IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

UD04

PLAN DE IMPLANTACIÓN DE SEGURIDAD

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO.
3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS.

1. INTRODUCCIÓN

HEMOS VISTO LOS CONCEPTOS FUNDAMENTALES DE LA **SEGURIDAD DE LA INFORMACIÓN (SI),** *LOS ACTIVOS, LAS AMENAZAS, EL IMPACTO, EL RIESGO*, Y SU NECESIDAD DE GESTIONARLO MEDIANTE UN **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).**

ADEMÁS, ESTUDIAMOS EL **BIA** PARA CONOCER SUS PROCESOS Y ACTIVOS CON UNA PERSPECTIVA ORIENTADA AL **ANÁLISIS Y GESTIÓN DE RIESGOS (AGR).**

1. INTRODUCCIÓN

EN ESTE CAPÍTULO SE ANALIZA , DENTRO DEL MARCO DE UN **SGSI**, CUÁLES SON LOS REQUISITOS Y CONDICIONES DEL **SI**.

LA DIFERENCIA ENTRE LO EXISTENTE Y LO DESEABLE ES LO QUE DEBE CORREGIRSE, MEDIANTE LA IMPLANTACIÓN DE CONTRAMEDIDAS.

TODO ELLO PARA ASEGURAR LA CONSECUCIÓN DE LOS **OBJETIVOS** DEL **SGSI:**

ESTABLECER, IMPLEMENTAR, OPERAR, MONITOREAR, REVISAR, MANTENER, Y MEJORAR LA SEGURIDAD DE LA INFORMACIÓN

CONTENIDOS

1. INTRODUCCIÓN
2. **DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO**
3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

LA NORMA **ISO 27001** DESCRIBE LOS REQUISITOS DEL ESTABLECIMIENTO Y ADMINISTRACIÓN DE UN **SGSI** EN 4 ETAPAS CÍCLICAS, QUE ENCIERRAN UNA EVALUACIÓN CONTINUA DE **¿DÓNDE QUEREMOS ESTAR? FRENTE A ¿DÓNDE ESTAMOS?**

Fase SGSI	Ciclo *Deming*	Preguntas	Conceptos claves de SI
Establecimiento	Planear	¿Dónde queremos estar?	Requisitos de Seguridad
Implementación y operación	Hacer	¿Cómo llegamos?	Implantación de salvaguardas
Monitorear y revisar	Verificar	¿Dónde estamos? ¿Hemos llegado?	Medida de eficacia de salvaguardas
Mantener y mejorar	Corregir	¿Cómo modificar el rumbo?	Medidas correctivas y lecciones aprendidas

Fases de un SGSI, y su relación con las fases del ciclo de mejora continua de Deming, con las preguntas esenciales que se responden con algunos conceptos claves.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DE LOS REQUISITOS DE SEGURIDAD

PARA UNA EMPRESA **ES ESENCIAL IDENTIFICAR SUS REQUISITOS DE SEGURIDAD**. YA HEMOS VISTO COMO DETERMINARLOS EN SUS **DIMENSIONES CIA** MEDIANTE **DOS TÉCNICAS** SENCILLAS:

- UN MÉTODO DE **VALORACIÓN CIA DE LOS PROCESOS**, COINCIDENTE CON LA VALORACIÓN CIA DE SU INFORMACIÓN CRUCIAL.
- UN SISTEMA CONSTRUCTIVO QUE, PARTIENDO DE LAS **VALORACIONES CIA DE LOS ACTIVOS INTEGRANTES DE UN PROCESO**, REPERCUTÍA EL VALOR, DE MANERA ASCENDENTE A LOS PROCESOS DE NEGOCIO DE LAS CAPAS SUPERIORES.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DE LOS REQUISITOS DE SEGURIDAD

SIN EMBARGO, ESTO NO ES SUFICIENTE, Y SE PRECISA ATENDER A OTRAS FUENTES DE INFORMACIÓN PARA ESTUDIAR LOS REQUISITOS DE SEGURIDAD DE LA EMPRESA DE UNA MANERA COMPLETA, MÁS AMPLIA.

SEGÚN LA **NORMA ISO 17799:2005** (EN LA QUE SE INSPIRA LA NORMA **ISO 27002**), **EXISTEN 3 FUENTES PRINCIPALES DE REQUERIMIENTOS DE SEGURIDAD**:

- **EVALUAR LOS RIESGOS PARA LA ORGANIZACIÓN**
- **LOS REQUISITOS LEGALES, REGULADORES, ESTATUTARIOS**
- **CONJUNTO PARTICULAR DE PRINCIPIOS, OBJETIVOS, Y REQUERIMIENTOS**

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DE LOS REQUISITOS DE SEGURIDAD

EVALUAR LOS RIESGOS PARA LA ORGANIZACIÓN

TOMANDO EN CUENTA LA ESTRATEGIA GENERAL, Y LOS OBJETIVOS DE LA EMPRESA.

AQUÍ SE RECURRE A UN **AGR**, IDENTIFICANDO LAS AMENAZAS PARA LOS ACTIVOS, SIEMPRE BAJO LA PERSPECTIVA DE LA ESTRATEGIA Y OBJETIVOS DE LA EMPRESA.

POR EJEMPLO, SEGÚN SE DESPRENDA DE UN **BIA**, Y TENIENDO EN MENTE QUE EL **AGR** DEBE SER PROPORCIONAL A SUS FINES.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DE LOS REQUISITOS DE SEGURIDAD

LOS REQUISITOS LEGALES, REGULADORES, ESTATUTARIOS

O LOS REQUISITOS INCLUIDOS O DERIVADOS DE LOS CONTRATOS CONTRAÍDOS POR LA EMPRESA CON SUS SOCIOS COMERCIALES, PROVEEDORES, Y CLIENTES.

SE INCLUYEN AQUÍ INCLUSO LAS NORMAS O BUENAS PRÁCTICAS DEL AMBIENTE SOCIAL Y CULTURAL EN QUE SE HALLE LA EMPRESA.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DE LOS REQUISITOS DE SEGURIDAD

CONJUNTO PARTICULAR DE PRINCIPIOS, OBJETIVOS, Y REQUERIMIENTOS

ESTO DA CABIDA A REQUISITOS CUALITATIVOS, QUE CONVIENE CONTROLAR: INTRODUCIÉNDOLOS EN EL **AGR** SIEMPRE QUE SEA POSIBLE, O COMO CONTRAMEDIDAS PARTICULARES, TAMBIÉN CABEN MÉTRICAS O FÓRMULAS, QUE PLASMEN CRITERIOS ESPECÍFICOS DE LA EMPRESA TRADUCIDOS AL **AGR**.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE

PARA DETERMINAR EL NIVEL DE SEGURIDAD EXISTENTE, HAY QUE **ESTUDIAR Y ANALIZAR** INFORMACIÓN PROCEDENTE BÁSICAMENTE DE **4 FUENTES**:

- **AUDITORÍAS BASADAS EN RIESGO, QUE IMPLICAN REALIZAR UN AR**
- **REGISTROS DE INCIDENTES DE SEGURIDAD**
- **MEDICIONES DE EFECTIVIDAD DE LAS SALVAGUARDAS**
- **SUGERENCIAS Y RETROALIMENTACIÓN DE LOS INTERESADOS**

LA INFORMACIÓN ANTERIOR DEBE EMPLEARSE PARA EVALUAR LOS REQUISITOS DE SEGURIDAD ESTABLECIDOS EN EL EPÍGRAFE ANTERIOR.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO

DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE

HABITUALMENTE **SE DEFINEN MÉTRICAS DE REQUISITOS PARTICULARES, Y SE EVALÚAN** PARA SABER EL GRADO DE CUMPLIMIENTO.

INCLUIRÁN RESULTADOS DEL **AGR**. **LO IMPORTANTE ES APLICARLAS DE MANERA HOMOGÉNEA, DOCUMENTÁNDOLAS** POR ESCRITO, **Y MANTENIÉNDOLAS EN EL TIEMPO**, PARA OBSERVAR LA TENDENCIA EN EL CUMPLIMIENTO DE LOS REQUISITOS Y NO SU VALOR ABSOLUTO.

LAS DIFERENCIAS ENTRE EL NIVEL DE SEGURIDAD EXISTENTE Y EL NIVEL REQUERIDO SERVIRÁN PARA ELABORAR UN **INFORME DE INSUFICIENCIAS** , QUE SERÁ EL PUNTO FINAL DEL **AR**.

CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO
3. **SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

A CONTINUACIÓN, SE PRESENTAN VARIOS **CRITERIOS PARA LA SELECCIÓN DE SALVAGUARDAS**.

LA NORMA **ISO 27002** NO DA MUCHOS DETALLES SOBRE LA SELECCIÓN, SINO MÁS BIEN SOBRE LOS OBJETIVOS QUE DEBEN ALCANZARSE.

POR OTRO LADO, EN **MAGERIT** SE ENCUENTRAN CRITERIOS MÁS PRECISOS, QUE RESULTAN PERFECTAMENTE VÁLIDOS PARA LA SELECCIÓN DE SALVAGUARDAS **ISO 27002**.

POR ESTE MOTIVO, SE ESTUDIARÁN PRIMERO LAS TÉCNICAS DE **MAGERIT**, Y DESPUÉS LAS DE **ISO 27002**.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

LA **APLICACIÓN DE CONTRAMEDIDAS** ES UN PROCESO QUE CONSISTE EN:

1. DETERMINAR RESPONSABLES
2. ESTABLECER OBJETIVOS PARA SABER QUE LA AMENAZA HA SIDO TRATADA
3. DAR PROCEDIMIENTOS PASO A PASO DE CÓMO EJECUTAR LA CONTRAMEDIDA
4. EJECUTAR LA CONTRAMEDIDA
5. EVALUAR SI TODO ESTÁ FUNCIONANDO SEGÚN LO PREVISTO

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

LO MÁS ABIERTO ES EL **PASO 3**, QUE CONLLEVA SELECCIONAR LAS SALVAGUARDAS.

EN ESTA SELECCIÓN RESULTARÁ MUY VALIOSA LA EXPERIENCIA, AUNQUE EN LA PRÁCTICA, LAS SITUACIONES MÁS HABITUALES ESTÁN PERFECTAMENTE DOCUMENTADAS, Y BASTA ELEGIR DE ENTRE UN CATÁLOGO EN FUNCIÓN DE LA MAGNITUD DEL RIESGO.

MAGERIT DEFINE UN **CRITERIO GENERAL**, Y UN **CRITERIO BASADO EN PÉRDIDAS Y GANANCIAS**.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO GENERAL DE SELECCIÓN

PRIORITARIAMENTE, DEBEN ELEGIRSE **CONTROLES PREVENTIVOS**.

ES NECESARIO DISPONER DE ELEMENTOS QUE DETECTEN EL INICIO DEL INCIDENTE LO ANTES POSIBLE: ESTOS SON LOS **CONTROLES DE DETECCIÓN**.

SEGUIDAMENTE, INTERVENDRÍAN LAS **MEDIDAS DE EMERGENCIA** (QUE BUSCAN PARAR Y LIMITAR EL INCIDENTE).

POR ÚLTIMO, LAS **MEDIDAS DE RECUPERACIÓN** (QUE BUSCAN REGRESAR A DONDE SE DEBE ESTAR).

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO GENERAL DE SELECCIÓN

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO GENERAL DE SELECCIÓN

ADEMÁS DE LA ANTERIOR PRECEDENCIA DE PRIORIDADES, **DEBE PERSEGUIRSE UN EQUILIBRIO ENTRE**:

- **CONTRAMEDIDAS TÉCNICAS**
- **CONTRAMEDIDAS FÍSICAS**
- **CONTRAMEDIDAS ORGANIZATIVAS**
- **LAS MEDIDAS DE POLÍTICA DE PERSONAL**

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO GENERAL DE SELECCIÓN

LA PROTECCIÓN INTEGRAL DE UN SISTEMA REQUIERE UNA COMBINACIÓN DE CONTROLES, DEBIENDO LA SOLUCIÓN FINAL:

- ESTAR EQUILIBRADA EN LOS DIFERENTES ASPECTOS (FASES DE INTERVENCIÓN Y NATURALEZA DE LA CONTRAMEDIDA).
- TENER EN CUENTA LAS SALVAGUARDAS ADECUADAS A LA AMENAZA.
- TENER EN CUENTA LAS SALVAGUARDAS ADECUADAS PARA CADA TIPO DE ACTIVOS, Y PARA LA DIMENSIÓN DE CADA ACTIVO.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO DE PÉRDIDAS Y GANANCIAS

HAY QUE BUSCAR EL EQUILIBRIO ENTRE EL COSTE DE LAS PÉRDIDAS POR UN INCIDENTE, Y EL COSTE DE LA GANANCIA EN SEGURIDAD QUE LO EVITE.

EL EQUILIBRIO SE ALCANZA CUANDO AMBOS COSTES SON MÍNIMOS.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO DE PÉRDIDAS Y GANANCIAS

GANANCIAS

SE DEBEN **REALIZAR VALORACIONES DEL COSTE DE LA SEGURIDAD** O CONTRAMEDIDAS, **FRENTE AL NIVEL DE PROTECCIÓN QUE LOGRAN**.

EXISTEN EN GENERAL TENDENCIAS CRECIENTES Y EXPONENCIALES (QUE REFLEJAN QUE INICIALMENTE SE LOGRA MUCHA SEGURIDAD CON POCA INVERSIÓN, Y QUE POSTERIORMENTE, INCLUSO PEQUEÑOS INCREMENTOS DE LA SEGURIDAD SON CADA VEZ MÁS CAROS).

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO DE PÉRDIDAS Y GANANCIAS

PÉRDIDAS

EL COSTE DE LA INSEGURIDAD O RIESGO **DECRECE EXPONENCIALMENTE** (REFLEJANDO QUE EL RIESGO DESCIENDE INICIALMENTE MUY RÁPIDO CON PEQUEÑAS MEDIDAS, PARA POSTERIORMENTE PRECISAR MUCHAS MEDIDAS PARA REDUCIRLO UN POCO).

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO DE PÉRDIDAS Y GANANCIAS

LA SITUACIÓN ANTERIOR **ES TEÓRICA**, Y PUEDE RESULTAR COMPLEJO REPRESENTAR. **EN LA PRÁCTICA, SE ESTUDIA EL COSTE FRENTE AL TIEMPO, Y PARA DIVERSOS ESCENARIOS** (E0, E1,... EN), EN LOS QUE SE APLICAN UN CONJUNTO DE CONTRAMEDIDAS DE LAS QUE SE EVALÚA SU COSTE ANUAL:

E0: SITUACIÓN EN LA QUE NO SE APLICA NINGUNA CONTRAMEDIDA.

E1: SITUACIÓN EN LA QUE SE APLICA UN CONJUNTO DE CONTRAMEDIDAS C1.

...

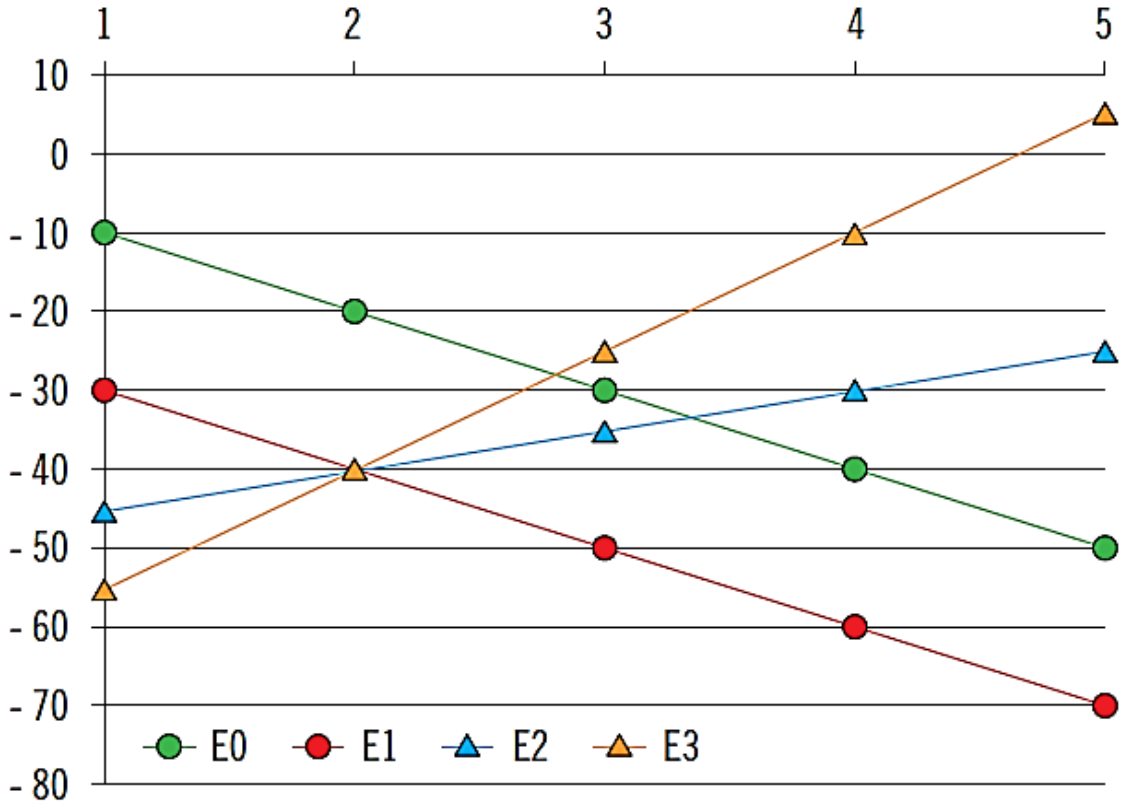
EN: SITUACIÓN PARA UN CONJUNTO DE CONTRAMEDIDAS CN.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CRITERIO DE PÉRDIDAS Y GANANCIAS

Representación del coste a 5 años de diferentes conjuntos de contramedidas



3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CATÁLOGO DE SALVAGUARDAS DE MAGERIT

MAGERIT CLASIFICA LAS SALVAGUARDAS EN 4 TIPOS:

- SOLUCIONES TÉCNICAS EN HARDWARE-SOFTWARE-COMUNICACIONES.
- SEGURIDAD FÍSICA DE LOS LOCALES Y ÁREAS DE TRABAJO
- MEDIDAS ORGANIZATIVAS O PROCEDIMIENTOS
- POLÍTICA DE PERSONAL

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CATÁLOGO DE SALVAGUARDAS DE MAGERIT

MAGERIT TAMBIÉN AGRUPA LAS SALVAGUARDAS **SEGÚN EL TIPO DE ACTIVO** AL QUE DEFIENDE:

- ENCONTRANDO SERVICIOS (CAPA 4)
- LA INFORMACIÓN O LOS DATOS (CAPA 3)
- LAS APLICACIONES, EQUIPOS, Y LAS COMUNICACIONES (EN CAPA 2)
- EL ENTORNO Y LAS PERSONAS (CAPA 1) CAPAS.

EXISTEN CONTROLES QUE AFECTAN A TODAS LAS CAPAS.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CATÁLOGO DE SALVAGUARDAS DE MAGERIT

LAS SALVAGUARDAS PERMITEN HACER FRENTE A LAS AMENAZAS. ÉSTAS, ESPECIALMENTE LAS TÉCNICAS, **VARÍAN CON EL AVANCE TECNOLÓGICO**

- PORQUE APARECEN TECNOLOGÍAS NUEVAS
- PORQUE VAN DESAPARECIENDO TECNOLOGÍAS ANTIGUAS
- PORQUE CAMBIAN LOS [TIPOS DE] ACTIVOS A CONSIDERAR
- PORQUE EVOLUCIONAN LAS POSIBILIDADES DE LOS ATACANTES
- PORQUE EVOLUCIONA EL CATÁLOGO DE SALVAGUARDAS DISPONIBLES

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

CATÁLOGO DE SALVAGUARDAS DE MAGERIT

EN CONSECUENCIA, ESTE CATÁLOGO DE SALVAGUARDAS NO ENTRA EN LA SELECCIÓN DE PAQUETES O PRODUCTOS A INSTALAR, **LIMITÁNDOSE A ESTABLECER UN PARAGUAS TAXONÓMICO** PARA ORDENAR Y CLASIFICAR LAS DIFERENTES CONCRECIONES MATERIALES, TECNOLÓGICAS, ORGANIZATIVAS Y PROCEDIMENTALES QUE SEAN DE APLICACIÓN EN CADA MOMENTO.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

CATÁLOGO DE SALVAGUARDAS DE MAGERIT

- PROTECCIONES GENERALES U HORIZONTALES
- PROTECCIÓN DE LOS DATOS / INFORMACIÓN
- PROTECCIÓN DE LAS CLAVES CRIPTOGRÁFICAS
- PROTECCIÓN DE LOS SERVICIOS
- PROTECCIÓN DE LAS APLICACIONES (SOFTWARE)
- PROTECCIÓN DE LOS EQUIPOS (HARDWARE)
- PROTECCIÓN DE LAS COMUNICACIONES
- PROTECCIÓN EN LOS PUNTOS DE INTERCONEXIÓN CON OTROS SISTEMAS
- PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN
- PROTECCIÓN DE LOS ELEMENTOS AUXILIARES
- SEGURIDAD FÍSICA – PROTECCIÓN DE LAS INSTALACIONES
- SALVAGUARDAS RELATIVAS AL PERSONAL
- SALVAGUARDAS DE TIPO ORGANIZATIVO
- CONTINUIDAD DE OPERACIONES
- EXTERNALIZACIÓN
- ADQUISICIÓN Y DESARROLLO

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

PROTECCIÓN BÁSICA SEGÚN MAGERIT

MAGERIT ES UN MÉTODO **MUY ADECUADO** PARA EL ANÁLISIS Y GESTIÓN DE RIESGOS.

POR CONTRAPARTIDA, PUEDE SER **LABORIOSO**, Y REQUERIR MUCHOS ESFUERZOS.

CONVIENE REALIZAR **APROXIMACIONES SUCESIVAS.** SE EMPIEZA POR UN ANÁLISIS DE ALTO NIVEL, IDENTIFICANDO RÁPIDAMENTE LO MÁS CRÍTICO.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT

PROTECCIÓN BÁSICA SEGÚN MAGERIT

LAS RECOMENDACIONES QUE MAGERIT DA COMO **PROTECCIÓN BÁSICA**, PERSIGUEN ORIENTARSE HACIA EL OBJETIVO DE CONTROLAR LOS RIESGOS, DESPLEGANDO RÁPIDAMENTE SISTEMAS RAZONABLEMENTE PROTEGIDOS, CUANDO NO HAY TIEMPO PARA UN ANÁLISIS DE RIESGOS COMPLETO.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN MAGERIT.

PROTECCIÓN BÁSICA SEGÚN MAGERIT

LAS MEDIDAS DE PROTECCIÓN BÁSICA CONSTITUYEN UNA **LÍNEA BASE** DE SEGURIDAD, QUE DEBE TENERSE EN TODOS LOS SISTEMAS DE INFORMACIÓN.

CONLLEVAN **MEDIDAS QUE PODRÍAN CALIFICARSE DE PURO SENTIDO COMÚN Y ABSOLUTAMENTE NECESARIAS**.

UNA VEZ ALCANZADA ESTA LÍNEA BASE, PUEDE PROGRESARSE A NIVELES MÁS ELABORADOS Y ESPECÍFICOS PARA CADA SUBSISTEMA.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN ISO 27001

EL **ANEXO A** DE LA **ISO 27001** CONTIENE UNA **LISTA DE 114 CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DE BUENAS PRÁCTICAS**. DEBERÁ CONSIDERAR CADA UNO DE ESTOS CONTROLES AL FORMULAR SU PLAN DE TRATAMIENTO DE RIESGOS.

LA DESCRIPCIÓN DE LA MAYORÍA DE LOS CONTROLES EN **MAGERIT** ES BASTANTE VAGA, POR LO QUE SE RECOMIENDA QUE REVISE LA **ISO 27002**, QUE CONTIENE MÁS INFORMACIÓN SOBRE SU IMPLEMENTACIÓN.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

SELECCIÓN DE CONTROLES EN ISO 27001

PARA CADA UNO DE LOS 114 CONTROLES DEBE REGISTRAR:

- **SI ES APLICABLE** A SUS ACTIVIDADES, PROCESOS Y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.
- **SI LO HAS IMPLEMENTADO O NO**.
- **SI LO HAS CONSIDERADO NO APLICABLE, SU JUSTIFICACIÓN** PARA HACERLO.

PARA LA MAYORÍA DE LAS ORGANIZACIONES, LOS 114 CONTROLES SERÁN APLICABLES, Y ES PROBABLE QUE YA HAYAN IMPLEMENTADO ALGUNOS DE ELLOS.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ANEXO A ISO 27001

Grupo		Descripción	Cant
5	Políticas de seguridad de la Información	Controles acerca de cómo deben ser escritas y revisadas las políticas.	2
6	Organización de la seguridad de la información	Controles acerca de cómo se asignan las responsabilidades; también incluye los controles para los dispositivos móviles y el teletrabajo.	7
7	Seguridad de los Recursos Humanos	Controles antes, durante y después de emplear.	6
8	Gestión de activos	Controles acerca de lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento.	10
9	Control de acceso	Controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario.	14
10	Criptografía	Controles relacionados con la gestión de encriptación y claves.	2
11	Seguridad física y del entorno	Controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.	15
12	Seguridad de las operaciones	Controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, vulnerabilidades, etc.	15
13	Seguridad de las comunicaciones	Controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc	7
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	Controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte.	13
15	Relación con proveedores	Controles acerca de qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores.	5
16	Gestión de incidentes de seguridad de la información	Controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias.	7
17	Aspectos de seguridad de la información para la gestión de la continuidad de negocio	Controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI.	4
18	Cumplimiento	Controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información	8

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

EXISTEN MUCHOS CATÁLOGOS DE CONTROLES QUE SE EMPLEAN COMO REFERENCIAS EN EL ÁMBITO DE LA SI, ENTRE LAS QUE DESTACAN POR SU AMPLIA ACEPTACIÓN:

- **IT-GRUNDSCHUTZ,** DE LA FEDERAL OFFICE FOR INFORMATION SECURITY (BSI)
- **ENISA** (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY)
- **ISF** (INFORMATION SECURITY FORUM)
- **ENS** (ESQUEMA NACIONAL DE SEGURIDAD)

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ADEMÁS DE LOS CATÁLOGOS ANTERIORES, EXISTEN **NORMAS Y MARCOS DE TRABAJO** QUE INCLUYEN CONJUNTOS COMPLETOS DE SALVAGUARDAS Y MEDIDAS DE SEGURIDAD.

A CONTINUACIÓN, SE RESUMEN LAS PRINCIPALES REFERENCIAS EN EL SECTOR DE LA **SI.**

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ISO 13335-4

ES UNA **NORMA ESPECÍFICA PARA LA SELECCIÓN DE SALVAGUARDAS**.

RESULTA ESPECIALMENTE VALIOSA, NO POR DAR UN EXHAUSTIVO CATÁLOGO DE SALVAGUARDAS, SINO POR PROPONER VARIOS MECANISMOS DE COMPLEJIDAD CRECIENTE, PARA DETERMINAR LOS CONTROLES QUE DEBERÍAN FORMAR PARTE DE LA LÍNEA BASE DE SEGURIDAD.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ISO 13335-4

- LÍNEA BASE DE SEGURIDAD, **DE ACUERDO AL TIPO DE SISTEMA** (ESTACIÓN DE TRABAJO AISLADA, ESTACIÓN DE TRABAJO CONECTADA A UNA RED SIN COMPARTIR RECURSOS, O SERVIDOR O ESTACIÓN DE TRABAJO CONECTADA A RED QUE COMPARTE RECURSOS).
- LÍNEA BASE DE SEGURIDAD **DE ACUERDO A LAS AMENAZAS** (AMENAZAS QUE PRODUCEN PÉRDIDA EN LA CONFIDENCIALIDAD, EN LA INTEGRIDAD, EN LA DISPONIBILIDAD, EN LA AUTENTICIDAD, EN LA DETERMINACIÓN DE LA RESPONSABILIDAD, Y EN LA CONFIABILIDAD).
- SELECCIÓN DE SALVAGUARDAS MEDIANTE **MECANISMOS MÁS DETALLADOS** DE ANÁLISIS DE RIESGOS DE LOS ACTIVOS.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S.)

SU *MANUAL AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK*, INCLUYE SALVAGUARDAS, AGRUPADAS EN:

- **CONTROLES DE GESTIÓN** (POLÍTICA DE SEGURIDAD EN COMPUTADORES, PROYECTOS Y PROGRAMAS DE GESTIÓN SEGURIDAD, GESTIÓN DEL RIESGO, ETC.).
- **CONTROLES DE OPERACIÓN** (PERSONAL, CONTINGENCIAS Y DESASTRES, GESTIÓN DE INCIDENTES, FORMACIÓN Y EDUCACIÓN, SEGURIDAD FÍSICA, ETC.).
- **CONTROLES TÉCNICOS** (IDENTIFICACIÓN Y AUTENTICACIÓN, CONTROL DE ACCESO LÓGICO, AUDITORÍAS, ENCRIPTACIÓN).

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY)

TÉCNICAS DE GESTIÓN DE LAS TIC, QUE INCLUYEN LA GESTIÓN DE LA SI. PUBLICADO POR **ISACA** (INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION), **COBIT** RESPALDA LA GESTIÓN Y GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN, PARA ASEGURAR QUE LAS TIC ESTÁN ALINEADAS CON LA EMPRESA.

ESTÁ ORIENTADO AL CONTROL, Y **DEFINE 34 PROCESOS CON MÁS DE 200 CONTROLES,** QUE TIENEN ENTRE SUS OBJETIVOS PROTEGER Y ASEGURAR LOS SISTEMAS DE INFORMACIÓN.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ENS (ESQUEMA NACIONAL DE SEGURIDAD)

EL **ENS** ES UNA NORMA CONCISA Y COMPLETA, QUE **DA CRITERIOS MUY SENCILLOS PARA PROTEGER LOS SISTEMAS DE INFORMACIÓN**, SEGÚN EL NIVEL DE LOS REQUISITOS, ELIGIENDO CONTROLES DE ENTRE SALVAGUARDAS ORGANIZATIVAS, DE TIPO OPERATIVO, Y MEDIDAS DE PROTECCIÓN DE CARÁCTER TÉCNICO.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ENS (ESQUEMA NACIONAL DE SEGURIDAD)

EL ENS **ESTABLECE LA POLÍTICA DE SEGURIDAD EN LA UTILIZACIÓN DE MEDIOS ELECTRÓNICOS**, Y ESTÁ CONSTITUIDO POR PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS PARA UNA ADECUADA SI.

SE DIRIGE A LAS ADMINISTRACIONES PÚBLICAS, PERO SU CONTENIDO ES VALIOSO Y DE UTILIDAD GENERAL.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ENS (ESQUEMA NACIONAL DE SEGURIDAD)

PROPORCIONA UN CRITERIO MUY SENCILLO, Y AMPLIAMENTE ACEPTADO **PARA VALORAR LOS REQUISITOS DE SI DE UNA ORGANIZACIÓN**:

- **NIVEL BAJO**
- **NIVEL MEDIO**
- **NIVEL ALTO**

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ENS (ESQUEMA NACIONAL DE SEGURIDAD)

- **NIVEL BAJO**

  CUANDO UN INCIDENTE SUPONGA UN **PERJUICIO LIMITADO** SOBRE LAS FUNCIONES DE LA ORGANIZACIÓN, SUS ACTIVOS, O LOS INDIVIDUOS AFECTADOS.

- **NIVEL MEDIO**

  CUANDO UN INCIDENTE SUPONGA UN **PERJUICIO GRAVE** SOBRE LAS FUNCIONES DE LA ORGANIZACIÓN, SUS ACTIVOS O LOS INDIVIDUOS AFECTADOS.

3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

OTROS CONTROLES

ENS (ESQUEMA NACIONAL DE SEGURIDAD)

- **NIVEL ALTO**

  CUANDO UN INCIDENTE SUPONGA UN **PERJUICIO MUY GRAVE** SOBRE LAS FUNCIONES DE LA ORGANIZACIÓN, SUS ACTIVOS O LOS INDIVIDUOS AFECTADOS.

CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO
3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
4. **GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS**

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

EN EL CAPÍTULO 1 SE PRESENTABAN LAS **FASES DE UN SGSI** INCLUYENDO LAS PREGUNTAS **¿DÓNDE QUEREMOS IR?** Y ***¿DÓNDE ESTAMOS?***

ESTE MOVIMIENTO DE LA POSICIÓN **CIA** DEL SISTEMA DE INFORMACIÓN, SE LLEVA A CABO **IMPLANTANDO LAS SALVAGUARDAS O CONTROLES SELECCIONADOS**.

LA IMPLANTACIÓN DE ESTAS SALVAGUARDAS SE REALIZA DE MANERA PLANIFICADA, Y **SE DEBE RECOGER EN UN DOCUMENTO**.

EN **ISO 27001** SE DEFINEN ALGUNOS **DOCUMENTOS A CONSIDERAR**, MIENTRAS QUE EN **MAGERIT** SE DEFINE **EL PLAN DE SEGURIDAD**.

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN PARA EL TRATAMIENTO DEL RIESGO EN ISO 27001

LA NORMA **ISO 27001** ESTABLECE QUE LA EMPRESA DEBERÁ PREPARAR UNA **DECLARACIÓN DE APLICABILIDAD**, QUE INCLUYA:

- **LOS OBJETIVOS DE CONTROL SELECCIONADOS Y POR QUÉ**, LOS OBJETIVOS DE CONTROL EXISTENTES, **Y** POR ÚLTIMO, **LOS OBJETIVOS DE CONTROL EXCLU**IDOS, Y POR QUÉ.
- PARTE DE LA **INFORMACIÓN NECESARIA PARA IMPLANTAR LAS SALVAGUARDAS**, PORQUE ESTABLECE LAS CONTRAMEDIDAS ELEGIDAS Y POR QUÉ, PERO NO ES COMPLETO.

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

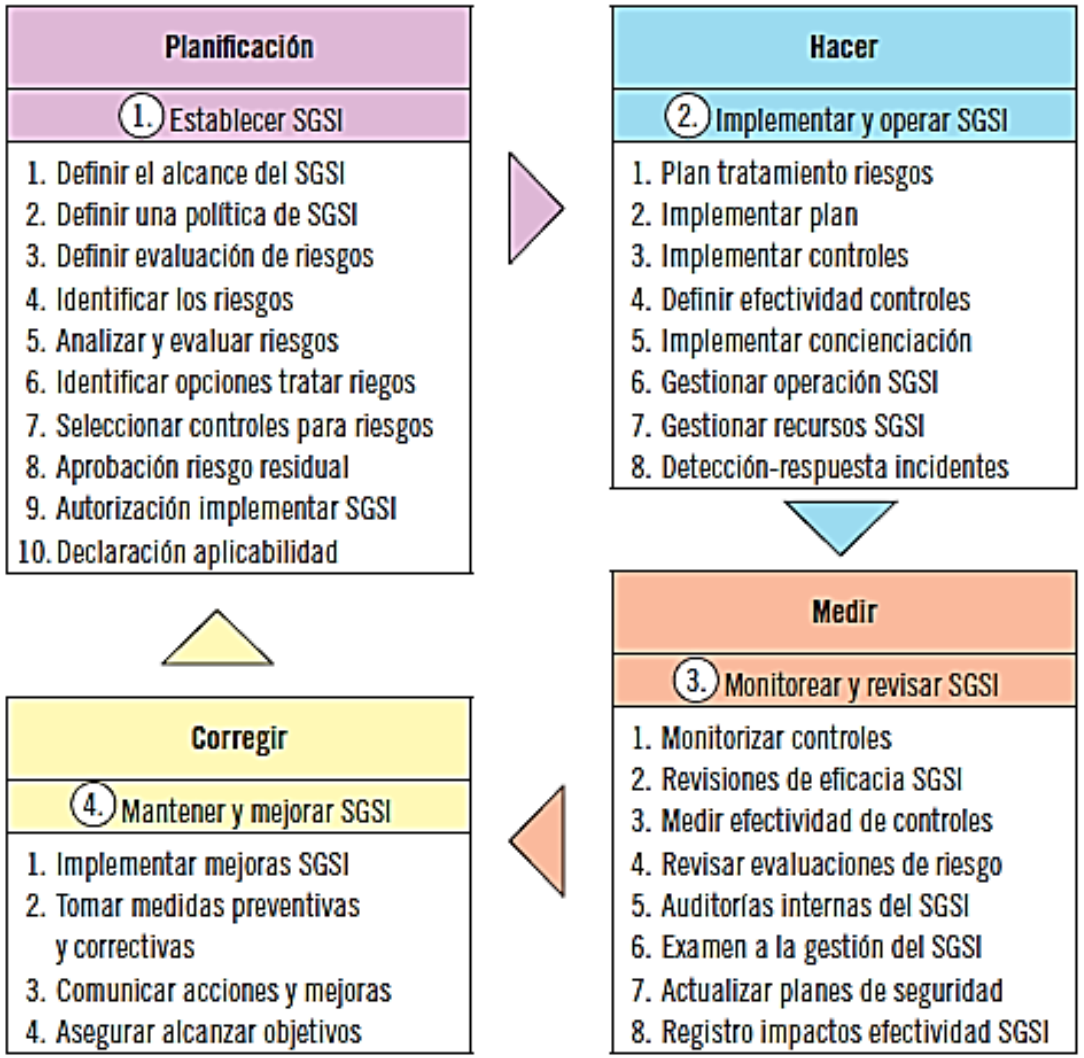
PLAN PARA EL TRATAMIENTO DEL RIESGO EN ISO 27001

CON UN CARÁCTER MÁS ORIENTADO A LA IMPLANTACIÓN, LA NORMA **ISO 27001 ESTABLECE QUE LA EMPRESA DEBERÁ REALIZAR UN PLAN DE TRATAMIENTO DE RIESGOS** QUE:

- **IDENTIFIQUE** LA ACCIÓN, LOS RECURSOS, LAS RESPONSABILIDADES Y LAS PRIORIDADES DE LA GERENCIA PARA MANEJAR LOS RIESGOS
- I**NCLUYA** CONSIDERAR LA FINANCIACIÓN Y LA ASIGNACIÓN DE FUNCIONES Y RESPONSABILIDADES
- **IMPLEMENTE** LOS CONTROLES SELECCIONADOS PARA CUMPLIR LOS OBJETIVOS DE CONTROL
- **DEFINA** CÓMO MEDIR LA EFECTIVIDAD DE LOS CONTROLES Y CÓMO USAR ESTAS MEDICIONES PARA EVALUAR LA EFICACIA DEL CONTROL DE MANERA COMPARATIVA Y REPRODUCIBLE

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

FASES SGSI



4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN PARA EL TRATAMIENTO DEL RIESGO EN ISO 27001

TAMBIÉN ES DE APLICACIÓN LA NORMA **ISO 27003**, QUE **GUÍA LA IMPLANTACIÓN DE UN SGSI** APOYÁNDOSE EN LA CONSTRUCCIÓN DE UN DOCUMENTO DE MUCHA MAYOR ENVERGADURA, EL **PLAN DEL PROYECTO SGSI**.

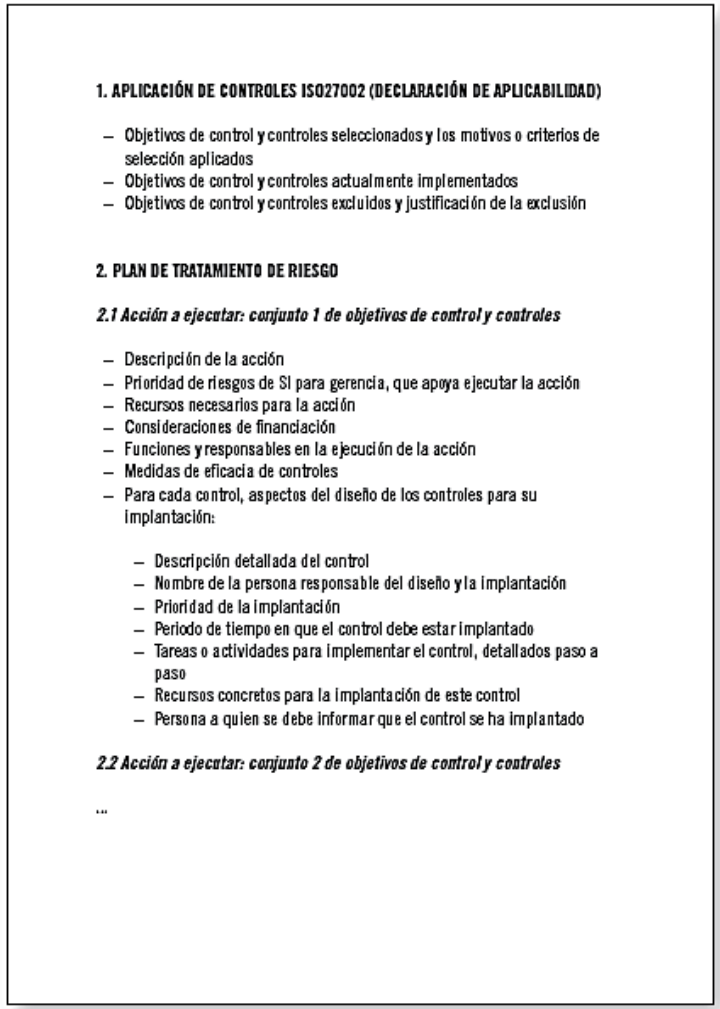
DENTRO DE ESTA NORMA **LOS PROCESOS 9.2 Y 9.3 SE DEDICAN AL DISEÑO DE CONTRAMEDIDAS**, RESPECTIVAMENTE EN LA SEGURIDAD ORGANIZACIONAL Y EN LA SEGURIDAD FÍSICA Y DE LAS TIC.

ESTOS PROCESOS DAN UNAS PAUTAS DE LA INFORMACIÓN QUE SE DEBE RECOGER DE CADA CONTROL, QUE RESULTAN MUY VALIOSAS PARA SU IMPLANTACIÓN.

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN PARA EL TRATAMIENTO DEL RIESGO EN ISO 27001

EL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SEGÚN SE RECOGE EN **ISO 27001**, Y CON LOS DETALLES DE **ISO 27003**, PUEDE SER UN DOCUMENTO CON LA SIGUIENTE ESTRUCTURA Y CONTENIDO:



1. APLICACIÓN DE CONTROLES ISO27002 (DECLARACIÓN DE APLICABILIDAD)

- Objetivos de control y controles seleccionados y los motivos o criterios de selección aplicados
- Objetivos de control y controles actualmente implementados
- Objetivos de control y controles excluidos y justificación de la exclusión

2. PLAN DE TRATAMIENTO DE RIESGO

2.1 Acción a ejecutar: conjunto 1 de objetivos de control y controles

- Descripción de la acción
- Prioridad de riesgos de SI para gerencia, que apoya ejecutar la acción
- Recursos necesarios para la acción
- Consideraciones de financiación
- Funciones y responsables en la ejecución de la acción
- Medidas de eficacia de controles
- Para cada control, aspectos del diseño de los controles para su implantación:
  - Descripción detallada del control
  - Nombre de la persona responsable del diseño y la implantación
  - Prioridad de la implantación
  - Periodo de tiempo en que el control debe estar implantado
  - Tareas o actividades para implementar el control, detallados paso a paso
  - Recursos concretos para la implantación de este control
  - Persona a quien se debe informar que el control se ha implantado

2.2 Acción a ejecutar: conjunto 2 de objetivos de control y controles

...

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN DE SEGURIDAD EN MAGERIT

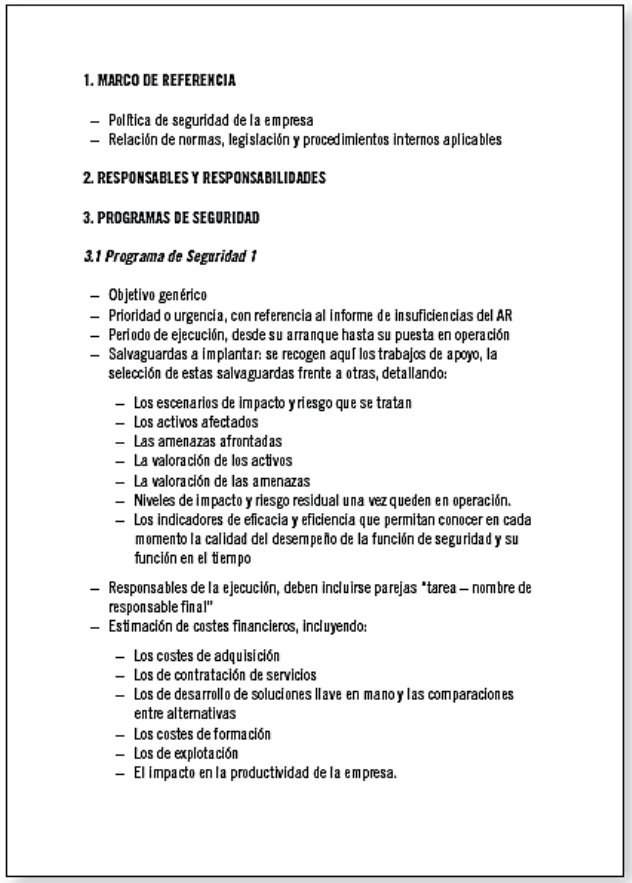
RECOGE EL CONJUNTO DE PROYECTOS (PROGRAMAS) QUE PERMITEN MATERIALIZAR LAS DECISIONES SOBRE LA GESTIÓN DE RIESGOS.

SE APOYA EN LOS DOCUMENTOS DEL AR (MODELO DE VALOR, MAPA DE RIESGOS, ESTADO DE RIESGOS, EVALUACIÓN DE SALVAGUARDAS, INFORME DE INSUFICIENCIAS), SIN REPETIRLOS, Y RECOGE LA INFORMACIÓN NECESARIA PARA LLEVAR A CABO LA IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS.

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN DE SEGURIDAD EN MAGERIT

LA GUÍA PARA ELABORAR ESTE PLAN DE SEGURIDAD PUEDE SER:



1. MARCO DE REFERENCIA

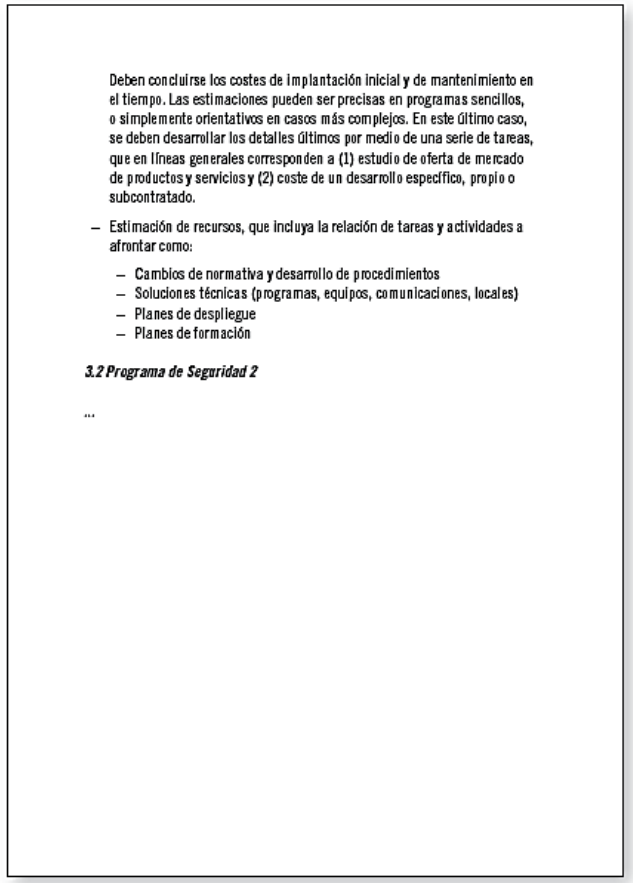
- Política de seguridad de la empresa
- Relación de normas, legislación y procedimientos internos aplicables

2. RESPONSABLES Y RESPONSABILIDADES

3. PROGRAMAS DE SEGURIDAD

3.1 Programa de Seguridad 1

- Objetivo genérico
- Prioridad o urgencia, con referencia al informe de insuficiencias del AR
- Periodo de ejecución, desde su arranque hasta su puesta en operación
- Salvaguardas a implantar: se recogen aquí los trabajos de apoyo, la selección de estas salvaguardas frente a otras, detallando:
  - Los escenarios de impacto y riesgo que se tratan
  - Los activos afectados
  - Las amenazas afrontadas
  - La valoración de los activos
  - La valoración de las amenazas
  - Niveles de impacto y riesgo residual una vez queden en operación.
  - Los indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad y su función en el tiempo
- Responsables de la ejecución, deben incluirse parejas "tarea – nombre de responsable final"
- Estimación de costes financieros, incluyendo:
  - Los costes de adquisición
  - Los de contratación de servicios
  - Los de desarrollo de soluciones llave en mano y las comparaciones entre alternativas
  - Los costes de formación
  - Los de explotación
  - El impacto en la productividad de la empresa.



Deben concluirse los costes de implantación inicial y de mantenimiento en el tiempo. Las estimaciones pueden ser precisas en programas sencillos, o simplemente orientativos en casos más complejos. En este último caso, se deben desarrollar los detalles últimos por medio de una serie de tareas, que en líneas generales corresponden a (1) estudio de oferta de mercado de productos y servicios y (2) coste de un desarrollo específico, propio o subcontratado.

- Estimación de recursos, que incluya la relación de tareas y actividades a afrontar como:
  - Cambios de normativa y desarrollo de procedimientos
  - Soluciones técnicas (programas, equipos, comunicaciones, locales)
  - Planes de despliegue
  - Planes de formación

3.2 Programa de Seguridad 2

...

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN DE SEGURIDAD EN MAGERIT

EL CONTENIDO ES MUY PARECIDO A LA GUÍA ELABORADA CON LAS NORMAS **ISO 27000**.

EN AMBOS CASOS, EL DETALLE SERÁ MÁS O MENOS EXHAUSTIVO, PERO **SIEMPRE DEBE APLICARSE UN CRITERIO DE PROPORCIONALIDAD**, DE MANERA QUE LA ELABORACIÓN DEL PLAN NO COMPROMETA LA IMPLANTACIÓN CONSECUENTE DEL MISMO.

4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

PLAN DE SEGURIDAD EN MAGERIT

EN CASO DE NECESITAR UNA VERSIÓN MÁS REDUCIDA, RESULTA COMÚN A AMBAS GUÍAS, Y POR LO TANTO **IMPRESCINDIBLE, DETALLAR**:

- **LO QUE SE HACE** (DESCRIPCIÓN DE LOS CONTROLES Y MEDIDA DE SU EFICACIA)
- **QUIÉN LO HACE** (RESPONSABLE)
- **CUÁNDO SE HACE** (PERIODO DE EJECUCIÓN)
- **CÓMO SE HACE** (ACTIVIDADES Y PROCEDIMIENTOS PASO A PASO)
- **POR QUÉ SE HACE** (PERSPECTIVA DE RIESGO PREVIO Y RESIDUAL
- **CUÁNTO CUESTA HACERLO** (RECURSOS Y COSTES FINANCIEROS)

CONTENIDOS

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO
3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

RESUMEN

LA INTERVENCIÓN EN **SI** PASA PRIMERO POR ANALIZAR LOS REQUISITOS QUE DEBE TENER LA EMPRESA.

LOS CRITERIOS PARA ESTO SON LAS LEYES, LAS NORMAS, LOS OBJETIVOS, Y LA RENTABILIDAD.

ESTOS CRITERIOS SUBYACEN EN LAS 3 FUENTES DE INFORMACIÓN QUE SE USAN PARA ACOTAR ESTOS REQUISITOS: UN **AGR**, EL CONJUNTO DE **REGULACIÓN Y NORMATIVA** QUE SE DEBE CUMPLIR, Y **LOS OBJETIVOS** (INCLUIDOS LOS COMERCIALES), QUE EL SISTEMA DE INFORMACIÓN DEBA CUMPLIR PARA SOSTENER LAS OPERACIONES.

RESUMEN

ESTA LABOR NO ES SENCILLA, Y DEBEN DEDICARSE RECURSOS PROPORCIONALES, Y UN ENFOQUE CONSTRUCTIVO DE MEJORA REITERADA. ES DECIR, LOS REQUISITOS PUEDEN SER EN UNA O EN TODAS LAS DIMENSIONES CIA (U OTRAS), Y PUEDEN FIJARSE PARA EL PROCESO MÁS CRÍTICO, PARA DOS, O PARA TODOS.

LOS REQUISITOS PUEDEN INCLUIR UNA LISTA DE CHEQUEO DE RESULTADOS O CONTROLES ESPECÍFICOS PARA LA EMPRESA.

UNA VEZ DETERMINADO EL PERFIL DE **SI** REQUERIDO, PROCEDE CONOCER DE QUÉ SITUACIÓN PARTE LA EMPRESA.

AQUÍ SE TRATA DE EVALUAR EL **SI** DE LA EMPRESA, Y NUEVAMENTE, NO ES TAREA SENCILLA RESUMIRLO EN UN NÚMERO O UNA PALABRA..

RESUMEN

LAS HERRAMIENTAS SON LOS **INFORMES DE AUDITORÍAS BASADAS EN RIESGO** QUE PUEDAN EXISTIR (Y QUE INCLUIRÁN UN AR QUE EXPRESE EL RIESGO RESIDUAL), UN **REGISTRO DE INCIDENTES DE SEGURIDAD** DEBIDAMENTE ENTENDIDO E INTERPRETADO, LAS **MEDICIONES DE EFECTIVIDAD DE LOS CONTROLES IMPLANTADAS**, Y **LAS OPINIONES O RECOMENDACIONES DE LOS INTERESADOS**, QUE PUEDAN SER RELEVANTES

LA DIFERENCIA ENTRE REQUISITOS DESEADOS Y GRADO DE CUMPLIMIENTO DE LOS MISMOS ES LA **MEJORA O DIFERENCIA** QUE SE DEBE LOGRAR.

PARA ELLO, SE APLICARÁN UNAS **CONTRAMEDIDAS** DIRIGIDAS A TENER MAYORES NIVELES CIA, QUE LOGRE QUE SE RESPONDA POSITIVAMENTE A TODAS LAS PREGUNTAS DE UNA LISTA DE CHEQUEO.

RESUMEN

LA SELECCIÓN DE ESTAS MEDIDAS ES UN TRABAJO DE DISEÑO, DONDE APLICAN CRITERIOS GENERALES Y OTROS ESPECÍFICOS DE **PÉRDIDAS Y GANANCIAS**.

SIEMPRE, ANTE LA DUDA, PUEDEN EMPLEARSE UN CONJUNTO DE **MEDIDAS MÍNIMAS**, O **LÍNEA BASE DE PARTIDA**.

CON FRECUENCIA SE ENCONTRARÁ QUE, BIEN APLICADA, PODRÍA SER SUFICIENTE EN LA MAYORÍA DE EMPRESAS Y CASUÍSTICAS.

PARA LA APLICACIÓN DE ESTE CONJUNTO DE SALVAGUARDAS MÍNIMO, U OTROS QUE SE DECIDAN AÑADIR, EL TRABAJO DEBE ORDENARSE EN TORNO A UN PLAN DE IMPLANTACIÓN. ESTE DOCUMENTO TIENE COMPONENTES COMUNES PARA LA ÓPTICA DE **ISO 27002**, O PARA LA PERSPECTIVA MAGERIT.

RESUMEN

SE TRATA DE ESTABLECER, PRIMERO, UN **MARCO DE REFERENCIA** Y UN **CONJUNTO DE PLANES DE ACCIÓN**, QUE AGRUPEN LOS PAQUETES DE SALVAGUARDAS O MEDIDAS A IMPLANTAR.

PARA CADA PROGRAMA O **PLAN DE ACCIÓN**, DEBE DARSE: **UNA DESCRIPCIÓN Y OBJETIVO, UNA PRIORIDAD, UN PERIODO DE EJECUCIÓN, UNOS RECURSOS, UNAS TAREAS A REALIZAR, EL DETALLE DE LA FINANCIACIÓN, UNOS RESPONSABLES, Y UNA MEDIDA DE LA EFICACIA**, QUE AFECTE A UNO O VARIOS DE LOS CONTROLES A IMPLANTAR.


ESTO ES
TODO