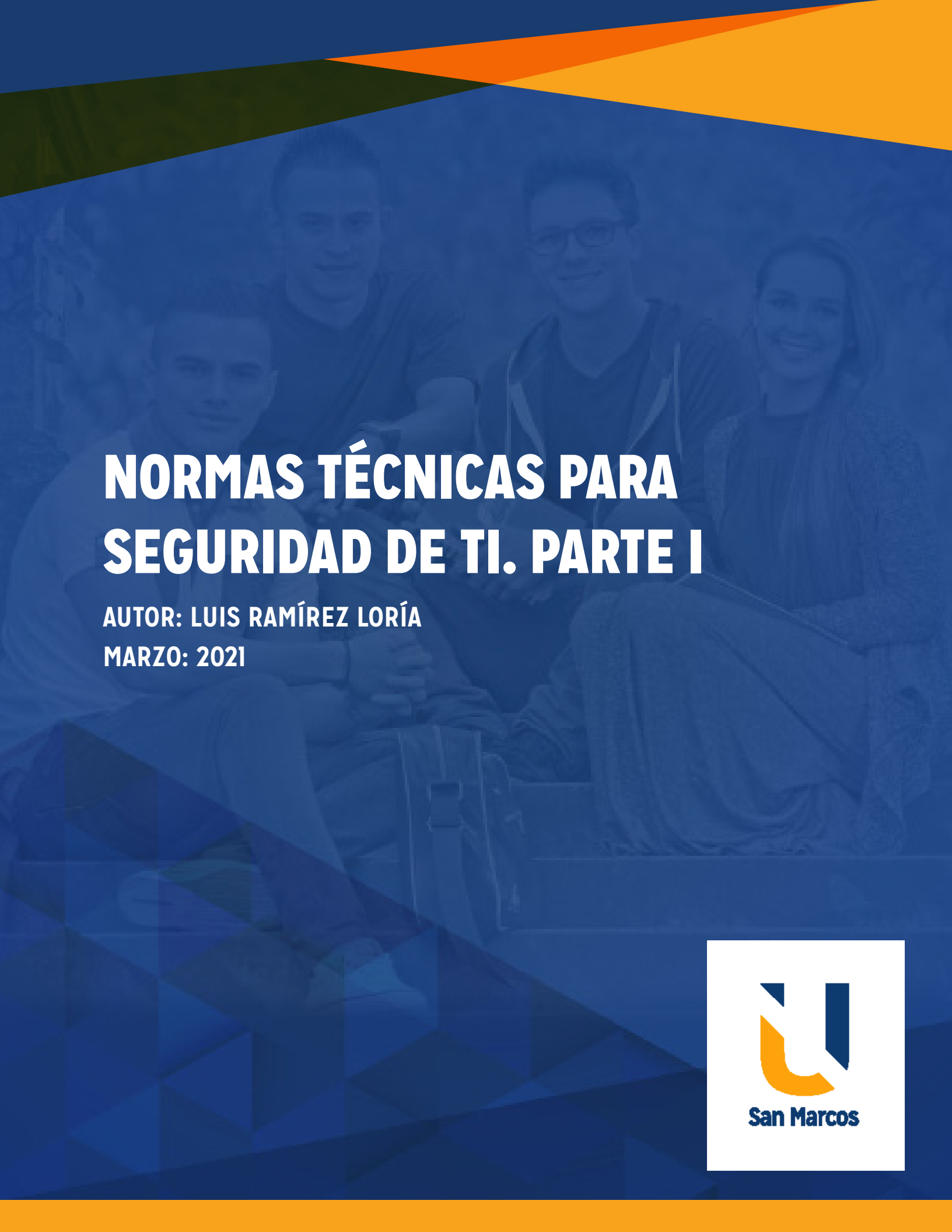


NORMAS TÉCNICAS PARA SEGURIDAD DE TI. PARTE I

AUTOR: LUIS RAMÍREZ LORÍA

MARZO: 2021

San Marcos

Tabla de contenido

Introducción

En el primer módulo del curso, se analizó la implementación de un Sistema de Gestión de Seguridad Informática (SGSI) como un requisito indispensable que debe permitir a las organizaciones el establecimiento de políticas y normativas de seguridad de la información, lógicas, incrementales y principalmente alineadas con el entorno y capacidades de la organización, lo cual requiere un alineamiento estratégico y una gestión oportuna por parte de la organización, lo cual no puede ser solamente dirigido por los procesos o Gerencia de Tecnologías de la Información, sino que requiere el patrocinio, conocimiento e impulso gerencia de forma general, identificando la seguridad de la información como un factor estratégico e incluso como un factor crítico para asegurar el éxito de la empresa.

En complemento a estas bases, se busca dilucidar si existen metodologías y prácticas sobre el tema de gestión de riesgos informáticos que impliquen un nivel de mayor detalle que lo analizado en las recomendaciones de mejores prácticas del marco COBIT 5 sobre dicho SGSI, para lo cual en las próximas dos lecturas ahondaremos sobre la metodología de análisis y gestión de riesgos que ha sido elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España, conocida como MAGERIT.

Esta metodología aborda elementos tales como la estructura del submodelo de procesos de esta metodología, el esquema de etapas y actividades del submodelo, las técnicas y herramientas utilizadas; y para la siguiente lectura, siempre en el marco de la metodología MAGERTI, se analizará el submodelo de eventos e interfaz con otros métodos, las normas técnicas y las normas legales sobre seguridad de los sistemas de información, buscando con esto estudiar los riesgos que soporta un sistema de información y su entorno, estableciendo un análisis de riesgos que implica la evaluación del impacto que una violación de seguridad tiene en la organización.

Introducción al Submodelo de entidades y procesos de MAGERIT

Tal cual se menciona en las lecturas anteriores los servicios y gestión de negocios que se soportan en los sistemas de información, las tecnologías de información y el entorno asociado requieren un adecuado análisis de riesgos, la evaluación del impacto ante las violaciones de seguridad, la detección y control de amenazas, la determinación y prevención de vulnerabilidades, entre otros factores, lo cuales requieren seguir las medidas apropiadas para conocer, prevenir, reducir, impedir o controlar los riesgos identificados y minimizar su impacto en las operaciones y con esto el perjuicio hacia el negocio.

La metodología de análisis y gestión de riesgos MAGERIT permite realizar una valoración de los servicios y la información para que las empresas puedan determinar o visualizar cuánto ponen en riesgo y esto apoya los procesos para la protección de los recursos y la gestión de los riesgos informáticos.

Adicionalmente la metodología busca satisfacer, en las empresas, el principio de proporcionalidad en el cumplimiento de principios básicos y requisitos mínimos para la protección adecuada de la información, brindando un instrumento para facilitar la implantación y aplicación de esquemas para asegurar esta protección, lo cual es una tarea que requiere esfuerzo y coordinación, debe ser planificada y justificada.

Así mismo, al igual que se realiza durante los análisis de riesgos empresariales, una vez recopilada la información de los posibles riesgos en seguridad de la información, MAGERIT orienta el proceso para que se establezcan aquellos de mayor impacto (máximo impacto – máximo riesgo), para determinar la relación de los controles pertinentes para el sistema y que posteriormente deben ser analizados (incluso inspeccionados y certificados por un ente externo) para garantizar el cumplimiento, confiabilidad y desempeño en su aplicación, para la protección responsable de los activos de información de la organización.

MAGERIT, por tanto, implementa el Proceso de Gestión de Riesgos, señalado en estándares como ISO/IEC 31000, pero dentro de un marco de trabajo para que los órganos de Gobierno de TI, tomen decisiones considerando para esto los riesgos derivados de uso de tecnologías de la información, o como se ha mencionado los riesgos informáticos, en términos generales se busca tener:

1. **Un buen gobierno.**
    1.1. Gestionar los riesgos fundamentadas en principios de gobierno para asegurar el establecimiento adecuado de beneficios, costos, riesgos, oportunidades y factores a considerar en la toma de decisiones.
2. **Confianza.**
    2.1. Tener firmeza y claridad en que se responderán los riesgos previstos de una forma adecuada para asegurar la continuidad de servicios y operaciones.
    2.2. Siendo los sistemas de información un factor clave del cumplimiento de objetivos deben generar confianza, evitar fallos y salidas de operación, lo cual implica una definición e inversión importante en mecanismos de continuidad.

3. **Gestión**

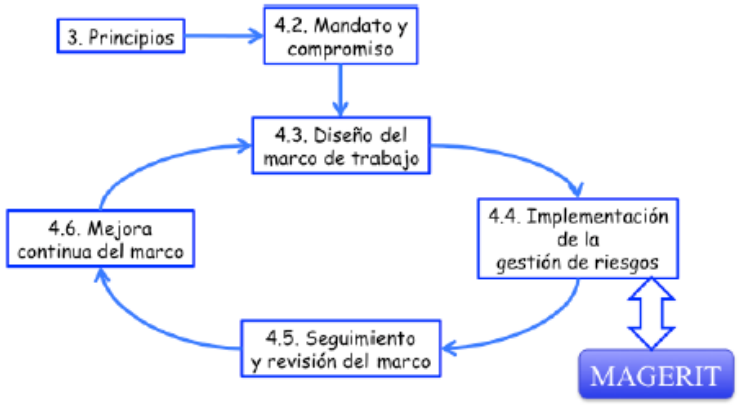
3.1. El riesgo debe ser sometido a elementos de control y trabajo tales como:

3.1.1. Evaluación del riesgo.

3.1.2. Gestión de la seguridad basada en riesgos.

3.1.3. Gestión de riesgos.

A partir de lo anterior MAGERIT responde e implementa el “Proceso de Gestión de Riesgos” dentro de un marco de órganos de gobierno y su marco se trabajo es el siguiente:



Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Objetivos de MAGERIT

Esta metodología persigue los siguientes objetivos:

Directos:

- Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirecto:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Estructura del Submodelo de Procesos de MAGERIT

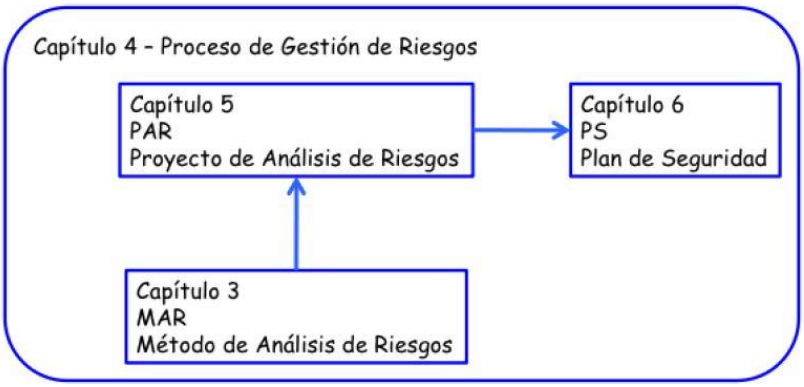
Actualmente se tiene vigente el MAGERIT versión 3, metodología que se organiza en tres libros:

- Libro 1. "Método"
- Libro 2. "Catálogo de Elementos"
- Libro 3. "Guía de Técnicas".

Libro 1. Método

En esta primera parte se ubican los capítulos iniciales de la Gestión de Riesgos, consta de 8 capítulos, el primero de introducción y generalidades, los siguientes contiene:

- El capítulo 2 expone los distintos conceptos informales que se requieren para las actividades de análisis y tratamiento, dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 expone, determina y formaliza las actividades a seguir para el análisis de los riesgos.
- El capítulo 4 incluye la descripción de las opciones y criterios para el tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que se realiza el análisis de riesgos de un sistema.
- El capítulo 6 donde se explican las actividades de los planes de seguridad, denominados por la metodología como planes directores o planes estratégicos.
- El capítulo 7 en el cual se aclara cómo en el desarrollo de sistemas de información y el análisis de riesgos sirve para gestionar la seguridad del producto o sistemas de información terminados, incluyéndose en fases tales como conceptualización, pruebas, o puesta en producción, así como a la protección del propio proceso de desarrollo.
- Por último, el capítulo 8 anticipa algunos problemas que pueden aparecer recurrentemente cuando se realizan análisis de riesgos.



Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Este libro también incluye en sus apéndices materiales diversos tales como:

1. Un glosario de conceptos
2. Referencias bibliográficas relacionadas con el desarrollo la metodología
3. Referencias al marco legal, tareas de análisis y gestión (relativos a la Administración Pública en España)
4. El marco normativo para aspectos de evaluación y certificación
5. Las características de herramientas que puedan soportar el proceso de análisis y gestión de riesgos
6. Una guía comparativa de la evolución de las versiones 1, 2 y 3 de la metodología MAGERTI.

Libro 2. Catálogo de Elementos

SALVAGUARDA: "GUARDA QUE SE PONE PARA LA CUSTODIA DE UNA COSA, COMO PARA LOS PROPIOS DE LAS CIUDADES, VILLAS, LUGARES Y DEHESAS COMUNES Y PARTICULARES, Y PARA LOS EQUIPAJES EN LOS EJÉRCITOS", "CUSTODIA, AMPARO, GARANTÍA". (Real Academia Española, 2020)

Este segundo libro asociado a la metodología MAGERIT señala una serie de pautas, asociadas a la Gestión de Riesgo de Información, donde establecer aspectos clave relacionados con el tratamiento de los siguientes temas:

- Los tipos de activos
- Las dimensiones de valoración de activos
- Los criterios de valoración de activos
- Las amenazas típicas en las organizaciones asociadas a los sistemas de información y la Gestión de los sistemas de información
- Las salvaguardas a considerar para proteger sistemas de información

En esta segunda parte se busca cumplir dos objetivos primordiales:

1. Establecer las recomendaciones para facilitar la labor de las personas que desarrollan Proyectos de TI, ofreciéndoles los elementos estándar a los que puedan acudir o aplicar de forma rápida, para concentrarse en específico del sistema objeto del análisis.
2. Estandarizar los resultados de los análisis de riesgos, promoviendo una terminología y criterios uniformes o estandarizados que permitan comparar e incluso integrar los análisis realizados por diferentes equipos.

Este catálogo busca proporcionar a las organizaciones o empresas una base de datos amplia sobre los riesgos y establecer datos para conocimiento que incorporen puntos de partir para el avance rápido de procesos de gestión de riesgos que recién inicien en un proceso, departamento, sistema de información o proyecto de sistemas de información.

Libro 3. Guía de Técnicas

Este tercer elemento de la metodología MAGERIT incluye una serie de guías técnicas que pueden o son empleadas de forma habitual sobre los proyectos de análisis y gestión de riesgos, entre estas técnicas expone elementos tales como:

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones
- Valoración Delphi

Más en específico este documento de la metodología ofrece un material de consulta o guía de consulta, para que puedan ser abordadas al momento de realizar tareas o acciones específicas durante en análisis o gestión de riesgos. Se señala como una serie de recomendaciones introductorias o de referencia que permiten al encargado de la gestión una base sobre la cual profundizar.

Esquema de Etapas y Actividades del Submodelo

Dentro de las etapas señaladas por MAGERIT para la gestión de riesgos tenemos:

Fuente: Elaboración propia

Visión de conjunto

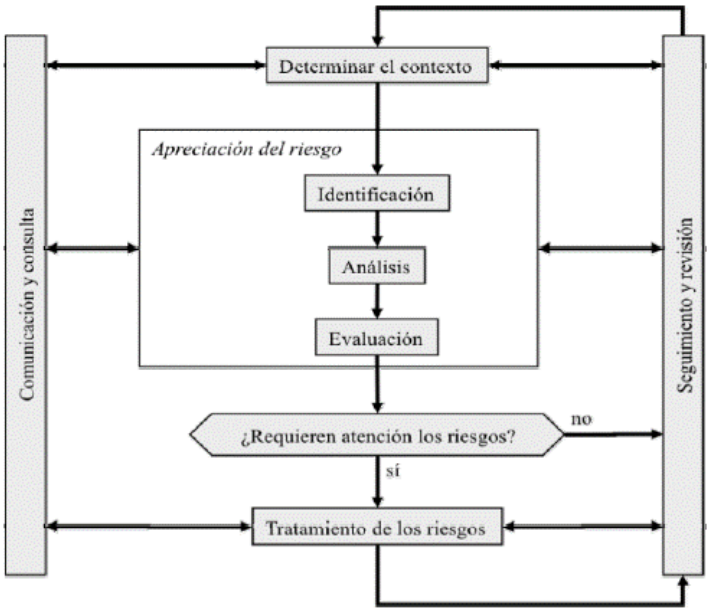
Implica dos grandes tareas el análisis de riesgos y el tratamiento de riesgos.

Análisis de Riesgos

- Busca estimar qué tiene la organización y qué podría pasar
- Considera análisis de activos y elementos de los sistemas de información
- Analiza las amenazas y perjuicios para la organización
- Considera las salvaguardas
- Estima el impacto y probabilidad del riesgo
- Permite un anolis metódico de riesgos e incorpora la gestión de seguridad de los sistemas de información

Tratamiento de riesgos

Propone seguir un esquema de trabajo tal como:



Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Acorde con MAGERTI, en este esquema deben aplicarse procesos para:

1. **Determinar el contexto:** Determinación de parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos.
2. **Identificar riesgos:** Buscando determinar la relación de los posibles puntos de peligro.
3. **Analizar los riesgos:** Lo cual permite calificar los riesgos identificados, cuantificando sus consecuencias (análisis cuantitativo), o bien ordenando su importancia relativa (análisis cualitativo).
4. **Evaluar los riesgos:** En este paso se requiere profundizar sobre los análisis técnicos y establecer o traducir las consecuencias a términos de negocio.
5. **Tratar los riesgos:** Este proceso busca determinar y recopilar las actividades encaminadas a modificar la situación de riesgo.
6. **Comunicación y consulta.** La metodología también incorpora los sistemas de información como un elemento de soporte de la productividad de la Organización, el cual debe ser seguro, pero no al extremo de intervenir en la productividad e incorporan elementos tales como:

   6.1. Los usuarios de un sistema de información como un elemento a evaluar.

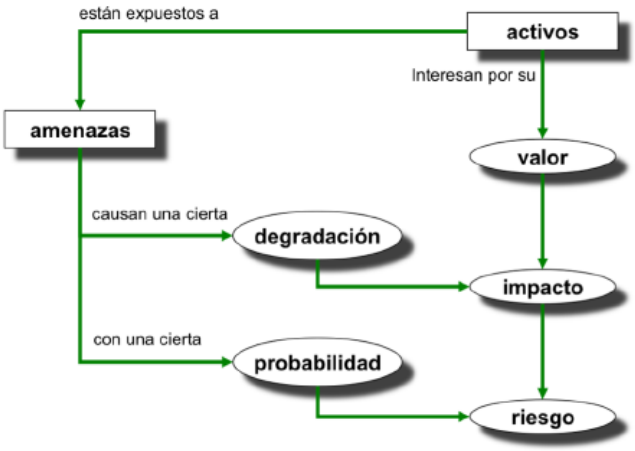
   6.2. Los proveedores externos y socios de negocio.

   6.3. Los órganos de gobierno y reguladores
7. **Seguimiento y revisión:** Debe ser constante, consecuente y comprobada, la gestión de seguimiento y revisión no debe tomarse a la ligera.

Método de análisis de riesgos

Este método es una aproximación metódica para determinar el riesgo siguiente pautas:

1. Determinar activos relevantes de la organización (relaciones, valor, prejuicio, coste)
2. Determinar amenazas y exposición de activos
3. Determinar salvaguardas y niveles de eficacia
4. Estimar impacto
5. Estimar niveles de riesgo. Los elementos del análisis de riesgos potenciales son:

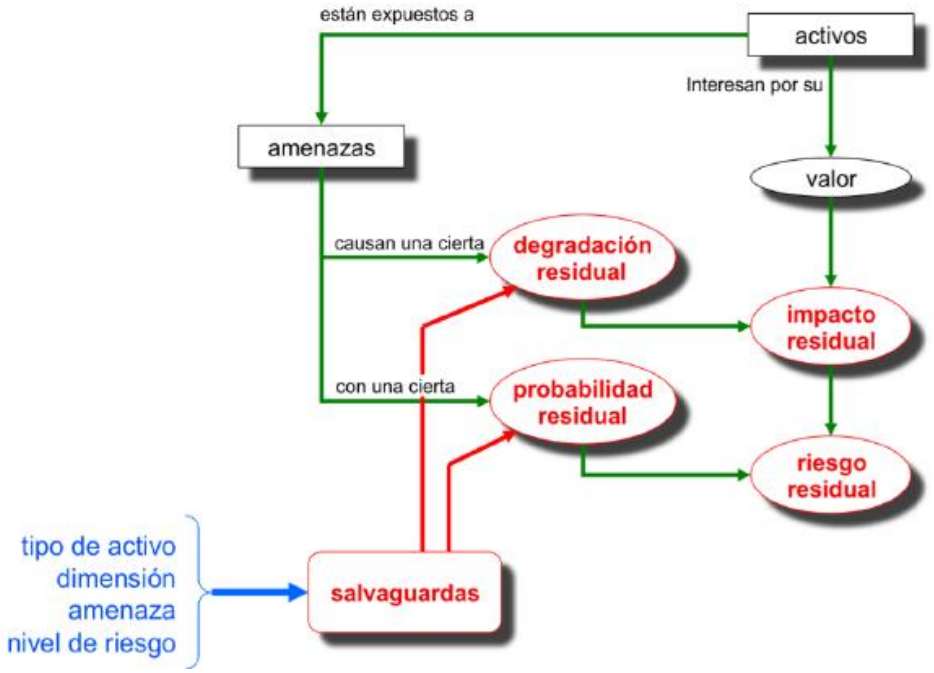


Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Este proceso requiere ejecutar una serie importante de pasos:

- Paso 1. Activos. Identificar componentes o funcionalidades de los Sistemas de Información, incluyendo datos, servicios de TI, aplicaciones informáticas (software), equipos informáticos (hardware), soportes de información o dispositivos de almacenamiento de datos, equipamiento auxiliar, redes de comunicaciones, instalaciones, equipos informáticos y de comunicaciones, personas. Dependiendo del tipo de activo, es susceptible a ser atacado con consecuencias para la organización. Su análisis debe incluir
    - Dependencias entre activos, activos esenciales, servicios internos, equipamiento informático y todas sus comunicaciones.
    - Valoración. Un activo interesa por lo que vale. Se requiere respetar la homogeneidad y la relatividad (valor relativo).
    - Dimensiones. Confidencialidad, Integridad y disponibilidad. Incluyen la revisión de autenticidad, trazabilidad de uso, trazabilidad de acceso.
    - Evaluar la “salud” de los activos. Coste de reposición, adquisición, instalación, mano de obra, lucro cesante, operaciones, sanciones por incumplimiento de leyes o SLA, daño a personas, daño a otros activos.

  - Una adecuada valoración cualitativa del activo.
  - Una adecuada valoración cuantitativa del activo, incluyendo valorar si vale la pena invertir en salvaguardas, optimización, evaluaciones de retorno de inversión.
  - Valorar el coste de la interrupción del servicio en términos de lucro cesante o pérdidas de negocio.
- Paso 2. Amenazas. Causa potencial de un incidente que cause daño a un sistema de información o a un activo, lo cual incluye procesos para:
  - Identificación de las amenazas. De origen natural, del entorno, defectos de las aplicaciones, causadas por las personas de forma accidental o deliberada.
  - Valoración de las amenazas: Afectación de un activo cuando es víctima de una amenaza, valora su degradación, probabilidad, daño causado
- Paso 3. Determinación del impacto potencial. Daño sobre el activo derivado de la materialización de una amenaza, incluyendo aspectos residuales por la dependencia entre activos. Incorpora procesos como:
  - Impacto acumulado. Según la dimensión y valoración del activo.
  - Impacto repercutido. Valor propio del activo y amenaza sobre otros activos dependientes que son expuestos.
  - Agregación de valores de impacto. Suma del impacto acumulado, el impacto repercutido y cualquier otro activo dependiente entre sí.
- Pago 4. Determinación del riesgo potencial. Medida del daño probable sobre un sistema. Al igual que el proceso anterior incorpora la evaluación del.
  - Riesgo acumulado sobre el activo debido a la amenaza.
  - Riesgo repercutido.
  - Agregación de riesgos
- Paso 5. Salvaguardas. Son las contramedidas, procedimientos y mecanismos tecnológicos que reducen el riesgo. Este proceso incluye:
  - Selección de salvaguardas. Por tipo de activos a proteger, según la dimensión de seguridad requerida, según el nivel de las amenazas, salvaguardas alternativas. Pueden priorizarse para el tratamiento del riesgo mayor al menor, por probabilidad o por impacto.
  - Efecto de las salvaguardas. Sus efectos deben evaluar si, reducen la probabilidad de las amenazas. Limitando el daño causado. Sin embargo, implican un análisis de riesgo residual para evitar abrir nuevas amenazas de seguridad.



Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

- Tipos de protección. Los tipos de protección son las posibles respuestas a las salvaguardas o contramedidas y por lo general se clasifican como:
  - [PR] Prevención. Son preventivos y reducen la oportunidad de un incidente ocurra.
  - [DR] Disuasión. Tiene un efecto tal sobre los atacantes que estos no se atreven o piensan varias veces el ataque.
  - [EL] Eliminación. Elimina un incidente cuando impide que tenga lugar.
  - [IM] Minimización del impacto. Limita el impacto cuando acota las consecuencias del incidente.
  - [CR] Corrección. Repara el daño producido.
  - [RC] Recuperación. Permite regresar al estado anterior al incidente.
  - [MN] Monitorización. Monitorea lo que ha ocurrido y lo que está ocurriendo.
  - [DC] Detección. Detecta e informa cuando un ataque está ocurriendo
  - [AW] Concientización. Actividades de formación de las personas con nexos al sistema y que ejercen influencia sobre él.
  - [AD] Administración. Componentes de Seguridad el sistema.
- Eficacia de la protección. Evalúan la eficacia de la salvaguarda frente al riesgo,

si es técnicamente idónea, si se emplea siempre, si es desplegada, configurada y mantenida correctamente.

- Vulnerabilidades: Es toda debilidad aprovechada por una amenaza, tanto en el activo como en sus medidas de protección.

- Paso 4. Impacto residual. La magnitud de degradación tomando en cuenta la eficacia de las contramedidas y es la proporción que resta entre la eficacia perfecta y la eficacia real, puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

- Paso 5. Riesgo residual. El sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

Formulación de actividades.

Para todo lo anterior se propone una etapa de formulación de actividades, en la cual se busque:

- *"Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.*
- *Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.*
- *Levantar un conocimiento de la situación actual de salvaguardas.*
- *Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salva-guardas), como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).*
- *Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).".* (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Para su operacionalización se requiere definir características tales como:

- Caracterización de los activos
- Caracterización de las amenazas
- Caracterización de las salvaguardas.
- Estimación del estado de riesgo.

Documentación

Para todos estos procesos se propone a nivel de MAGERIT la documentación de varias formas.

- Documentación intermedia
  - Resultados de entrevistas,
  - Fuentes, estadísticas, observaciones
  - Información reutilizable
  - Documentación auxiliar
- Documentación final
  - Modelo de valor
  - Mapa de riesgos
  - Declaración de aplicabilidad
  - Evaluación de salvaguardas
  - Informa insuficiencias o vulnerabilidades

Proceso de gestión de riesgos

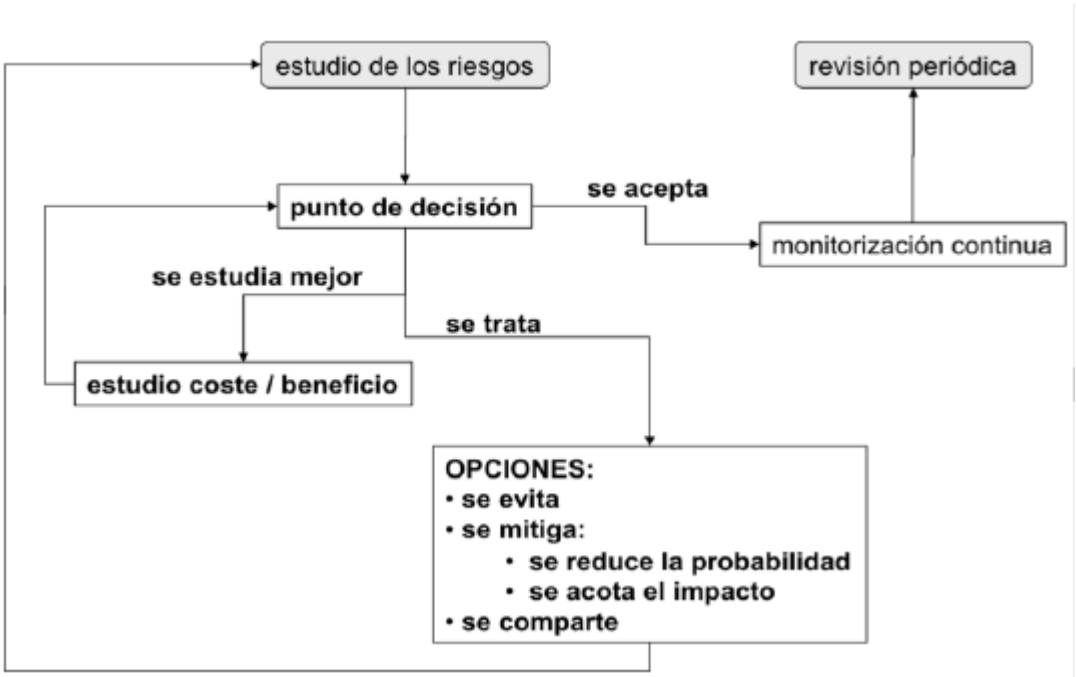
Lo que propone la metodología es analizar una serie de factores y dimensiones asociados con:

- la gravedad del impacto y/o del riesgo
- las obligaciones a las que por ley esté sometida la empresa
- las obligaciones a las que por reglamentos sectoriales esté sometida la organización
- las obligaciones a las que por contrato esté sometida la empresa

Cada riesgo se clasifica como:

- **Crítico. R**equiere atención urgente
- **Grave.** Requiere atención
- **Apreciable.** Pueda ser objeto de estudio para su tratamiento.
- **Asumible.** No se van a tomar acciones para atajarlo, esta aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia

Lo anterior implica la ejecución del siguiente proceso de gestión de riesgos:

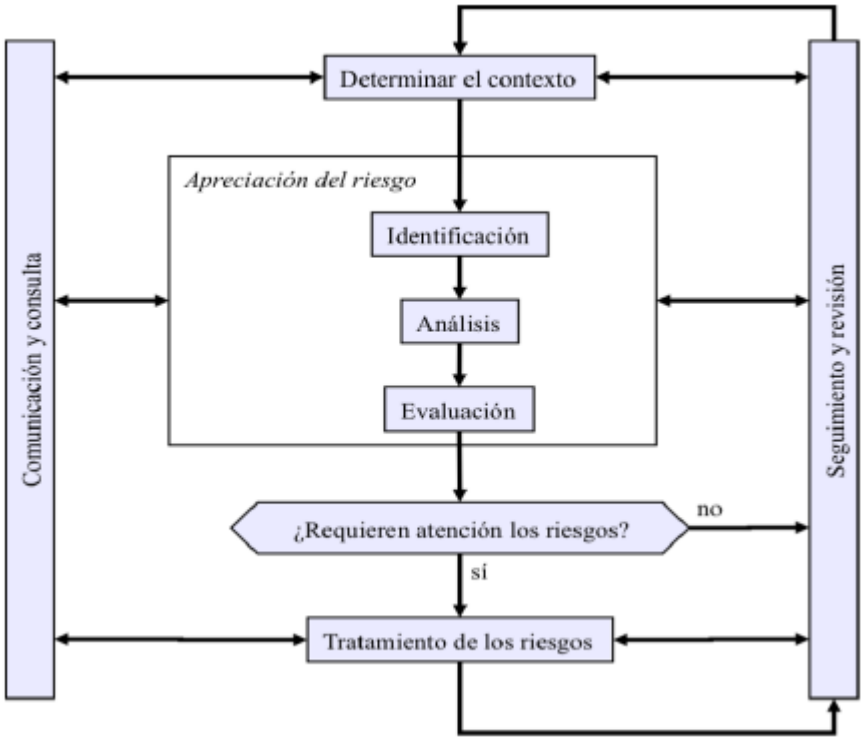


Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Todos estos aspectos se desarrollan por secciones, cada cual incorporando documentación a la gestión de riesgo según su relevancia:

- Proceso de Evaluación: interpretación de los valores de impacto y riesgo residuales
- Proceso de Aceptación del riesgo
- Proceso de Tratamiento del riesgo
- Estudio cuantitativo de costes / beneficios
- Estudio cualitativo de costes / beneficios
- Estudio mixto de costes / beneficios
- Opciones de tratamiento del riesgo: eliminación
- Opciones de tratamiento del riesgo: mitigación
- Opciones de tratamiento del riesgo: compartición
- Opciones de tratamiento del riesgo: financiación

Formalización de las actividades



Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Para MAGERIT esto implica la definición de los responsables, para lo cual se requiere la definición de:

- Roles y funciones
  - Órganos de gobierno
  - Dirección ejecutiva
  - Dirección operacional
- Esquema Nacional de Seguridad
  - Responsable de la información
  - Responsable del servicio
  - Responsable de la seguridad
  - Responsable del sistema
  - Administradores y operadores

Aunado a lo anterior es necesaria la definición de la matriz de Responsabilidades conocida como Matriz RACI (Responsable, Aprobador, Consultado, Informado)

	rol	descripción
R	Responsible	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	Accountable	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	Consulted	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	Informed	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tarea	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
aceptación del riesgo residual	I	A	A	R	I	
implantación de las medidas de seguridad		I	I	C	A	R
					C	R

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Otros de los aspectos que se recomienda incluir en el proceso de gestión de riesgos es la definición de:

- Contexto. Tratamiento de datos personales, clasificación, propiedad intelectual, etc.
- Criterios. Requisitos de seguridad de la información, disponibilidad de servicios.
- Evaluación de los riesgos. Siguiendo la metodología.
- Decisión de tratamiento. Eliminar, reducir, implantar, externalizar, aceptar.
- Comunicación y consulta a interesados, gobierno, reguladores.
- Seguimiento y revisión.

Proyectos de análisis de riesgos

Al igual que lo proponen los estándares de gestión de proyectos, cuando se realiza un análisis de riesgos se necesita de una serie de recursos apreciables y conviene planificar estas actividades dentro de un proyecto, sea interno o se sub-contrate a una consultora externa. La metodología MAGERIT implica considerar al menos las:

- Actividades preliminares

    - Estudio de oportunidad
    - Determinación del alcance del proyecto
    - Planificación del proyecto
    - Lanzamiento del proyecto
    - Estudio de oportunidad
- Elaboración del análisis de riesgos
- Comunicación de resultados
- Control del proyecto
    - Hitos de control
    - Documentación resultante (intermedia y final)

Se promueve en primer lugar la definición de roles y funciones, en las cuales se establezcan los siguientes equipos:

- Comité de seguimiento
- Equipo de proyecto
- Grupos interlocutores
- Promotor
- Director de Proyecto
- Enlace operacional

Plan de seguridad

MAGERIT promueve llevar acabo planes de seguridad, entendiendo como tales a los proyectos para materializar las decisiones adoptadas para el tratamiento de riesgo:

- Plan de mejorar de la seguridad
- Plan Director de Seguridad
- Plan Estratégico de Seguridad
- Plan de Adecuación

Para lo anterior se propone a ejecución de un primer plan de seguridad que genere la identificación de proyectos de seguridad, una segunda tarea que genera el plan de ejecución y por último se realice la ejecución, MAGERIT nos resume:

Tarea 1: Identificación de proyectos de seguridad

PS: Plan de seguridad *PS.1: Identificación de proyectos de seguridad*
Objetivos • Elaborar un conjunto armónico de programas de seguridad
Productos de entrada • Resultados de las actividades de análisis y tratamiento de riesgos • Conocimientos de técnicas y productos de seguridad • Catálogos de productos y servicios de seguridad
Productos de salida • Relación de programas de seguridad
Técnicas, prácticas y pautas • Planificación de proyectos
Participantes • El equipo de proyecto • Especialistas en seguridad • Especialistas en áreas específicas de seguridad

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Tarea 2: Planificación de los proyectos de seguridad

PS: Plan de seguridad *PS.2: Plan de ejecución*
Objetivos • Ordenar temporalmente los programas de seguridad
Productos de entrada • Resultados de las actividades de análisis y tratamiento de riesgos • Resultados de la tarea PS.1 Programas de seguridad
Productos de salida • Cronograma de ejecución del plan • **Plan de Seguridad**
Técnicas, prácticas y pautas • Análisis de riesgos (ver "Método de Análisis de Riesgos") • Planificación de proyectos
Participantes • Departamento de desarrollo • Departamento de compras

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Tarea 3: Ejecución del plan

PS: Plan de seguridad *PS.3: Ejecución*
Objetivos • Alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado
Productos de entrada • Resultados de las actividades PS.1 (proyectos de seguridad) y PS.2 (planificación) • Proyecto de seguridad que nos ocupa
Productos de salida • Salvaguardas implantadas • Normas de uso y procedimientos de operación • Sistema de indicadores de eficacia y eficiencia del desempeño de los objetivos de seguridad perseguidos • Modelo de valor actualizado • Mapa de riesgos actualizado • Estado de riesgo actualizado (impacto y riesgo residuales).
Técnicas, prácticas y pautas • Análisis de riesgos (ver "Método de Análisis de Riesgos") • Planificación de proyectos
Participantes • El equipo de proyecto: evolución del análisis de riesgos • Personal especializado en la salvaguarda en cuestión

Fuente: (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Desarrollo de sistemas de información

Siendo las aplicaciones y sistemas de información un activo intangible de las organizaciones, cuya relevancia se ha venido acrecentando con las tendencias de transformación digital y la industria 4.0, el tratamiento de la información y por tanto de su desarrollo debe formar parte de la gestión integral de riesgos, la metodología promueve la incorporación durante la fase de desarrollo, las funciones y mecanismos que refuercen la seguridad del sistema, del proceso de desarrollo y así se asegure la consistencia y seguridad vigente, al incorporar los sistemas. Por tanto, la seguridad se aplica en las actividades relacionadas con la propia seguridad del sistema de información y con las actividades que velan por la seguridad del proceso de desarrollo del sistema de información.

Como principios básicos se promueven los siguientes:

- ***"Artículo 5. La seguridad como un proceso integral.***

  1. La seguridad se entenderá como un proceso integral constituido por todos los

elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. *Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.*

- ***Artículo 6. Gestión de la seguridad basada en los riesgos.***

1. *El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.*
2. *La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.*

- ***Artículo 9. Reevaluación periódica.***

1. *Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario." Fuente:* (Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012)

Iniciación de los procesos

Durante la iniciación deben considerarse los factores de riesgos y de seguridad que deben incorporarse en:

- Nuevos servicios y/o datos.
- Evolución tecnológica de los sistemas de información, sistemas operativos, arquitectura tecnológica como bases de datos, servidores de aplicaciones, servicios en la nube y otros.
- Modificación de la calificación de seguridad de servicios o datos.
- Consideración de nuevas amenazas.
- Modificación de los criterios de calificación de riesgos

Seguridad del sistema de información

El análisis de riesgos debe basar sus estimaciones de impacto y riesgo en la realidad de los sistemas, concretada en sus activos. En consecuencia, se puede entender el modelo de valor como evolutivo, recogiendo en cada momento el nivel de detalle de que se dispone. Magerit, como metodología, permite un tratamiento sistemático y homogéneo que es esencial para poder comparar opciones alternativas y para gestionar la evolución de los

sistemas, para lo cual deben considerarse todos los aspectos del ciclo de vida de las aplicaciones, dependiendo de si se aplican metodologías tradicionales de desarrollo, metodologías ágiles, DevOps, microservicios y otros estándares. Por ejemplo, en la metodología tradicional debemos considerar:

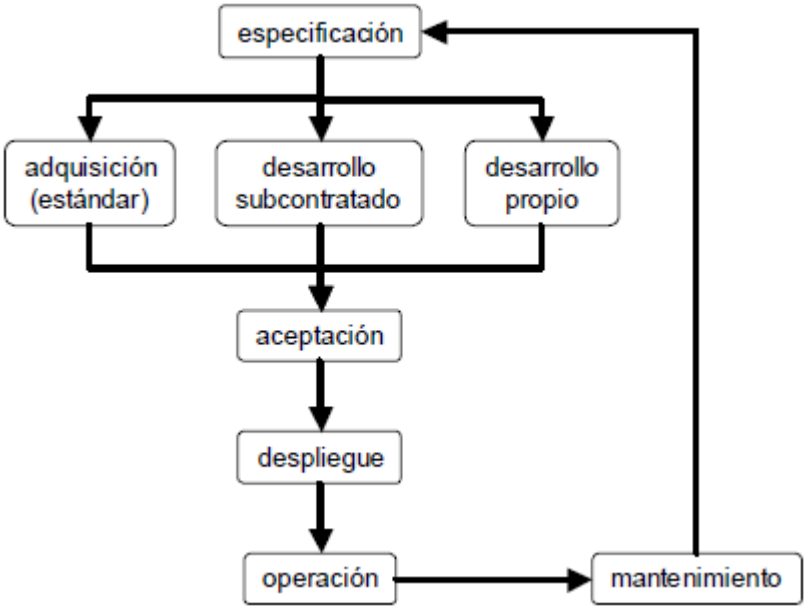


Diagrama. Ciclo de vida tradicional

En este ejemplo, deben analizarse aspectos de seguridad en cada una de las etapas del ciclo de vida, tales como: Especificación. Adquisición o desarrollo. Aceptación. Despliegue. Operación. Mantenimiento. Para lo cual MAGERIT propone, en resumen:

- Analizar el contexto, políticas de seguridad, normas, requisitos normativos, obligaciones contractuales, criterios de valoración y aceptación del riesgo.
- Fase de especificación, evaluar la seguridad durante el modelado de datos y su adquisición.
- Fase de diseño: estudio de opciones de seguridad. Análisis y tratamiento de los riesgos
- Soporte al desarrollo: puntos críticos, riesgos de la actividad, mecanismos para procesar registros, disparo de alarmas.
- Aceptación y puesta en marcha: puntos críticos, selección de datos de prueba, pruebas funcionales con simulación de ataques, pruebas de carga e intrusión, inspección de servicios y código, análisis de fugas de información, puertas traseras de acceso, desbordamiento de registros.
- Operación: análisis y gestión dinámicos, evaluación de nuevas amenazas, vulnerabilidades sobrevenidas, incidentes de seguridad, cambios en la utilización del sistema.

- Ciclos de mantenimiento: análisis marginal.
- Terminación, protección del valor de la información generada, claves criptográficas y de autenticación extraídas del ambiente productivo y migradas al ambiente de desarrollo, datos de operaciones
- Documentación de seguridad

Seguridad en el proceso de desarrollo:

- Datos que se manejan:
    - Especificaciones y documentación de los sistemas
    - Código fuente
    - Manuales del operador y del usuario
    - Datos de prueba
    - Entorno software de desarrollo:
        - herramientas de tratamiento de la documentación: generación, publicación, control de documentación, etc.
        - herramientas de tratamiento del código: generación, compilación, control de versiones, etc.
    - El entorno hardware de desarrollo: equipos centrales, puestos de trabajo, equipos de archivo, etc.
    - Entorno de comunicaciones de desarrollo
    - Instalaciones
    - Personal involucrado: desarrolladores, personal de mantenimiento y usuarios (de pruebas)

Consejos prácticos

MAGERIT promueve la practicidad de los procesos de seguridad y el escalonamiento por medio de seguimiento y control, de forma que se vaya madurando el modelo y prácticas que en principio pueden resultar un poco abstractas para los involucrados, por lo cual recomienda el establecimiento de catálogos de elementos, tipos de activos, dimensiones de valoración, guías prácticas sobre riesgos, valoración, amenazas, salvaguardas (y catálogos de estas últimas). Adicionalmente presenta recomendaciones importantes en temas tales como:

- Alcance y profundidad. Se requiere determinar criterios máximos de interés de los usuarios y del equipo de seguridad para concentrar esfuerzos.
- Analizar activos críticos, medidas generales, salvaguardas de mayor interés, detalles

cualitativos o cuantitativos que logren reducir gastos elevados.

- Identificar activos tangibles e intangibles de sumo interés por el valor de los recursos, servicios e información soportados en estos.
- Descubrir y modelar las dependencias entre los activos como para de las arquitecturas de negocio, sistemas e información.
- Establecer los errores típicos y lecciones aprendidas.
- Evaluar de forma periódica los modelos de trabajo, las dependencias modeladas y los factores de mayor interés.
- Analizar el tratamiento de datos personales, ya que por lo general están tipificados por leyes y reglamentos de protección.
- Analizar e identificar de forma periódica amenazas, salvaguardas y aproximaciones, incluso previendo o validando movimientos futuros de la información y de los recursos TIC.
- Mantener actualizados los esquemas de protección, incluso los de protección básica como lo señalan las normas y mejores prácticas de administración de recursos de TI.

Conclusiones y recomendaciones

Al finalizar el presente estudio sobre la metodología MAGERIT podemos concluir cómo la gestión de riesgos informáticos debe establecerse dentro de las operaciones y estrategia de los negocios y dentro de los marcos de Gobierno de las Tecnologías de la Información como aspectos de suma relevancia para el aseguramiento de la información de las organizaciones, su constante evaluación desde la perspectiva de vulnerabilidad y para el establecimiento de condiciones de respuesta y de gestión, acorde con los niveles de automatización, dependencia de la tecnología y regulación que ejerzan una inferencia directa en las organizaciones y por tanto en las actividades de las áreas de Tecnología de la Información y Comunicación.

El estudio de estas condiciones prepara al estudiante para enfrentarse con un vector diferenciado de las TIC, pero que con la evolución de la tecnología, tendencias de digitalización de servicios y empresas, lo vuelve un conocimiento indispensable y brinda también un factor diferenciador para el desempeño futuro como profesional en las Tecnologías de la Información, lo cual por medio de la Universidad San Marcos busca posicionar al estudiante como un profesional que sea requerido y solicitado en el mercado laboral.

Para mejorar los conceptos asociados a MAGERIT es importante que el estudiante amplíe los conocimientos mediante la lectura del documento adjunto:

- 2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.

Referencias bibliográficas

- Baca Urbina, G. (2016). *Introducción a la Seguridad Informática* (Primera ed.). México: Grupo Editorial Patria. Obtenido de https://elibro.net/es/ereader/usanmarcos/40458
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT Versión 3.0. Metodología de análisis y gestión de riesgo de los sistemas de información.* Madrid: Gobierno de España.
- ISACA®. (2012). *Cobit 5. Procesos Catalizadores.* Estados Unidos: ISACA.
- LaRepublica.Net. (20 de 02 de 2020). *LaRepublica.net*. Obtenido de https://www.larepublica.net/noticia/costa-rica-registro-casi-32-millones-de-intentos-de-ciberataques-en-primeros-tres-meses
- López, L. F. (2018). *Análisis de riesgos informáticos. Eje 1. Conceptualicemos.* Fundación Universitaria del Área Andina.
- Madrigal Chaves, W. (2019). *SUWA Universidad San Marcos, Repositorio.* Obtenido de http://repositorio.usam.ac.cr/xmlui/
- Real Academia Española. (12 de 12 de 2020). *Diccionario de la Lengua Española*. Obtenido de https://dle.rae.es/
- Red Global de Conocimientos en Auditoría y Control Interno. (01 de 01 de 2021). *www.Auditool.com*. Obtenido de https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque
- Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alcoy - Alicante, España: Editorial Área de Innovación y Desarrollo,S.L. doi:http://dx.doi.org/10.17993/IngyTec.2018.46
- UNICEM. (22 de 12 de 2020). *El Modelo OSI*. Obtenido de http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica