Gestión de Seguridad Informática

La información es un activo que es esencial al negocio de una organización y requiere en consecuencia una protección adecuada.
La información puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos

Ing. Clara Vidovich, MBA
CISA

ISO/IEC 27000

Familia de normas ISO/IEC 27000

Esta norma especifica los requisitos para establecer, implantar, documentar y evaluar un SGSI.

Especifica los requisitos de los controles de seguridad de acuerdo con las necesidades de las organizaciones, independientemente de su tipo, tamaño o actividad.

- 27000 Fundamentos y vocabulario
- 27001 Requisitos para certificación
- 27002 Buenas prácticas
- 27003 Directrices para la implementación

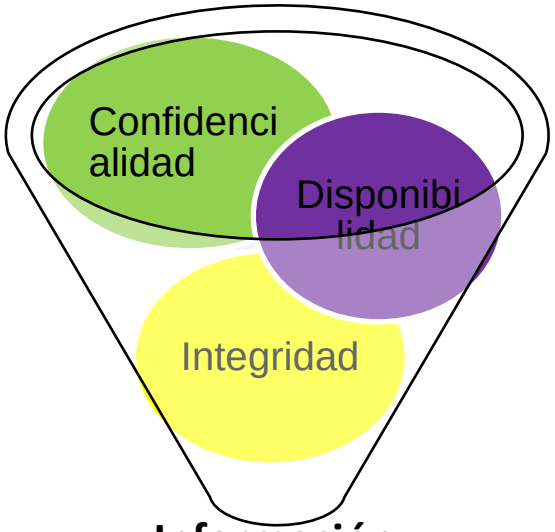
Sistema de Gestión de Seguridad de la Información

La seguridad de la información según la norma 27000, consiste en preservar las siguientes características:

- Integridad
- Confidencialidad
- Disponibilidad

Sistema de Gestión de Seguridad de la Información

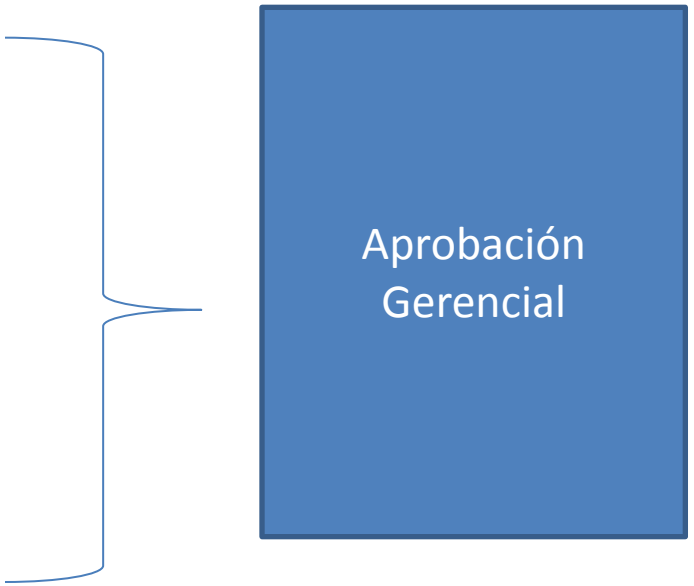
- **Integridad**
  - La información podrá ser modificada solamente por quien esté autorizado y de manera controlada.
- **Confidencialidad**
  - La información deberá ser leída solamente por quien esté autorizado
- **Disponibilidad**
  - La información deberá estar disponible siempre que se la necesite.



Estrategia de Seguridad

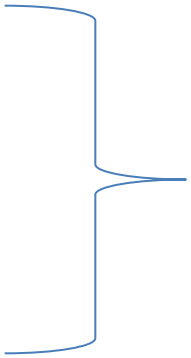
Norma 27001

- Sistema de Gestión de la Seguridad de la Información
  - Organización
  - Alcance
  - Política de Seguridad
  - Evaluación de Riesgos
  - Estrategia
  - Implementación



Implementación de la Norma 27001

- Planificar el tratamiento del riesgo
- Implementación de controles
- Formación y conciencia
- Gestionar
  - Operaciones
  - Recursos
  - Incidentes

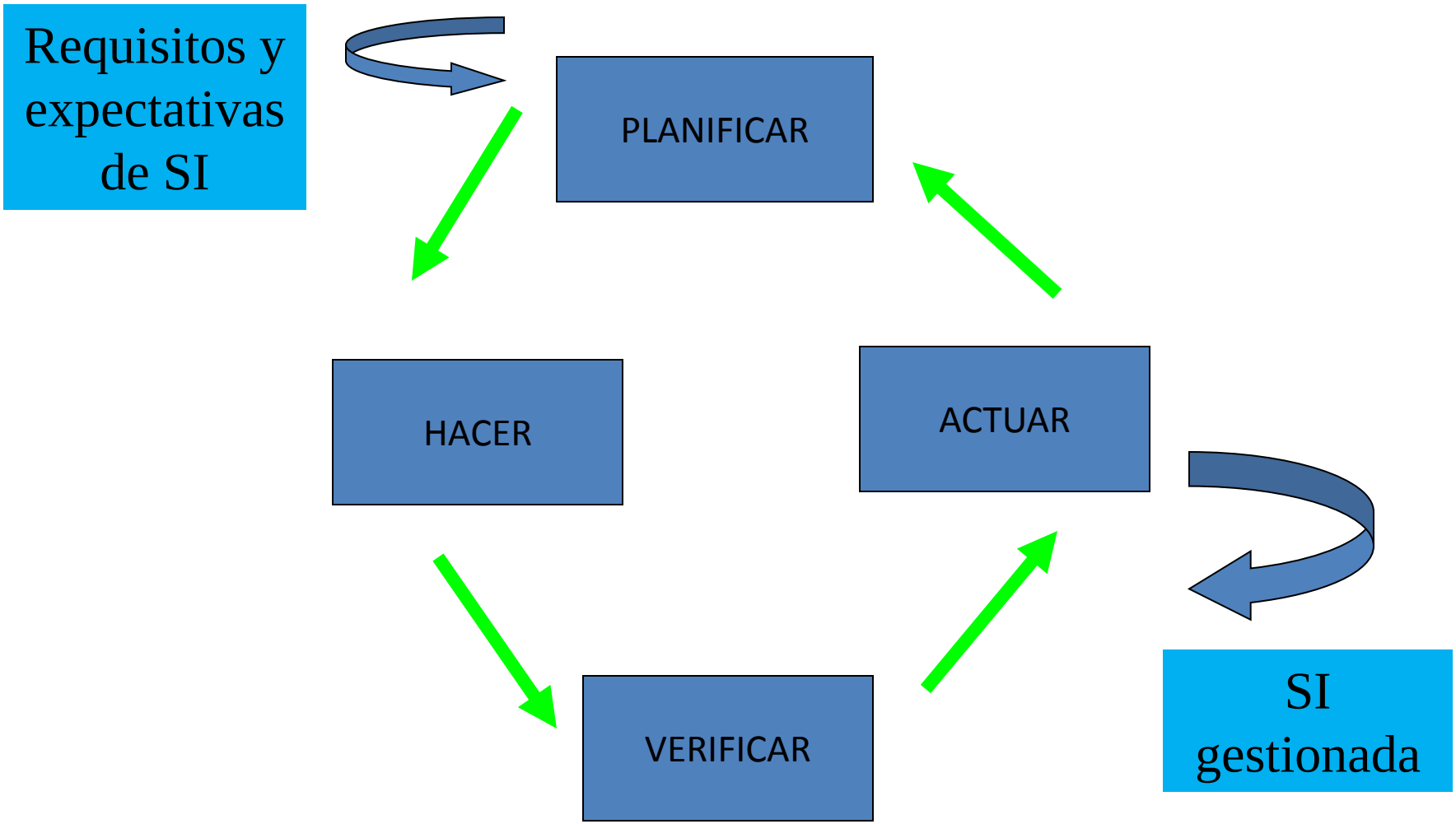


DOCUMENTACION

SGSI Gestionado

- Seguimiento y revisión
- Respuesta de la Dirección
  - Compromiso de la Dirección
  - Disponibilidad de recursos
  - Formación y conciencia
- Auditoría del SGSI
- Revisión de la Dirección
- Mejora Continua
  - Acciones correctivas
  - Acciones preventivas

Modelo PHVA aplicado a los procesos SGSI



Análisis de Riesgos

El análisis de riesgos es parte de la gestión y ayuda a identificar los riesgos y las vulnerabilidades para que se pueda determinar los controles para mitigarlos.

Definición de riesgo

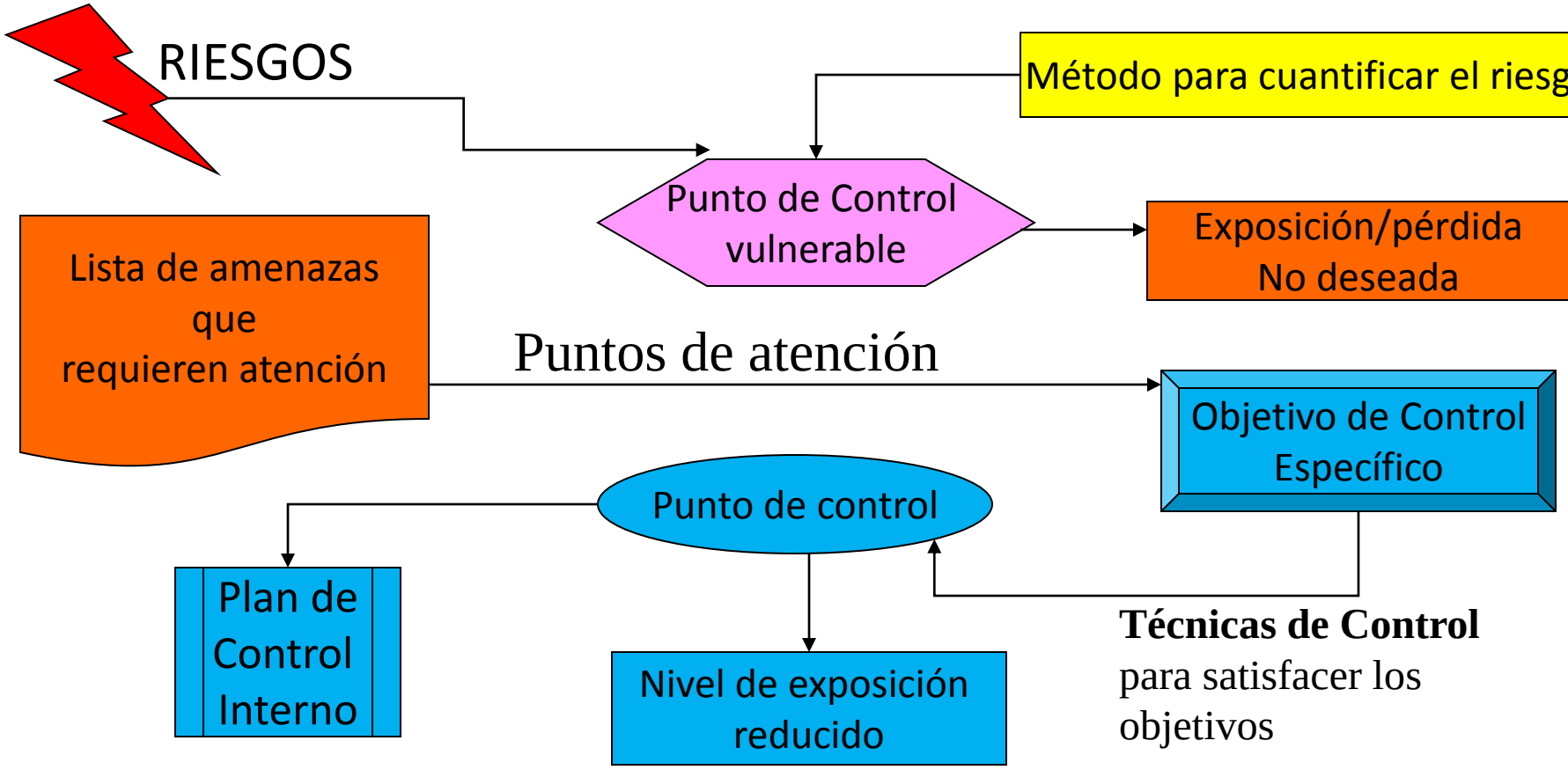
El potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a los mismos. El impacto o severidad relativa del riesgo es proporcional al valor para el negocio, de las pérdidas o daños y a la frecuencia estimada de la amenaza

Análisis de Riesgos

Proceso de gerenciamiento del riesgo

- ✓ Los riesgos del negocio son aquellas amenazas que pueden tener un impacto negativo sobre los activos, procesos u objetivos del negocio.
- ✓ La naturaleza de la amenaza puede ser financiera, regulatoria, operacional y puede surgir como interacción de la negocio con su medio o como resultado de estrategias.
- ✓ Enfocarse en asuntos de alto riesgo asociados a la confidencialidad, disponibilidad o integridad de información sensitiva y critica .
- ✓ Al revisar estos riesgos evaluaran el proceso de administración. Se evaluarán medidas para mitigarlos en función al costo beneficio. El costo de mitigarlo no sea mayor que la perdida del mismo
- ✓ Monitoreo de los riesgos, si los riesgos es están mitigando en un nivel aceptable por la dirección

Proceso para diseñar controles internos



Controles generales en SI

- Estrategia y dirección
- Organización y gerencia
- Acceso a datos y programas
- Metodología de desarrollo y cambio
- Operativa de procesamiento de datos
- Funciones de soporte y programación de sistemas
- Procedimientos de control de calidad
- Control de acceso físico
- Plan de contingencia y recuperación de desastres
- Redes y comunicaciones
- Administración de la base de datos

Controles Internos según la norma ISO

Dominio	Objetivos	Controles
Política de Seguridad	1	2
Aspectos organizativos para la seguridad	2	11
Gestión de los Activos	2	5
Seguridad de los Recursos Humanos	3	9
Seguridad física y del entorno	2	13
Gestión de comunicaciones y operaciones	10	32
Control de accesos	7	25
Adquisición, Desarrollo y mantenimiento de Sistemas	6	16
Gestión de Incidentes de Seguridad de la Información	2	15
Gestión de continuidad del negocio	1	5
Conformidad	3	10

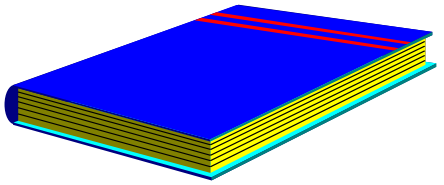
Objetivos de Control de los Sistemas de Información

- Salvaguardar los activos de tecnología de la información
- Cumplimiento con las políticas corporativas y marcos legales
- Asegurar la integridad de la información sensitiva in critica a través de :
  - Autorización del ingreso
  - Exactitud e integridad en el procesamiento de transacciones
  - Salida de información
  - Confiabilidad de los procesos
  - Integridad de la BD

Gracias a la implantación del SGSI se consigue **“CONFIANZA EN LOS SISTEMAS DE INFORMACIÓN”**

DEFINICIÓN DE SEGURIDAD

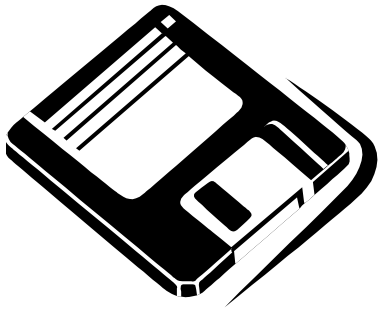
- **“CONJUNTO DE MEDIOS QUE ASEGURAN EL CORRECTO FUNCIONAMIENTO DE ALGUNA COSA”**
- **“CONJUNTO DE MEDIOS (NORMAS, PROCEDIMIENTOS, CONTROLES, DISPOSITIVOS, ETC...) DESTINADOS A PROTEGER A LA ORGANIZACIÓN Y SUS RECURSOS DE DIFERENTES TIPOS DE AMENAZAS”**



SEGURIDAD DE DATOS

ES EL CONJUNTO DE MEDIOS DESTINADOS A PRESERVAR LOS RECURSOS, QUE ASEGUREN LA PROVISIÓN DE INFORMACIÓN QUE

LA ORGANIZACIÓN NECESITA.



DEFINICIÓN DE PRIVACIDAD

- **“ DERECHOS DE INDIVIDUOS Y ORGANIZACIONES A DETERMINAR POR SÍ MISMOS CUANDO, COMO Y HASTA QUE PUNTO, INFORMACIÓN ACERCA DE ELLOS VA A SER COMUNICADA A TERCEROS.”**
- http://www.datospersonales.gub.uy/sitio/index.aspx
  - **Ley N° 18.331 (11 de Agosto de 2008)**

Ley de Protección de Datos Personales y Acción de Habeas Data.

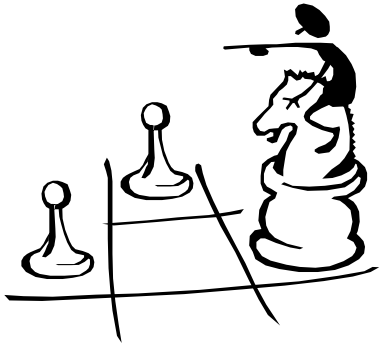
Estrategia de Seguridad

Políticas de Seguridad

REFLEJAN ORIENTACIÓN Y DIRECCIÓN DE LA GERENCIA sobre el CONTROL de:

- Sistemas de Información
- Recursos relacionados
- Procesos de SI

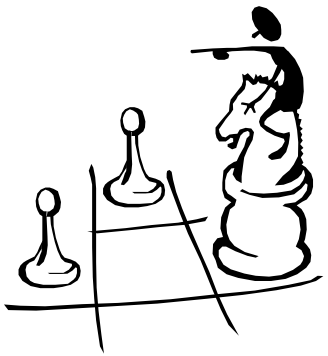
Políticas



- Las políticas son documentos de alto nivel. Ellas representan la filosofía corporativa de una organización y el pensamiento estratégico de la alta gerencia y de los dueños de los procesos del negocio. Las políticas deben ser claras y concisas para que sean efectivas.

Componentes de una buena política

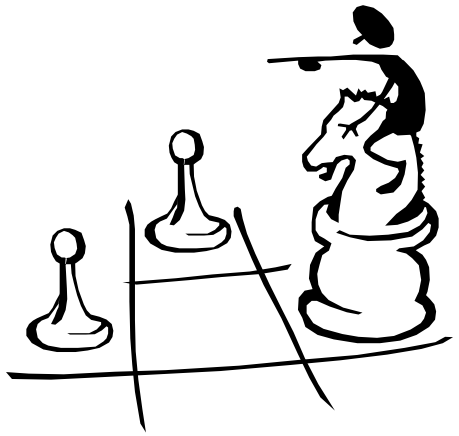
- **Soporte y compromiso de la gerencia**
- **Filosofía de acceso (Necesidad de saber)**
- **Procedimiento de autorización directo**
- **Revisión periódica del control de acceso**
- **Conciencia en seguridad (entrenamiento, comunicaciones, etc.**
- **Administración de seguridad**
- **Comité de seguridad**
- **Control de inventario de H y S (licencias)**



ESTABLECIMIENTO DE POLÍTICA

POLÍTICA DE SEGURIDAD QUE CUBRA:

- **PROTECCIÓN DE ACTIVOS**
- **PROCEDIMIENTOS DE EMERGENCIA**
- **RESPONSABILIDADES**



Políticas y Procedimientos

Gestión de Activos

Leyes y Regulaciones

Valor

Inventario

Necesidades del negocio

Información

Criterios de clasificación

Niveles de criticidad

CLASIFICACION

DUEÑOS de los Datos

Clasificación de Activos de Información

- La información debe ser clasificada, indicando la necesidad, las prioridades y el grado de protección esperada en el manejo de la misma
- Como resultado de la clasificación, queda definido un conjunto de Activos Críticos para la organización

Responsabilidad sobre los activos…

El DUEÑO de la información es el negocio.

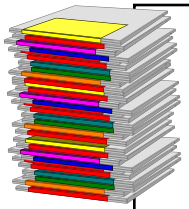
Seguridad asesora en COMO protegerlos

TI actúa como CUSTODIO de Datos

Organización de Seguridad

- Sector especializado en Seguridad Informática
  - Establecimiento de pautas de Seguridad
  - Control de aplicación de las pautas de seguridad
  - Participa en procesos de seguridad información

INFORMACIÓN = ACTIVOS

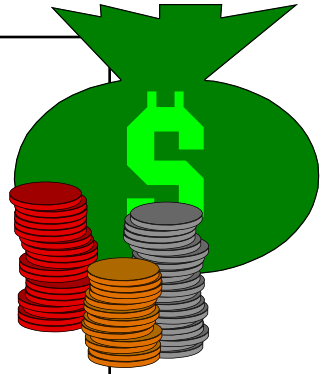


SEGURIDAD DE LA

INFORMACIÓN

=

PROTECCIÓN DE ACTIVOS



Activo

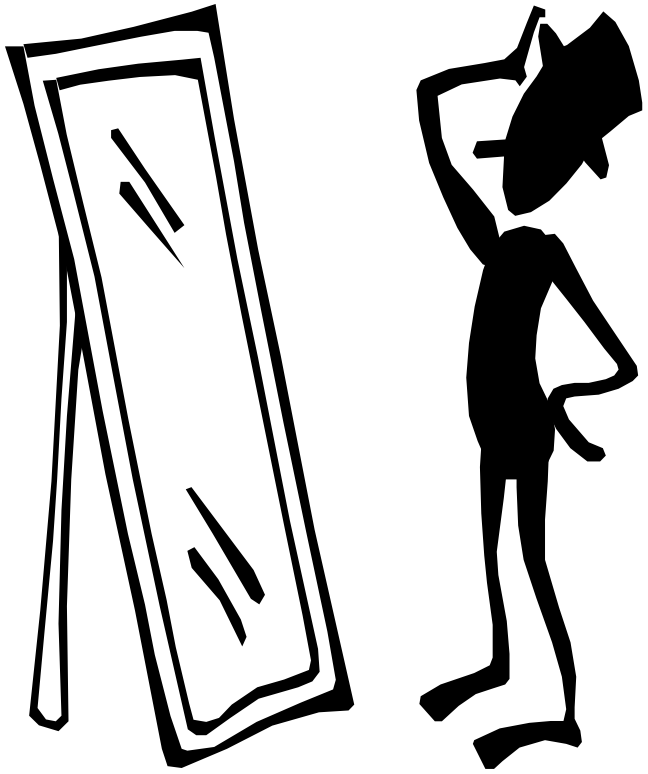
Recurso del sistema de información, necesario para que la organización funcione correctamente

Valor de los Activos

Es la criticidad que tiene un recurso para el negocio

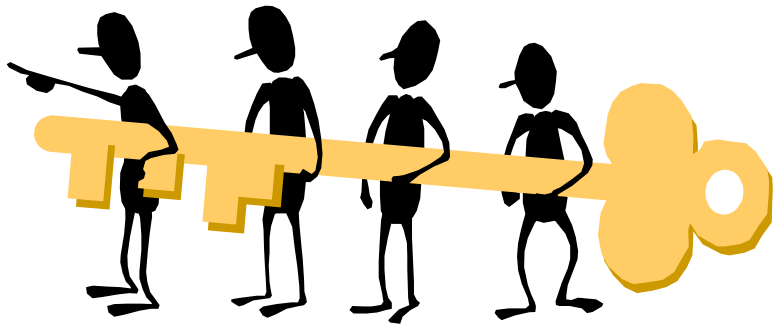
¿QUÉ SE PROTEGE?

- **FACTORES TANGIBLES**
  - **INMUEBLES**
  - **PROGRAMAS**
  - **MATERIALES**
  - **DATOS**
  - **PERSONAS**
- **FACTORES INTANGIBLES**
  - **PRESTIGIO**
  - **TRADICIÓN**
  - **REPUTACIÓN**
  - **NOMBRE**



DEBEMOS PROTEGER

- DATOS
- PERSONAS
- EQUIPOS
- PROGRAMAS
- REDES DE COMUNICACIÓN
- CINTAS, DISCOS, DISQUETES
- IMPRESOS
- SUMINISTROS

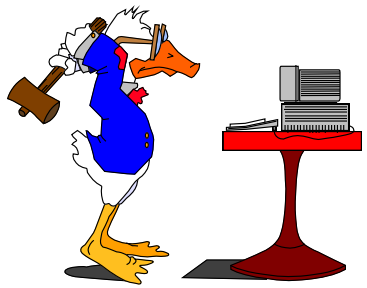


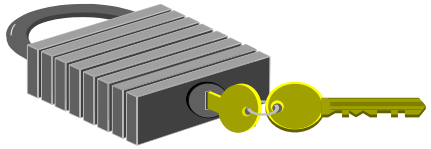
¿DE QUE DEBEMOS PROTEGERLOS?

DE CUALQUIER RIESGO, QUE PUEDA DISMINUIR O SUPRIMIR NUESTRA CAPACIDAD DE SERVICIO.

EJEMPLOS

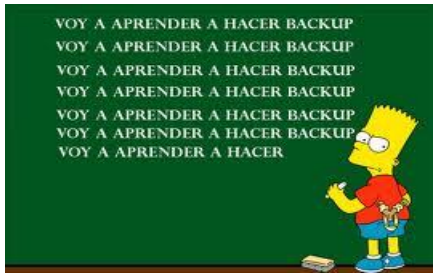
- **ERRORES-OMISIONES-ACCIDENTES**
- **FALLAS EN LOS EQUIPOS**
- **DESASTRES NATURALES**
- **ACCIONES HOSTILES INTERNAS O EXTERNAS**





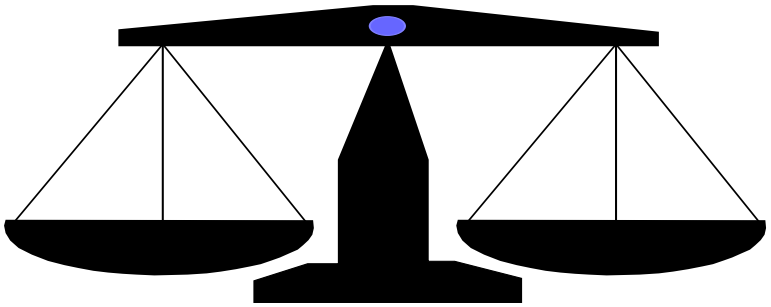
Ejemplos

- **INSTALACIÓN DE GUARDIAS ARMADOS**
- **PUERTAS BLINDADAS**
- **MUEBLES IGNÍFUGOS**
- **CONTRASEÑAS o LLaves**
- **RESPALDOS DE ARCHIVOS VITALES**
- **Escritorios limpios**




Amenazas
Aprovechan
Vulnerabilidades
Protegen de
Aumentan
Aumentan
Exponen
Controles
Disminuyen
Riesgos
Activos
Imponen
Marcan
Impactan si se materializan
Aumenta
Tienen
Requerimientos de seguridad
Valor de los activos
Fuente: www.ISO27000.es

PRESUPUESTO DE SEGURIDAD



RIESGO **PROTECCIÓN**

COSTO ASUMIR **VS.** **COSTO EVITAR**

Importancia de la Administración de la Seguridad de la Información

- Elementos Clave de la Administración de la Seguridad de la información
  - **El compromiso y soporte de la Alta Gerencia**
  - **Políticas y Procedimientos**
  - **La Organización**
  - **Concientización y educación en seguridad**
  - **Monitoreo y cumplimiento**
  - **Manejo y respuesta a incidentes**

Muchas Gracias

cvidovich@gmail.com
Ing. Clara Vidovich, MBA
CISA