IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UD03

GESTIÓN DE RIESGOS

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

1. INTRODUCCIÓN

PARA **GARANTIZAR LA SEGURIDAD** DE LA INFORMACIÓN SERÁ **NECESARIO DEDICAR UNOS MEDIOS Y UNOS ESFUERZOS** PARA CONSEGUIRLO.

ESTA APLICACIÓN DEBE RACIONALIZARSE. PARA ELLO, SE EMPLEAN MÉTODOS DE **ANÁLISIS Y GESTIÓN DE RIESGOS (AGR)** EN DOS PASOS:

- **HAY QUE MEDIR LOS RIESGOS (ANÁLISIS)**
- **DECIDIR CÓMO AFRONTARLOS (GESTIÓN)**

1. INTRODUCCIÓN

EL ANÁLISIS DE RIESGOS (AR)

ES EL PROCESO SISTEMÁTICO PARA ESTIMAR LA MAGNITUD DE LOS RIESGOS A QUE ESTÁ EXPUESTA UNA ORGANIZACIÓN.

LA GESTIÓN DE RIESGOS (GR)

ES LA SELECCIÓN E IMPLANTACIÓN DE SALVAGUARDAS PARA CONOCER, PREVENIR, IMPEDIR, REDUCIR, O CONTROLAR LOS RIESGOS IDENTIFICADOS.

1. INTRODUCCIÓN

EL **AGR SERÁ UNA ACTIVIDAD CONTINUA**, A REALIZAR EN LOS CICLOS DE EJECUCIÓN DE UN SGSI.

PRIMERO, PORQUE **EL SGSI SIEMPRE SE PODRÁ MEJORAR.**

EN SEGUNDO LUGAR, PORQUE **LOS SISTEMAS INFORMÁTICOS SON DINÁMICOS, Y ESTÁN EXPUESTOS A CONTINUOS CAMBIOS Y NUEVAS AMENAZAS**.

1. INTRODUCCIÓN

EL **AGR** ES LA HERRAMIENTA QUE **PERMITE** EJERCITAR UNA **PROTECCIÓN RESPONSABLE DE LOS ACTIVOS** DE INFORMACIÓN DE LA EMPRESA.

POR SIMPLICIDAD EL **AGR** SE SUELE ACORTAR A **GESTIÓN DE RIESGOS**, PERO EN NINGÚN CASO ESTE NOMBRE CORTO SUPONE ELIMINAR LA ETAPA INICIAL DE ANÁLISIS DE RIESGOS.

NO DEBE EXISTIR GESTIÓN SIN ANÁLISIS.

CONTENIDOS

1. INTRODUCCIÓN
2. **APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES**
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

CONVIENE REALIZAR UN **AGR** EN UNA EMPRESA ANTES DE EMPRENDER CAMBIOS PROFUNDOS.

HACERLO ANTES, PERMITE QUE **LAS MEDIDAS DE SEGURIDAD FORMEN PARTE DEL DISEÑO**.

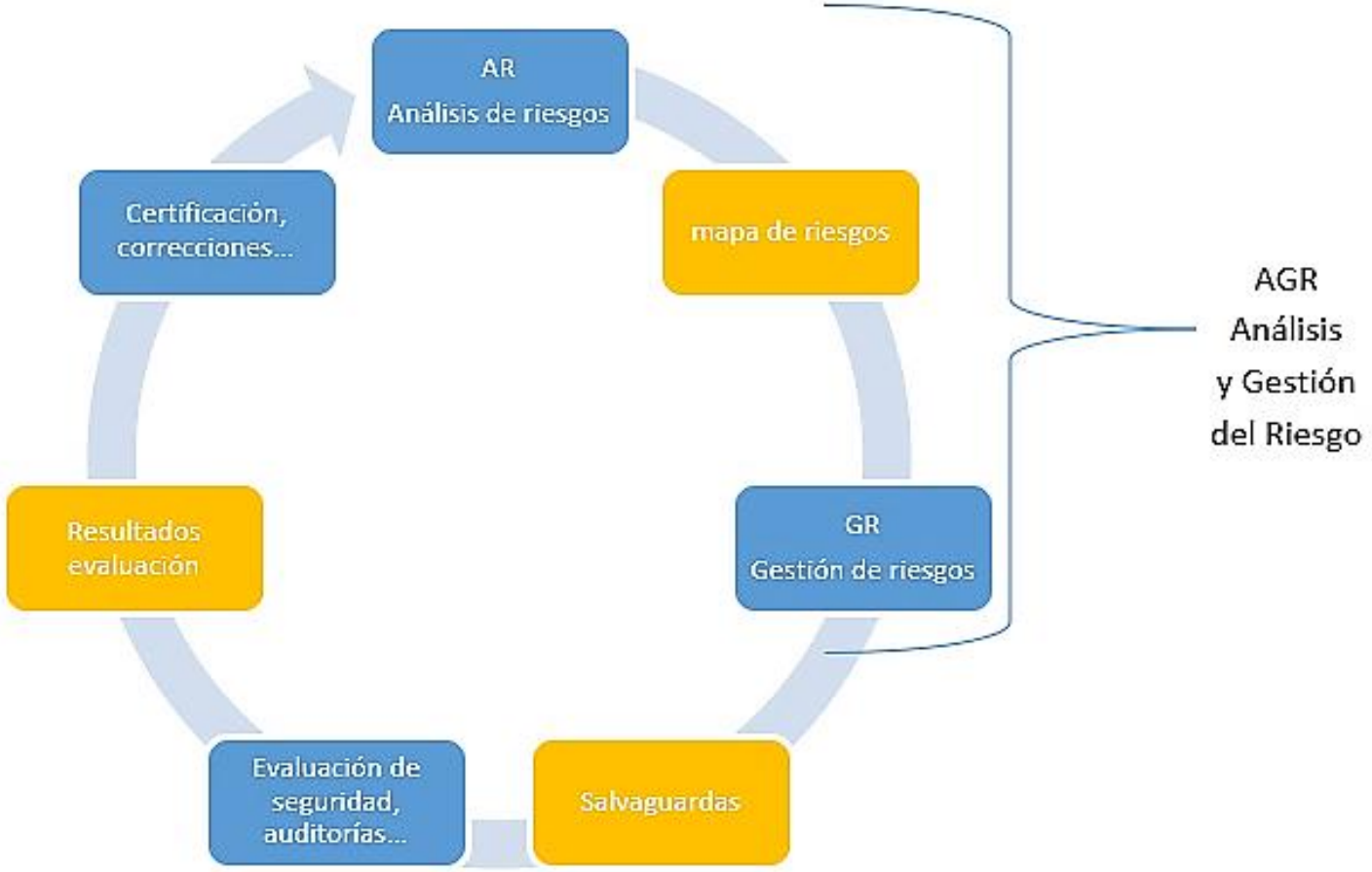
SI LA SEGURIDAD SE APORTA A POSTERIORI, *CONLLEVARÁ POSIBLEMENTE UN SOBRECOSTE Y UN SOBRESFUERZO*.

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

SERÁ NECESARIO REALIZAR UN AGR CUANDO LA EMPRESA QUIERA **OBTENER DETERMINADAS CERTIFICACIONES DE CUMPLIMIENTO DE NORMAS DE SEGURIDAD (ISO 27001).**

TAMBIÉN POR PRECEPTO LEGAL, POR EJEMPLO, PARA **CONDUCIR UNA AUDITORÍA DE SEGURIDAD**, O PARA DEFINIR EL **MARCO DE CUMPLIMIENTO DE UNA LEY (RGPD)**

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES



Proceso de gestión del riesgo para obtener una certificación o cumplimiento de una norma

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

REALIZAR UN **AGR** REQUIERE DE LA **INTERVENCIÓN DE DIFERENTES PERSONAS** EN LA EMPRESA Y UN **CRITERIO HOMOGÉNEO** PARA CUANTIFICAR LOS RIESGOS.

LA HOMOGENEIDAD ES FUNDAMENTAL, PORQUE RESULTA DIFÍCIL DECIDIR POR DÓNDE EMPEZAR Y LOS CRITERIOS PARA DECIDIRLO DEBEN MANTENERSE POSTERIORMENTE.

LA SOLUCIÓN ES:

PRIMERO DONDE HAYA MÁXIMO IMPACTO (DAÑO POSIBLE) Y MÁXIMO RIESGO (DAÑO PROBABLE)

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

EL **AGR** CONSTA DE 2 FASES:

- EN LA PRIMERA (**AR**), SE MIDE EL RIESGO
- EN LA SEGUNDA (**GR**), SE DECIDE QUÉ HACER CON EL RIESGO

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

PARA LA PRIMERA FASE (**AR**) EXISTEN **DIFERENTES MÉTODOS**, QUE DIFIEREN EN LAS FÓRMULAS EMPLEADAS PARA CALCULAR LOS RIESGOS.

LA SEGUNDA FASE (**GR**) ES EL PROCESO DE SELECCIONAR E IMPLEMENTAR MEDIDAS PARA MODIFICAR EL RIESGO. ENTRE LAS ALTERNATIVAS PARA TRATAR EL RIESGO, EXISTEN LAS SIGUIENTES **ACCIONES**:

- **MITIGAR EL RIESGO.** APLICAR CONTRAMEDIDAS QUE REDUZCAN EL IMPACTO DE UN INCIDENTE O REDUCIR LA PROBABILIDAD DE LA AMENAZA
- **EVITAR EL RIESGO.** ELIMINAR LOS ACTIVOS O SERVICIOS BAJO RIESGO
- **TRANSFERIR EL RIESGO.** MITIGAR EL RIESGO PROPIO, TRASLADÁNDOSELO A OTROS
- **ACEPTAR EL RIESGO.** NO HACER NADA

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

LA DECISIÓN DE ADOPTAR UNA ACCIÓN U OTRA SE TOMARÁ ATENDIENDO A DIVERSOS **CRITERIOS**:

- **REQUISITOS LEGALES O REGULATORIOS**
- **REQUISITOS OPERACIONALES**
- **OBJETIVOS DE LA EMPRESA**
- **RENTABILIDAD DE LA ACCIÓN**

LA SEGURIDAD TOTAL NO EXISTE, POR LO QUE **SIEMPRE HABRÁ UN DETERMINADO NIVEL DE RIESGO**, QUE LA EMPRESA ACEPTARÁ.

LA APLICACIÓN SISTEMÁTICA DEL PROCESO DE GESTIÓN DE RIESGOS PERMITE REPARTIR LAS INVERSIONES EN SEGURIDAD, **MINIMIZANDO EL RIESGO RESIDUAL** TOTAL DE LA EMPRESA.

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

LOS PASOS GENERALES DE UN PROCESO CLÁSICO Y SIMPLIFICADO DE GESTIÓN DE RIESGOS SON LOS SIGUIENTES:

AR (ANÁLISIS DE RIESGOS)

- IDENTIFICAR LOS ACTIVOS Y SUS RELACIONES DE DEPENDENCIA
- IDENTIFICAR LAS AMENAZAS Y SUS VULNERABILIDADES
- ESTIMAR EL IMPACTO, Y LA PROBABILIDAD DEL MISMO
- ESTIMAR EL NIVEL DE RIESGO DE LA OCURRENCIA DE LA AMENAZA
- ESTIMAR EL COSTE DE MITIGAR EL RIESGO

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES

GR (GESTIÓN DE RIESGOS)

- IDENTIFICAR LOS CRITERIOS DE ACEPTACIÓN DE RIESGO
- DETERMINAR SI EL RIESGO CALCULADO EN AR ES ACEPTABLE, O SI DEBE MITIGARSE
- IDENTIFICAR LAS MEDIDAS DE SEGURIDAD NECESARIAS, Y EVALUAR LA REDUCCIÓN DE RIESGO QUE APORTAN
- SELECCIONAR LAS MEDIDAS QUE SE IMPLEMENTARÁN
- ESTIMAR EL NIVEL DE RIESGO RESIDUAL
- ADOPTAR LAS MEDIDAS SEGÚN SEAN:
  - MEDIDAS PROACTIVAS (PREVENTIVAS).
  - MEDIDAS REACTIVAS (CONTINUIDAD Y RECUPERACIÓN).
  - ACEPTAR EL RIESGO RESIDUAL SI SE CUMPLEN LOS CRITERIOS DE ACEPTACIÓN (NO HACER NADA).
- EVALUAR LA EFECTIVIDAD DE LAS MEDIDAS PARA VOLVER A INICIAR EL AR.

CONTENIDOS

1. INTRODUCCIÓN
2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES
3. **METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS**
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

EL PROCESO DE GESTIÓN DE RIESGOS SE INICIA MIDIENDO LOS RIESGOS.

SE EMPLEARÁ UN **MODELO DE OCURRENCIA DEL INCIDENTE DE SEGURIDAD**, ES DECIR, **DEBEN EXISTIR UNOS ACTIVOS QUE RESULTEN VULNERABLES A UNAS AMENAZAS**.

ANALIZAREMOS ALGUNOS DE LOS MÉTODOS DE ANÁLISIS DE RIESGOS, COMENZANDO POR LA **METODOLOGÍA MAGERIT**.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT

EL CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA, DENTRO DEL MINISTERIO DE ADMINISTRACIONES PÚBLICAS, PUBLICÓ EN 2012 UNA **METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN (MAGERIT).** ACTUALMENTE ESTÁ EN SU VERSIÓN 3

EL GRAN **RETO** DE LOS **MÉTODOS DE ANÁLISIS DE RIESGOS** ES LA **COMPLEJIDAD DEL PROBLEMA AL QUE SE ENFRENTAN**, Y SI NO SE ES RIGUROSO, LAS CONCLUSIONES SERÁN POCO FIABLES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT

SE TRATA, POR LO TANTO, DE ENCONTRAR **MÉTODO QUE NO DEJE LUGAR A LA IMPROVISACIÓN**.

UN AGR BUSCA CONOCER PARA CONFIAR: CONOCER LOS RIESGOS PARA PODER AFRONTARLOS Y CONTROLARLOS

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS

SE DIVIDE EN 5 PASOS PARA OBTENER UNA LISTA DE LOS RIESGOS QUE SOPORTA EL SISTEMA DE INFORMACIÓN:

- **PASO 1.** DETERMINAR LOS ACTIVOS Y SU VALORACIÓN DE CIA
- **PASO 2.** DETERMINAR LAS AMENAZAS, CUÁNTO DEGRADAN LA CIA DE UN ACTIVO, Y CON QUÉ FRECUENCIA O PROBABILIDAD APARECEN
- **PASO 3.** DETERMINAR LAS SALVAGUARDAS EXISTENTES Y SU EFICACIA
- **PASO 4.** DETERMINAR EL IMPACTO, O MEDIDA DEL DAÑO POSIBLE AL ACTIVO POR LA MATERIALIZACIÓN DE UNA AMENAZA
- **PASO 5.** DETERMINAR EL RIESGO, O MEDIDA DEL DAÑO PROBABLE AL ACTIVO

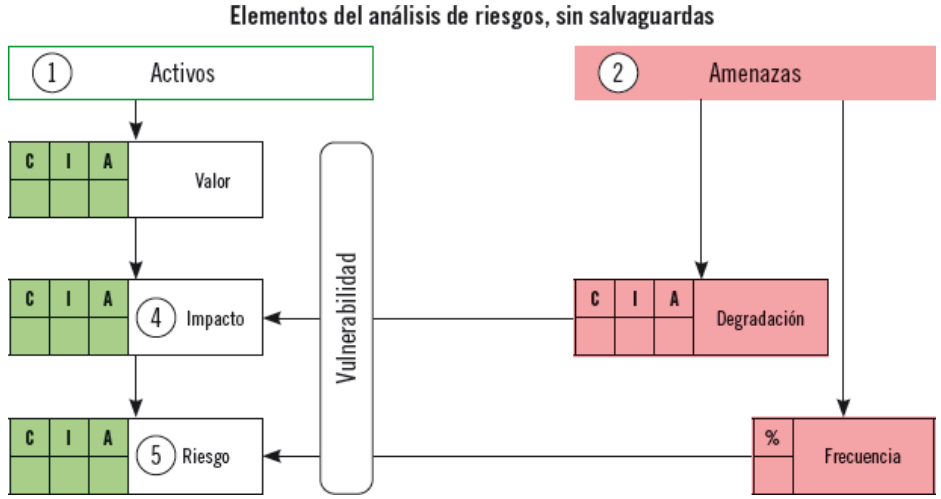
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS

PRIMERO SE ANALIZA EL SISTEMA EN AUSENCIA DE SALVAGUARDAS,

PARA **OBTENER EL RIESGO POTENCIAL** O TEÓRICO AL QUE ESTÁ EXPUESTO EL SISTEMA SIN NINGUNA PROTECCIÓN.

ESTO CONSISTE EN:



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.

- **REALIZAR LOS PASOS 1, 2, 4, Y 5**.
- **POSTERIORMENTE, SE AÑADEN LAS SALVAGUARDAS**, O **PASO 3**, DE LO CUAL SE OBTIENE EL **RIESGO REAL**.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

LOS ACTIVOS SON LOS RECURSOS DEL SISTEMA DE INFORMACIÓN O RELACIONADOS CON ESTE, NECESARIOS PARA QUE LA ORGANIZACIÓN FUNCIONE CORRECTAMENTE, Y ALCANCE LOS OBJETIVOS PROPUESTOS POR SU DIRECCIÓN.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

EL ACTIVO ESENCIAL ES LA **INFORMACIÓN**, O **DATOS** (D), Y ALREDEDOR SE ENCUENTRAN TAMBIÉN LAS SIGUIENTES **FAMILIAS** DE:

- **LOS SERVICIOS (S),** QUE SE PRESTAN GRACIAS A LOS DATOS, Y QUE SE NECESITAN PARA LOS MISMOS.
- **LAS APLICACIONES (SW),** QUE MANEJAN DICHOS DATOS.
- **LOS EQUIPOS INFORMÁTICOS (HW),** QUE EJECUTAN LAS APLICACIONES, Y ENTREGAN LOS SERVICIOS Y LOS DATOS.
- **LOS SOPORTES DE ALMACENAMIENTO (SI),** QUE ALMACENAN LOS DATOS.
- **EL EQUIPAMIENTO AUXILIAR (AUX),** QUE COMPLEMENTA A LOS EQUIPOS.
- **LAS REDES DE COMUNICACIONES (COM),** QUE INTERCAMBIAN LOS DATOS.
- **LAS INSTALACIONES (L),** DONDE RESIDEN LOS EQUIPOS Y LAS REDES.
- **LAS PERSONAS (P),** QUE EXPLOTAN U OPERAN LOS ELEMENTOS ANTERIORES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

PARA CADA ACTIVO, SE TENDRÁN UNAS AMENAZAS Y UNAS SALVAGUARDAS.

ADEMÁS, LOS ACTIVOS GUARDAN UNAS **RELACIONES DE DEPENDENCIA**, DE MANERA QUE **LOS ACTIVOS SUPERIORES DEPENDEN DE ACTIVOS INFERIORES**.

UN INCIDENTE DE SEGURIDAD EN LOS ACTIVOS INFERIORES PROVOCA UN PERJUICIO A LOS ACTIVOS SUPERIORES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

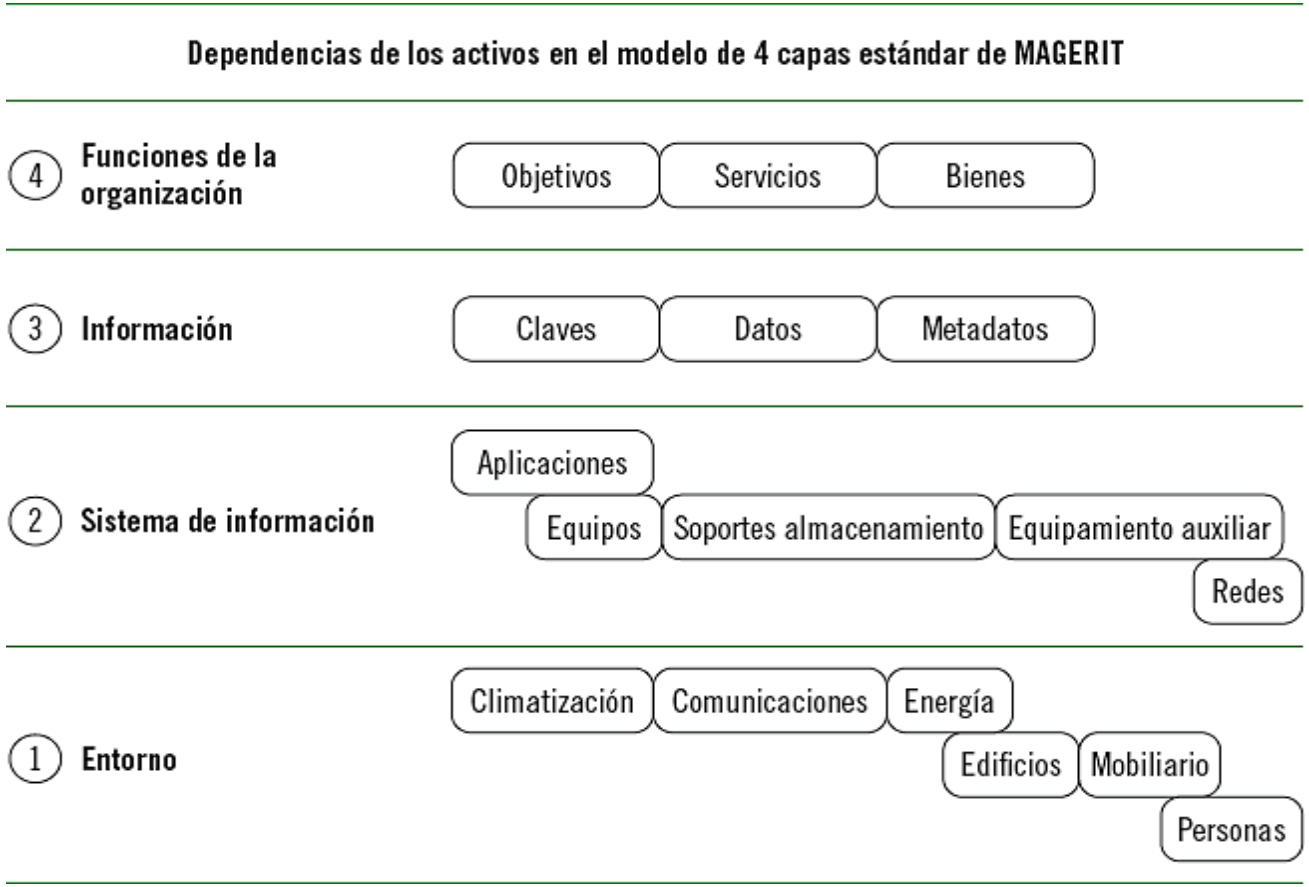
ES FRECUENTE **ORGANIZAR LA DEPENDENCIA DE LOS ACTIVOS EN CAPAS**, SEGÚN:

- **CAPA 4. FUNCIONES** Y PROCESOS DE LA ORGANIZACIÓN.
- **CAPA 3.** LA **INFORMACIÓN** Y LOS DATOS.
- **CAPA 2.** EL **SISTEMA DE INFORMACIÓN** PROPIAMENTE DICHO.
- **CAPA 1.** EL **ENTORNO** QUE SE PRECISA.

SEGÚN EL CASO, **SE PUEDEN INCLUIR CAPAS SUPERIORES**, PARA CONSIDERAR OTROS ACTIVOS DE MAYOR ENVERGADURA, **O SUBDIVIDIR EN MÁS CAPAS** LOS ACTIVOS.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS



3. 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 UN ACTIVO PUEDE SER **PROPIO O ACUMULADO**.

EL **ACUMULADO** ES EL QUE VAN **HEREDANDO LOS ACTIVOS INFERIORES DE LOS SUPERIORES**, QUE DEPENDEN DE ELLOS.

EN UN ÁRBOL DE DEPENDENCIAS, **EL VALOR SUELE ASIGNARSE A LOS SERVICIOS FINALES Y/O A LA INFORMACIÓN**, QUE PERMITEN CARACTERIZAR FUNCIONALMENTE UNA EMPRESA.

EL VALOR DE LOS ACTIVOS INFERIORES QUEDA SUBORDINADO AL VALOR DE SUS ELEMENTOS SUPERIORES

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

VALORACIÓN DE LOS ACTIVOS

EL VALOR SE ESTABLECE EN LAS DIMENSIONES DE **CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD**. **MAGERIT** PROPONE AÑADIR HASTA DOS DIMENSIONES DE VALORACIÓN ADICIONALES:

- **LA AUTENTICIDAD**
- **LA TRAZABILIDAD**

LAS DIMENSIONES DE SEGURIDAD QUE SE ESTUDIEN PODRÁN SER TODAS, O SOLO ALGUNAS. ES DECIR, HAY QUE FIJARLAS, PARA IR CONCRETANDO EL ÁMBITO DEL ANÁLISIS.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

VALORACIÓN DE LOS ACTIVOS

- **LA AUTENTICIDAD**, MIDIENDO EL *PERJUICIO QUE CAUSARÍA NO SABER EXACTAMENTE QUIÉN HA HECHO CADA COSA*, DISTINGUIENDO:
  - EN EL USO DE UN SERVICIO, O ***AUTENTICIDAD DEL USUARIO***.
  - EN EL ACCESO A LOS DATOS, O ***AUTENTICIDAD DE QUIÉN ACCEDE*** PARA CONSULTAR LOS DATOS O PARA MODIFICARLOS.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

VALORACIÓN DE LOS ACTIVOS

- **LA TRAZABILIDAD**, *¿QUIÉN HACE QUÉ, Y CUÁNDO?* EN DOS ASPECTOS:
  - EN EL USO DE UN SERVICIO, MIDIENDO EL PERJUICIO QUE CAUSARÍA NO SABER EXACTAMENTE ***QUIÉN HA USADO UN SERVICIO***.
  - EN EL ACCESO A DATOS, MIDIENDO EL PERJUICIO QUE CAUSARÍA NO SABER EXACTAMENTE ***QUIÉN HA ACCEDIDO A UNOS DATOS***, Y QUÉ HA HECHO CON ELLOS.

3. 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 UN ACTIVO ES **EL COSTE QUE SUPONDRÍA SALIR DE UNA INCIDENCIA QUE DESTROZARA EL ACTIVO**. SE PUEDEN CONSIDERAR LOS SIGUIENTES **FACTORES**:

- COSTE DE REPOSICIÓN
- COSTE DE MANO DE OBRA INVERTIDA EN RECUPERAR EL ACTIVO
- LUCRO CESANTE O PÉRDIDA DE INGRESOS
- CAPACIDAD DE OPERAR
- SANCIONES POR INCUMPLIMIENTO DE LEY U OBLIGACIONES CONTRACTUALES
- DAÑO A OTROS ACTIVOS PROPIOS O AJENOS
- DAÑO A PERSONAS
- DAÑOS MEDIOAMBIENTALES

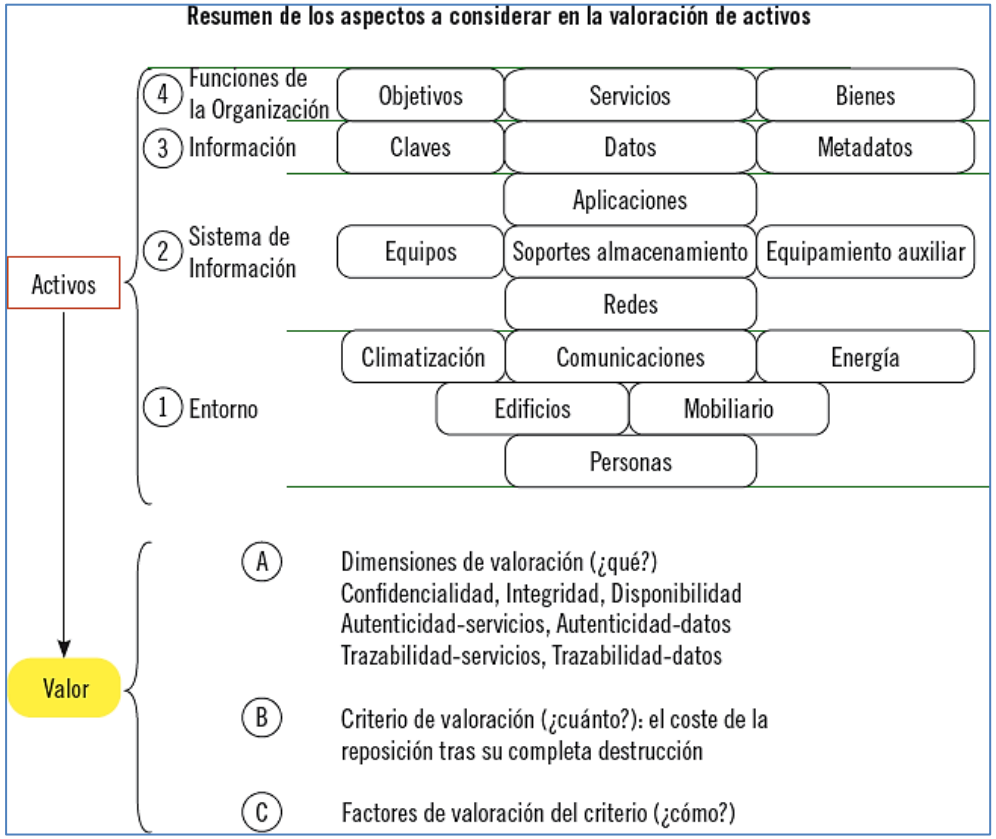
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 1: ACTIVOS

VALORACIÓN DE LOS ACTIVOS

ES CONVENIENTE DAR UNA DESCRIPCIÓN DE CUÁLES SERÁN LOS **CRITERIOS DE VALORACIÓN**, Y LOS FACTORES A CONSIDERAR.

EN CUANTO A LAS **TÉCNICAS** PARA DAR LOS VALORES, SE PUEDEN EMPLEAR *FORMULARIOS, ENTREVISTAS, O REUNIONES*.



3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

EL SIGUIENTE PASO CONSISTE EN **ANALIZAR LAS AMENAZAS PARA LOS ACTIVOS CONSIDERADOS**.

ESTO SUPONE REFLEXIONAR SOBRE **QUÉ COSAS PUEDEN OCURRIRLE AL ACTIVO** QUE PUEDAN CAUSARLE DAÑO.

¿CUÁLES SON LAS AMENAZAS?

EL ANALISTA DE RIESGOS DEBE CONSTRUIR EN CADA CASO LA LISTA DE AMENAZAS DE INTERÉS.

NO TODAS LAS AMENAZAS AFECTAN A TODOS LOS ACTIVOS, NI LO HACEN DE LA MISMA MANERA.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

¿CUÁLES SON LAS AMENAZAS?

LAS AMENAZAS EN MAGERIT SE AGRUPAN EN **4 CATEGORÍAS:**

- DESASTRES NATURALES
- DE ORIGEN INDUSTRIAL
- ERRORES Y FALLOS NO INTENCIONADOS
- ATAQUES INTENCIONADOS

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

AMENAZA	FAMILIA DEL ACTIVO									DIMENSIÓN VALOR						
DESASTRES NATURALES	**S**	**D**	**SW**	**HW**	**COM**	**SI**	**AUX**	**L**	**P**	**C**	**I**	**A**	**A.S**	**A.D**	**T.S**	**T.D**
Fuego				X	X	X	X	X				1			2	3
Daños por agua				X	X	X	X	X				1			2	3
Desastres naturales				X	X	X	X	X				1			2	3
DE ORIGEN INDUSTRIAL	**S**	**D**	**SW**	**HW**	**COM**	**SI**	**AUX**	**L**	**P**	**C**	**I**	**A**	**A.S**	**A.D**	**T.S**	**T.D**
Fuego				X	X	X	X	X				1			2	3
Daños por agua				X	X	X	X	X				1			2	3
Desastres industriales				X	X	X	X	X				1			2	3
Contaminación mecánica				X	X	X	X					1			2	3
Contaminación electromagnética				X	X	X	X					1			2	3
Avería de origen físico o lógico			X	X	X	X	X					1			2	3
Corte del suministro eléctrico				X	X	X	X					1			2	3
Condiciones inadecuadas de temperatura y/o humedad				X	X	X	X					1			2	3
Fallo servicios de comunicaciones					X							1				
Interrupción de otros servicios y suministros esenciales							X					1				
Degradación de los soportes de almacenamiento de la información						X						1			2	3
Emanaciones electromagnéticas				X	X			X		1						

S: servicios, SW: aplicaciones, HW: equipos informáticos, SI: soportes de almacenamiento, AUX: equipamiento auxiliar, COM: redes de comunicaciones, L: instalaciones, P: personas
C: confidencialidad, I: integridad, A: disponibilidad, A.S: Autenticidad en el servicio, A.D: Autenticidad en los datos, T.S: trazabilidad en el servicio, T.D: trazabilidad en los datos.
Las dimensiones se ordenan de mayor a menor daño, por ejemplo, según criterio de daño mitad. Por ejemplo, si: A = 1, I = 2, C = 3, se puede estimar que el daño mayor es en la disponibilidad, que el daño en la integridad es el 50 % del daño en la disponibilidad, y que el daño en la confidencialidad es el 50 % del daño a la integridad.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

AMENAZA	FAMILIA DEL ACTIVO									DIMENSIÓN VALOR						
ERRORES Y FALLOS NO INTENCIONADOS	**S**	**D**	**SW**	**HW**	**COM**	**SI**	**AUX**	**L**	**P**	**C**	**I**	**A**	**A.S**	**A.D**	**T.S**	**T.D**
Errores de los usuarios	X	X	X								1	2				
Errores del administrador	X	X	X	X	X					3	2	1	4	5	6	7
Errores de monitorización	X	X	X												1	2
Errores de configuración	X	X	X	X	X					3	2	1	4	5	6	7
Deficiencias en la organización									X			1				
Difusión de *software* dañino			X							3	2	1	4	5	6	7
Errores de re-encaminamiento	X		X		X					1	2		3		4	
Errores de secuencia	X		X		X						1					
Escapes de información		X	X		X					1						
Alteración de la información		X									1					
Introducción información incorrecta		X									1					
Degradación de la información		X									1					
Destrucción de la información		X										1				
Divulgación de información		X								1						
Vulnerabilidades de los programas			X							3	1	2				

S: servicios, SW: aplicaciones, HW: equipos informáticos, SI: soportes de almacenamiento, AUX: equipamiento auxiliar, COM: redes de comunicaciones, L: instalaciones, P: personas
C: confidencialidad, I: integridad, A: disponibilidad, A.S: Autenticidad en el servicio, A.D: Autenticidad en los datos, T.S: trazabilidad en el servicio, T.D: trazabilidad en los datos.
Las dimensiones se ordenan de mayor a menor daño, por ejemplo, según criterio de daño mitad. Por ejemplo, si: A = 1, I = 2, C = 3, se puede estimar que el daño mayor es en la disponibilidad, que el daño en la integridad es el 50 % del daño en la disponibilidad, y que el daño en la confidencialidad es el 50 % del daño a la integridad.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

AMENAZA	FAMILIA DEL ACTIVO									DIMENSIÓN VALOR						
Errores de mantenimiento/ actualización de programas			X								1	2				
Errores de mantenimiento/ actualización de equipos				X								1				
Caída del sistema por agotamiento de recursos	X			X	X							1				
Indisponibilidad del personal									X			1				
ATAQUES INTENCIONADOS	**S**	**D**	**SW**	**HW**	**COM**	**SI**	**AUX**	**L**	**P**	**C**	**I**	**A**	**A.S**	**A.D**	**T.S**	**T.D**
Manipulación de la configuración	X	X	X	X	X					2	1	7	3	4	5	6
Suplantación de la identidad del usuario	X		X		X					1	4		2	3		
Abuso de privilegios de acceso	X		X	X	X					1	2					
Uso no previsto	X		X	X	X	X	X	X				1				
Difusión de *software* dañino			X							3	2	1	4	5	6	7
Re-encaminamiento de mensajes	X		X		X					1	2		3		4	
Alteración de secuencia	X		X		X						1					
Acceso no autorizado	X	X	X	X	X	X	X	X		1	2		3			
Análisis de tráfico					X					1						
Repudio	X														1	

S: servicios, SW: aplicaciones, HW: equipos informáticos, SI: soportes de almacenamiento, AUX: equipamiento auxiliar, COM: redes de comunicaciones, L: instalaciones, P: personas
C: confidencialidad, I: integridad, A: disponibilidad, A.S: Autenticidad en el servicio, A.D: Autenticidad en los datos, T.S: trazabilidad en el servicio, T.D: trazabilidad en los datos.
Las dimensiones se ordenan de mayor a menor daño, por ejemplo, según criterio de daño mitad. Por ejemplo, si: A = 1, I = 2, C = 3, se puede estimar que el daño mayor es en la disponibilidad, que el daño en la integridad es el 50 % del daño en la disponibilidad, y que el daño en la confidencialidad es el 50 % del daño a la integridad.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

AMENAZA	FAMILIA DEL ACTIVO									DIMENSIÓN VALOR						
Interceptación de información (escucha)		X	X	X	X					1						
Modificación de la información		X									1					
Introducción de falsa información		X									1					
Corrupción de la información		X									1					
Destrucción de la información		X										1				
Divulgación de la información		X								1						
Manipulación de programas			X							1	2		3	4	5	6
Denegación de servicio	X			X	X							1				
Robo				X	X	X	X			2		1				
Ataque destructivo				X	X	X	X	X				1				
Ocupación enemiga				X	X	X	X	X		2		1				
Indisponibilidad del personal									X			1				
Extorsión									X	1	2		3	4	5	6
Ingeniería social									X	1	2		3	4	5	6

S: servicios, SW: aplicaciones, HW: equipos informáticos, SI: soportes de almacenamiento, AUX: equipamiento auxiliar, COM: redes de comunicaciones, L: instalaciones, P: personas
C: confidencialidad, I: integridad, A: disponibilidad, A.S: Autenticidad en el servicio, A.D: Autenticidad en los datos, T.S: trazabilidad en el servicio, T.D: trazabilidad en los datos.
Las dimensiones se ordenan de mayor a menor daño, por ejemplo, según criterio de daño mitad. Por ejemplo, si: A = 1, I = 2, C = 3, se puede estimar que el daño mayor es en la disponibilidad, que el daño en la integridad es el 50 % del daño en la disponibilidad, y que el daño en la confidencialidad es el 50 % del daño a la integridad.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

DEGRADACIÓN

MIDE EL **DAÑO CAUSADO POR UN INCIDENTE,** SI OCURRIERA. SE DEBE ESTIMAR **PARA CADA ACTIVO**, Y PARA CADA DIMENSIÓN.

MEDIR EL DAÑO QUE UNA AMENAZA PUEDE CAUSAR EN UN ACTIVO ES EXTREMADAMENTE COMPLEJO. SE NECESITA SIMPLIFICAR, EMPLEANDO VALORES PORCENTUALES. ASÍ, POR EJEMPLO, SE PUEDEN ENCONTRAR:

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

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

DEGRADACIÓN

HABRÁ QUE REVISAR LAS CALIFICACIONES SI LOS **RESULTADOS DE RIESGO FINAL** SON **MUY ALTOS**, **O SE NECESITA JUSTIFICAR UNA PROPUESTA DE FUERTE INVERSIÓN** ECONÓMICA EN SALVAGUARDAS DE SEGURIDAD. COMO APROXIMACIÓN:

- LAS **AMENAZAS INTENCIONADAS** PRODUCIRÁN NORMALMENTE UNA **DEGRADACIÓN MUY ALTA**.
- LAS **AMENAZAS NO INTENCIONADA**S LA DEGRADACIÓN **NO SUELE SER TOTAL**.
- LOS **DESASTRES** PRODUCIRÁN UNA **DEGRADACIÓN TOTAL**.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

FRECUENCIA DE LA AMENAZA

ES LA **POSIBILIDAD DE OCURRENCIA DE UNA AMENAZA**. ESTA PUEDE ACARREAR UNA DEGRADACIÓN MUY ALTA EN EL VALOR DEL ACTIVO, PERO SER DE MUY IMPROBABLE MATERIALIZACIÓN. OTRAS AMENAZAS PUEDEN PRODUCIR MENOR DEGRADACIÓN, PERO SER MUCHO MÁS FRECUENTES.

LA DIFICULTAD PARA DETERMINAR CON QUÉ FRECUENCIA OCURRIRÁ UNA AMENAZA ES MUY ALTA.

EN LA PRÁCTICA, **INTERESA LA TENDENCIA DE REDUCCIÓN DEL RIESGO RESIDUAL** ENTRE EJECUCIONES; NO EL VALOR ABSOLUTO DEL RIESGO EN SÍ.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 2: AMENAZAS

FRECUENCIA DE LA AMENAZA

MAGERIT PROPONE ENTENDER LA FRECUENCIA COMO EL NÚMERO DE OCURRENCIAS ANUALES, Y PROPONE:

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

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 4: IMPACTO

CONOCIDOS **LOS ACTIVOS** (JERARQUIZADOS CON VALORES EN VARIAS DIMENSIONES) Y **LAS AMENAZAS** (DEGRADACIÓN Y FRECUENCIA), LO SIGUIENTE ES **CALCULAR EL IMPACTO**.

ES LA MEDIDA DEL DAÑO SOBRE EL ACTIVO POR LA MATERIALIZACIÓN DE LA AMENAZA. SE CALCULA PARA CADA ACTIVO, PARA CADA AMENAZA, Y PARA CADA DIMENSIÓN:

IMPACTO = VALOR X DEGRADACIÓN

NO SE DEBE CONFUNDIR EL IMPACTO, QUE ES DAÑO O VALOR PERDIDO, CON EL VALOR QUE TENDRÍA EL ACTIVO TRAS LA AMENAZA: **VALOR FINAL = VALOR INICIAL – IMPACTO**

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 4: IMPACTO

EL IMPACTO TAMBIÉN SE PUEDE CALCULAR DE UNA **MANERA CUALITATIVA**:

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

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 4: IMPACTO

EL **VALOR DEL SISTEMA DE INFORMACIÓN SUELE ESTAR EN LOS SERVICIOS E INFORMACIÓN** (ACTIVOS DE CAPA 4 Y 3), MIENTRAS QUE **LAS AMENAZAS SUELEN MATERIALIZARSE SOBRE LOS MEDIOS** (ACTIVOS DE CAPA 2 Y 1).

SURGEN ASÍ DOS CONCEPTOS:

- **IMPACTO ACUMULADO**
- **IMPACTO REPERCUTIDO**

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 4: IMPACTO

IMPACTO ACUMULADO

ES **EL IMPACTO PRODUCIDO SOBRE EL VALOR ACUMULADO DE UN ACTIVO, A RAÍZ DE SUS AMENAZAS**. NÓTESE QUE SE EMPLEA SU VALOR TOTAL O ACUMULADO, ES DECIR, EL PROCEDENTE DE SUS ACTIVOS SUPERIORES Y EL SUYO PROPIO.

FACILITA DETERMINAR LAS SALVAGUARDAS A APLICAR A LOS MEDIOS.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 4: IMPACTO

IMPACTO REPERCUTIDO

ES **EL IMPACTO EN UN ACTIVO A CONSECUENCIA DE SU VALOR PROPIO, Y DE LAS AMENAZAS A LAS QUE ESTÁN EXPUESTOS SUS ACTIVOS INFERIORES.**

FACILITA VALORAR LAS CONSECUENCIAS DE INCIDENCIAS TÉCNICAS SOBRE LA MISIÓN DEL SISTEMA DE INFORMACIÓN, DE CARA A DECIDIR EL NIVEL DE RIESGO QUE SE ACEPTA.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 4: IMPACTO

AGREGACIÓN DE IMPACTOS

CUANDO SE PRECISE AGREGAR IMPACTOS, SE DEBE OBSERVAR QUE:

- SE PUEDEN AGREGAR IMPACTOS REPERCUTIDOS SOBRE DIFERENTES ACTIVOS.
- SE PUEDEN AGREGAR IMPACTOS ACUMULADOS SOBRE DIFERENTES ACTIVOS QUE NO DEPENDAN ENTRE ELLOS, NI DE NINGÚN ACTIVO SUPERIOR COMÚN.
- EN GENERAL, PUEDE AGREGARSE EL IMPACTO DE DIFERENTES AMENAZAS SOBRE UN MISMO ACTIVO, PERO CONVIENE CONSIDERAR EN QUÉ MEDIDA LAS AMENAZAS SON INDEPENDIENTES, Y PUEDEN SER CONCURRENTES.
- PUEDE AGREGARSE EL IMPACTO DE UNA AMENAZA EN DIFERENTES DIMENSIONES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 5: RIESGO

CONOCIDO EL IMPACTO Y LA FRECUENCIA CON QUE OCURRE UNA AMENAZA, DERIVAR EL RIESGO ES INMEDIATO.

EL RIESGO CRECE CON LA FRECUENCIA Y CON EL IMPACTO.

SE CALCULA PARA CADA ACTIVO, PARA CADA AMENAZA, Y EN CADA DIMENSIÓN.

RIESGO = IMPACTO X FRECUENCIA

NO OBSTANTE, PODRÍAN EMPLEARSE OTRAS FUNCIONES CUANTITATIVAS O SIMPLEMENTE CUALITATIVAS

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 5: RIESGO

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

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 5: RIESGO

AL IGUAL QUE EN EL CASO DEL IMPACTO, CONVIENE DETENERSE EN ESTUDIAR EL RIESGO EN SU RELACIÓN CON LA JERARQUÍA DE ACTIVOS, LO QUE ORIGINA UN **RIESGO ACUMULADO** Y UN **RIESGO REPERCUTIDO**.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 5: RIESGO

RIESGO ACUMULADO

ES **EL RIESGO PRODUCIDO POR EL IMPACTO ACUMULADO DE UN ACTIVO, A RAÍZ DE LA FRECUENCIA DE SU AMENAZA**. FACILITA DETERMINAR LAS SALVAGUARDAS A APLICAR A LOS MEDIOS.

RIESGO REPERCUTIDO

ES **EL RIESGO EN UN ACTIVO A CONSECUENCIA DE SU IMPACTO REPERCUTIDO, Y DE LA FRECUENCIA DE LA AMENAZA.** FACILITA VALORAR LAS CONSECUENCIAS DE INCIDENCIAS TÉCNICAS SOBRE LA MISIÓN DEL SISTEMA DE INFORMACIÓN, DE CARA A DECIDIR EL NIVEL DE RIESGO QUE SE ACEPTA.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 5: RIESGO

AGREGACIÓN DE RIESGOS

CUANDO SE PRECISE AGREGAR RIESGOS, SE DEBE OBSERVAR QUE:

- SE PUEDEN AGREGAR RIESGOS REPERCUTIDOS SOBRE DIFERENTES ACTIVOS.
- SE PUEDEN AGREGAR RIESGOS ACUMULADOS SOBRE DIFERENTES ACTIVOS QUE NO DEPENDAN ENTRE ELLOS, NI DE NINGÚN ACTIVO SUPERIOR.
- PUEDE AGREGARSE EL RIESGO DE DIFERENTES AMENAZAS SOBRE UN MISMO ACTIVO, PERO CONVIENE CONSIDERAR EN QUÉ MEDIDA LAS AMENAZAS SON INDEPENDIENTES, Y PUEDEN SER CONCURRENTES.
- PUEDE AGREGARSE EL RIESGO DE UNA AMENAZA EN DIFERENTES DIMENSIONES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

MAGERIT. FASE 1. ANÁLISIS DE RIESGOS. PASO 5: RIESGO

UNA VEZ REALIZADOS LOS PASOS 1, 2, 4 Y 5 DE LA FASE 1, CONOCEMOS **EL RIESGO MÁXIMO POTENCIAL**, QUE ES AL QUE ESTÁ EXPUESTO EL SISTEMA SI NO HAY NINGUNA SALVAGUARDA.

ESTE ANÁLISIS DARÁ LA **LÍNEA BASE DE MÁXIMA INSEGURIDAD DEL SISTEMA DE INFORMACIÓN**.

LA SIGUIENTE ITERACIÓN EN EL **AGR**, CONSISTE EN TENER EN CUENTA LAS SALVAGUARDAS O CONTRAMEDIDAS QUE YA ESTÉN INSTALADAS EN EL SISTEMA (**FASE 1, PASO 3**).

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS

EXISTEN MUCHÍSIMAS METODOLOGÍAS DE EVALUACIÓN DE RIESGOS. SE INTRODUCEN MUY BREVEMENTE DOS POR SU AMPLIA DIFUSIÓN, APLICACIÓN, Y ABUNDANTES RECURSOS FORMATIVOS DE LIBRE ACCESO Y DISTRIBUCIÓN.

- **ISO 27005**
- **ISO 31000**

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 27005

ES UNA **GUÍA INTERNACIONAL DE SEGURIDAD DE LA INFORMACIÓN** QUE **PROPORCIONA UN MARCO PARA LA GESTIÓN DE RIESGOS Y LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD ADECUADAS**.

ESTÁ DISEÑADO PARA **AYUDAR A LAS ORGANIZACIONES A PROTEGER SUS ACTIVOS DE INFORMACIÓN** VALIOSOS, INCLUYENDO INFORMACIÓN CLASIFICADA COMO CONFIDENCIAL Y SENSIBLE.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 27005

LA NORMA **ESTABLECE UN PROCESO SISTEMÁTICO PARA IDENTIFICAR Y EVALUAR LOS RIESGOS**, SELECCIONAR MEDIDAS DE SEGURIDAD APROPIADAS, IMPLEMENTARLAS Y MONITOREAR SU EFECTIVIDAD.

LA **ISO/IEC 27005** ES UNA PARTE INTEGRAL DE LA FAMILIA DE NORMAS **ISO/IEC 27000** QUE TRATAN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBER SEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 27005

LA **ISO/IEC 27005** SE APLICA A CUALQUIER TIPO DE ORGANIZACIÓN, INDEPENDIENTEMENTE DE SU TAMAÑO O SECTOR, QUE ALMACENE, PROCESE O TRANSMITA INFORMACIÓN CONFIDENCIAL Y SENSIBLE.

EL ALCANCE DE LA **ISO/IEC 27005** INCLUYE LA **GESTIÓN DE RIESGOS, LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD, LA EVALUACIÓN DE LA EFICACIA DE LA SEGURIDAD DE LA INFORMACIÓN, LA MEJORA CONTINUA, LA DOCUMENTACIÓN Y LA AUDITORÍA INTERNA**.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 27005

LA NORMA **SE ENFOCA EN LA GESTIÓN DE RIESGOS Y NO EN LA TECNOLOGÍA EN SÍ MISMA**. LA NORMA ES APLICABLE A CUALQUIER FASE DEL CICLO DE VIDA DE LA INFORMACIÓN, DESDE LA PLANIFICACIÓN HASTA LA ELIMINACIÓN.

LA GESTIÓN DE RIESGOS **NO ES UN EVENTO PUNTUAL, SINO UN PROCESO CONTINUO** QUE DEBE SER REVISADO Y ACTUALIZADO REGULARMENTE.

CABE DESTACAR QUE EL PROCESO DE GESTIÓN DE RIESGOS **ES UNA HERRAMIENTA DE APOYO PARA LA TOMA DE DECISIONES** Y, ESTE CASO, ESPECIALIZADA EN LA SEGURIDAD DE LA INFORMACIÓN.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

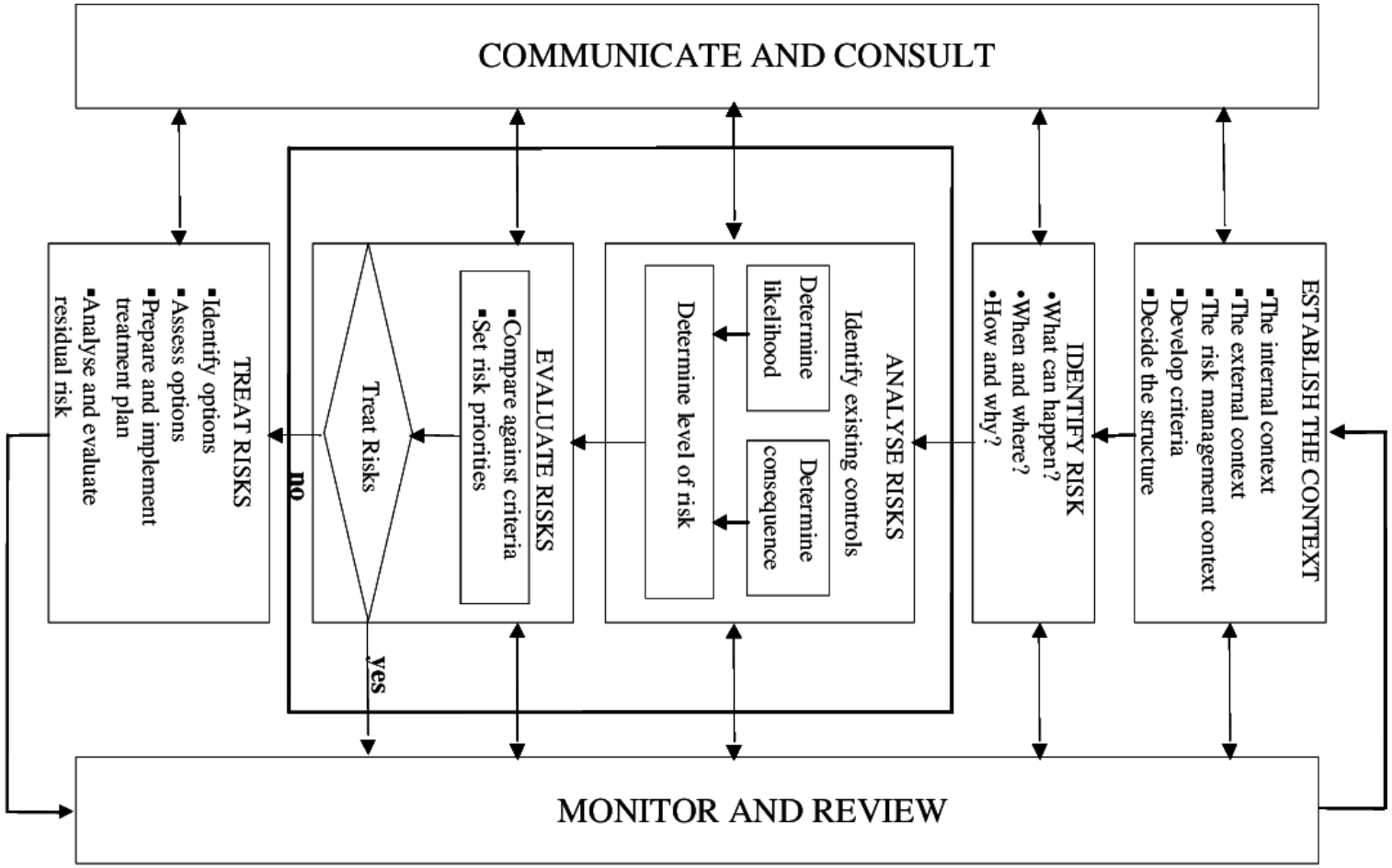
ISO 27005

LA ITERACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN SE FUNDAMENTA EN ESTAS **5 ACTIVIDADES**:

- FORMULAR Y SELECCIONAR OPCIONES DE TRATAMIENTO DE RIESGO
- PLANEAR E IMPLEMENTAR EL TRATAMIENTO
- EVALUAR LA EFICACIA DEL TRATAMIENTO
- DECIDIR SI EL RIESGO RESIDUAL ES ACEPTABLE
- AUMENTAR EL TRATAMIENTO SI EL RIESGO RESIDUAL NO ES ACEPTABLE

ESTAS ACTIVIDADES NOS PERMITEN DEFINIR EL CICLO DE VIDA DE LA GESTIÓN DE RIESGOS SEGÚN EL SIGUIENTE ESQUEMA:

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS



3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

SE BASA EN UN **ESTÁNDAR INTERNACIONAL** QUE OFRECE UNA SERIE DE DIRECTRICES QUE **PERMITE QUE CUALQUIER EMPRESA**, INDEPENDIENTEMENTE DE SU TAMAÑO, SECTOR O UBICACIÓN **PUEDA CONSIDERAR EL RIESGO COMO UN ELEMENTO QUE GENERE VALOR**

ES DECIR, **PROPORCIONA UNA SERIE DE PRINCIPIOS Y GUÍAS QUE PERMITE QUE LAS ORGANIZACIONES ANALICEN Y EVALÚEN LOS RIESGOS** A LOS QUE SON SUSCEPTIBLES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

PRETENDE **AUNAR LAS MEJORES PRÁCTICAS** PERMITIENDO ASÍ QUE LAS EMPRESAS MEJOREN SUS TÉCNICAS DE GESTIÓN Y LOGREN UNA MEJORA DE LA SEGURIDAD.

ESTA NORMA SE PUBLICÓ EN **2018** Y CONTINUA VIGENTE ACTUALMENTE. ESTÁ ESTRUCTURADA EN **SEIS CAPÍTULOS O SECCIONES**:

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

SECCIÓN 1. OBJETO Y CAMPO DE APLICACIÓN: HACE REFERENCIA A LA APLICACIÓN DE LAS DIRECTRICES.

SECCIÓN 2. REFERENCIAS NORMATIVAS: NO CONTIENE NINGUNA REFERENCIA NORMATIVA ADICIONAL.

SECCIÓN 3. TÉRMINOS Y DEFINICIONES: PARA EL CORRECTO ENTENDIMIENTO DE ESTA NORMA ISO, SE APLICAN LAS BASES DE DATOS TERMINOLÓGICAS DE LA **ISO** Y LA **IEC**.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

SECCIÓN 4. PRINCIPIOS: ESTA SECCIÓN RECOGE LOS DIFERENTES PRINCIPIOS REFERENTES A LA MEJORA DEL DESEMPEÑO, LA INNOVACIÓN Y LA CONSECUCIÓN DE LOS OBJETIVOS.

SE RECOGEN **11 PRINCIPIOS** QUE ENCAJAN A LO LARGO DE TODA LA ESTRUCTURA Y OBJETIVOS DE LAS ORGANIZACIONES Y QUE, ADEMÁS, SE ENCUENTRAN RELACIONADOS CON LA GESTIÓN DE LOS RIESGOS.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

SECCIÓN 4. PRINCIPIOS:

ESTOS PRINCIPIOS **REQUIEREN QUE LA GESTIÓN SEA INTEGRADA, ESTRUCTURADA Y EXHAUSTIVA, ADAPTADA, INCLUSIVA, DINÁMICA**, QUE **LA INFORMACIÓN SE ENCUENTRE ACTUALIZADA Y DISPONIBLE**, QUE **SE TENGAN EN CUENTA LOS FACTORES HUMANOS Y CULTURALES**, Y **SE DESARROLLE UNA MEJORA CONTINUA A TRAVÉS DEL APRENDIZAJE Y LA EXPERIENCIA.**

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

SECCIÓN 5. MARCO DE REFERENCIA: ESTA SECCIÓN PRETENDE AYUDAR EN LA INTEGRACIÓN DE LA GESTIÓN DEL RIESGO A LO LARGO DE TODAS LAS ACTIVIDADES Y FUNCIONES DE LAS ORGANIZACIONES, ES DECIR, HACE REFERENCIA A LA INTEGRACIÓN, EL DISEÑO, LA IMPLEMENTACIÓN, LA VALORACIÓN Y LA MEJORA DE LA GESTIÓN DEL RIESGO.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

SECCIÓN 6. PROCESO: EL PROCESO DE GESTIÓN DEL RIESGO ABARCA TODAS AQUELLAS POLÍTICAS, PROCEDIMIENTOS Y PRÁCTICAS RESPECTO DE LAS ACTIVIDADES Y PROCESOS DE LA ORGANIZACIÓN, PERMITIENDO ASÍ AFRONTAR TODOS AQUELLOS RIESGOS QUE PUEDA ENFRENTAR, NO SOLO MITIGARLOS Y PREVENIRLOS, SINO LLEGANDO INCLUSO A CONVERTIRLOS EN OPORTUNIDADES.

3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

OTRAS METODOLOGÍAS COMÚNMENTE ACEPTADAS.

ISO 31000

UNA DE LAS FIGURAS QUE SE PUEDE DESPRENDER DE ESTA NORMA ES EL **PROPIETARIO DEL RIESGO**, QUE SERÁ EL RESPONSABLE DE LA GESTIÓN, SEGUIMIENTO Y CONTROL DE UN RIESGO IDENTIFICADO.

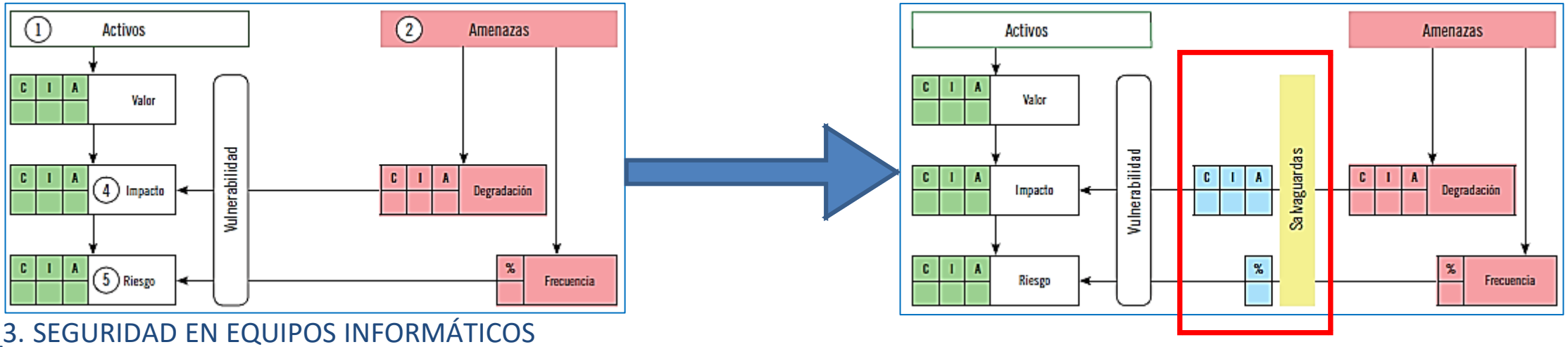
ESTA PERSONA DEBERÁ SER CAPAZ DE ADMINISTRAR EL RIESGO, ADEMÁS DE TENER EL CONOCIMIENTO, LOS RECURSOS Y LA AUTORIDAD PARA GESTIONARLO.

CONTENIDOS

1. INTRODUCCIÓN
2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
4. **APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO**

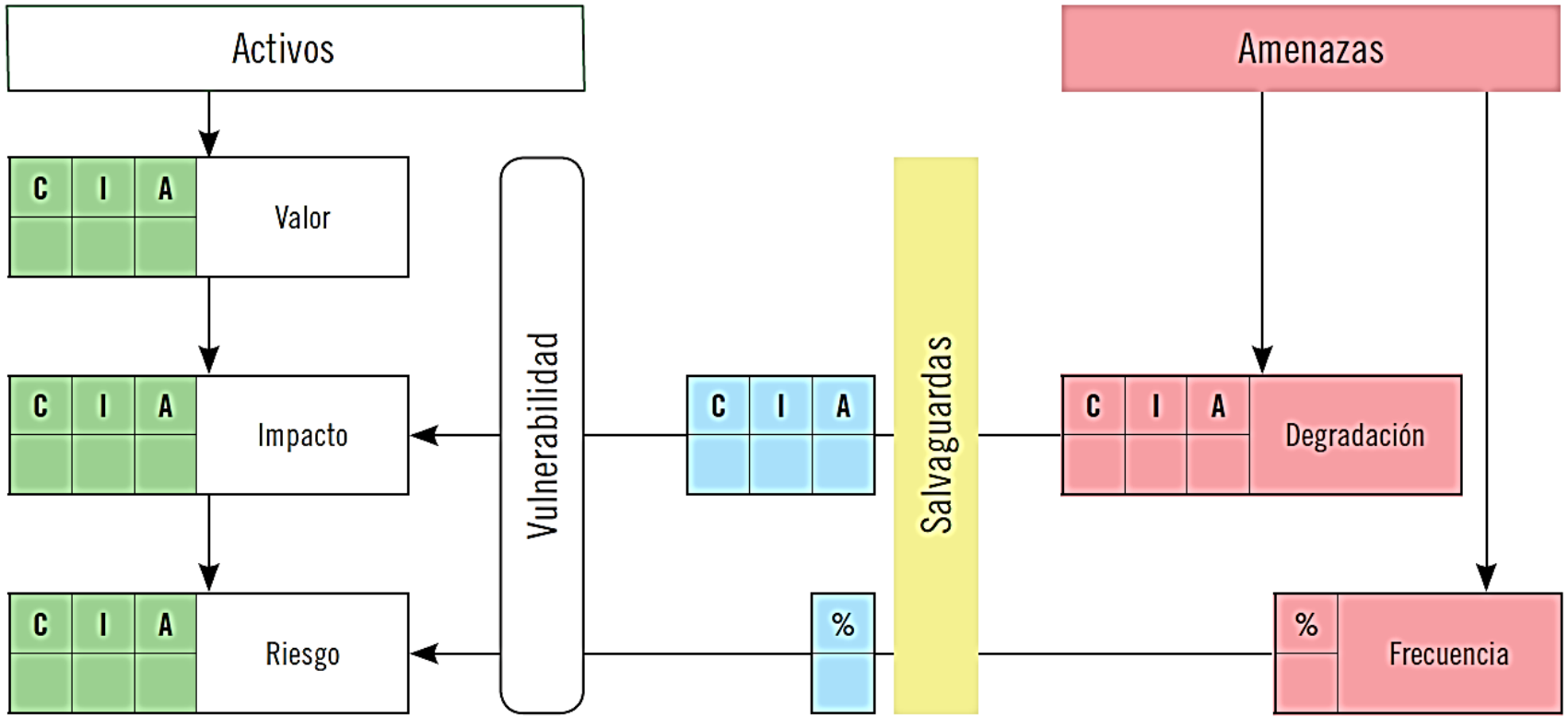
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

DEL **ANÁLISIS DE RIESGOS** SE **OBTIENE EL RIESGO EN COMPLETA AUSENCIA DE SALVAGUARDAS.** ES DECIR, EL **RIESGO MÁXIMO TEÓRICO** QUE ES POSIBLE ENCONTRAR. **PARA REDUCIRLO SE INTRODUCEN SALVAGUARDAS** O CONTRAMEDIDAS QUE CONTROLEN EL RIESGO, ACTUANDO SOBRE LAS AMENAZAS (BIEN REDUCIENDO LA DEGRADACIÓN QUE INTRODUCEN, BIEN SU FRECUENCIA DE APARICIÓN.



4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

Elementos del análisis de riesgos, con salvaguardas



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".

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

LA APLICACIÓN DE CONTROLES REDUCE EL RIESGO. PARA ELLO, SE COMPLETA LA ÚLTIMA PARTE DEL ANÁLISIS DE RIESGOS

PASO 3: SALVAGUARDAS O CONTRAMEDIDAS

LAS SALVAGUARDAS O CONTRAMEDIDAS **SON LOS PROCEDIMIENTOS O MECANISMOS TECNOLÓGICOS QUE REDUCEN EL RIESGO**.

NO EXISTE UNA LISTA COMPLETA DE CONTRAMEDIDAS. LAS SALVAGUARDAS INTERVIENEN **REDUCIENDO EL RIESGO DE DOS MANERAS**:

- **LIMITANDO EL DAÑO CAUSADO**
- **REDUCIENDO LA FRECUENCIA DE LAS AMENAZAS**.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

PASO 3: SALVAGUARDAS O CONTRAMEDIDAS

LIMITANDO EL DAÑO CAUSADO

SE APLICAN CUANDO LA AMENAZA SE MATERIALIZA, **LIMITANDO SUS CONSECUENCIAS**. VALORAR LA EFICACIA DE UNA SALVAGUARDA ES UNA TAREA COMPLEJA.

LA EFICACIA SERÁ UNA VALORACIÓN DEL PROFESIONAL DE SI, CUYO CRITERIO DE CÁLCULO SIEMPRE DEBE QUEDAR ESCRITO PARA CONSULTAS FUTURAS, QUE PERMITAN UNA VALORACIÓN HOMOGÉNEA EN EL TIEMPO.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

PASO 3: SALVAGUARDAS O CONTRAMEDIDAS

LIMITANDO EL DAÑO CAUSADO

COMO **INDICADORES PARA MEDIR LA EFICACIA DE UNA CONTRAMEDIDA**, SE PUEDEN VALORAR CADA UNO DE LOS SIGUIENTES ASPECTOS, QUE SOLO CUMPLIRÍA UNA CONTRAMEDIDA CON EFICACIA DEL 100 %:

- ES TEÓRICAMENTE IDÓNEA
- ESTÁ PERFECTAMENTE DESPLEGADA, CONFIGURADA, Y MANTENIDA
- SE EMPLEA SIEMPRE
- EXISTEN PROCEDIMIENTOS CLAROS DE USO EN CASO DE INCIDENCIAS

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

PASO 3: SALVAGUARDAS O CONTRAMEDIDAS

LIMITANDO EL DAÑO CAUSADO

- LOS USUARIOS ESTÁN FORMADOS Y CONCIENCIADOS.
- EXISTEN CONTROLES QUE AVISAN DE POSIBLES FALLOS.

EN EL EXTREMO OPUESTO, CON UNA EFICACIA DEL 0%, ESTARÍAN LAS QUE PUEDEN ELIMINARSE O APAGARSE SIN REPERCUSIÓN ALGUNA EN EL SISTEMA.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

PASO 3: SALVAGUARDAS O CONTRAMEDIDAS

REDUCIENDO LA FRECUENCIA DE LAS AMENAZAS

SON LAS **MEDIDAS PREVENTIVAS**.

IDEALMENTE, **LLEGAN A IMPEDIR COMPLETAMENTE QUE LA AMENAZA SE MATERIALICE**.

ESTIMAR LA REDUCCIÓN EN LA FRECUENCIA ES UNA TAREA MUY COMPLEJA, POR LO QUE SE EMPLEARÁN VALORES CUALITATIVOS PARA ESTIMAR LA NUEVA OCURRENCIA DE LA AMENAZA CON LA CONTRAMEDIDA APLICADA.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

PASO 3: SALVAGUARDAS O CONTRAMEDIDAS

ANALIZADAS LAS SALVAGUARDAS, RESULTA MUY RÁPIDO ESTIMAR EL NUEVO RIESGO DEL SISTEMA, A PARTIR DE LA NUEVA DEGRADACIÓN MEJORADA (**NUEVO IMPACTO RESIDUAL**), Y DE LA FRECUENCIA MEJORADA (**NUEVO RIESGO RESIDUAL**).

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

REVISIÓN DEL PASO 4: IMPACTO RESIDUAL

SI LAS SALVAGUARDAS SON 100 % EFICACES, ELIMINAN COMPLETAMENTE LA DEGRADACIÓN QUE PRODUCIRÍAN LAS AMENAZAS, Y **EL IMPACTO RESIDUAL SERÍA DESPRECIABLE**.

EN LA REALIDAD, EXISTIRÁN NORMAS IMPRECISAS, PROCEDIMIENTOS INCOMPLETOS, SALVAGUARDAS INADECUADAS, Y OTROS FACTORES, QUE HACEN QUE EL SISTEMA DE INFORMACIÓN PERMANEZCA SOMETIDO A UN IMPACTO RESIDUAL.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

REVISIÓN DEL PASO 4: IMPACTO RESIDUAL

EL CÁLCULO ES SENCILLO, YA QUE LO ÚNICO QUE VARÍA ES LA DEGRADACIÓN DE LA AMENAZA QUE SE VE MEJORADA POR LA EFICACIA DE LA CONTRAMEDIDA:

DEGRADACIÓN MEJORADA = DEGRADACIÓN X (100 – EFICACIA CONTRAMEDIDA)

IMPACTO RESIDUAL = VALOR X DEGRADACIÓN MEJORADA

IMPACTO RESIDUAL = IMPACTO X (100 – EFICACIA CONTRAMEDIDA)

EL IMPACTO RESIDUAL PUEDE RECALCULARSE, ACUMULADO SOBRE LOS ACTIVOS INFERIORES, O REPERCUTIDO SOBRE LOS ACTIVOS SUPERIORES.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RIESGO TRAS LA INTRODUCCIÓN DE SALVAGUARDAS

REVISIÓN DEL PASO 5: RIESGO RESIDUAL

SI LAS SALVAGUARDAS SON 100 % EFICACES, ELIMINAN COMPLETAMENTE LA FRECUENCIA DE LAS AMENAZAS, Y **EL RIESGO RESIDUAL SERÍA DESPRECIABLE**.

SE DEBEN REPETIR LOS CÁLCULOS CON ESTE NUEVO IMPACTO Y FRECUENCIAS, DE MANERA QUE:

RIESGO RESIDUAL = IMPACTO RESIDUAL X FRECUENCIA MEJORADA

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

SI EL RIESGO RESIDUAL ES DESPRECIABLE, O ADMISIBLE PARA LA EMPRESA, **SE HA TERMINADO**. **EN CASO CONTRARIO**, SE DEBE **REDUCIRLO AÚN MÁS**.

UN RIESGO RESIDUAL NO DESPRECIABLE PRECISA SER INTERPRETADO MÁS ALLÁ DE SU SIMPLE VALOR NUMÉRICO.

POR EJEMPLO, SI EL VALOR ES SIMILAR AL RIESGO POTENCIAL (SIN CONSIDERAR NINGUNA SALVAGUARDA), SE PUEDE CONCLUIR QUE LAS SALVAGUARDAS APLICADAS NO SIRVEN.

SE OBTENDRÁ LA LISTA DE COSAS POR CORREGIR, QUE DEBE DERIVAR EN UN INFORME DE TAREAS O **INFORME DE INSUFICIENCIAS**.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

MAGERIT CONCRETA QUE **LA APLICACIÓN DE SALVAGUARDAS DEBE REALIZARSE DE MANERA ORDENADA**, SIGUIENDO **5 ETAPAS**:

1. DEBE **EXISTIR UNA POLÍTICA DE ORGANIZACIÓN** QUE DETERMINE LOS RESPONSABLES DE CADA COSA.
2. **ESTABLECER UNOS OBJETIVOS CLAROS**, PARA DECIDIR SI LA AMENAZA HA SIDO CONJURADA.
3. **ESTABLECER UNAS INSTRUCCIONES** PASO A PASO (UN PROCEDIMIENTO) DE LO QUE HAY QUE HACER.
4. **DESPLEGAR LAS SALVAGUARDAS**.
5. **DESPLEGAR LOS CONTROLES** QUE PERMITAN SABER QUE LAS SALVAGUARDAS ESTÁN FUNCIONANDO COMO SE HABÍA PREVISTO.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

SELECCIÓN DE MEDIDAS A APLICAR

LAS **MEDIDAS DESEABLES** SON **PREVENTIVAS**, PERO *NO SIEMPRE SERÁ POSIBLE O SU COSTE ASUMIBLE*.

DESPUÉS, CONVIENE DISPONER DE **CONTRAMEDIDAS DE DETECCIÓN**, YA QUE EN *NO DEBE PERMITIRSE QUE UN ATAQUE PASE INADVERTIDO*.

POSTERIORMENTE, CONVIENE APLICAR LAS **MEDIDAS REACTIVAS DE EMERGENCIA**, *QUE PAREN Y LIMITEN EL INCIDENTE*

POR ÚLTIMO, LAS **MEDIDAS REACTIVAS DE RECUPERACIÓN**, PARA VOLVER A DONDE SE DEBE ESTAR, *CON UN PLAN DE CONTINUIDAD* ADECUADO.

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

SELECCIÓN DE MEDIDAS A APLICAR

POR SU NATURALEZA, LAS **SALVAGUARDAS** PUEDEN SER DE TIPO:

- **TÉCNICO**

  APLICACIONES, EQUIPOS, Y COMUNICACIONES
- **FÍSICAS**

  APLICADAS PARA PROTEGER EL ENTORNO Y LOS EQUIPOS
- **ORGANIZATIVAS**

  DE PREVENCIÓN Y GESTIÓN DE INCIDENCIAS
- **POLÍTICA DE PERSONAL**

  CONTRATACIÓN, FORMACIÓN, ORGANIZACIÓN, PLAN DE REACCIÓN Y POR ÚLTIMO, MEDIDAS DISCIPLINARIAS

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

SELECCIÓN DE MEDIDAS A APLICAR

PARA LA SELECCIÓN SE DEBE CONSIDERAR TAMBIÉN UN **CRITERIO ECONÓMICO**, PORQUE NO RESULTA PROPORCIONADO APLICAR CONTRAMEDIDAS CUYO COSTE SUPERE AL DEL ACTIVO A PROTEGER.

PROCEDE REALIZAR UNA VALORACIÓN DEL **COSTE DE LA SEGURIDAD** Y DEL **COSTE DE LA INSEGURIDAD**.

TEÓRICAMENTE, EXISTIRÍA UNA CURVA, EN LA QUE EL COSTE DE LAS SALVAGUARDAS SE DISPARA, PARA ALCANZAR NIVELES MUY ALTOS DE SEGURIDAD, Y EL COSTE DEL RIESGO RESIDUAL SE REDUCE MUCHO, CON POCA SEGURIDAD QUE SE APLIQUE.

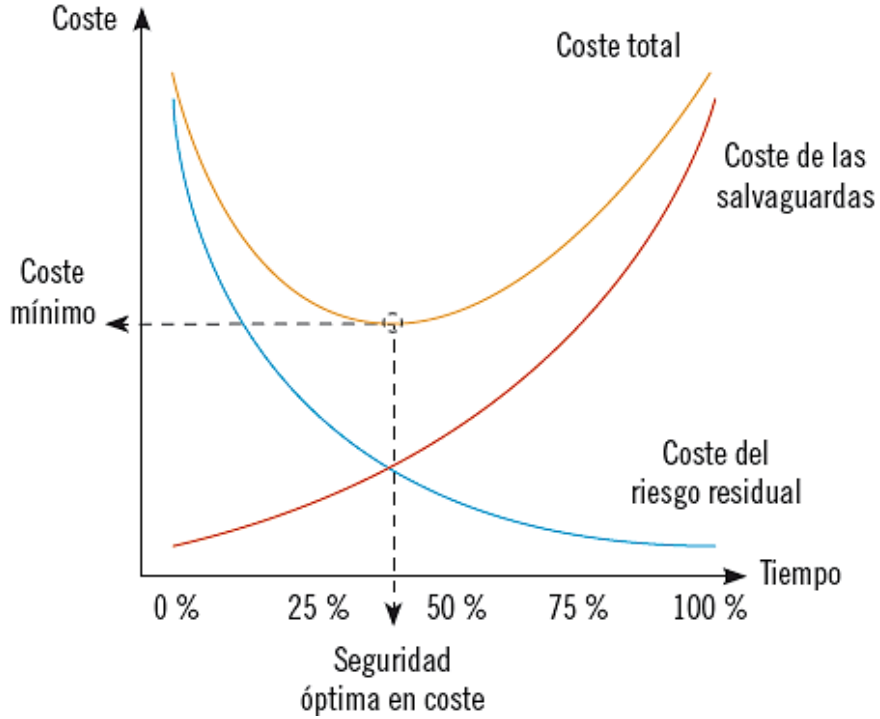
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

SELECCIÓN DE MEDIDAS A APLICAR

ESTA CURVA, NO SE PUEDE CALCULAR, Y PRETENDE REFLEJAR CONCEPTUALMENTE EL EQUILIBRIO QUE EL ANALISTA DE RIESGOS DEBE REALIZAR PARA SELECCIONAR UNA SALVAGUARDA U OTRA.

Representación conceptual del equilibrio económico para elegir una salvaguarda



4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

ACTITUD DE LA DIRECCIÓN

LA DIRECCIÓN DEBE DETERMINAR EL NIVEL DE IMPACTO Y RIESGO QUE ESTÁ DISPUESTA A ASUMIR.

LOS **REQUISITOS** QUE INTERVENDRÁN EN LA DETERMINACIÓN DE ESTE UMBRAL DE RIESGO SERÁN AL MENOS:

- **LEGALES**
- **OPERACIONALES O NORMATIVOS**
- **PARA EL LOGRO DE LOS OBJETIVOS DE LA EMPRESA**
- **ECONÓMICOS**

4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

GESTIÓN DEL RIESGO RESIDUAL

REVISIÓN DEL RIESGO INTRODUCIDO POR LAS SALVAGUARDAS

LAS SALVAGUARDAS INTRODUCEN INDIRECTAMENTE EN LOS SISTEMAS DE INFORMACIÓN **NUEVOS RIESGOS**, PORQUE LOS ACTIVOS A LOS QUE PROTEGEN PASAN A DEPENDER DE ELLAS, Y PORQUE LAS PROPIAS SALVAGUARDAS ESTÁN SUJETAS A AMENAZAS.

ES PRECISO ITERAR EL AGR, PARA QUE EL RIESGO RESIDUAL DEL SISTEMA CON LAS CONTRAMEDIDAS AÑADIDAS SEA INFERIOR AL RIESGO RESIDUAL PREVIO A LA ADICIÓN DE LA SALVAGUARDA.

ESTA DIFERENCIA ES LA **PROTECCIÓN EFECTIVA** QUE APORTAN.

CONTENIDOS

1. INTRODUCCIÓN
2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

RESUMEN

LA INVERSIÓN DE ESFUERZO EN SEGURIDAD DE LA INFORMACIÓN DEBE REALIZARSE SEGÚN UN MÉTODO DE ANÁLISIS Y GESTIÓN DE RIESGOS. **MAGERIT** ES UNA NORMA ESPAÑOLA, QUE CUMPLE PERFECTAMENTE ESTE COMETIDO, Y CUYO ANÁLISIS **CONSTA DE 5 PASOS**:

- EVALUACIÓN DE ACTIVOS **(1)**
- EVALUACIÓN DE AMENAZAS **(2)** EN TÉRMINOS DE LA DEGRADACIÓN
- CALCULAR EL IMPACTO **(4)**
- FRECUENCIA QUE DETERMINE EL RIESGO **(5)**
- EL PASO **(3)** ES CONSIDERAR LAS CONTRAMEDIDAS, Y SE REALIZA HABITUALMENTE DESPUÉS, PARA MEDIR LA MEJORA QUE APORTAN.

RESUMEN

LO IMPORTANTE, ES QUE **LOS CRITERIOS** APLICADOS **SE PONGAN POR ESCRITO**, **Y SE APLIQUEN DE MANERA HOMOGÉNEA** ENTRE SISTEMAS Y ANUALIDADES DEL AGR.

MAGERIT APORTA UNA **CLASIFICACIÓN DE LOS ACTIVOS**, Y UNA METODOLOGÍA PARA ORDENAR SUS DEPENDENCIAS JERÁRQUICAS, E INTRODUCE LOS CONCEPTOS DE IMPACTO ACUMULADO Y REPERCUTIDO, Y DE RIESGO ACUMULADO Y REPERCUTIDO.

TAMBIÉN APORTA UN **CATÁLOGO DE AMENAZAS**, INCLUIDA LA NATURALEZA DEL ACTIVO AFECTADO, Y LA PRIORIDAD DE LA DIMENSIÓN DE SEGURIDAD AFECTADA.

RESUMEN

TRAS EL ANÁLISIS DEL RIESGO RESIDUAL, SE DEBE GESTIONAR, MITIGÁNDOLO, EVITÁNDOLO, TRANSFIRIÉNDOLO, O ACEPTÁNDOLO.

SI LA OPCIÓN ES MITIGAR, SE ELIGEN **CONTRAMEDIDAS** SEGÚN SU EFECTO EN LA REDUCCIÓN DEL RIESGO, DEBIENDO SER PRIORITARIAMENTE **PREVENTIVAS, DE DETECCIÓN, Y REACTIVAS** (PRIMERO DE EMERGENCIA, Y DESPUÉS DE RECUPERACIÓN).

EN LA EVALUACIÓN ECONÓMICA, SE PERSEGUIRÁ EL **EQUILIBRIO ENTRE EL COSTE DE LA SEGURIDAD, Y EL COSTE DE LA INSEGURIDAD**.

RESUMEN

PARA LA APLICACIÓN DE SALVAGUARDAS, **MAGERIT** PROPONE UN **PROCEDIMIENTO ORDENADO**, QUE EXIGE:

- UNA POLÍTICA ORGANIZATIVA,
- UNOS OBJETIVOS DEFINIDOS PARA SABER SI EL RIESGO SE LOGRA REDUCIR
- UNAS INSTRUCCIONES PASO A PASO DE CÓMO PONER EN MARCHA LAS SALVAGUARDAS ELEGIDAS, PARA A CONTINUACIÓN APLICARLAS Y EVALUAR SU EFICACIA.


ESTO ES
TODO