Capitulo 1. Introducción a la seguridad informática.

Patricia Medina Mgp.

Seguridad Informática:

- Como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema

ASPECTOS DE LA SEGURIDAD INFORMÁTICA:

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
- Control en el acceso a los servicios ofrecidos y la información guardada por un sistema informático.
- Control en el acceso y utilización de ficheros protegidos por la ley: contenidos digitales con derechos de autor, ficheros con datos de carácter personal, etc…
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático, etc..

SEGURIDAD DE LA INFORMACIÓN

SEGÚN LA NORMA ISO/TEC 17799

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.

FACTORES A TENER EN CUENTA EN LA SEGURIDAD DE UN SISTEMA INFORMÁTICO

- La sensibilización de los directivos y responsables de la organización, que deben ser Conscientes de la necesidad de destinar recursos a esta función.
- Los conocimientos, capacidades e implicación de los responsables del sistema informático: dominio de la tecnología utilizada en el sistema informático y conocimiento sobre las posibles amenazas y los tipos de ataques.
- La mentalización, formación y asunción de responsabilidades de todos los usuarios del sistema.
- La correcta instalación, configuración y mantenimiento de los equipos.

FACTORES A TENER EN CUENTA EN LA SEGURIDAD DE UN SISTEMA INFORMÁTICO

- La limitación en la asignación de los permisos y privilegios de los usuarios
- El soporte de los fabricantes de hardware y software, con la publicación de parches y actualizaciones de sus productos que permitan corregir los fallos y problemas relacionados con la seguridad.
- Contemplar no solo la seguridad frente a las amenazas del exterior, sino también las amenazas procedentes del interior de la organización , aplicando además el principio de “Defensa en profundidad”.
- La adaptación de los objetivos de seguridad y de las actividades a realizar a las necesidades reales de la organización

OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las perdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

PLANOS DE ACTUACIÓN EN LA SEGURIDAD INFORMÁTICA

SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

- Confidencialidad
- Autenticación
- Integridad
- No repudiación
- Disponibilidad
- Autorización (control de acceso a equipos y servicios)
- Auditabilidad
- Reclamación de origen
- Reclamación de propiedad
- Anonimato en el uso de los servicios
- Protección a la replica
- Confirmación de la prestación de un servicio la realización de una transacción
- Referencia temporal (certificación de fechas)
- Certificación mediante terceros de confianza

TÉCNICAS Y MECANISMOS DE SEGURIDAD

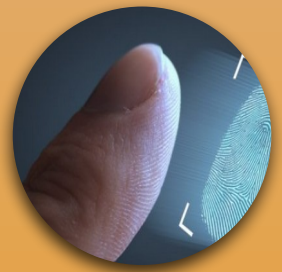
Identificación de usuarios y política de contraseñas

Control lógico de acceso a los recursos

Copias de seguridad

Centros de respaldo

Cifrado de las transmisiones

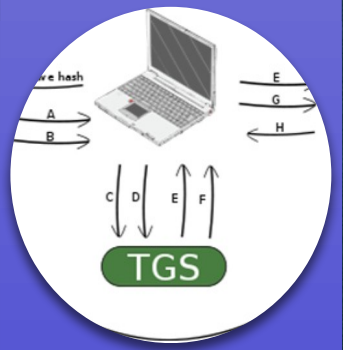


Huella digital de mensajes

TÉCNICAS Y MECANISMOS DE SEGURIDAD

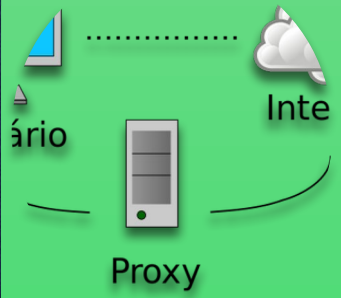
Sellado temporal de mensajes

Utilización de la firma electrónica



Protocolos Criptográficos

Análisis y filtrado del trafico (cortafuegos)



Servidores proxy

Sistema de detección de intrusiones

Antivirus

CONSECUENCIAS DE LA FALTA DE SEGURIDAD

Así, el famoso 11 de septiembre de 2001 en los atentados contra las Torres Gemelas de Nueva York muchas empresas perdieron sus oficinas centrales y, sin embargo, pudieron continuar con la actividad de su negocio a los pocos días, ya que sus datos estaban protegidos y sus sistemas informáticos contaban con los adecuados planes de contingencia y de respuesta a emergencias.

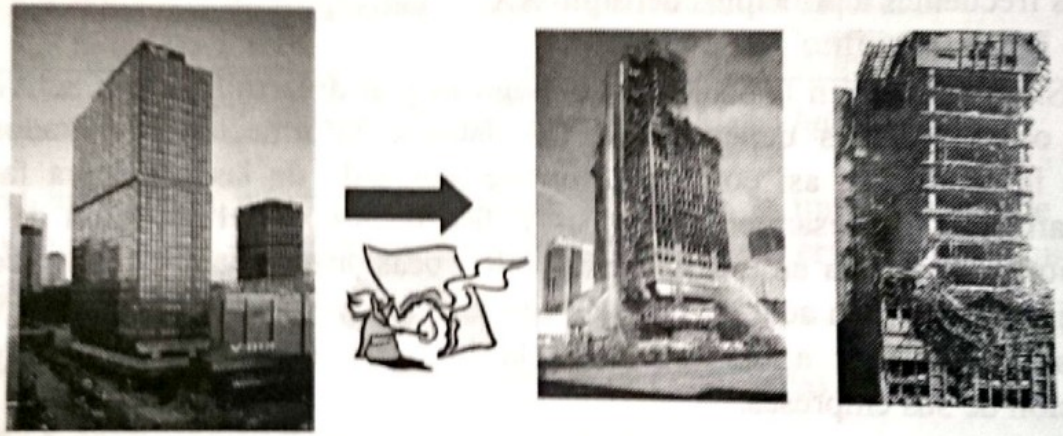


Figura 1.6. Incendio de la Torre Windsor en Madrid (12 febrero 2005)

En España el incendio del rascacielos Windsor en Madrid (12 de febrero de 2005), un edificio de 28 plantas dedicado a oficinas, en el que la consultora y auditora Deloitte & Touche ocupaba 20 plantas y el bufete de abogados Garrigues ocupaba 2 plantas, fue un acontecimiento que contribuyó a despertar un mayor interés por la necesidad de contemplar las medidas seguridad y los planes de contingencia para garantizar la continuidad del negocio.

Según un estudio publicado a principios de 2006 y realizado por la consultora especializada Computer Economics , la creación y difusión de programas informáticos maliciosos a traes de internet (virus, troyanos, gusanos) represento durante esta ultima década un costo financiero para las empresas de todo el mundo de unos 110,000 millones de dólares.

Los nuevos delitos relacionados con la informática y las redes de ordenadores se han convertido en estos últimos años en uno de los mayores problemas de

PRINCIPIO DE “DEFENSA EN PROFUNDIDAD”

- Consiste el diseño e implantación de varios niveles de seguridad dentro del sistema informático de la organización.
- S una de las barreras es franqueada por los atacantes , conviene disponer de medidas de seguridad adicionales que dificulten y retrasen su acceso a información confidencial o el control por su parte de recursos críticos del sistema: seguridad perimetral, seguridad en los servidores, auditorias y monitorización de eventos de seguridad.

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

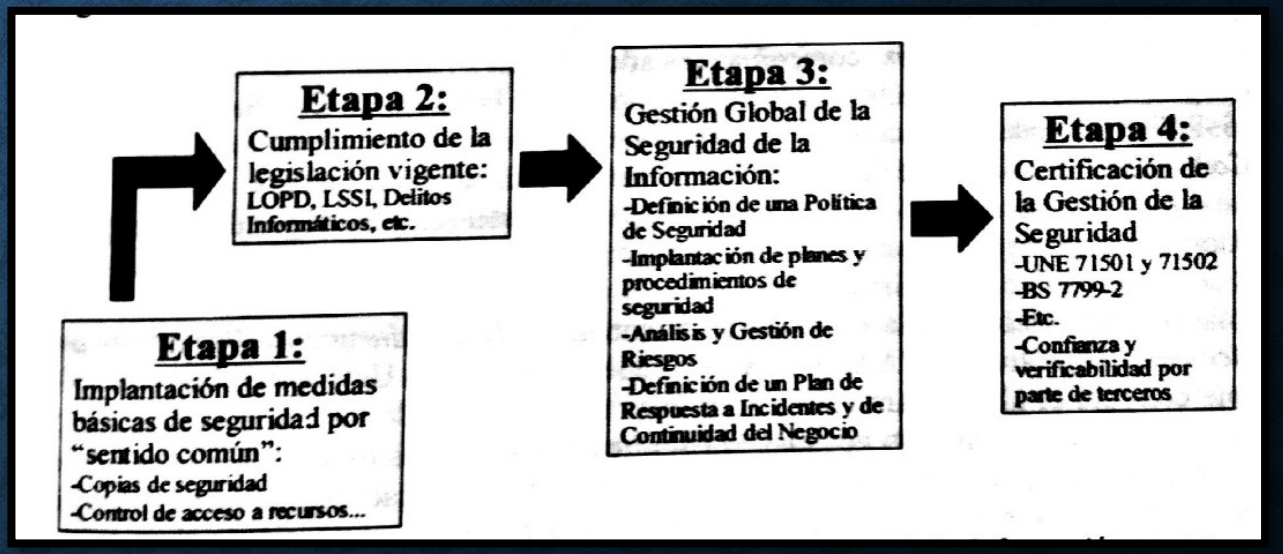
POLÍTICAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Están constituidas por el conjunto de normas reguladoras , procedimientos reglas y buenas practicas que terminan el modo en que todos los activos y recursos , incluyendo la información , son gestionados , protegidos y distribuidos dentro una organización.

1. Formalizar la gestión de la seguridad de la información.
2. Analizar y gestionar los riesgos.
3. Establecer procesos de gestión de la seguridad siguiendo la metodología (PDCA)
4. Certificación de la gestión de la seguridad.

ETAPAS O NIVELES DE MADUREZ EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. Implantación de medidas básicas de seguridad por "sentido común"
2. Adaptación a los requisitos del marco legal y de las exigencias de los clientes
3. Gestión integral de la seguridad de la información.
4. Certificación de la gestión de la seguridad de la información.



NIVELES DE MADUREZ LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Nivel 1	• Practicas de seguridad realizadas de manera informal.
Nivel 2	• Planificación y seguimiento de las prácticas de seguridad
Nivel 3	• Definición y coordinación de las políticas y procedimientos de seguridad.
Nivel 4	• Seguridad controlada a través de distintos controles y objetivos de calidad
Nivel 5	• Implantación de un proceso de mejora continua.

ETAPAS O FACES PARA LA IMPLANTACIÓN DE UN SGSI

1. Definición de las políticas de seguridad y del alcance del SGSI.
2. Definición de responsabilidades y asignación de recursos.
3. Identificación y registro de activos.
4. Análisis y gestión de riesgos.
5. Selección e implantación de controles de seguridad.
6. Establecer un programa de mejora de la seguridad.
7. Completar la documentación del SGSI
8. Revisión y auditoria interna del proyecto de implantación del SGSI
9. Realización de la auditoria de certificación.
10. Ejecutar las recomendaciones de la auditoria.

ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO

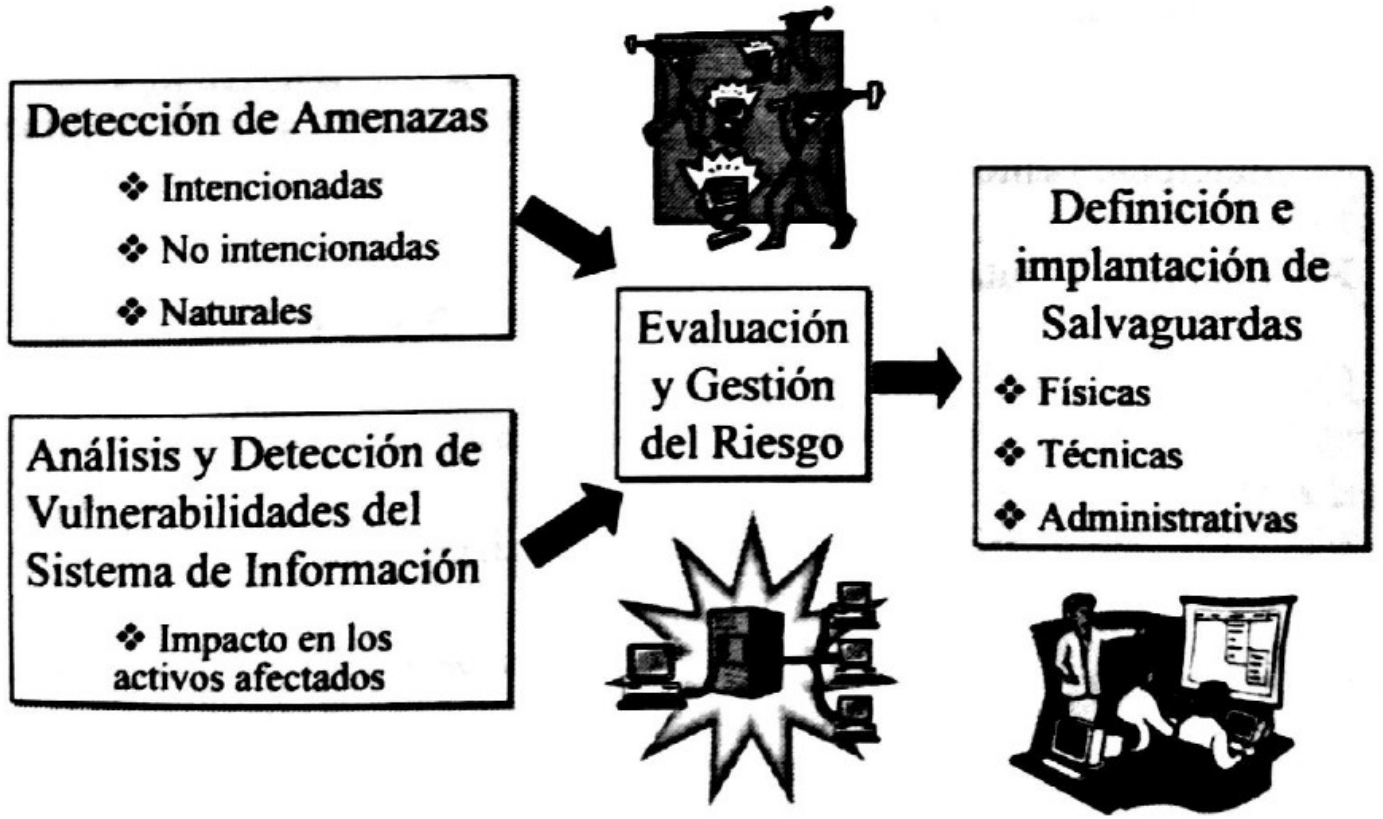


Figura 1.11. Análisis y Gestión de Riesgos en una organización

RECURSOS DEL SISTEMA

- Recursos hardware: servidores y estaciones de trabajo, ordenadores portátiles, impresoras, escáneres y otros periféricos.
- Recursos software: sistemas operativos, herramientas ofimáticas, software de gestión, herramientas de programación, aplicaciones desarrolladas a medida, etcétera.
- Elementos de comunicaciones: dispositivos de conectividad (*hubs*, *switches*, *routers*), armarios con paneles de conexión, cableado, puntos de acceso a la red, líneas de comunicación con el exterior, etcétera.
- Información que se almacena, procesa y distribuye a través del sistema (activo de naturaleza intangible).
- Locales y oficinas donde se ubican los recursos físicos y desde los que acceden al sistema los usuarios finales.
- Personas que utilizan y se benefician directa o indirectamente del funcionamiento del sistema.
- Imagen y reputación de la organización.

AMENAZAS

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión...
- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etcétera.
- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema.

- Accidentes: averías del hardware y fallos del software, incendio, inundación...
- Errores: errores de utilización, de explotación, de ejecución de determinados procedimientos, etcétera.
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etcétera.

VULNERABILIDADES

- Se corresponden con fallos en los sistemas físicos y lógicos (defectos de ubicación, instalación, configuración y mantenimiento de los equipos)
- Procedimientos mal definidos o sin actualizar
- Ausencia de políticas de seguridad.
- A los propios equipos, a los programas y herramientas lógicas del sistema.
- A las condiciones ambientales del sistema.

INCIDENTES DE SEGURIDAD

- Es cualquier evento que tenga o puede tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles perdidas físicas , de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

IMPACTOS

Es la medición y valoración del daño que podría producir a la organización un incidente de seguridad. Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles (incluida la información).

Alto	➢ Pérdida o inhabilitación de recursos críticos ➢ Interrupción de los procesos de negocio ➢ Daños en la imagen y reputación de la organización ➢ Robo o revelación de información estratégica o especialmente protegida
Moderado	➢ Pérdida o inhabilitación de recursos críticos pero que cuentan con elementos de respaldo ➢ Caída notable en el rendimiento de los procesos de negocio o en la actividad normal de la organización ➢ Robo o revelación de información confidencial, pero no considerada estratégica
Bajo	➢ Pérdida o inhabilitación de recursos secundarios ➢ Disminución del rendimiento de los procesos de negocio ➢ Robo o revelación de información interna no publicada

Tabla 1.1. Escala propuesta para medir el impacto del daño en la organización

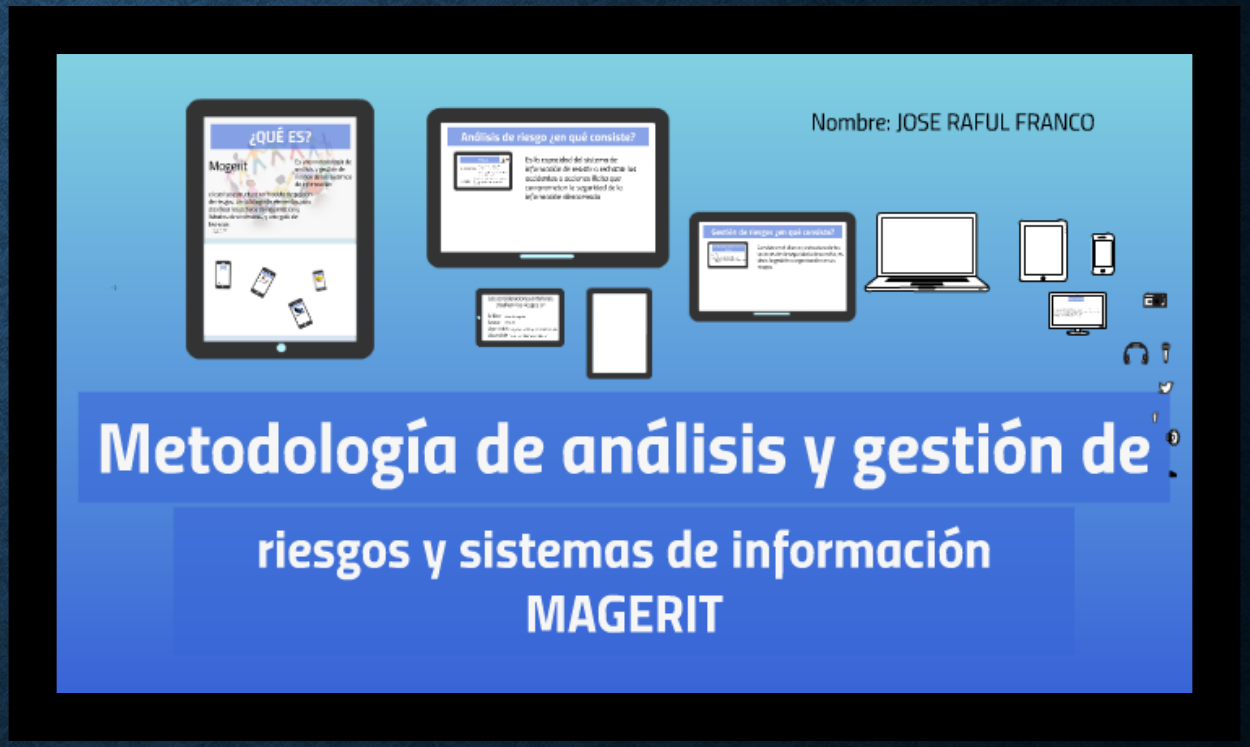
RIESGOS

- Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. El nivel de riesgo depende, por lo tanto, del análisis previo de vulnerabilidades del sistema, de las amenazas del posible impacto que estas puedan tener en el funcionamiento de la organización.

METODOLOGÍA MAGERIT

Los objetivos de Magerit son:

- Concienciar a los responsables de los sistemas de información de la existencias de riesgos y de la necesidad de adoptar las medidas para limitar su impacto.
- Ofrecer un método sistemático para analizar tales riesgos.
- Planificar las medidas oportunas para mantener los riesgos identificados bajo control.
- Facilitar todos los procesos de evaluación , auditoria, certificación o acreditación.



https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

EJEMPLO DE EVALUACIÓN DE RIESGO:

- Activo: Servidor de ficheros de la organización
- Amenaza: Fallo hardware en un servidor, con una probabilidad de ocurrencia baja (una vez cada 5 años).
- Vulnerabilidad del sistema: alta, ya que no se dispone de un servidor alternativo ni de medidas redundantes. (como los discos Raid)
- Impacto: Indisponibilidad durante 24 horas del activo afectado (hasta que sea reparado por el servicio técnico) por lo que se puede considerar como un impacto de nivel alto.
- Nivel de riesgo: Se obtiene a partir de las tablas de valoración que se hayan adoptado, teniendo en cuenta que la amenaza es baja, la vulnerabilidad es alta y el impacto es alto.

TABLA PARA LA EVALUACIÓN DE RIESGOS

	Importancia para la organización (factor de ponderación)	Identificación de una amenaza	Probabilidad de materialización de una amenaza	Vulnerabilidad del sistema ante esta amenaza	Evaluación del impacto (económico)	Evaluación del riesgo
Recurso 1	8	Amenaza X	20%	50%	100.00	80.00
Recurso 2	6	Amenaza y	30%	40%	200.00	180.00

DEFENSAS, SALVAGUARDAS O MEDIDAS DE SEGURIDAD

- Es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.

Medida de seguridad activa:
Es cualquier medida utilizada para anular o reducir el riesgo de una amenaza.
(medidas de prevención y medidas de detección)
Medida de seguridad pasiva: es cualquier medida empleada para reducir el impacto cuando se produzca un incidente de seguridad (medidas de corrección)

EJEMPLOS:

- **medidas preventivas:** autenticación de usuarios, el control de accesos a los recursos, el cifrado de datos sensibles, la formación de los usuarios.
- **Medidas detectivas:** sistemas de detección de intrusiones (IDS) o las herramientas y procedimientos para el análisis de los logs (registro de actividad de los equipos)
- **Medidas correctivas:** las copias de seguridad, el plan de respuesta a incidentes
- **Defensas físicas:** Medidas que implican el control de acceso físico a los recursos y de las condiciones ambientales en que tienen que ser utilizadas (temperatura, humedad, suministro eléctrico, interferencias)
- **Defensas lógicas:** se encuentran relacionadas a autenticación de usuarios, control de acceso a los ficheros, cifrado de los datos

NIVEL DE RIESGO RESIDUAL

- Se obtiene tras un nuevo proceso de evaluación de riesgos teniendo en cuenta que los recursos ya se encuentran protegidos por las medidas de seguridad seleccionadas
- Representa el nivel de riesgo que la organización estaría dispuesta a aceptar , teniendo en cuenta que no resultaría beneficioso reducirlo aun mas debido al esfuerzo técnico y económico que ello conllevaría.

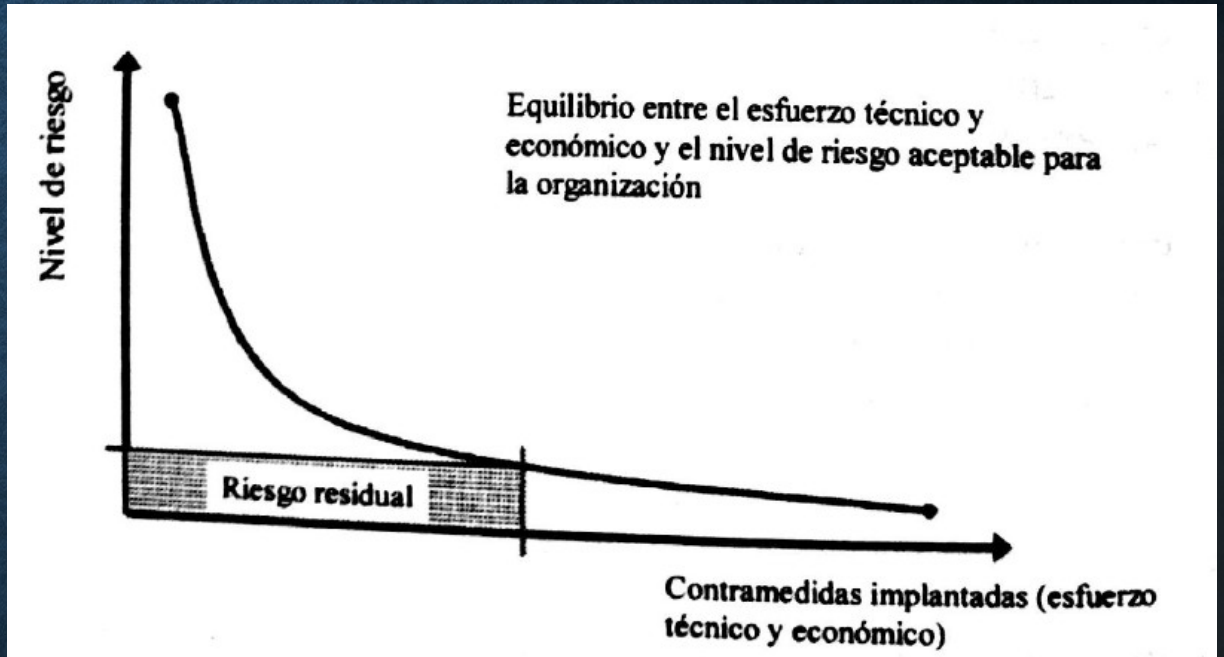


Figura 1.13. Nivel de riesgo residual

TODO LO ANTERIOR SE RESUME EN ESTE DIAGRAMA:

PROCESO DE EVALUACIÓN Y GESTIÓN DE RIESGOS

Figura 1.14. El proceso de Evaluación y Gestión de Riesgos

TRANSFERENCIA DE RIESGO A TERCEROS

- Mediante la contratación de una póliza de seguros especializada o bien a través de la subcontratación de un proveedor especializado en ofrecer determinados servicios de seguridad informática.
- En lo que se refiere a la contratación de un seguro frente a daños o ataques informáticos , es necesario tener en cuenta que los aseguradores suelen exigir una valoración externa del sistema de seguridad de la organización.
- Y la subcontratación de un proveedor especializado , con un planteamiento similar al de la propia seguridad física de las instalaciones de la organización que hoy en día suele estar subcontratada a una empresa especializada que se encarga del mantenimiento de las alarmas, el control de acceso del personal a las instalaciones.

REFERENCIAS

- Álvaro Gómez Enciclopedia de la seguridad Informática 2da edición, 2011 ISBN 9788499640365