ENISE

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

INTECO

Instituto Nacional de Tecnologías de la Comunicación

Modelo Unificado de Análisis de Riesgos de Seguridad Física y Lógica

T22: Contenidos mínimos de los Planes Estratégicos Sectoriales

Enrique Bilbao Lázaro

Responsable de Producción

Cuevavaliente Ingenieros

cuevavaliente ingenieros

Índice

Introducción

Metodología particular y concreta de Análisis de Riesgos que permite unificar dos metodologías de análisis de riesgos tradicionalmente independientes: riesgos lógicos y riesgos físicos.

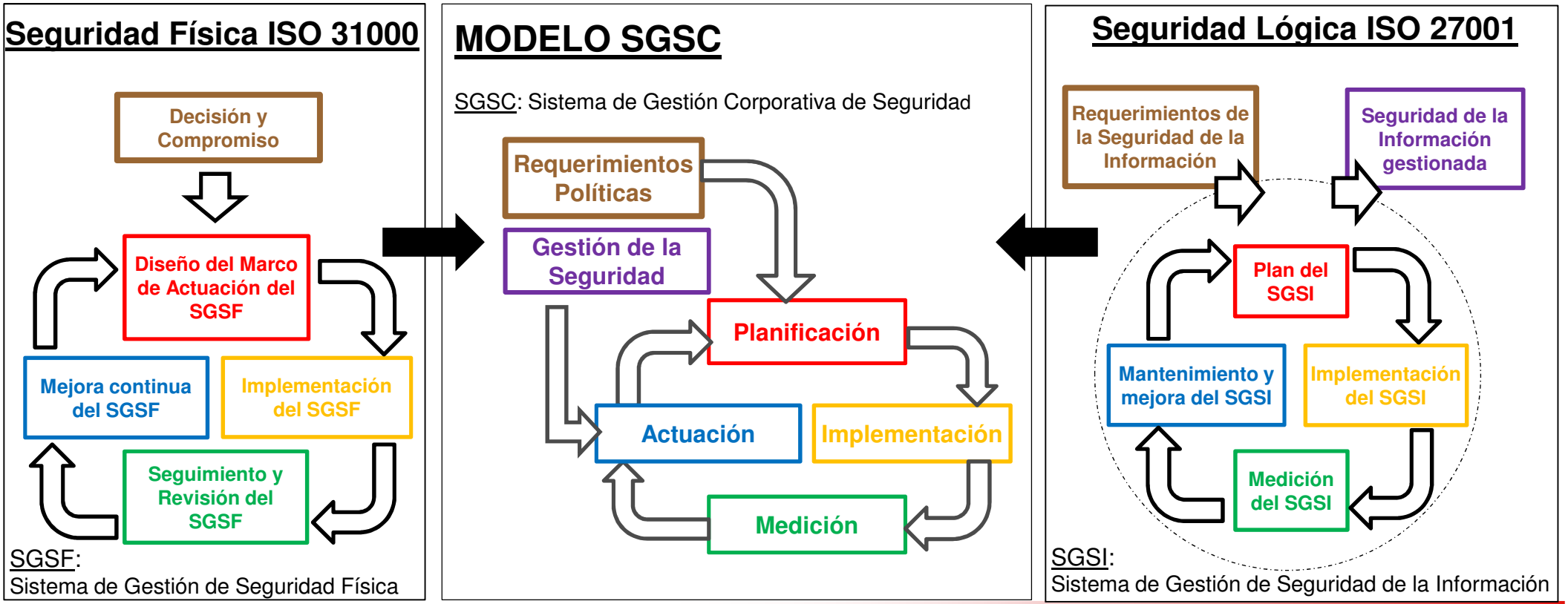
Cumple con los estándares ISO 31000 e ISO 27001, lo que permite usar terminología común y el mismo ciclo de vida de gestión de riesgos

Resuelve problemas muy habituales como son:

- Consideraciones opuestas de cuáles son los activos a proteger y su entorno
- Diferencias en los pasos a seguir
- Distintas normas y mejores prácticas sobre los que basar el proceso
- Nomenclatura y vocabulario diferente
- Métodos de evaluación y consecuencias a medir diferentes

Fundamento normativo de la metodología

Esta metodología se ajusta al marco normativo de ISO 27001 para la gestión de Riesgos de Seguridad Lógica, y de ISO 31000 para la gestión de riesgos de Seguridad Física. Se emplea un modelo único que surge de la unión de ambos: el modelo SGSC (modelo del Sistema de Gestión Corporativa de Seguridad)



Bases de la Metodología

Metodología basada en la confluencia de dos metodologías maduras de Análisis de Riesgos que son específicas para cada sector:

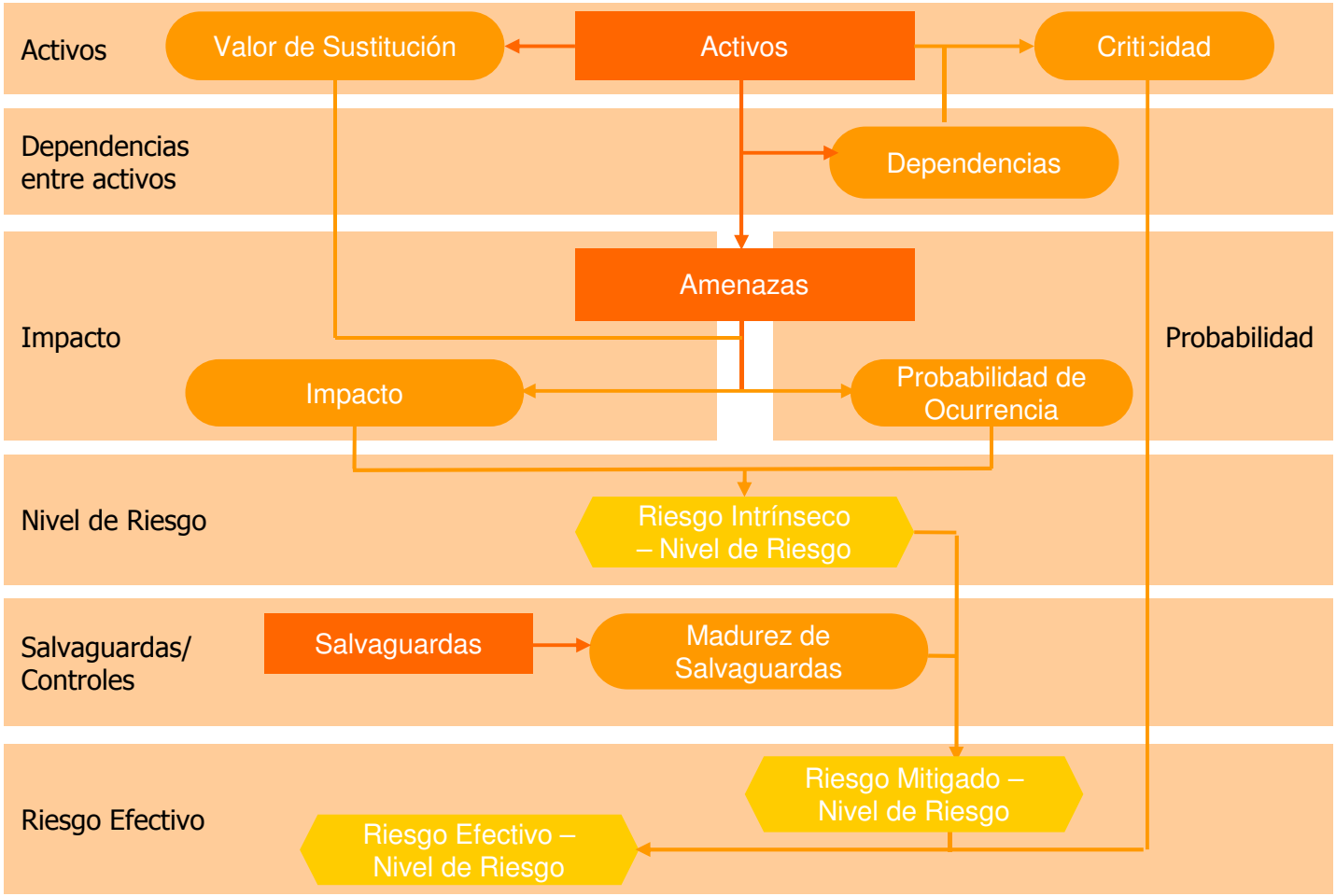
- **Seguridad Física**: metodología propia de Cuevavaliente, basada en ISO 31000, e implementada a través de herramientas software propias. También se utilizan algunos aspectos y recomendaciones del estándar AS/NZS 4360 [8] y su addendum en forma de guía: “Risk Management Guidelines”.

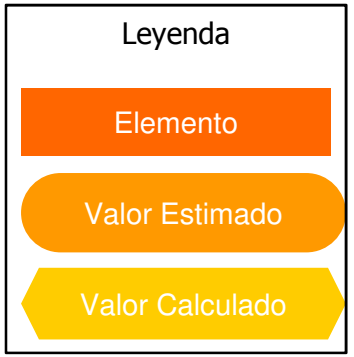
- **Seguridad Lógica**: MAGERIT II. Desarrollada por el Consejo Superior de Administración Electrónica (CSAE). La metodología MAGERIT II pretende dar respuesta a la dependencia que tiene la Administración de las tecnologías de la información para el cumplimiento de su misión.

Gestión de ambos riesgos en un mismo proceso en el que amenazas y activos comparten indicadores y criterios, permitiendo su comparación y evaluación conjunta.

3 – Fundamentos de la Metodología

Aspectos adoptados de Magerit II





PASOS A SEGUIR:

1. Determinar activos
2. Determinar amenazas
3. Estimar Impactos/probabilidad
4. Estimar el coste/criticidad
5. Estimar madurez de salvaguardas
6. Cálculo de los riesgos

Aspectos adoptados de Magerit II

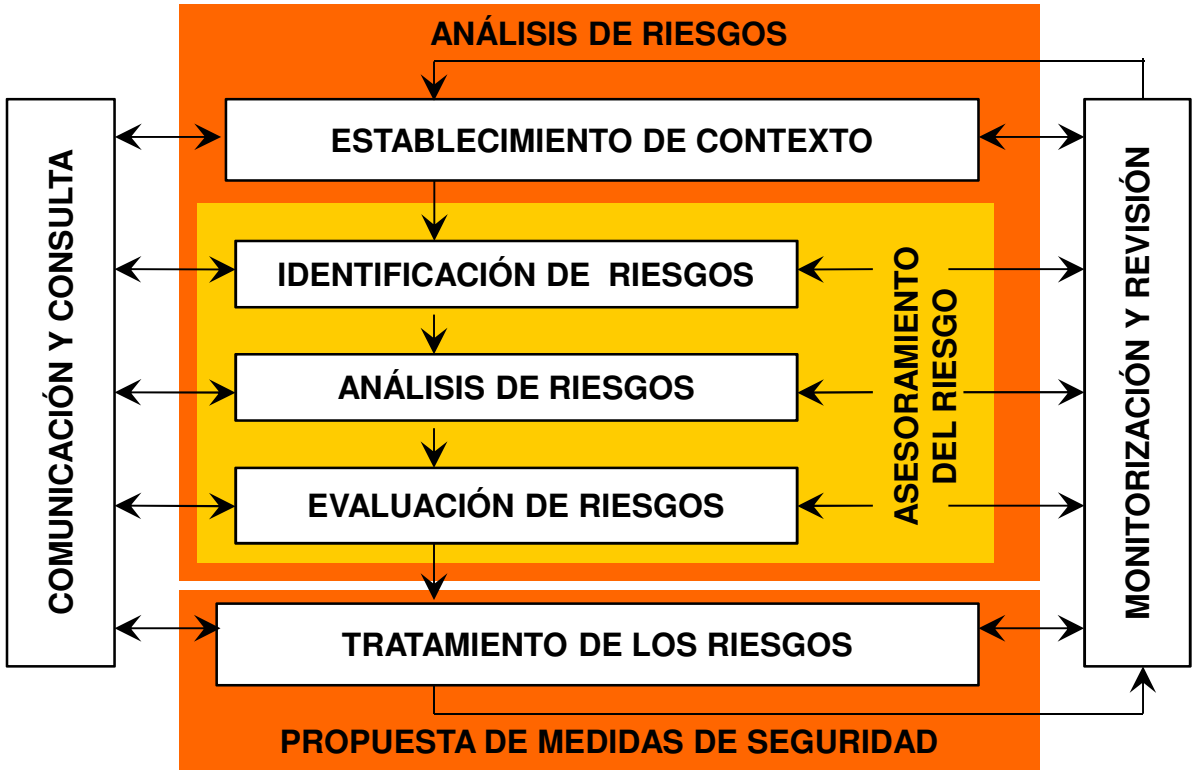
La metodología propuesta tiene en cuenta estas etapas, aunque las agrupa según la estructura del estándar ISO 31000.

El método propuesto por MAGERIT II da cumplimiento en lo establecido en:

- **ISO 27005, epígrafe 4.2.1.d**, "Identificar Riesgos"
- **ISO 27005, epígrafe 4.2.1.e**, "Analizar y Evaluar Riesgos"
- **ISO 27001/2005**, "Sistemas de Gestión de Seguridad de la Información"
- **ISO 27002/2005**, 2005 "Manual de Buenas Prácticas de Gestión de Seguridad de la Información"
- **ISO 27005/2008**, "Gestión de Riesgos de Seguridad de Información"
- **ISO 15408-1/2009** , "Criterios de Evaluación de Seguridad de la Información"

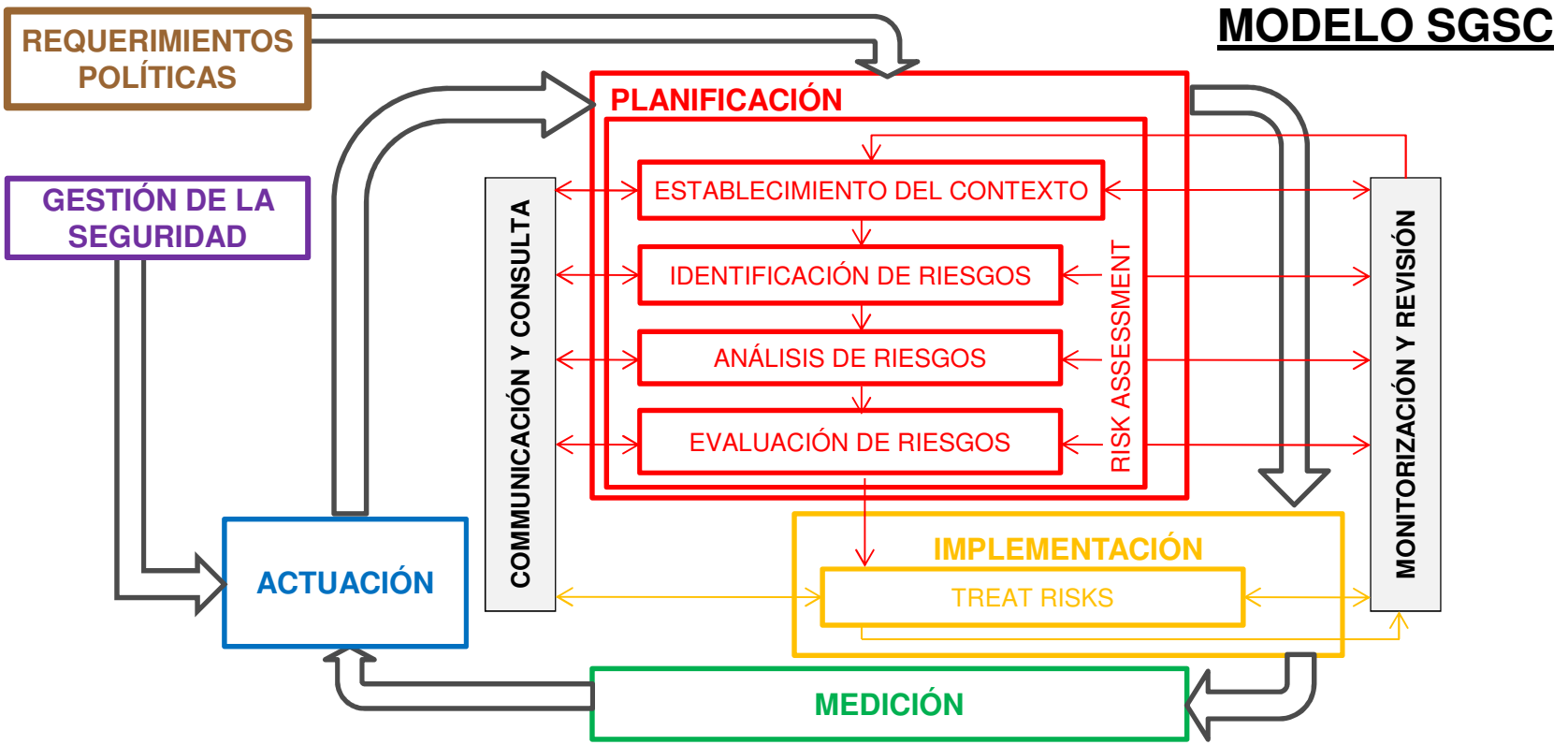
Aspectos adoptados de las Normas ISO 31000 y AS/NZS 4360

Adopción de las etapas definidas por las normas ISO 31000 y AS/NZS 4360, para una correcta gestión de los riesgos y su relación para un continuo proceso de mejora.



Aspectos adoptados de las Normas ISO 31000 y AS/NZS 4360

Las etapas referidas por las normas son asumidas por los dos conjuntos de actividades: el Análisis de Riesgos y la Propuesta de Medidas de Seguridad



4 – Etapas del Análisis de Riesgos

Resumen de las etapas

- **A. Establecimiento de Contexto**
  - Activos
  - Amenazas
  - Tiempos
- **B. Identificación de Riesgos**
  - Situaciones de Riesgo
- **C. Análisis de Riesgos**
  - Impacto
  - Probabilidad
  - Criticidad
  - Nivel de Necesidad de Salvaguardas
- **D. Evaluación de Riesgos**
  - Riesgo Intrínseco
  - Riesgo Reducido
  - Riesgo Efectivo

A. Establecimiento de Contexto

Activos: todos aquellos bienes, espacios, procesos y cualquier otro elemento de consideración que sea susceptible de sufrir las consecuencias de una amenaza.

Proceso de Selección e Identificación de Activos:

- Analizar los procesos clave de la organización/instalación considerada
- Listado de los activos requeridos por estos procesos
- Identificar, enumerar y clasificarlos entre 9 categorías adoptadas de MAGERIT II
- Identificar la ubicación física de los activos considerados

Tipos de Activos:

- **Tipos de Activos Físicos considerados**
  - Escenarios
- **Tipos de Activos Lógicos considerados**
  - Servicios
  - Aplicaciones (Software)
  - Redes de Comunicaciones
  - Equipamiento Auxiliar
  - Personal
  - Datos/información
  - Equipos Informáticos (Hardware)
  - Soportes de información
  - Instalaciones

A. Establecimiento de Contexto

Amenazas: Contingencias o riesgos específicos de los activos analizados, dependientes de su del entorno y circunstancias, cuya potencial materialización debe ser baremada.

Cada amenaza considerada pertenece a uno de los siguientes Tipos de Amenaza:

- **Grupos de Amenazas Físicas consideradas** (de Metodología de Cuevavaliente)
  - Delincuencia Común
  - Crímenes Agresivos o Violentos
  - Crimen Organizado y Terrorismo

- **Grupos de Amenazas Lógicas consideradas** (del catálogo Magerit II)
  - Desastres Naturales
  - De Origen Industrial
  - Ataques Intencionados
  - Errores y Fallos No Intencionados

B. Identificación de Riesgos

En esta etapa las combinaciones aplicables de activos-tiempos-amenazas son consideradas.

Cada posible combinación de activo-tiempo-amenaza se denomina **Situación de Riesgo**. El conjunto de ellas generan el **Mapa de Riesgos**.

La dimensión de Tiempos se obvia con frecuencia en los riesgos de origen lógico, con lo que es frecuente disponer de situaciones de riesgo lógicas de dos dimensiones (activo-amenaza).

C. Análisis de Riesgos

El Análisis de Riesgos Físico se ha basado tradicionalmente en parámetros cuantitativos.

El Análisis de Riesgos Físicos y Lógicos unificado se simplifica, utilizando escalas cualitativas para los parámetros considerados.

Los resultados con la nueva metodología han sido validados y comprobados respecto a los obtenidos con la metodología tradicional, manteniéndose la coherencia y la experiencia acumulada con las metodologías usadas previamente.

Parámetros que deben analizarse y estimarse:

- **Parámetros a considerar para cada Situación de Riesgo**
  - Impacto
  - Probabilidad
  - Nivel de Necesidad de Salvaguardas
- **Parámetros a considerar para cada Activo**
  - Criticidad

C. Análisis de Riesgos- Parámetros para cada Situación de Riesgo

Impacto: Medida de las consecuencias que puede sufrir un activo, en caso de materialización de una amenaza en un tiempo determinado.

El impacto se valora para cada situación de riesgo considerada, asumiendo uno de los siguientes valores:

IMPACTO	
MA	Impacto Muy Alto/Muy Grave o Severo para la Organización
A	Impacto Alto/Grave para la Organización
M	Impacto Medio/Moderado/Importante para la Organización
B	Impacto Bajo/Menor para la Organización
MB	Impacto Muy Bajo/Irrelevante para la Organización

C. Análisis de Riesgos- Parámetros para cada Situación de Riesgo

Probabilidad de Ocurrencia de Riegos Lógicos: suele basarse en estudios estadísticos sobre la materialización de sucesos, averías o amenazas.

Probabilidad de Ocurrencia de Riesgos Físicos deliberados: se refiere a un indicador no probabilístico que pretende indicar el grado de materialización de una amenaza. Como tal, es el resultado de multiplicar dos indicadores:

- Atractivo: en qué medida es atractivo para el potencial agente de la amenaza el llevarla a cabo. Se debe evaluar desde la perspectiva del sujeto actuante teórico.
- Vulnerabilidad: indicador de cuán sencillo es llevar a cabo una amenaza en el activo y tiempo considerados, considerándose que no existen salvaguardas.

En ambos casos (riesgos físicos y lógicos), la Probabilidad podrá tomar uno de los siguientes valores:

PROBABILIDAD	
MA	Probabilidad Muy Alta de Ocurrencia del Evento/Evento Probablemente ocurra
A	Probabilidad Alta de Ocurrencia del Evento/Evento Posible
M	Probabilidad Moderada de Ocurrencia del Evento/Evento Improbable
B	Probabilidad Baja de Ocurrencia del Evento/Evento Raro
MB	Probabilidad Muy Baja de Ocurrencia del Evento/Evento Muy Raro

C. Análisis de Riesgos- Parámetros para cada Situación de Riesgo

Las salvaguardas reducen ciertos riesgos a través de 2 vías:

- Reduciendo el impacto de las amenazas
- Reduciendo la probabilidad o frecuencia de ocurrencia

La necesidad de salvaguardas: (o carencia de salvaguardas existentes), es inversamente proporcional al nivel de salvaguardas que afectan a un activo. Se calculan siguiendo un modelo propio similar al modelo CMMI, obteniendo valores cuantitativos:

NIVEL DE NECESIDAD DE SALVAGUARDAS		NIVEL CMMI
Activos Físicos	Activos Lógicos	
MB	**MB**	Optimizado
B	**M**	Gestionado
M	**A**	Definido
MA	**MA**	Repetible
MA	**MA**	Inicial
MA	**MA**	No Existente

C. Análisis de Riesgos- Parámetros para cada Activo

Niveles CMMI y Necesidades de Salvaguardas:

GRADO DE MADUREZ Y NECESIDAD DE SALVAGUARDAS PARA RIESGOS FÍSICOS			
GRADO DE MADUREZ	NECESIDAD DE SALVAGUARDAS	NIVEL CMMI	PRACTICAS DE GESTIÓN DE SEGURIDAD FÍSICA
5	MB	OPTIMIZADO	Las salvaguardas han sido implementadas y revisadas hasta un nivel de "best practice", sobre la base de mejora continua.
4	B	GESTIONADO	Las salvaguardas han sido implementadas.
3	M	DEFINIDO	Se conocen las necesidades y se han planteado las necesidades a implementar basadas en "best practices".
2	MA	REPETIBLE	Se conocen las necesidades y se han planteado las necesidades a implementar, aunque no basadas en "best practices".
1	MA	INICIAL	Se conocen las necesidades, aunque no se han planteado las salvaguardas a implementar para solventarlas.
0	MA	NO EXISTENTE	No se conocen las necesidades.

GRADO DE MADUREZ Y NECESIDAD DE SALVAGUARDAS PARA RIESGOS LÓGICOS			
GRADO DE MADUREZ	NECESIDAD DE SALVAGUARDAS	NIVEL CMMI	PRACTICAS DE GESTIÓN DE SEGURIDAD LÓGICA
5	MB	OPTIMIZADO	Los procesos han sido revisados hasta un nivel de “best practice”, sobre la base de una mejora continua.
4	M	GESTIONADO	Los procesos están en mejora continua y proporcionan mejores prácticas. Se usan herramientas automatizadas de manera aislada o fragmentada.
3	A	DEFINIDO	La organización asegura que el control se planifica, documenta, ejecuta, monitoriza y controla.
2	MA	REPETIBLE	Los procesos han evolucionado de forma de que se siguen procedimientos similares para realizar la misma tarea. No existe formación ni comunicación de procedimientos estándar y la responsabilidad recae en el individuo.
1	MA	INICIAL	No existen procesos estándar aunque existen planteamientos “ad hoc” que se utilizan en cada situación.
0	MA	NO EXISTENTE	Ausencia total de procesos reconocibles.

C. Análisis de Riesgos- Parámetros para cada Activo

Criticidad: Consecuencias que se estiman o asignan a cada dimensión de Seguridad en los activos considerados, independiente de amenazas o tiempos.

La metodología considera la estimación de la criticidad para la Organización, en caso de ocurrencia, para cada combinación aplicable de las siguiente consecuencias de amenazas y las dimensiones de Seguridad y que se verían afectadas por estas consecuencias:

CONSECUENCIAS Y DIMENSIONES DE SEGURIDAD A CONSIDERAR	
CONSECUENCIAS	**DIMENSIONES CRÍTICAS A ESTIMAR**
Activos de Seguridad Física: Daños físicos sufridos	Reducción del Beneficio
Activos de Seguridad Lógica: Disponibilidad	Consecuencias en la Salud y Daños a las Personas
Activos de Seguridad Lógica: Integridad	Daños a la Herencia Socio-Cultural
Activos de Seguridad Lógica: Confidencialidad	Comunidad, Gobierno, Reputación y Medios
	Consecuencias Legales
	Reducción del Beneficio

D. Evaluación de Riesgos

Riesgo Intrínseco: Medida del daño probable sobre un sistema sin considerar las salvaguardas que pudieran proteger a éste.

- Se calcula para cada Situación de Riesgo
- El resultado se toma de unas tablas de Impacto vs. Probabilidad, diferentes para los riesgos físicos y lógicos

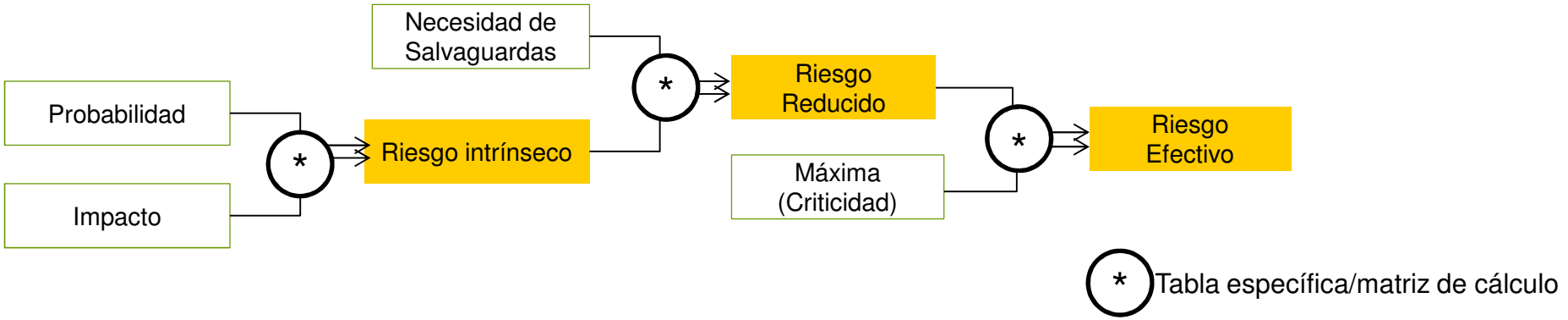
Riesgo Reducido: Nivel de Riesgo o medida del daño probable sobre un sistema, una vez consideradas las salvaguardas que pudieran proteger a éste.

- Se calcula para cada Situación de Riesgo
- El resultado se toma de una tablas de Riesgo Intrínseco vs. Nivel de Necesidad de Salvaguardas, común para ambos tipos de riesgos

D. Evaluación de Riesgos

Riesgo Efectivo: Nivel de Riesgo o medida de daño probable al que está sometido el activo tras la valoración de las salvaguardas implantadas en la actualidad, tomando en consideración el valor propio del activo (criticidad).

- Se calcula para cada Situación de Riesgo
- La criticidad a considerar es la máxima de las criticidades que se hayan calculado para las combinaciones de Consecuencias y Dimensiones de Seguridad que afecten al Activo.
- El resultado se toma de una tablas de Riesgo Reducido vs. Nivel de Necesidad de Salvaguardas, común para ambos tipos de riesgos



Conclusiones e Impactos

Nueva metodología propuesta, fruto de la experiencia de Cuevavaliente Ingenieros con sus partners expertos en Seguridad Lógica.

Presenta una solución práctica a uno de los problemas más complejos en el diseño de un Sistema de Gestión de Seguridad Física y Lógica.

Actualmente se está empezando a utilizar con éxito en diferentes empresas españolas

Permite proponer Planes de Seguridad comunes a la Alta Dirección de las organizaciones.

En el caso de España, y otros países europeos, permite cumplir con la legislación específica de Protección de Infraestructuras Críticas, donde se exige a las empresas que operan servicios críticos a la ciudadanía, que presenten Planes de Conjuntos de Seguridad Física y Lógica.

Referencias

[1] Legislación sobre Infraestructuras Críticas Española:
a) Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
b) Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

[2] Alfonso Bilbao, Enrique Bilbao, Koldo Peciña; "Physical and Logical Security Risk Analysis Model", International Carnahan Conference on Security Technology Proceedings, Barcelona 2011

[3] Alfonso Bilbao; "TUAR, a model of Risk Analysis in the Security Field", International Carnahan Conference on Security Technology Proceedings, Atlanta 1992

[4] Alfonso Bilbao, Enrique Bilbao, Alejandro Castillo; "A risk management method based on the AS/NZS 4360 Standard", International Carnahan Conference on Security Technology Proceedings, Ottawa 2008

[5] Metodología MAGERIT II; Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Administraciones Públicas de España. http://www.csi.map.es/csi/pg5m20.htm

Referencias

[6] ISO/IEC 27001 (BS7799-2:2002): Information security management systems - Requirements
[7] ISO 31000 Risk management — Principles and guidelines
[8] “AS/NZS 4360:2004 Standard – Risk Management”; Standards Australia/Standards New Zealand, 2004
[9] “HB 436:2004 – Risk Management Guidelines. Companion to AS/NZS 4360:2004”; Standards Australia/Standards New Zealand, 2004
[10] ISO/IEC 27001 / 2005 “Information security management systems — Requirements”
[11] ISO/IEC 27002 / 2005 “Code of practice for information security management”
[12] ISO/IEC 27005 / 2008 “Information security risk management”
[13] ISO/IEC 15408-1 / 2009 “Common Criteria for Information Technology Security Evaluation”
[14] www.cuevavaliente.com

Muchas gracias

Anexo 1 – Ejemplos

Amenazas

LOGICAL SECURITY THREATS			PHYSICAL SECURITY THREATS
INDUSTRIAL ORIGIN	**ERRORS AND UNINTENCIONAL FAILURES**	**WILLFUL ATTACKS**	**ORDINARY DELINQUENCY**
Fire	Users Errors	Manipulation of the Configuration	Burglary
Water Damages	Administrator Errors	Masquerading of User Identity	Theft
Industrial Disasters	Monitoring (logging) Errors	Abuse of Access Privileges	Vandalism
Mechanical Pollution	Configuration Errors	Misuse	Inappropriate Occupation
Electromagnetic Pollution	Organizational Deficiencies	Malware Diffusion	**AGGRESSIVE AND VIOLENT CRIMES**
Hardware or Software Failure	Malware Diffusion	[Re-]Routing of Messages	Aggression
Power Interruption	[Re-]Routing Errors	Sequence Alteration	Hold Up
Unsuitable temperature and/or moisture conditions	Sequence Errors	Unauthorized Access	Sabotage
Communications Service Failure	Information Leaks	Traffic Analysis	**TERRORISM AND ORGANIZED CRIMES**
Interruption of Other Services and Essential Supplies	Information Alteration	Repudiation	Explosives carried by Suicidal Individuals
Media Degradation	Entry of Incorrect Information	Eavesdropping	Explosives at Manned Vehicles (suicides)
Electromagnetic Radiation	Information Degradation	Alteration of Information	Explosives at Unmanned Land Vehicles
NATURAL DISASTERS	Destruction of Information	Entry of False Information	Explosives at Unmanned Air Vehicles
Fire	Disclosure of Information	Corruption of Information	Explosives at Unmanned River/Sea Vehicles
Water Damages	Software Vulnerabilities	Destruction of Information	Explosives at Parked Vehicles
Other Natural Disasters	Defects in Software Maintenance/Updating	Disclosure of Information	Explosives by Mail
	Defects in Hardware Maintenance/Updating	Software Manipulation	Explosives Placed/Abandoned Packages
	System Failure due to Exhaustion of Resources	Denial of Service	Rocket-Propelled Grenades and Mortar Attacks
	Staff Shortage	Theft	Organized Armed Terrorist Attack
		Destructive Attack	Massive Poisoning
		Enemy Over-Run	Listening Devices Deployment
		Staff Shortage	
		Extortion	
		Social Engineering	

Anexo 1 – Ejemplos

Ejemplo de Contexto

Activos:

- Campo de juego (Activo Físico)
- Sala técnica de pantallas (Activo Físico)
- Ordenador que controla las pantallas (Activo Lógico)

Tiempo:

- Durante el Partido
- Después del Partido

Amenazas:

- Ocupación Indebida (Física)
- Robo (Física)
- Acceso No Autorizado (Lógica)
- Vandalismo (Física)
- Sabotaje (Física)

AMENAZA/ ACTIVO Y TIEMPO	Campo de Juego		Sala técnica de pantallas		Ordenador que controla las pantallas	
	Durante Partido	Después Partido	Durante Partido	Después Partido	Durante Partido	Después Partido
Ocupación Indebida	X	X				
Vandalismo	X	X				
Robo		X				
Sabotaje			X	X		
Acceso No Autorizado					X	

Anexo 1 – Ejemplos

Ejemplo de Impacto y Probabilidad

SITUACIÓN DE RIESGO			IMPACTO	PROBABILIDAD
ACTIVO	TEMPO	AMENAZA		
Campo de Juego	Durante Partido	Ocupación Indebida	A	A
Campo de Juego	Durante Partido	Vandalismo	M	A
Campo de Juego	Después de Partido	Ocupación Indebida	B	MB
Campo de Juego	Después de Partido	Vandalismo	B	B
Campo de Juego	Después de Partido	Robo	B	B
Sala técnica de pantallas	Durante Partido	Sabotaje	A	MB
Sala técnica de pantallas	Después de Partido	Sabotaje	B	B
Ordenador que Controla las Pantallas	Durante Partido	Acceso No Autorizadp	A	B

Anexo 1 – Ejemplos

Ejemplo de Criticidad

ACTIVOS	CONSEQUENCIAS	CRITICIDAD PARA CADA DIMENSIÓN DE SEGURIDAD				MAX (CRITICIDAD)
		Reducción Beneficio	Salud y Daños	Reputación y Medios	Legal	
Campo de Juego	Physically harming the asset	H	H	H	M	H
Sala técnica de pantallas	Physically harming the asset	M	H	H	M	H
Ordenador que Controla las Pantallas	Integridad	M	H	H	M	H
	Disponibilidad	M	VL	L	L	

RISK SITUATION			IMPACTO	PROBABILIDAD	NECESIDAD SALVAGUARDIAS	MAX (CRITICIDAD)
ASSET	TIME	THREAT				
Campo de Juego	Durante Partido	Ocupación Indebida	A	A	L	H
Campo de Juego	Durante Partido	Vandalismo	M	A	L	H
Campo de Juego	Después de Partido	Ocupación Indebida	B	MB	M	H
Campo de Juego	Después de Partido	Vandalismo	B	B	M	H
Campo de Juego	Después de Partido	Robo	B	B	M	H
Sala técnica de pantallas	Durante Partido	Sabotaje	A	MB	M	H
Sala técnica de pantallas	Después de Partido	Sabotaje	B	B	M	H
Campo de Juego	Durante Partido	Ocupación Indebida	A	B	H	H

Ejemplo de Necesidad de Salvaguardas

Salvaguardas en el Campo de Juego Durante el Partido:

- Vigilantes (1/10 metros de borde de campo)
- Lista Negra (espectadores no admitidos)
- Redes evitando lanzamiento de objetos
- Comprobación de identificaciones
- Cámaras cubriendo el 100% de la escena
- Salvaguardas revisadas anualmente

Salvaguardas en el Campo de Juego Después del Partido :

- Puertas de estadio cerradas tras partido
- Detección de Intrusión
- Sin Vigilantes de Seguridad
- Salvaguardas no revisadas/no suficientes

SITUACIÓN DE RIESGO			NECESIDAD DE SALVAGUARDAS	NIVEL CMMI
ACTIVO	TIEMPO	AMENAZA		
Campo de Juego	Durante Partido	Ocupación Indebida	L	GESTIONADO
Campo de Juego	Durante Partido	Vandalismo	L	GESTIONADO
Campo de Juego	Después de Partido	Ocupación Indebida	M	DEFINIDO
Campo de Juego	Después de Partido	Vandalismo	M	DEFINIDO
Campo de Juego	Después de Partido	Robo	M	DEFINIDO