SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.1.0. Capítulo 1

Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Los equipos informáticos ejecutan aplicaciones que manejan información importante:

- **Datos financieros**
- **Datos de carácter estratégico**
- **Controlan procesos productivos**
- **Hospitales y laboratorios.**
- **Plantas de producción y distribución eléctrica, centrales nucleares,**
- **Sistemas de transporte aéreo o ferroviario,**
- **Infraestructuras de telecomunicaciones,**
- **Sistemas de defensa.**

2. MODELO DE SEGURIDAD

Problema de seguridad :

- **Amenaza**
- **Vulnerabilidad**
- **Incidente de seguridad**

2. MODELO DE SEGURIDAD

Definición de 'seguridad de la información':

- **ISO 17799 e ISO 27001**

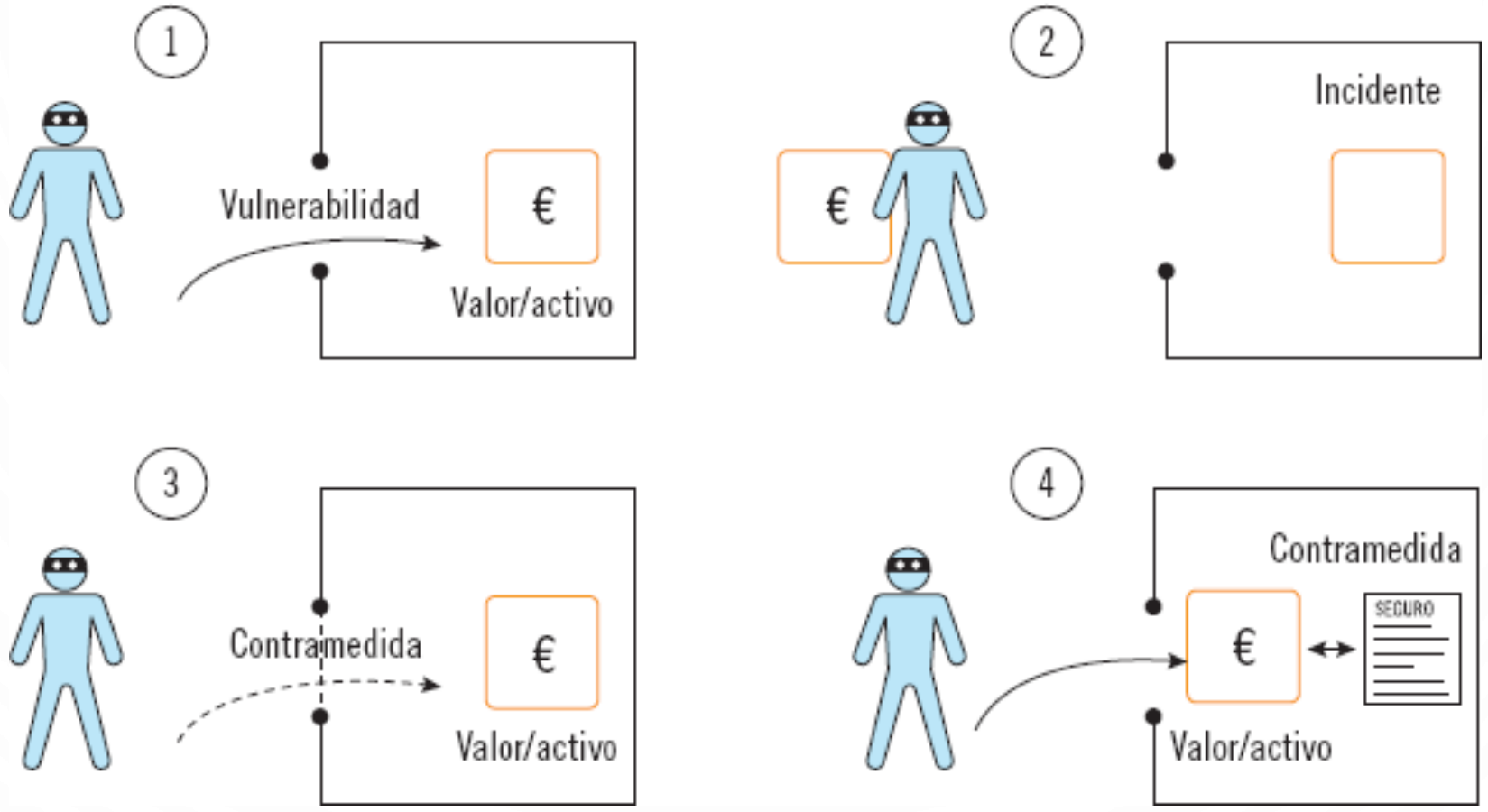
  "la preservación de confidencialidad, integridad y disponibilidad de la información"

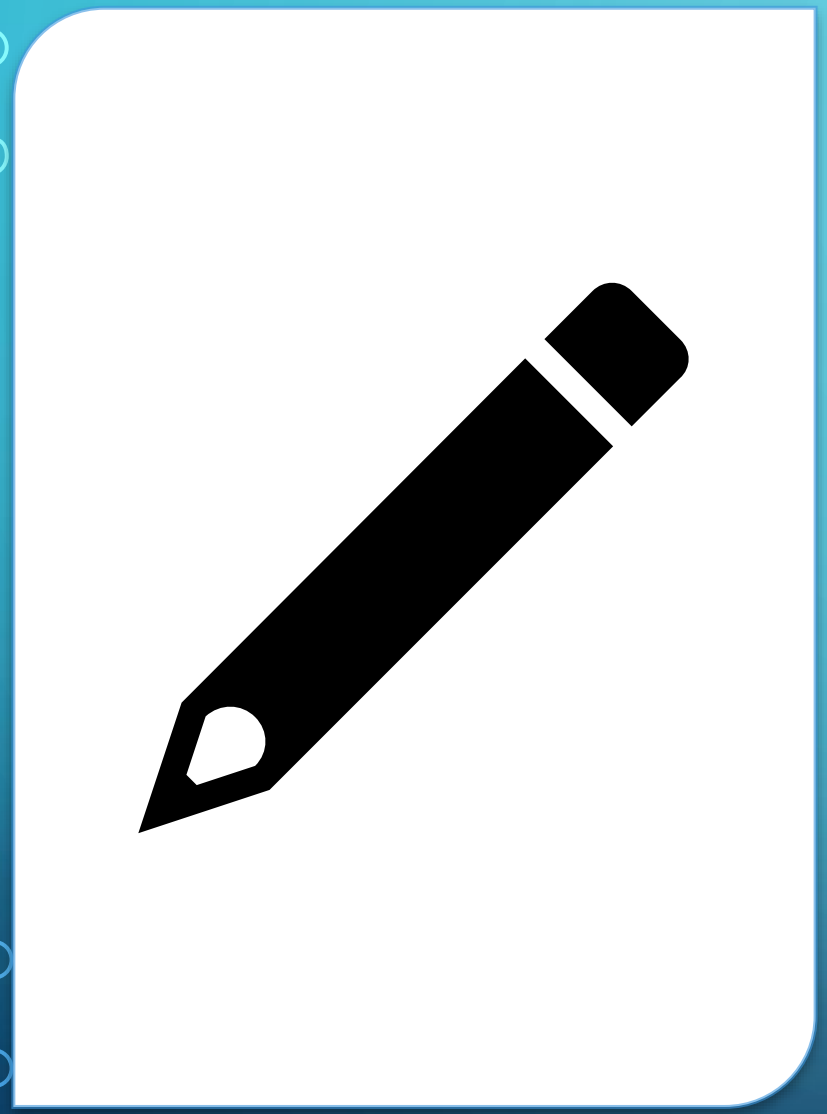
- **MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del Ministerio de Administraciones Públicas)**

  "la capacidad de las redes o de los sistemas de información, de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles"

2. MODELO DE SEGURIDAD

Representación gráfica de los conceptos de amenaza y vulnerabilidad (1) de un objeto valioso para la empresa o activo. El incidente de seguridad (2) es la suma de la existencia de la amenaza y de la vulnerabilidad. Las posibles contramedidas incluyen dificultar la ocurrencia del incidente (3), reduciendo su probabilidad, o reducir el daño, reembolsando parte del importe robado (4)





Actividades

INTENTE CLASIFICAR LAS SIGUIENTES AMENAZAS SEGÚN SEAN “NATURALES O FABRICADAS”, “ACCIDENTALES O INTENCIONADAS”, Y “HUMANAS O AMBIENTALES”, JUSTIFICANDO LAS SUPOSICIONES QUE SE PRECISEN AÑADIR: INCENDIO DEL EDIFICIO, SEÍSMO, INUNDACIÓN POR PRECIPITACIONES, GUERRA, ROBO, VIRUS INFORMÁTICO, Y FALLO EN DISCO DURO.

IDENTIFIQUE LAS AMENAZAS Y VULNERABILIDADES QUE PERMITIERON LA OCURRENCIA DE LOS SIGUIENTES INCIDENTES DE SEGURIDAD, ASÍ COMO LOS DAÑOS PRODUCIDOS:

UN VIRUS HA BORRADO ARCHIVOS DEL SISTEMA OPERATIVO, Y AHORA NO ARRANCA.
EL INCENDIO DE LA TORRE WINDSOR DESTRUYÓ LOS SERVIDORES DEL CENTRO DE PROCESO DE DATOS, PERDIÉNDOSE MUCHOS ARCHIVOS DIGITALES.
EL CAFÉ SE CAYÓ SOBRE EL TECLADO, PRODUCIENDO UN CORTOCIRCUITO QUE APAGÓ EL ORDENADOR, Y SE PERDIERON LOS DOCUMENTOS QUE NO SE HABÍAN GUARDADO.

2. MODELO DE SEGURIDAD

Triada de la seguridad de la información (CIA)

Asegurar que la información es accesible solo para aquellos autorizados a tener acceso.

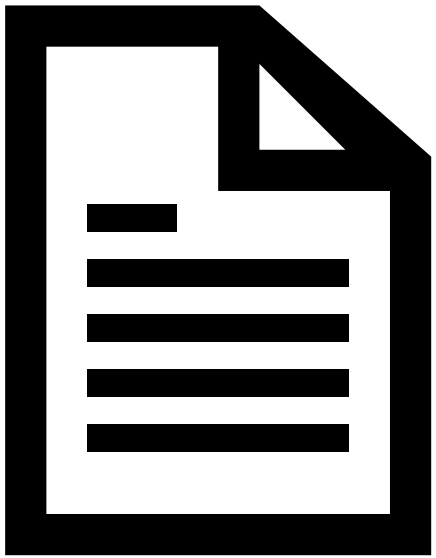
Garantizar la exactitud y completitud de la información y los métodos de su proceso

Asegurar que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

2. MODELO DE SEGURIDAD

Riesgo de un incidente de seguridad

Riesgo = (probabilidad de ocurrencia de la amenaza) x (impacto o daño)

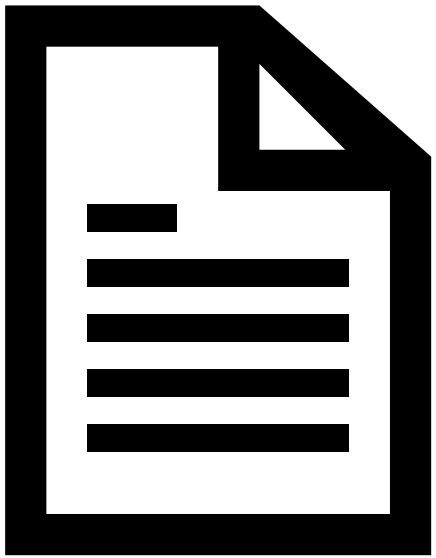


Ejemplo

SE PARTE DE UNA EMPRESA QUE PROVEE ALOJAMIENTO DE PÁGINAS WEB, CON UN SISTEMA DE INFORMACIÓN VALORADO EN 250.000 €. UN ANÁLISIS DE RIESGOS REVELA QUE HAY DOS AMENAZAS:

UN FALLO DEL SUMINISTRO ELÉCTRICO, CARACTERIZADO POR:
IMPACTO O DAÑO = 10.000 €
PROBABILIDAD DE OCURRENCIA DE LA AMENAZA= 0. 1
UN ATAQUE DIRIGIDO DESDE INTERNET, CARACTERIZADO POR:
IMPACTO O DAÑO =500.000 €
PROBABILIDAD DE OCURRENCIA DE LA AMENAZA= 0.005
EL MODELO DE SEGURIDAD DE LA EMPRESA TIENE EL CRITERIO DE "OPTIMIZAR LA INVERSIÓN CONCENTRANDO LOS RECURSOS EN ELIMINAR LA MAYOR AMENAZA, Y ASUMIR EL RIESGO DE LAS AMENAZAS MENORES". SE PIDE QUE:

SE CUANTIFIQUE EL RIESGO DE CADA AMENAZA.
SE CALCULE EL PRESUPUESTO EN SEGURIDAD QUE RESULTARÍA JUSTIFICADO INVERTIR.
SE CALCULE EL RIESGO QUE ASUME LA EMPRESA TRAS LA INVERSIÓN.



Ejemplo. Solución

CÁLCULO DE RIESGOS:

AMENAZA 1: RIESGO = 10.000 X 0. 1 = 1.000 €.
AMENAZA 2: RIESGO = 500.000 X 0.005 = 2.500 €.
LA AMENAZA 2, PESE A SER VEINTE VECES MENOS PROBABLE QUE LA AMENAZA 1, ES LA DE MAYOR RIESGO A CAUSA DE SU ELEVADO IMPACTO.

PRESUPUESTO EN SEGURIDAD:

EL MODELO DE SEGURIDAD INDICA QUE, POR CRITERIO DE LA EMPRESA, DEBE ELIMINARSE LA MAYOR AMENAZA, QUE ES LA QUE TIENE UN RIESGO DE 2.500 €. EL PRESUPUESTO QUE SE PUEDE DEDICAR A COMBATIR LA AMENAZA ES DE 2.500 €.

RIESGO TRAS LA INVERSIÓN:

EL MODELO DE SEGURIDAD INDICA QUE, POR CRITERIO DE LA EMPRESA, SE ASUME EL RIESGO DEL RESTO DE AMENAZAS, ES DECIR EL DE AMENAZA 1. EL RIESGO ASUMIDO RESULTANTE ES DE 1.000 €.

2. MODELO DE SEGURIDAD

Para estudiar el riesgo, existen dos pasos claramente diferenciados:

- **El análisis de riesgos, que consiste en identificar amenazas, determinar las vulnerabilidades, y medir el impacto o daño que causaría un incidente. Se pueden emplear métodos cuantitativos (como en la aplicación práctica anterior), o cualitativos (valorando el riesgo en muy alto, alto, bajo, medio, etc.), para ordenar los riesgos.**
- **La gestión de riesgos, que partiendo de los resultados del análisis de riesgos, y una vez determinados los criterios para aceptar un riesgo (legales, económicos, etc.), permite elegir las contramedidas de seguridad que se implantarán.**

El análisis y gestión de riesgos aporta un valor extraordinario a la gestión de seguridad, reduciendo la probabilidad de fracaso de una empresa, y protegiéndola, al ser una herramienta que facilita que la actividad futura se realice de manera efectiva y controlada.

3. AMENAZAS, RIESGOS Y SALVAGUARDAS

Para determinar las amenazas, o encontrar nuevas, ayudará saber que pueden clasificarse como:

- **Amenazas naturales o artificiales.**
- **Amenazas debidas al entorno (ambiente), o debidas al hombre.**
- **Amenazas accidentales o intencionadas.**

Ver capítulo 5 del documento:

1.1.2.Magerit_v3_libro2_catalogo_elementos

4. SALVAGUARDAS Y CONTRAMEDIDAS MÁS HABITUALES

Las salvaguardas, o contramedidas, persiguen detectar, prevenir, impedir, reducir, y controlar una amenaza y el daño que pueda generar.

Por ejemplo:

- **Salvaguardas preventivas o proactivas, que persiguen anticiparse a la ocurrencia del incidente.**
- **Salvaguardas reactivas, que persiguen reducir el daño una vez ocurre el incidente.**
- **Salvaguarda de "no hacer nada", o de aceptar el riesgo existente para los equipos (cuando se cumplan los criterios de aceptación de riesgo de la empresa, y solo cuando esta decisión sea autorizada por la Dirección).**

Información ampliada

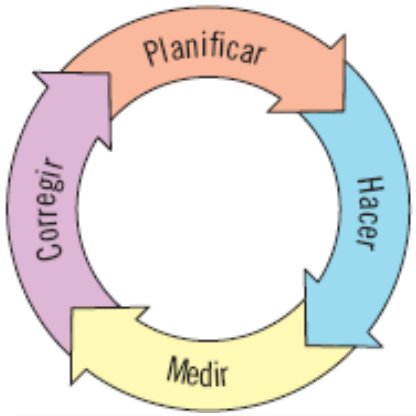
VER DOCUMENTO

1.1.4.SALVAGUARDAS.DOCX

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Sistema de Gestión de Seguridad de la Información (SGSI)

Ciclo de mejora continua de Deming, aplicable al proceso de ejecución de un SGSI



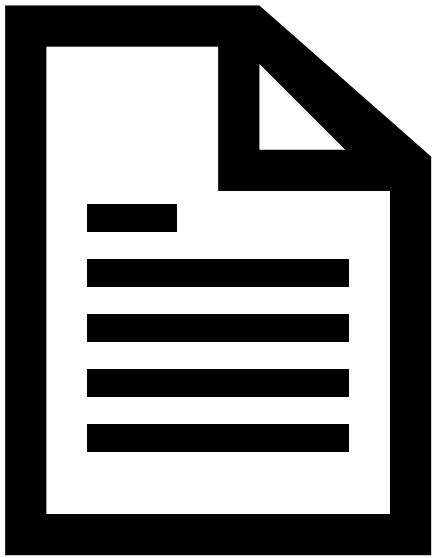
La anterior secuencia describe una repetición continua de fases de planificación (en inglés, *plan*), ejecución (en inglés, *do*), medida (en inglés, *check*) y corrección (en inglés, *act*), constituyendo un ciclo de mejora continua de Deming (P-D-C-A)

5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

Principio de proporcionalidad:

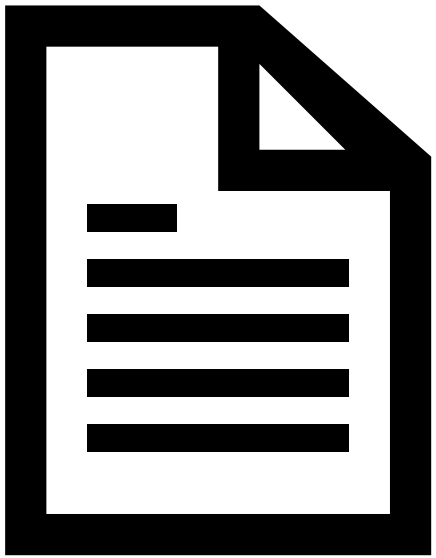
- **Las salvaguardas deben ser proporcionales al riesgo**
- **El SGSI debe ser proporcional al valor de la continuidad del negocio**

Ejemplo



EN UNA EMPRESA OCURREN MUCHOS INCIDENTES DE SEGURIDAD; ALGUNOS SON DE PEQUEÑA IMPORTANCIA, COMO LAS FRECUENTES INTERRUPCIONES EN LA CONEXIÓN A INTERNET, Y OTROS SON MÁS CRÍTICOS, COMO LAS PARADAS DEL SISTEMA DURANTE JORNADAS COMPLETAS, DEBIDO A ERRORES EN LOS SERVIDORES. TAMBIÉN SE PRODUCEN FUGAS DE INFORMACIÓN, PEQUEÑOS HURTOS DE PERIFÉRICOS, Y OTROS ACCESORIOS. LA EMPRESA TAMBIÉN ES CONSCIENTE DEL INCUMPLIMIENTO DE ALGUNA LEY REFERENTE A LA INFORMACIÓN. LA DIRECCIÓN EXPONE LA SITUACIÓN, Y PIDE QUE SE PROPONGA UN PLAN DE ACCIÓN PARA CORREGIR TODOS ESOS PROBLEMAS.

RESUMIR BREVEMENTE LAS ACCIONES A REALIZAR, DANDO AL MENOS UNA JUSTIFICACIÓN DE LAS MISMAS.



Ejemplo. Solución

- JUSTIFICACIÓN:

LA SITUACIÓN DESCRITA INCLUYE MULTITUD DE AMENAZAS, LO QUE INDICA QUE NO CONVIENE EMPRENDER UN CONJUNTO DE MEDIDAS DE SEGURIDAD AISLADAS PARA OBJETOS CONCRETOS. SE NECESITAN TAMBIÉN ASPECTOS DE GESTIÓN, ASPECTOS LEGALES, ASPECTOS ÉTICOS U OTROS ESPECÍFICOS DE LA NATURALEZA Y AMBIENTE INTERNO Y EXTERNO DE LA EMPRESA.

- ACCIONES A REALIZAR:

SE DEBE IMPLANTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), COMO SISTEMA PARA ESTABLECER Y MANTENER UN ENTORNO SEGURO, CONSISTENTE EN LAS SIGUIENTES 4 TAREAS DE EJECUCIÓN CONTINUA:

* PLANIFICAR: ANALIZAR LAS NECESIDADES DE SEGURIDAD DE LA EMPRESA.
* HACER: IMPLANTAR LAS MEDIDAS DE SEGURIDAD NECESARIAS.
* CHEQUEAR: MEDIR SI SE HAN ALCANZADO LAS NECESIDADES DE SEGURIDAD.
* CORREGIR: DETECTAR Y APLICAR MEJORAS EN LAS MEDIDAS DE SEGURIDAD.

EL SGSI SE APOYARÁ EN DOS HERRAMIENTAS MUY IMPORTANTES:
* UNA POLÍTICA DE SEGURIDAD, A PARTIR DE NORMAS COMO ISO 17799, LA SERIE ISO 20000 Y LA LEGISLACIÓN QUE SEA APLICABLE, COMO LA LOPDGDD.
* UNA METODOLOGÍA DE EVALUACIÓN DEL RIESGO, COMO MAGERIT.