MF0486_3 Seguridad en Equipos Informáticos

UD1. Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos

UM1. Modelo de seguridad orientada a la **gestión del riesgo** relacionado con el uso de los sistemas de información.

2.1 Amenaza
No se pueden eliminar

↓

Vulnerabilidad
Debilidades de los equipos ante las amenazas

↓

Riesgo
2.3 Probabilidad de ocurrencia de una amenaza x impacto o daño

2.2 Principios de Seguridad **Disponibilidad, Integridad y Disponibilidad (CIA)**

3. RELACION DE AMENAZAS MAS FRECUENTES (MAGERIT)

a) **DESASTRES NATURALES**
b) **ORIGEN INDUSTRIAL**
c) **ERRORES O FALLOS NO INTENCIONADOS**
d) **ATAQUES INTENCIONADOS**

4. AREAS DE SEGURIDAD

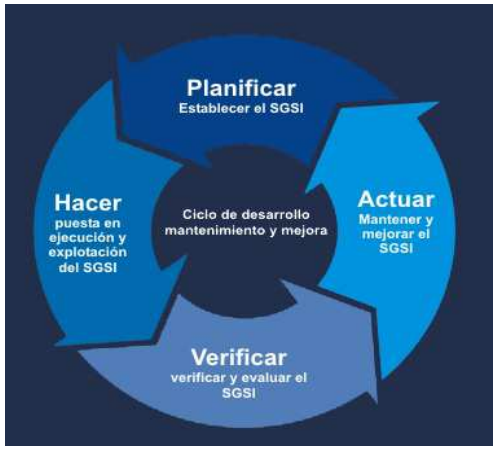
1. **SEGURIDAD DE RECURSOS HUMANOS**
2. **SEGURIDAD AMBIENTAL**
3. **SEGURIDAD FISICA**
4. **SEGURIDAD DE ACCESO LÓGICO**

4. SALVAGUARDAS O CONTRAMEDIDAS

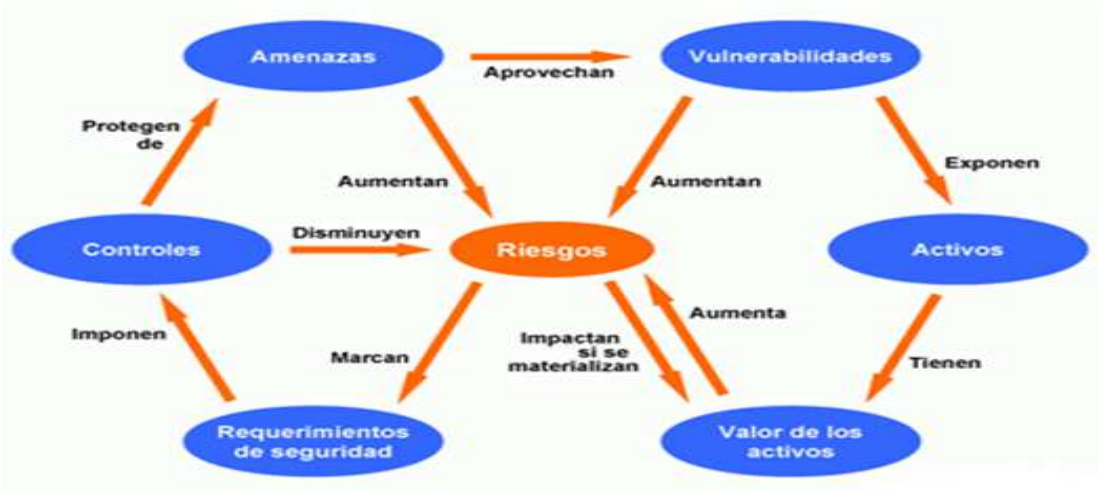
1. PREVENTIVAS O PROACTIVAS
2. REACTIVAS
3. NO HACER NADA

SGSI – Redacción de políticas de seguridad según Normas ISO 17799 – Normas ISO 27000

5. SISTEMAS DE GESTION DE LA SEGURIDAD INFORMATICA - SGSI



Resumen



MODELO DE SEGURIDAD ORIENTADO AL RIESGO DE LOS SISTEMAS DE INFORMACION:

ISO 17799 – Preservar Confidencialidad-Integridad-Disponibilidad **CIA** (Availability)

MAGERIT – Resistir los ataques contra la Disponibilidad-Autenticidad-Integridad-Confidencialidad

AMENAZAS, VULNERABILIDADES E INCIDENTES

A-No se pueden eliminar. Su análisis minimiza el daño. (Virus

V-Debilidad de los equipos ante las amenazas

I-Amenaza que ocurre aprovechando la vulnerabilidad (Efecto->Impacto o Daño)

RIESGO DE UN INCIDENTE DE SEGURIDAD = Probabilidad de ocurrencia de la amenaza (0-1 Gauss) x impacto o daño

MODELO DE SEGURIDAD.

- **Organiza los procesos de GESTION DE LA INFORMACIÓN (en base a unas políticas odirectrices)**
- **Utiliza un método para el CALCULAR LOS RIESGOS**

ESTUDIO DE LOS RIESGOS

1. **ANALISIS**
   a. **Identificar amenazas**
   b. **Determinar vulnerabilidades**
   c. **Medir impacto**
2. **GESTION: Permite elegir las contramedidas que se implantarán partiendo del análisis (progresivo)**

AMENAZAS, RIESGOS Y SALVAGUARDAS

AMENAZAS

1. **N**aturales o **A**rtificiales
2. **E**ntorno (ambiente) o **H**umanas
3. **Acc**idental o **I**ntencionada

AMENAZAS (MAGERIT)

- **DESASTRES NATURALES**
- **ORIGEN INDUSTRIAL**
- **ERRORES O FALLOS NO INTENCIONADOS**
- **ATAQUES INTENCIONADOS**

RIESGOS MAS USUALES

- **A. Natural** -> Destrucción de sistemas
- **A. Industrial**-> Destrucción y paradas de sistemas
- **Errores** y fallos n.int.-> Parada sistema, perdida información, perdida de trazabilidad
- **A. Intencionada**-> P. Sistema, perdida de seguridad, …

CRIPTOGRAFIA: Arte de escribir con clave secreta.

4. SALVAGUARDAS O CONTRAMEDIDAS (Deben ser proporcionales al riesgo)

- **P**REVENTIVAS O PROACTIVAS
- **R**EACTIVAS
- **N**O HACER NADA

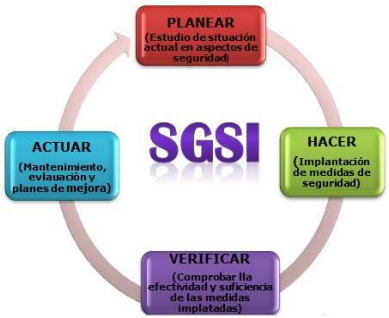
AREAS DE SEGURIDAD

1. **SEGURIDAD DE RECURSOS HUMANOS:** Definición de procesos y responsabilidades, devolución de activos, retirada de derechos, investigación de antecedentes
2. **SEGURIDAD AMBIENTAL:** Condiciones de temperatura ideales, medias ignifugas, chequeos periódicos, electricidad estable y continua. (**CPD**)
3. **SEGURIDAD FISICA:** Perímetro de seguridad, mecanismos de control físico, protección contra actividades cercanas.
4. **SEGURIDAD DE ACCESO LÓGICO:** Política de control de acceso, registro de usuarios, gestión de privilegios y claves, separación de redes, autentificación, caducidad, política de comunicaciones móviles.

5. Gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

SGSI: Sistema de gestión de la seguridad de la información.

- Analizar la empresa
- Fijar sus necesidades de seguridad
- Poner en práctica medidas de protección
- Ver si se han alcanzado



Espiral de mejora continua: **PDCA** son el acrónimo de las palabras inglesas **Plan, Do, Check, Act**, equivalentes en español a **Planificar, Hacer, Verificar, y Actuar** (Corregir).

Las normativas y metodologías que utilizaremos serán:

- ISO 17799. Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. http://www.shutdown.es/ISO17799.pdf
- ISO 27000. Es una norma que especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (SGSI). (Resumen - http://www.iso27000.es/download/doc_iso27000_all.pdf)