierta "frecuencia", generando así un "riesgo" constante o continuo.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Definición de activos según MAGERIT: recursos del sistema de información necesarios para el funcionamiento y logro de objetivos.

Tipos de activos incluyen datos (D), servicios (S), aplicaciones (SW), equipos informáticos (HW), soportes de almacenamiento (SI), equipamiento auxiliar (AUX), redes de comunicaciones (COM), instalaciones (L) y personas (P).

Cada uno de estos activos juega un papel crucial en el funcionamiento y seguridad del sistema de información.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Relaciones de Dependencia de Activos

La dependencia entre activos se organiza en capas para comprender mejor su interacción y dependencia:

- Capa 4: funciones y procesos de la organización, donde se definen los objetivos y actividades clave.
- Capa 3: información y datos, que sirven como el núcleo del sistema de información.
- Capa 2: sistema de información, que incluye aplicaciones, equipos, soportes de almacenamiento, equipamiento auxiliar y redes de comunicaciones.
- Capa 1: entorno necesario para el funcionamiento del sistema, como las instalaciones y el personal.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Metodología para Analizar Sistemas Complejos

La comprensión de sistemas complejos implica una reflexión profunda sobre sus componentes y relaciones.

Se enumeran los elementos del sistema y se agrupan según criterios relevantes, como la complejidad o la cercanía al producto/servicio final.

Se definen criterios de relación, como "depende de" o "se necesita para", y se representan gráficamente las relaciones entre los elementos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Consideraciones Adicionales

Es posible incluir capas adicionales según la envergadura y complejidad del sistema.

Se pueden subdividir las capas para adaptarse a las necesidades específicas del sistema y mejorar la comprensión.

La organización en capas facilita la identificación de activos críticos y la comprensión de su impacto en el sistema en su conjunto.

Ejemplos de activos adicionales que pueden ser considerados en capas superiores incluyen credibilidad, conocimiento acumulado, imagen de la empresa e intimidad de las personas.

Estos activos agregan un nivel adicional de complejidad y consideración en el análisis de riesgos y la gestión de la seguridad de la información.

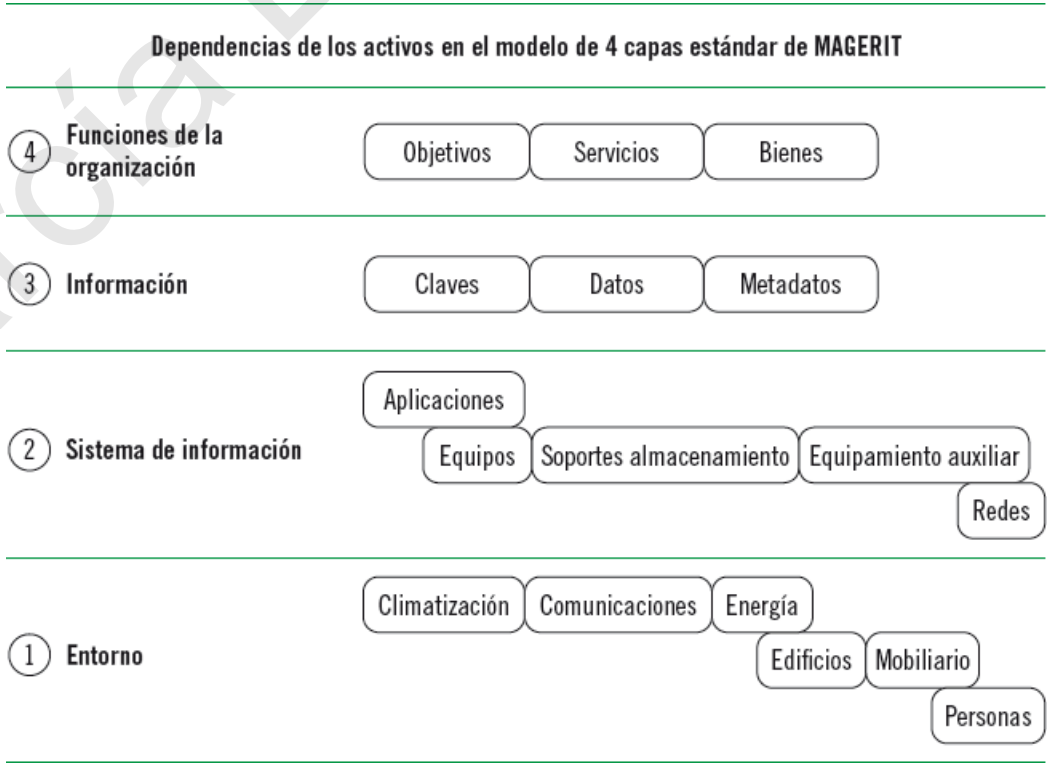
Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos Paso 1: Activos

Representación gráfica de las capas de activos, incluyendo las categorías que corresponden a cada una.

Se muestran las dependencias más comunes entre las capas, aunque estas pueden variar según la empresa o los servicios específicos.

La comprensión de estas capas y dependencias es fundamental para el análisis de riesgos y la gestión de la seguridad de la información.



Un activo superior, como un servicio entregado por la empresa (capa 4), depende de una información (capa 3), procesada por unas aplicaciones (capa 2), ejecutadas por unos equipos (capa 2), y almacenada en unos soportes (capa 2), que resultan accesibles gracias a unas redes (capa 2), que operan en unas condiciones de climatización (capa 1), suministro eléctrico (capa 1), y con unas facilidades de comunicaciones, (capa 1) sustentadas por un mobiliario, y unos edificios (capa 1), operados por unas personas (capa 1).

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Valoración de los activos

El valor de los activos en seguridad de la información no se limita a su costo de adquisición, requiere una evaluación más profunda.

Se distingue entre el valor propio de un activo y el valor acumulado, que se hereda de activos superiores en un árbol de dependencias.

MAGERIT propone que el valor se asigne a los servicios finales e información, que son críticos para el funcionamiento de la empresa.

Además de las dimensiones básicas (confidencialidad, integridad y disponibilidad), se sugiere considerar la autenticidad y la trazabilidad como dimensiones adicionales de valoración.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Autenticidad

En seguridad de la información, la autenticidad se refiere a la verificación de la identidad de un usuario, un sistema, un proceso o un recurso para garantizar que sean genuinos y legítimos.

La autenticidad asegura que la información provenga de una fuente confiable y autorizada, y que no haya sido alterada o manipulada de manera no autorizada durante su transmisión o almacenamiento.

La autenticidad garantiza la integridad y la confiabilidad de los datos y la identidad de los usuarios o entidades que interactúan con ellos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Trazabilidad

En seguridad de la información, la trazabilidad se refiere a la capacidad de rastrear y documentar el origen, los cambios y las interacciones de los datos y las acciones dentro de un sistema o proceso.

Implica registrar y mantener un historial detallado de todas las actividades relacionadas con la información, incluyendo quién accede a ella, qué cambios se realizan y cuándo se llevan a cabo estas acciones.

La trazabilidad es fundamental para garantizar la transparencia, la responsabilidad y la integridad de los datos, permitiendo identificar cualquier anomalía, auditoría o seguimiento de eventos en caso de incidentes de seguridad o investigaciones.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Valoración de los activos. Dimensiones

- La evaluación de los activos puede variar según las necesidades y el contexto de la empresa.
- Es esencial considerar diferentes criterios de valoración para cada dimensión de seguridad, especialmente para la disponibilidad, que tiene un carácter temporal.
- MAGERIT propone evaluar el valor de un activo como el costo estimado de recuperación en caso de una incidencia.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 1: Activos

Valoración de los activos. Factores

- Los factores que influyen en la valoración de los activos incluyen el costo de reposición, el tiempo y la mano de obra necesarios para recuperar el activo, el lucro cesante, la capacidad operativa y las posibles sanciones legales.
- También se deben considerar los daños potenciales a otros activos, a personas y al medio ambiente.
- Es crucial definir criterios de valoración y factores de manera clara y consistente para obtener resultados comparables y precisos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

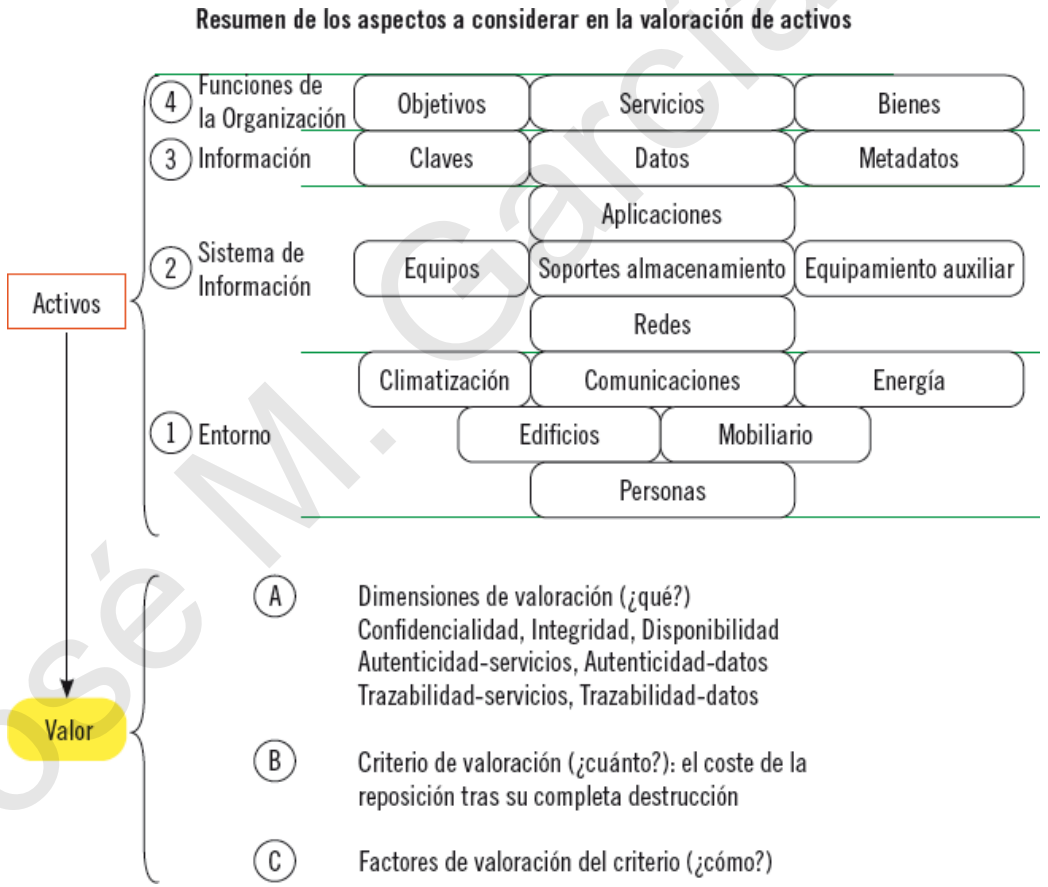
Fase 1.- Análisis de riesgos. Paso 1: Activos

Valoración de los activos. Técnicas

- Las técnicas para asignar valores a los activos pueden incluir el uso de formularios estructurados, entrevistas con expertos y reuniones de grupo.
- La precisión y coherencia en la aplicación de estas técnicas son fundamentales para garantizar una evaluación efectiva de los activos y riesgos.
- Además, es importante documentar y registrar los criterios de valoración utilizados para garantizar la consistencia en futuras evaluaciones y análisis de riesgos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos Paso 1: Activos



Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

En esta fase, se profundiza en el análisis de las amenazas que podrían afectar a los activos identificados en el paso anterior.

Es importante considerar una amplia gama de posibles escenarios que podrían representar riesgos para la seguridad de la información.

Algunas amenazas comunes incluyen ciberataques, desastres naturales, errores humanos y fallas en los sistemas tecnológicos.

Aunque existen catálogos de amenazas disponibles en diversas fuentes, es esencial que el analista de riesgos construya una lista de amenazas específica para el contexto de la organización o sistema en cuestión.

Esto implica considerar los riesgos más relevantes y probables en función de factores como la industria, el entorno operativo y las vulnerabilidades existentes.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Importancia de la selección de amenazas

La selección adecuada de las amenazas a analizar es crucial para garantizar la eficacia del proceso de gestión de riesgos.

En lugar de abordar todas las posibles amenazas de manera indiscriminada, es preferible enfocar los esfuerzos en aquellas que representan las mayores preocupaciones o tienen el potencial de causar el mayor impacto negativo en los activos de la organización.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Relación entre amenazas y activos

Es fundamental comprender la interacción entre las amenazas identificadas y los activos de la organización.

No todas las amenazas afectarán a todos los activos por igual, y algunas podrían tener consecuencias más graves que otras.

Evaluar la relación específica entre cada amenaza y cada activo permite priorizar los riesgos y asignar recursos de manera más eficiente para mitigarlos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Análisis de amenazas.

De las amenazas, se deberá calcular la degradación que producen, y la frecuencia con que aparecen.

Calcular la degradación y frecuencia de las amenazas es difícil.

La precisión requiere un esfuerzo desproporcionado.

Se emplean valoraciones cualitativas proporcionales al objetivo del análisis.

Esto permite una evaluación más práctica y efectiva de los riesgos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Degradación

La degradación evalúa el daño potencial causado por un incidente en un activo.

Se estima para cada activo y dimensión de valor, pero es difícil precisar un valor exacto.

Se simplifica mediante valores porcentuales que representan el impacto en la dimensión del activo: completamente, algo, o nada.

Ejemplos:

Para un ordenador y una amenaza de incendio, la degradación será máxima en disponibilidad.

Para una aplicación y una amenaza de programa malintencionado, la degradación puede variar.

Caracterizar el daño de una amenaza en un activo es complejo, por lo que se usan valores cualitativos como "completa" o "parcial".

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Degradación

Es importante registrar la justificación detrás de la asignación de valores de degradación.

Las amenazas intencionales tienden a causar degradación alta, mientras que las no intencionales pueden no ser tan severas.

Se debe revisar y justificar los valores de degradación, especialmente en casos de riesgos altos o inversiones significativas en seguridad.

Valoración cualitativa "la dimensión se ve."	Degradación	Dato para MAGERIT
Totalmente degradada	Completa	**100 %**
Algo afectada	Parcial	**10 %**
Prácticamente nada afectada	Inexistente	**1 %**

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Frecuencia de la amenaza

La frecuencia de la amenaza refleja la probabilidad de que ocurra un evento dañino.

Las amenazas pueden variar en su impacto y en su frecuencia de ocurrencia.

Determinar la frecuencia exacta de una amenaza puede ser desafiante y requiere interpretar datos relativos o parciales.

La estimación precisa de la frecuencia de una amenaza es crucial pero difícil.

A menudo, se utilizan datos históricos o indicativos para aproximar la frecuencia de las amenazas.

MAGERIT sugiere entender la frecuencia como el número de ocurrencias anuales de un incidente, facilitando así su cálculo y evaluación.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 2: Amenazas

Frecuencia de la amenaza

Emplear la tasa anual como frecuencia acabaría conduciendo a calcular el riesgo anual, o pérdidas anuales probables, por ello MAGERIT recomienda el uso de valoraciones cualitativas para simplificar la estimación de la frecuencia de las amenazas y facilitar el proceso de análisis de riesgos.

Valoración cualitativa "la amenaza sucede..."	Frecuencia	Dato para MAGERIT
A diario	Muy frecuente (MF)	**100 %**
Mensualmente	Frecuente (F)	**10 %**
Una vez al año	Normal (N)	**1 %**
Cada varios años	Poco frecuente (PF)	**1/10**

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Introducción al Impacto

El impacto es la medida del daño causado a un activo por la materialización de una amenaza.

Se calcula considerando la degradación causada por la amenaza en cada dimensión del activo.

Impacto = Valor x Degradación

Por ejemplo, si un activo tiene un valor CIA = (5, 8, 6) y se enfrenta a una amenaza con una degradación CIA = (100 %, 0 %, 50 %), el impacto en el activo será (5, 0, 3), que representa el daño en cada dimensión del activo.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Introducción al Impacto

No se debe confundir el impacto con el valor del activo después de la amenaza.

Valor final = Valor inicial – Impacto

En el ejemplo anterior, tras la materialización de la amenaza,el valor del activo sería:

(5, 8, 6) – (5, 0, 3) = (0, 8, 3).

El impacto también puede evaluarse cualitativamente utilizando combinaciones tabuladas, lo que permite una comprensión más fácil y rápida de las consecuencias de las amenazas.

IMPACTO		DEGRADACIÓN AMENAZA		
		1 %	10 %	100 %
Valor	Muy alto (MA)	M	A	MA
	Alto (A)	B	M	A
	Medio (M)	MB	B	M
	Bajo (B)	MB	MB	B
	Muy bajo (MB)	MB	MB	MB

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Impacto Acumulado

El impacto acumulado es el resultado de las amenazas que afectan al valor total de un activo, incluyendo tanto su valor propio como el valor de sus activos superiores.

Este tipo de impacto facilita la determinación de las salvaguardas necesarias para proteger los activos de un sistema de información.

Al considerar el valor total del activo y sus dependencias, se obtiene una visión integral de las posibles vulnerabilidades y se pueden tomar medidas preventivas más efectivas.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Impacto Repercutido

El impacto repercutido se refiere al impacto que sufre un activo debido a su valor propio y a las amenazas que afectan a sus activos inferiores.

Este tipo de impacto permite evaluar las consecuencias de incidentes técnicos en la misión del sistema de información, lo que ayuda a determinar el nivel de riesgo aceptable.

Al centrarse en el valor propio del activo y las amenazas directas a él, se puede identificar cómo afectan los problemas técnicos específicos a la funcionalidad del sistema.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Agregación de impactos

Cuando se necesite agregar impactos, es importante considerar varios factores, como la independencia de las amenazas y las dimensiones del impacto.

Se pueden agregar impactos repercutidos de diferentes activos, así como impactos acumulados de diferentes amenazas en un mismo activo.

Sin embargo, es crucial evaluar la independencia de las amenazas y su posible concurrencia para evitar sobrevalorar los activos o subestimar los riesgos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Agregación de impactos (ejemplo)

Independencia de las amenazas: Imagina que estás evaluando el riesgo de seguridad de un sistema informático que utiliza servidores en la nube para almacenar datos y una red interna para la comunicación entre los empleados.

Una de las amenazas es un corte de energía que afectaría tanto a los servidores en la nube como a la red interna.

Otra amenaza es un ataque cibernético dirigido específicamente a los servidores en la nube.

En este caso, la ocurrencia de un corte de energía y un ataque cibernético son eventos independientes entre sí, ya que uno puede ocurrir sin necesariamente desencadenar el otro.

Impactos Repercutidos: Supongamos que una amenaza de malware afecta a un servidor en la nube que almacena datos críticos. Esto no solo tendría un impacto directo en la confidencialidad e integridad de los datos en ese servidor, sino que también podría tener un impacto repercutido en el sistema en su conjunto.

Por ejemplo, si los datos críticos son inaccesibles debido al malware, los empleados no podrían realizar su trabajo de manera eficiente, lo que afectaría la disponibilidad de los servicios de la empresa.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 4: Impacto

Agregación de impactos (ejemplo)

Impactos Acumulados: Considera un escenario donde un servidor en la nube está expuesto a múltiples amenazas, como un corte de energía, un ataque de malware y un fallo de hardware.

Cada una de estas amenazas tendría un impacto acumulado en la confidencialidad, integridad y disponibilidad de los datos almacenados en ese servidor. Al sumar estos impactos, se obtiene una evaluación completa del riesgo asociado con ese activo en particular.

En resumen, al agregar impactos, es esencial considerar la independencia de las amenazas y cómo afectan a diferentes activos o dimensiones de impacto. Esto nos permite obtener una evaluación precisa del riesgo y tomar medidas adecuadas para mitigarlo.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 5: Riesgo

Cálculo del riesgo

El riesgo se calcula a partir del impacto y la frecuencia de las amenazas.

Crece con la frecuencia y el impacto, determinándose para cada activo, amenaza y dimensión.

Función de cálculo

La función comúnmente empleada es el producto de la frecuencia y el impacto.

Riesgo = Impacto x Frecuencia

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 5: Riesgo

Se pueden utilizar otras funciones cuantitativas o valoraciones cualitativas según la necesidad.

RIESGO		FRECUENCIA			
		Poco frecuente 0.1	Normal 1	Frecuente 10	Muy frecuente 100
Impacto	Muy alto (MA)	A	MA	MA	MA
	Alto (A)	M	A	MA	MA
	Medio (M)	B	M	A	MA
	Bajo (B)	MB	B	M	A
	Muy bajo (MB)	MB	MB	B	M

Consideraciones adicionales sobre el riesgo

Es importante analizar el riesgo en relación con la jerarquía de activos.

Esto conduce al riesgo acumulado y al riesgo repercutido, lo que proporciona una visión más completa de los riesgos del sistema.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 5: Riesgo

Riesgo acumulado

Este tipo de riesgo surge como resultado del impacto acumulado que experimenta un activo debido a la frecuencia con la que se materializa una amenaza.

Es esencialmente el riesgo que enfrenta un activo principal o crítico en el sistema de información.

Por ejemplo, si un servidor principal experimenta una amenaza de interrupción del servicio con una frecuencia anual, el riesgo acumulado se calculará en función de la probabilidad de que ocurra esta interrupción y el impacto que tendría en el sistema.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 5: Riesgo

Riesgo repercutido

Por otro lado, el riesgo repercutido se refiere al riesgo que afecta a un activo debido al impacto repercutido de una amenaza y su frecuencia.

Este riesgo se calcula para activos que tienen un valor propio y son afectados indirectamente por las amenazas que impactan a otros activos.

Por ejemplo, si un servidor de respaldo experimenta una interrupción debido a la falla del servidor principal, el riesgo repercutido se calculará en función de la probabilidad de que ocurra esta falla y el impacto que tendría en el servidor de respaldo.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 5: Riesgo

Agregación de riesgos

Aspectos a tener en cuenta al agregar los riesgos acumulados y repercutidos:

Se pueden agregar los riesgos repercutidos de diferentes activos, lo que permite obtener una visión general del riesgo para todo el sistema.

También se pueden agregar los riesgos acumulados de diferentes activos, siempre y cuando estos no dependan entre sí ni de ningún activo superior común. Esto garantiza que no se sobrevaloren los activos principales compartidos.

Además, se puede agregar el riesgo de una misma amenaza en diferentes dimensiones del activo, lo que proporciona una comprensión completa del impacto de esa amenaza en todo el sistema.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Fase 1.- Análisis de riesgos. Paso 5: Riesgo

Conclusiones

Riesgo máximo potencial.

Al finalizar la primera fase del análisis, se obtiene el riesgo máximo potencial, que representa el nivel de riesgo al que está expuesto el sistema de información sin ninguna salvaguarda instalada. Este análisis, aunque puede parecer teórico, es esencial para establecer una línea base de la máxima inseguridad del sistema.

Próxima iteración.

Se destaca que la próxima fase del análisis consistirá en considerar las salvaguardas existentes en el sistema para calcular el riesgo residual. Esta fase se abordará en detalle en la siguiente etapa del análisis, lo que indica una progresión natural en el proceso de evaluación y gestión de riesgos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Otras metodologías)

ISO 27005.

Visión general

Contexto: La norma ISO 27005 forma parte de la familia de normas ISO 27000, centrada en la seguridad de la información.

Complementa a la ISO 27001 y la ISO 27002, proporcionando un marco estructurado para la gestión de riesgos.

Estructura: Se compone de 6 cláusulas que guían el proceso de gestión de riesgos: establecimiento del contexto, valoración de riesgos, tratamiento de riesgos, aceptación de riesgos, comunicación de riesgos y monitorización y revisión de riesgos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Otras metodologías)

ISO 27005.

Proceso de gestión de riesgos

Valoración de riesgos: La cláusula 8 se centra en la valoración de riesgos, que abarca la identificación, estimación y evaluación de riesgos. Este paso es crucial para conocer y priorizar los riesgos de seguridad de la información.

Tratamiento de riesgos: La cláusula 9 establece estrategias para abordar los riesgos identificados, ya sea reduciéndolos, aceptándolos, evitándolos o transfiriéndolos. Esto ayuda a mitigar las vulnerabilidades y proteger los activos de información.

Monitorización y revisión: La cláusula 12 se enfoca en la actualización continua del proceso de gestión de riesgos para reflejar cambios internos o externos que puedan afectar la valoración de los riesgos. Esto garantiza que la organización esté preparada para enfrentar nuevos desafíos y amenazas de seguridad de la información.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Otras metodologías)

OCTAVE

Visión general de OCTAVE

OCTAVE. Operationally Critical Threat, Asset and Vulnerability Evaluation. Desarrollado por la Universidad de Carnegie Mellon, OCTAVE proporciona un marco flexible para evaluar amenazas, activos y vulnerabilidades de manera integral.

Métodos: Incluye tres métodos principales: OCTAVE original, OCTAVE-S para pequeñas empresas y OCTAVE-Allegro, centrado en activos de información.

Criterios: Se basa en criterios generales que garantizan la adaptabilidad, definición continua y futura del proceso de análisis, y el enfoque en riesgos críticos.

Resultados: El proceso se divide en fases organizativas, tecnológicas y estratégicas para identificar activos críticos, amenazas, vulnerabilidades y desarrollar planes de gestión de riesgos.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Otras metodologías)

CRAMM

Visión general de CRAMM

CRAMM: Metodología de la Agencia Central de Cómputo y Telecomunicaciones del Reino Unido, desarrollada en los años 80.

Fases:

- Análisis: Estudia activos, vulnerabilidades y amenazas para identificar riesgos.
- Gestión: Incluye contramedidas, implantación y auditoría.

Fortalezas: Define más de 400 activos, cerca de 40 amenazas, 25 tipos de impacto y más de 3500 salvaguardas.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Otras metodologías)

UNE 71504

Visión general de UNE 71504

Desarrollado por AENOR en 2008.

Fases:

1) Método de análisis: Incluye tareas preparatorias, caracterización de activos y amenazas, cálculo del riesgo intrínseco y caracterización de salvaguardas.
2) Evaluación de riesgos.
3) Tratamiento de riesgos: Define el plan de seguridad y lo aprueba.
4) Administración de la gestión de seguridad.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Otras metodologías)

FAIR

Visión general de FAIR

Pretende mejorar la precisión y el detalle en el análisis de riesgos empresariales.

Enfoque probabilístico: Reconoce la naturaleza probabilística del análisis de riesgos.

Ejemplo:

- Frecuencia de la amenaza: Considera el contacto aleatorio, habitual o intencionado.
- Magnitud de pérdidas: Divide las pérdidas en factores principales (pérdidas de activos y amenazas) y secundarios (temporalidad, diligencia, respuesta, etc.).

Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

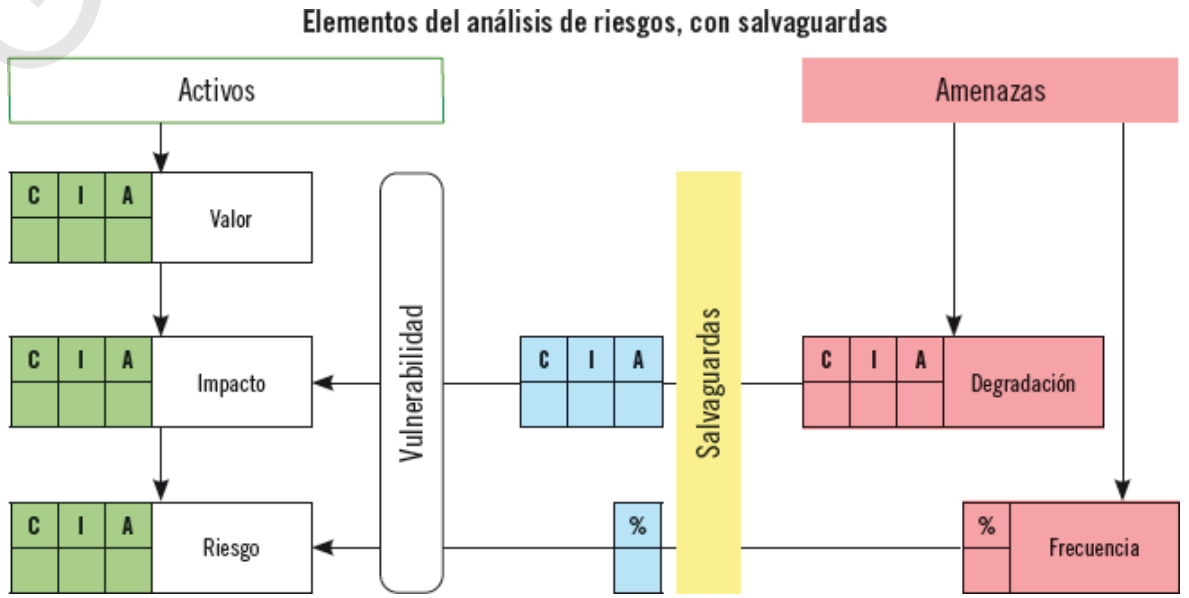
Reducción del Riesgo mediante Salvaguardas

Objetivo: Reducir el riesgo máximo teórico obtenido del análisis de riesgos.

Método: Introducción de salvaguardas o contramedidas para controlar el riesgo.

Enfoque: Actuar sobre las amenazas para reducir su degradación o frecuencia de aparición.

Las "salvaguardas" o bien reducen la degradación que produce una "amenaza", reduciendo por lo tanto su "impacto", o bien reducen la "frecuencia" con que ocurren, reduciendo por lo tanto el "riesgo".



Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Paso 3: Salvaguardas o contramedidas

Introducción a las Salvaguardas

Definición: Las salvaguardas o contramedidas son procedimientos o mecanismos tecnológicos que reducen el riesgo en un sistema de información.

Selección: No existe una lista completa de contramedidas, por lo que deben ser seleccionadas por el profesional de seguridad de la información en cada caso específico.

Catálogo de Elementos: El método en estudio incorpora un amplio catálogo de salvaguardas para los activos, disponible en "MAGERIT v2. II – Catálogo de elementos".

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Paso 3: Salvaguardas o contramedidas

Limitando el Daño Causado

Enfoque: Las salvaguardas limitan el daño causado por las amenazas de dos maneras: reduciendo la degradación y facilitando la detección o recuperación del sistema.

Valoración de Eficacia: La eficacia de una salvaguarda se valora mediante indicadores como su adecuación teórica, despliegue adecuado, utilización frecuente, procedimientos claros, formación de usuarios y presencia de controles.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Paso 3: Salvaguardas o contramedidas

Reduciendo la Frecuencia de las Amenazas

Medidas Preventivas: Estas medidas buscan reducir la frecuencia de las amenazas, idealmente impidiendo su materialización.

Valoración Cualitativa: Dada la complejidad de estimar la reducción de frecuencia, se emplean valores cualitativos para estimar la nueva ocurrencia de la amenaza con la contramedida aplicada.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Paso 3: Salvaguardas o contramedidas

Estimación del Nuevo Riesgo

Rápida Estimación: Analizadas las salvaguardas, es rápido estimar el nuevo riesgo del sistema a partir de la nueva degradación mejorada y la frecuencia mejorada.

Importancia: El proceso de selección y aplicación de salvaguardas es crucial para reducir eficazmente el riesgo en un sistema de información.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Revisión del paso 4: impacto residual

Concepto: El impacto residual representa el daño que permanece en el sistema de información después de la aplicación de las salvaguardas.

Cálculo: Se calcula considerando la eficacia de las contramedidas, donde las salvaguardas reducen la degradación que producirían las amenazas.

Degradación mejorada = Degradación x (100 – Eficacia Contramedida)

Realidad: En la práctica, debido a normas imprecisas, procedimientos incompletos y otras limitaciones, es común que el sistema siga expuesto a un impacto residual.

Impacto Residual = Valor x Degradación mejorada

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Revisión del paso 4: impacto residual

Evaluación: El impacto residual puede calcularse nuevamente, acumulado sobre los activos inferiores, repercutido sobre los superiores o agregado siguiendo las mismas reglas del paso anterior.

Impacto Residual = Impacto x (100 – Eficacia Contramedida)

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Riesgo tras la introducción de salvaguardas

Fase 1.- Análisis de riesgos. Revisión del paso 5: riesgo residual

Concepto: El riesgo residual representa la exposición del sistema de información a riesgos después de aplicar las salvaguardas.

Cálculo: Se calcula considerando la reducción en la frecuencia de las amenazas y la disminución en la degradación causada por las contramedidas.

Realidad: Aunque las salvaguardas reduzcan la probabilidad de ocurrencia de las amenazas y mitiguen su impacto, el sistema aún está expuesto a un riesgo residual debido a diversas limitaciones y factores.

Proceso: Los cálculos deben repetirse con el nuevo impacto y las frecuencias actualizadas para obtener el riesgo residual final del sistema.

Riesgo Residual = Impacto Residual x Frecuencia mejorada

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Gestión del riesgo residual

Evaluación del Riesgo Residual

El riesgo residual debe ser evaluado para determinar su nivel de aceptabilidad según las normas de la empresa.

La aceptación del riesgo residual es responsabilidad exclusiva de la Dirección, resaltando la importancia de su involucramiento en la gestión de riesgos.

Interpretación del Riesgo Residual

El riesgo residual requiere una interpretación más allá de su valor numérico para identificar deficiencias en las salvaguardas implementadas.

La comparación del riesgo residual con el riesgo potencial puede revelar la efectividad de las salvaguardas aplicadas y señalar áreas de mejora.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Gestión del riesgo residual

Implementación de Salvaguardas

La selección y aplicación de salvaguardas sigue un proceso ordenado, que incluye establecer responsabilidades, definir objetivos, desarrollar procedimientos, implementar las salvaguardas y establecer controles.

Las salvaguardas pueden ser de diferentes tipos y deben seleccionarse considerando criterios económicos para garantizar una inversión eficiente en seguridad.

Criterio Económico en la Selección de Salvaguardas

La evaluación económica de las salvaguardas implica comparar el costo de implementación con el costo del riesgo residual para identificar la opción más rentable.

Se busca encontrar un equilibrio entre el costo de las salvaguardas y la reducción del riesgo residual para optimizar los recursos de seguridad.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Gestión del riesgo residual

Involucración de la Dirección

La Dirección debe establecer el nivel de riesgo aceptable para la empresa, considerando requisitos legales, operativos, empresariales y económicos.

Es fundamental que la Dirección asuma la responsabilidad de mitigar riesgos inaceptables y garantizar la seguridad del sistema de información.

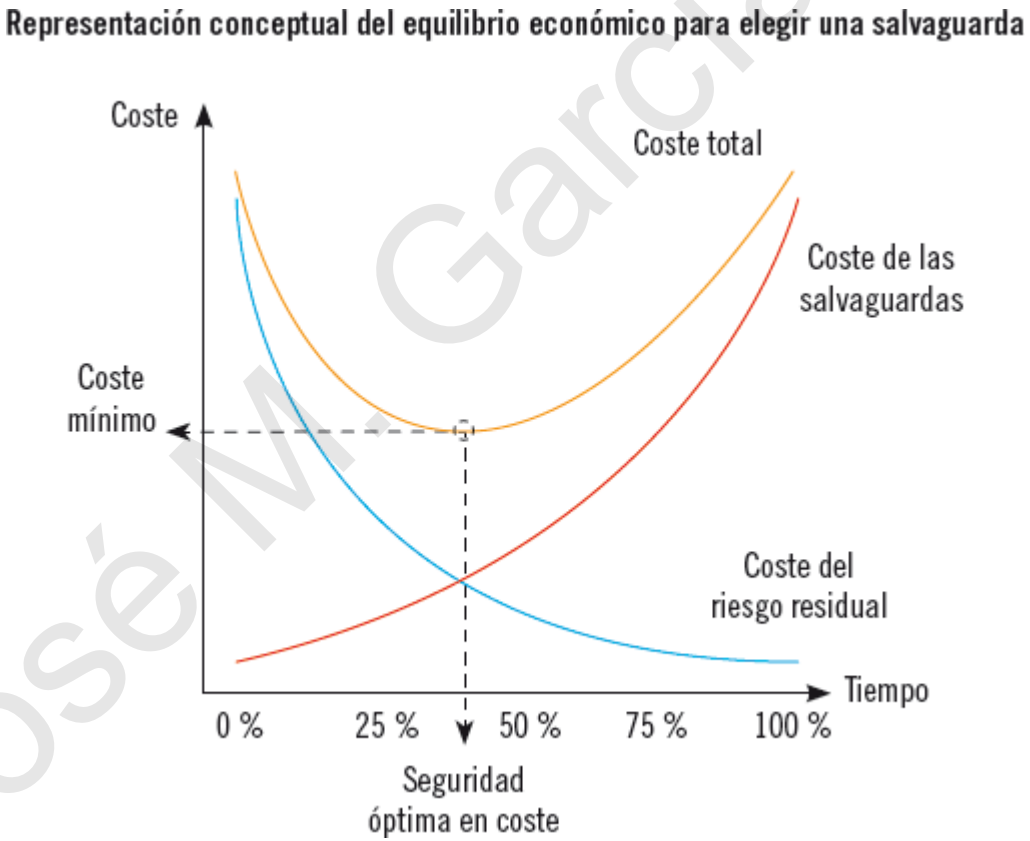
Revisión del Riesgo Introducido por las Salvaguardas

Las salvaguardas pueden introducir nuevos riesgos en el sistema y deben ser evaluadas para garantizar que la protección efectiva supere cualquier riesgo adicional.

Es necesario iterar el proceso de gestión de riesgos para garantizar que el riesgo residual con las nuevas salvaguardas sea menor que el riesgo residual previo a su implementación.

Metodologías comúnmente aceptadas de identificación y análisis de riesgos (Magerit)

Gestión del riesgo residual



Resumen

MAGERIT

MAGERIT es una norma española que proporciona un método estructurado para la gestión de riesgos de seguridad de la información.

El proceso de MAGERIT consta de 5 pasos: evaluación de activos, evaluación de amenazas, consideración de contramedidas, cálculo del impacto y riesgo, y gestión del riesgo residual.

Resumen

Gestión del Riesgo Residual y Aplicación de Salvaguardas

Después de analizar el riesgo residual, se debe gestionar mediante la mitigación, evitación, transferencia o aceptación, siendo esta última responsabilidad de la Dirección.

MAGERIT sugiere priorizar la aplicación de contramedidas preventivas, de detección y reactivas para reducir el riesgo.

La evaluación económica se centra en encontrar un equilibrio entre el costo de la seguridad y el costo del incidente de seguridad.

Para aplicar las salvaguardas, MAGERIT propone un procedimiento ordenado que incluye establecer una política organizativa, definir objetivos, desarrollar instrucciones paso a paso, implementar las salvaguardas y evaluar su eficacia.