Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Plan de implantación de seguridad

- Introducción
- 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
- Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
- Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas
- Resumen

Introducción

Implementación de Mejoras en el SGSI

- En este capítulo, nos adentramos en la fase de implementación de mejoras dentro del Sistema de Gestión de la Seguridad de la Información (SGSI). Después de haber explorado conceptos fundamentales en seguridad de la información en los capítulos anteriores, como activos, amenazas, impacto y riesgo, es momento de materializar estas mejoras.
- Se profundiza en herramientas cruciales del SGSI, como el Análisis de Impacto en el Negocio (BIA), que proporciona una visión detallada de los procesos y activos del negocio desde una perspectiva de gestión de riesgos.
- Es importante ajustar estos métodos según el estado de madurez del SGSI, evitando un análisis excesivo que obstaculice la implementación efectiva de salvaguardas.
- El objetivo ahora es identificar los requisitos deseados de seguridad de la información para la empresa y compararlos con las condiciones existentes. La diferencia entre estas dos situaciones, conocida como "gap" de seguridad, debe abordarse mediante la implementación ordenada de contramedidas.
- El proceso de implementación debe seguir una serie de pasos para garantizar el logro de los objetivos del SGSI: establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

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

Gestión de SGSI

- La norma ISO 150 27001 establece los requisitos para la creación y gestión de un SGSI (Sistema de Gestión de la Seguridad de la Información).
- Se basa en un ciclo de 4 etapas cíclicas que implican una evaluación continua de los requisitos de seguridad deseados frente a los existentes.
- El enfoque se centra en responder a la pregunta "¿dónde queremos estar?" comparado con "¿dónde estamos?", lo que implica una mejora continua en la seguridad de la información.
- Este ciclo incluye la planificación, implementación, evaluación y mejora continua del SGSI para garantizar la eficacia y la adaptación a los cambios en el entorno de seguridad.

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

Gestión de SGSI

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.

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

Ciclo de Mejora Continua de Deming (PDCA)

Desarrollado por el Dr. W. Edwards Deming. Es un enfoque sistemático para la gestión de calidad y mejora continua.

Cuatro etapas cíclicas: Planificar, Hacer, Verificar, Actuar (PDCA).

- Planificar (Plan): Establecer objetivos, identificar problemas y diseñar planes de acción.
- Hacer (Do): Implementar los planes diseñados y recopilar datos relevantes.
- Verificar (Check): Medir el rendimiento del proceso y comparar resultados con los objetivos.
- Actuar (Act): Tomar medidas correctivas, implementar mejoras y ajustar planes.

Enfoque iterativo: Se repite para identificar áreas de mejora y optimizar continuamente el rendimiento.

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

Introducción

- Identificar y comprender los requisitos de seguridad es fundamental para cualquier empresa.
- En el capítulo que abordamos el Análisis del impacto de negocio, se profundizó en la determinación de estos requisitos, centrándose en los procesos de negocio.
- Se utilizan dos técnicas simples: una valoración CIA de procesos y un sistema constructivo que asciende desde los activos hasta los procesos de negocio.

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

Fuentes de Requerimientos de Seguridad

La norma 150 27002 identifica tres fuentes principales de requisitos de seguridad.

- Evaluar los riesgos para la organización implica considerar la estrategia y los objetivos empresariales en el Análisis y Gestión de Riesgos (AGR).
- Los requisitos legales, regulatorios y contractuales también influyen en los requisitos de seguridad.
- Los principios, objetivos y requerimientos comerciales del sistema de información completan las fuentes de requisitos.

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

Traducción de Requisitos

- Cada requisito se traduce en valoraciones de activos y, a menudo, en contramedidas específicas.
- Las contramedidas pueden introducir nuevos activos y amenazas, lo que requiere una revisión adicional del análisis de riesgos (AGR).
- Los requisitos también pueden derivarse de los principios, objetivos y necesidades comerciales específicas de la empresa.

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

Actualización de Requisitos

- Es esencial mantener actualizados los requisitos de seguridad mediante una evaluación metódica de los riesgos.

- Se deben considerar varios aspectos al actualizar los requisitos, incluidos los aspectos legales, operativos, los objetivos empresariales y la rentabilidad.

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

Decisión sobre Requisitos

- La toma de decisiones sobre los requisitos de seguridad implica equilibrar diferentes factores, como los requisitos legales, operativos, los objetivos empresariales y la rentabilidad.
- Los mismos criterios se utilizan tanto para decidir sobre los requisitos de seguridad como para la gestión del riesgo.
- Es fundamental que los requisitos de seguridad se actualicen y mantengan constantemente para garantizar la protección adecuada de la empresa y sus activos.

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

Monitoreo y Revisión del SGSI

En la fase de "Monitorear y revisar SGSI", se evalúa el estado actual del sistema de gestión de seguridad de la información (SGSI).

Esto implica realizar revisiones periódicas de la eficacia del SGSI, medir la efectividad de los controles, revisar las evaluaciones de riesgos y realizar auditorías internas del SGSI.

Fuentes de Información para Evaluar el Nivel de Seguridad

Para determinar el nivel de seguridad existente, se recopila información de cuatro fuentes principales: auditorías basadas en riesgo, registros de incidentes de seguridad, mediciones de efectividad de las salvaguardas, y sugerencias y retroalimentación de los interesados.

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

Evaluación de Requisitos de Seguridad

La información recopilada se utiliza para evaluar los requisitos de seguridad establecidos.

Esto puede incluir el valor de los activos, la estructura del sistema y la implementación de contramedidas específicas o el cumplimiento de métricas particulares de la empresa.

Ejemplos de Métricas de Evaluación

Se pueden emplear métricas específicas para valorar el nivel de seguridad existente.

Ejemplos incluyen el conteo de "no conformidades" en una auditoría ISO 27001, el cumplimiento de la legislación aplicable y el cumplimiento de cláusulas de contratos relacionadas con la seguridad de la información.

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

Elaboración del Informe de Insuficiencias

Las diferencias entre el nivel de seguridad existente y el nivel requerido se utilizan para elaborar un informe de insuficiencias.

Este informe documenta las áreas en las que el SGSI no cumple con los requisitos establecidos y proporciona una base para futuras mejoras.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Introducción

La selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información es crucial.

La norma ISO 27002 proporciona objetivos a alcanzar en lugar de detalles sobre la selección específica.

En contraste, MAGERIT ofrece criterios más precisos para la selección de salvaguardas, que son aplicables a las directrices de ISO 27002.

Se estudiarán las técnicas de MAGERIT seguidas por las de ISO 27002, y se considerarán otras referencias, como catálogos de salvaguardas, para una selección completa y efectiva.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de controles en MAGERIT

Proceso Ordenado de Aplicación de Contramedidas en MAGERIT:

- Determinar responsables: Designar quiénes serán los encargados de implementar las medidas de seguridad.
- Establecer objetivos: Definir claramente qué se espera lograr con cada contramedida para confirmar que la amenaza ha sido tratada.
- Proporcionar procedimientos: Detallar paso a paso cómo llevar a cabo cada contramedida para garantizar su correcta implementación.
- Ejecutar la contramedida: Poner en práctica las medidas de seguridad según lo planeado.
- Evaluar la efectividad: Realizar una evaluación para verificar si las contramedidas están funcionando según lo previsto y corregir cualquier problema identificado.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de controles en MAGERIT

Selección de Salvaguardas

Valor de la experiencia: La experiencia es útil para elegir las medidas de seguridad, pero existen situaciones habituales que ya está documentado como actuar, en un catálogo de actuaciones posibles, y basta elegir la salvaguarda en función de la magnitud del riesgo.

Criterios de selección: MAGERIT ofrece un criterio general y otro basado en consideraciones de pérdidas y ganancias.

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:

Prioridad en controles preventivos: Se enfoca en evitar que los incidentes de seguridad ocurran.

Elementos de detección: Se incluyen para identificar y responder rápidamente a los incidentes que ocurren.

Medidas de emergencia y recuperación: Para detener y limitar el impacto de los incidentes, y luego restaurar la normalidad.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de controles en MAGERIT

Equilibrio entre Contramedidas:

Diversidad de contramedidas: Se busca un equilibrio entre las contramedidas técnicas, físicas, organizativas y de política de personal.

Protección integral: Se requiere una combinación equilibrada de controles que tenga en cuenta las características específicas de las amenazas, los tipos de activos y sus dimensiones.

Son preferibles las salvaguardas de prevención a las de detección, emergencia o recuperación; pero deben existir para todas las fases del incidente de seguridad, y estar preferiblemente equilibradas en su naturaleza (técnicas, físicas, organizativas o de personal).

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de controles en MAGERIT

Selección de Contramedidas:

Facilidad de uso: Se prefieren las contramedidas que sean fáciles de usar, especialmente aquellas que son "transparentes" para el usuario, es decir, que no requieren acciones adicionales por parte del usuario.

Riesgo de uso indebido: Las contramedidas complejas pueden aumentar el riesgo de uso indebido, por lo que se deben evitar en la medida de lo posible.

Mantenimiento y actualización: Es crucial considerar que una vez seleccionada la solución, esta debe mantenerse actualizada, especialmente las salvaguardas técnicas, debido al avance tecnológico, la obsolescencia de tecnologías, cambios en tipos de activos y amenazas, y actualizaciones en catálogos de salvaguardas.

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:

Equilibrio económico: Se busca un equilibrio entre el coste de las pérdidas por un incidente y el coste de las contramedidas para evitarlo.

Ganancias: Se evalúa el coste de las contramedidas en relación con el nivel de protección que proporcionan. Existen tendencias crecientes y exponenciales en la relación entre inversión y seguridad.

Pérdidas: El coste del riesgo decrece exponencialmente. Inicialmente, pequeñas medidas reducen significativamente el riesgo, pero se requieren más medidas para reducirlo aún más.

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.

Evaluación del Coste:

- Escenarios: Se evalúa el coste a lo largo del tiempo (por ejemplo, para 5 años) y en diferentes escenarios, considerando conjuntos de contramedidas específicas.
- Cálculo del Coste: Se consideran los beneficios recurrentes de productividad y capacidad de la organización, junto con el coste recurrente del riesgo residual y el mantenimiento de las contramedidas.

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.

Cálculo del Costo Anual de Contramedidas:

Factores Considerados:

- Mejora de productividad recurrente.
- Mejora de la capacidad organizativa para ofrecer nuevos servicios.
- Reducción del riesgo residual recurrente.
- Costo de las contramedidas puntuales.
- Costo anual de mantenimiento recurrente.

Proceso de Cálculo:

Se suman los beneficios recurrentes y se restan los costos recurrentes para determinar el costo neto anual de las contramedidas.

Ejemplo:

Se evalúan los efectos financieros a lo largo del tiempo para tomar decisiones estratégicas sobre la inversión en seguridad.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

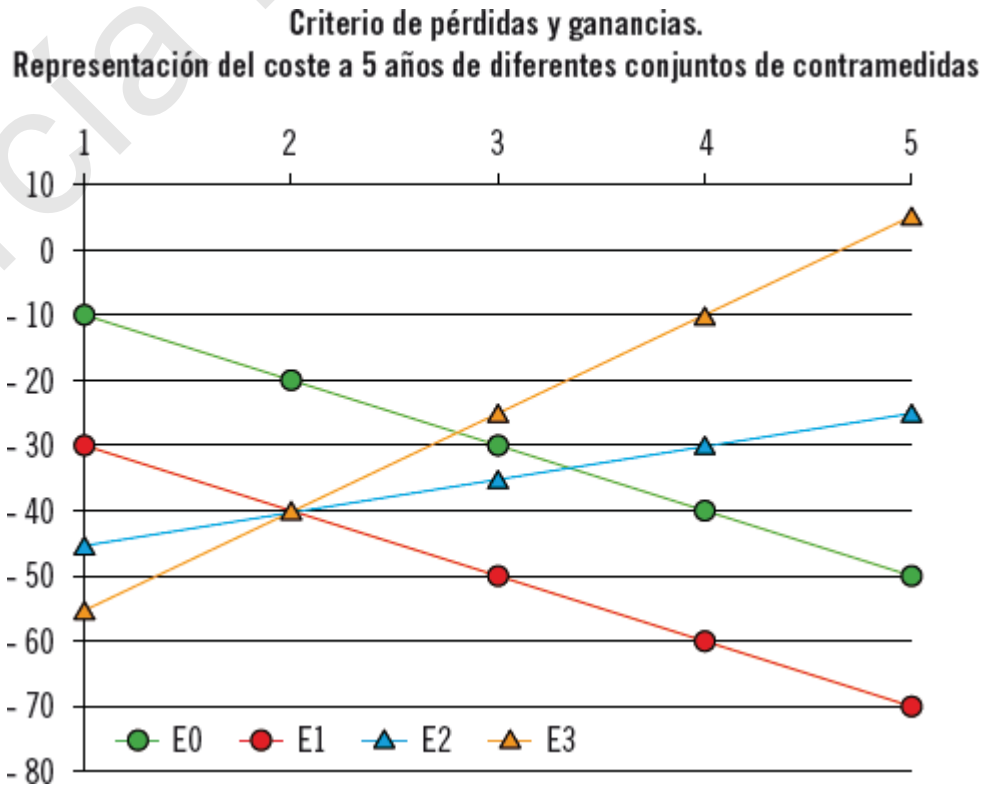
Selección de controles en MAGERIT

Criterio de Pérdidas y Ganancias.

Ejemplo Práctico:

Comparación de Escenarios: Se estudian diferentes conjuntos de contramedidas (E0, E1, E2, ….) y se calculan los costos para los primeros 5 años.

Interpretación de Costos: Se busca el escenario óptimo en el que la inversión inicial se recupera y se obtienen beneficios operativos a largo plazo.



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: medidas organizativas, política de personal, seguridad física, y soluciones técnicas.
- Las salvaguardas se agrupan según el tipo de activo que defienden, como servicios, información, aplicaciones, equipos, comunicaciones, entorno y personas.
- Existen controles que afectan a todas las capas de activos, proporcionando una cobertura integral de seguridad.

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 se agrupan en 42 contramedidas, abarcando áreas generales y específicas para cada tipo de activo.
- Se especifica la dimensión de seguridad afectada (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad).
- MAGERIT no tiene un catálogo fijo de salvaguardas, pudiendo variar según la necesidad y desglose de los controles.
- La flexibilidad del catálogo permite adaptarse a diferentes contextos y necesidades específicas de seguridad de la información.
- Es esencial comprender y aplicar adecuadamente las salvaguardas para garantizar una gestión efectiva de la seguridad de la información.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de controles en MAGERIT

Organización de activos en Magerit (Recordatorio)

Magerit clasifica los activos en 4 capas:

- Capa 4: Funciones y procesos (objetivos, bienes y servicios producidos).
- Capa 3: Información y datos.
- Capa 2: Sistema de información (aplicaciones, equipos, soportes, redes de comunicaciones).
- Capa 1: Entorno (equipamiento, suministros eléctricos, personal, edificio, mobiliario).

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 ofrece un método efectivo para el análisis y gestión de riesgos, aunque puede ser laborioso y requerir esfuerzos.

Las medidas de protección básica constituyen una "línea base" de seguridad y provienen de catálogos de contramedidas de normas internacionales como ISO 27002.

Permiten una implantación rápida y homogénea, pero pueden dejar desprotegido al sistema frente a amenazas reales no contempladas.

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 (Medidas)

- MAGERIT señala 12 medidas esenciales, evaluando el grado de seguridad de un sistema de información.
- Estas medidas abordan la protección en base a la tipificación, valor, amenazas y vulnerabilidades de los activos.
- Ejemplos incluyen el cifrado de datos sensibles, mantenimiento de equipos actualizado, y establecimiento de responsabilidades claras.
- La implementación de medidas de protección básica permite avanzar hacia niveles más elaborados de seguridad.
- Se debe tener en cuenta la evolución de las amenazas y tecnologías para mantener actualizadas las medidas de protección.
- La documentación y registro de estas medidas son fundamentales para una gestión efectiva de la seguridad de la información.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de Controles en ISO 27002

- Los controles en ISO 27002 deben reducir los riesgos a un nivel aceptable.
- Se consideran los requisitos legales, los objetivos organizacionales y operacionales, el costo de implementación y la necesidad de equilibrar la inversión con el daño probable.
- La selección de controles depende de decisiones empresariales basadas en la aceptación del riesgo y las regulaciones nacionales e internacionales.
- La norma ISO 27002:2013 define los controles para el desarrollo de un SGSI, agrupados en 14 dominios y 35 objetivos de control.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de Controles en ISO 27002

Línea Base de Seguridad en ISO 27001

- La norma establece una "línea base de seguridad" como punto de inicio para la seguridad de la información.
- Estos principios guía, esenciales y de práctica común, no reemplazan la evaluación del riesgo.
- La norma recomienda una declaración de aplicabilidad que incluya controles seleccionados, existentes y excluidos, justificando su elección.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de Controles en ISO 27002

La norma ISO 27001 marca que debe existir un documento que proporcione un resumen de las decisiones referentes a la selección de salvaguardas y tratamiento del riesgo. Este documento se denomina **declaración de aplicabilidad**, y debe incluir al menos lo siguiente:

- Controles seleccionados. Incluir los objetivos de control y los controles seleccionados, así como los motivos para seleccionarlos.
- Controles existentes. Incluir los objetivos de control y los controles actualmente implementados.
- Controles excluidos. Se deben enumerar expresamente los objetivos de control y los controles, excluidos de los propuestos en el anexo A de la norma ISO 27001 (es decir, los recomendados por la norma ISO 27002, justificando por qué se excluyen.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Selección de Controles en ISO 27002

Comparación de Controles de ISO 27002 y MAGERIT

- Se puede comparar los controles esenciales y de práctica común de ISO 27002 y MAGERIT.
- Estos controles son aplicables a la mayoría de las organizaciones y representan un punto de inicio para la seguridad de la información.
- La declaración de aplicabilidad en ISO 27001 documenta los controles seleccionados, existentes y excluidos, justificando su elección.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Otros controles

Catálogos de Controles en Seguridad de la Información

- En el ámbito de la Seguridad de la Información, se utilizan diversos catálogos de controles como referencia.
- Destacan "IT-Grundschutz" de la BSI, ENISA y el ISF, entre otros.
- Estos catálogos ofrecen una amplia gama de salvaguardas divididas en diferentes categorías para gestionar los riesgos de seguridad.

Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

Otros controles

Esquema Nacional de Seguridad (ENS)

- El ENS establece la política de seguridad en la utilización de medios electrónicos y proporciona requisitos mínimos para una adecuada seguridad de la información.
- Define niveles de seguridad (bajo, medio, alto) y establece medidas específicas para cada nivel.
- El cumplimiento del ENS es fundamental para garantizar la protección de los sistemas de información, especialmente en el contexto de las Administraciones Públicas.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Introducción

- La implantación de las salvaguardas seleccionadas es una fase crucial en el desarrollo de un Sistema de Gestión de la Seguridad de la Información (SGSI).
- Este proceso implica un movimiento o modificación de la posición de la confidencialidad, integridad y disponibilidad (CIA) del sistema de información.
- La implantación se lleva a cabo de manera planificada y se documenta en un plan de implantación de salvaguardas.
- En ISO 27001, se definen algunos documentos a considerar durante este proceso, mientras que en MAGERIT se establece el plan de seguridad como parte esencial del proceso de implantación.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Plan para el tratamiento del riesgo en ISO 27001

Declaración de Aplicabilidad (DoA)

- La norma ISO 27001 requiere la preparación de una Declaración de Aplicabilidad (DoA) como parte del establecimiento del SGSI.
- La DoA incluye los objetivos de control seleccionados y las razones detrás de su elección, los objetivos de control existentes y los excluidos.
- Proporciona información crucial para la implantación de salvaguardas al establecer contramedidas elegidas y justificar su selección.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Plan para el tratamiento del riesgo en ISO 27001

Plan de Tratamiento de Riesgos

- La norma ISO 27001 también exige la formulación de un Plan de Tratamiento de Riesgos como parte de la implementación y operación del SGSI.
- Este plan identifica acciones, recursos, responsabilidades y prioridades de la gerencia para manejar los riesgos de seguridad de la información.
- Incluye consideraciones financieras, asignación de funciones y responsabilidades, implementación de controles seleccionados y definición de medidas para evaluar su efectividad.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Plan para el tratamiento del riesgo en ISO 27001

Plan del Proyecto SGSI

- La norma ISO 27003 guía la implementación de un SGSI mediante la construcción de un Plan del Proyecto SGSI.
- Este documento, de mayor envergadura, incluye procesos específicos para el diseño de contramedidas en la seguridad organizacional y física de las TIC.
- Proporciona pautas detalladas sobre la información necesaria para la implantación efectiva de las salvaguardas.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Plan de seguridad en MAGERIT

Componentes del Plan de Seguridad

- El plan de seguridad recoge los proyectos (programas) para implementar las decisiones sobre la Gestión de Riesgos.
- Se basa en los documentos del Análisis de Riesgos (AR), como el modelo de valor, mapa de riesgos, estado de riesgos, evaluación de salvaguardas e informe de insuficiencias.
- Incluye información detallada sobre la implantación de las salvaguardas seleccionadas, como prioridad, periodo de ejecución, salvaguardas a implantar, responsables, costes financieros y recursos necesarios.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Plan de seguridad en MAGERIT

Detalles del Plan de Seguridad

- Las salvaguardas a implantar incluyen escenarios de impacto y riesgo tratados, activos afectados, amenazas enfrentadas, valoración de activos y amenazas, y niveles de impacto y riesgo residual.
- Se establecen indicadores de eficacia y eficiencia para evaluar la calidad del desempeño de la función de seguridad a lo largo del tiempo.
- Se estiman los costes financieros, incluyendo adquisición, contratación de servicios, desarrollo de soluciones, formación, explotación y su impacto en la productividad.

Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

Plan de seguridad en MAGERIT

Consideraciones Finales

- El contenido del plan es similar a las guías elaboradas con las normas ISO 27000, enfocándose en describir qué se hace, quién lo hace, cuándo se hace, cómo se hace, por qué se hace y cuánto cuesta hacerlo.
- Se enfatiza la necesidad de aplicar un criterio de proporcionalidad para que la elaboración del plan no comprometa su implantación.
- En resumen, el plan de seguridad proporciona una hoja de ruta detallada para la implementación efectiva de las salvaguardas seleccionadas.

Resumen

Análisis de Requisitos y Evaluación de la Situación

- El primer paso en la intervención en Seguridad de la Información (SI) implica analizar los requisitos de la empresa, considerando leyes, normas, objetivos y rentabilidad.
- Estos requisitos pueden abordar aspectos de confidencialidad, integridad, disponibilidad (CIA) y otros, adaptados a procesos críticos o generales.
- Se requiere un enfoque constructivo y recursos proporcionales para esta tarea, que puede implicar una lista de chequeo de controles específicos para la empresa.

Resumen

Identificación de Brechas y Diseño de Contramedidas

- Tras establecer los requisitos, se evalúa la situación actual de la empresa mediante informes de auditoría, registros de incidentes, mediciones de efectividad de controles y opiniones de los interesados.
- La diferencia entre los requisitos deseados y el grado de cumplimiento actual determina la mejora necesaria.
- Se diseñan contramedidas dirigidas a mejorar la seguridad y cumplir requisitos específicos, utilizando criterios generales y específicos de pérdidas y ganancias.

Resumen

Selección y Planificación de Contramedidas

- La selección de contramedidas se realiza mediante un enfoque de diseño, considerando criterios generales y específicos, así como un conjunto mínimo de medidas de seguridad que puede ser suficiente para muchas empresas.
- Se planifica la aplicación de estas contramedidas en un documento que incluye objetivos, prioridades, periodos de ejecución, recursos, responsables y medidas de eficacia.
- Este proceso de selección y planificación puede ser común para las perspectivas de ISO 27002 y MAGERIT, adaptándose a las necesidades y características de cada organización.