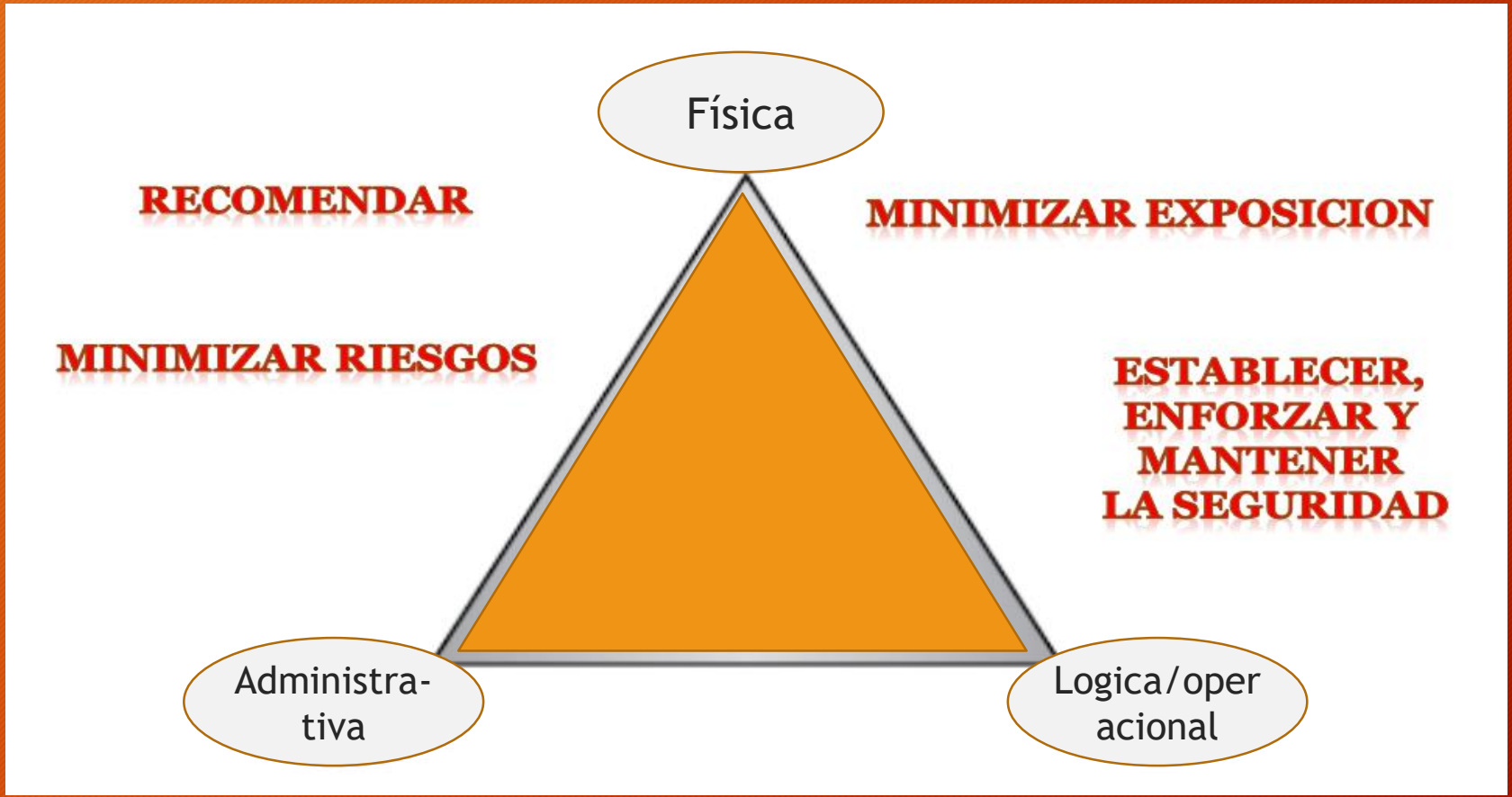
Seguridad de TI en la organización

SEGURIDAD DE LA TI EN LA ORGANIZACION



1. Asegurar el Ambiente Físico

Seguridad Física

Protección de Recursos e Información de un acceso físico por personas no autorizadas

- ¿Quién puede ser el atacante?
- ¿Qué puede robar?
- ¿Cuál es la motivación del atacante?
- ¿Cómo aseguramos el ambiente?

1. Asegurar el Ambiente Físico

Componentes de la Seguridad Física:

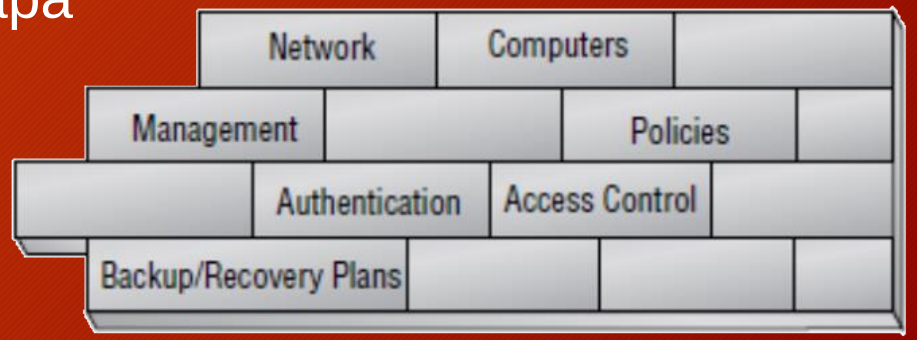
- El lugar físico debe ser lo menos tentador posible
- Bloqueo de puertas, cámaras de vigilancia, alarmas y otros.
- Detectar la invasión o el robo:
  - ¿Qué se vulnero?
  - ¿Qué se perdió?
  - ¿Cómo ocurrió la pérdida?

2. Seguridad Operacional

"Un estado en que el riesgo de lesiones a las personas o daños a los bienes se reduce y se mantiene en un nivel aceptable, o por debajo del mismo, por medio de un proceso continuo de identificación de peligros y gestión de riesgos".

- servidores, la información, las redes, los sistemas, sistemas de comunicaciones, etc.
- Luego que la red esta implementada viene la etapa de mantener la seguridad del ambiente operativo

Ejem amenazas: …expiración de contraseña, vulnerabilidad en las murallas de fuego, activación de bombas lógicas.



3. Administración y Políticas de seguridad

Guías, reglas y procedimientos para implementar un ambiente seguro.

Áreas que requieren planeamiento:

- ❑ Políticas Administrativas
- ❑ Plan de Recuperación ante Desastres
- ❑ Políticas de Información
- ❑ Políticas de Seguridad
- ❑ Requerimientos de diseño de software especifico.
- ❑ Políticas de Uso
- ❑ Políticas de Gestión de Usuario

3. Administración y Políticas

- ⇨ Políticas Administrativas:
- ❑ Guías para:
  - Upgrades
  - Monitoreo
  - Respaldo
  - Auditoria
- ❑ Responsables:
  - Administradores de Sistemas y
  - Personal de Soporte
- ❑ Objetivo:
  - Continuidad del Negocio

3 Administración y Políticas

- Plan de Recuperación de Desastres (DRP):

Incluye:

- Plan de Respaldo
- Hot Sites
- Se debe tomar en consideración cada tipo de ocurrencia o falla posible
- Objetivo

  Minimizar cualquier impacto negativo en las operaciones de la compañía.

3 Administración y Políticas

- **Política de Información:**

- ¿Cómo se maneja la información?
  - Acceso
  - Clasificación
  - Almacenamiento
  - Transmisión
  - Destrucción

3 Administración y Políticas

- **Políticas de Seguridad:**

Define:

- Configuración de Sistemas y Redes
- Instalación de Software y Hardware
- Conexiones de Red
- Seguridad de la Información
- Seguridad en el Centro de Computo
- Procesos de Autenticación y Autorización
- Manejo de Contraseñas y Cuentas de Usuario
- Etc..etc ...etc...

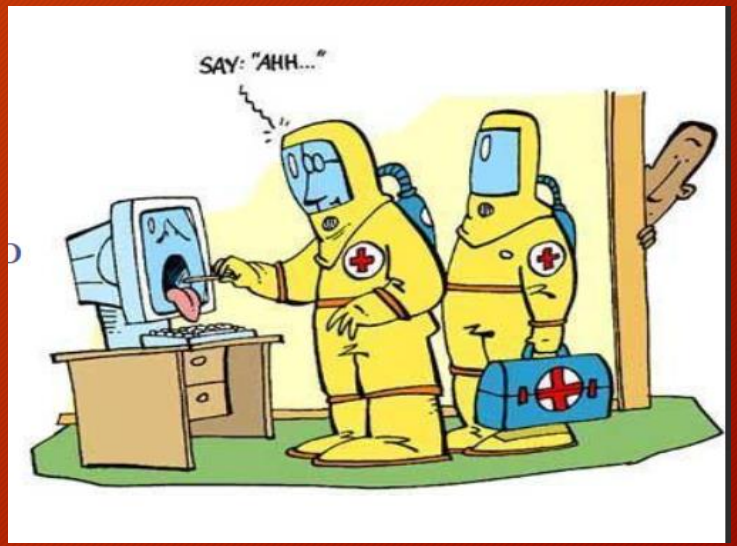
3 Administración y Políticas

- **Políticas de Uso:**
- Detalla:
  - Uso de los recursos
  - Uso de la información
- Involucra:
  - Privacidad
  - Establecimiento del Dueño
  - Consecuencias ante actos indebidos
- Controla:
  - Uso de Internet
  - Uso de Acceso Remoto
  - Uso de eMail

3. Administración y Políticas

- **Políticas de Gestión de Usuarios:**

- Gestión del Ciclo de Vida del Empleado:
  - Roles asignados a empleados
  - Control de Privilegios pre existentes
  - Cuentas Huérfanas



Las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger .
- Establecer niveles de prioridad e importancia sobre esta información.
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles .
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla
- Implementar respuesta a incidentes y recuperación para disminuir el impacto

- Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas.
- Un plan de acción para el manejo de incidentes y recuperación
- Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Seguridad de TI en la tecnología

…La tecnología no garantiza la seguridad informática…

Introducción

Nadie duda que las tecnologías de la información y la comunicación, especialmente el uso de la Internet, han producido grandes beneficios en lo social, cultural y económico. Tan solo pensemos en el frecuente uso de las redes sociales, donde la juventud de hoy construye su mundo por medio de sus contactos.

Introducción

Sin embargo, estas nuevas tecnologías también implican nuevos peligros y desafíos, ya que las tecnologías de la información y la comunicación se prestan para la comisión de nuevos delitos, con la agravante que las mismas tecnologías dificultan la persecución penal de los nuevos hechos ilícitos.

La sofisticación del uso y estrategia de Tecnología de Información conlleva la necesidad y obligación de mejorar las herramientas de seguridad. En todo el mundo los ataques cibernéticos se han incrementado con métodos innovadores.

¿Cuáles son los obstáculos de la seguridad?

1. **Tratar de cambiar todo de inmediato**
2. **Falta de capacitación de los empleados**
3. Baja capacidad de respuesta
4. Falta de conciencia
5. Poca articulación entre entidades
6. Complejidad heterogénea: debilidades organizacionales y múltiples plataformas que deben asegurarse.

Objetivos

1. Incrementar los niveles de madurez y fortalecer las capacidades en la apropiación de aspectos de seguridad y privacidad de la información.
2. Contar con un modelo de gestión de TI.
3. Generar confianza en la sociedad respecto al uso y apropiación de TI.

Acciones

1. Sensibilizar y concienciar
2. Apoyo para implementar el SGSI
3. Capacitar

Tipos de seguridad informática en las tecnologías

Debido a que todas las organizaciones son dependientes de la informática, la tecnología relacionada con la seguridad requiere un desarrollo constante. En este sentido es posible identificar tres diferentes **tipos de seguridad informática** en las tecnologías

Seguridad de Hardware

- Se puede relacionar con un dispositivo que se utiliza para escanear un sistema o controlar el tráfico de red.
- Los sistemas de hardware pueden proporcionar una seguridad más robusta, y pueden servir como capa adicional de seguridad para los sistemas importantes.
- Se refiere a cómo podemos proteger nuestros equipos físicos de cualquier daño.
- Para evaluar tener en cuenta las vulnerabilidades existentes desde su fabricación, así como otras fuentes potenciales, tales como código que se ejecuta en dicho hardware y los dispositivos entrada y salida de datos que hay conectados en la red.

Seguridad de Software

- Se utiliza para proteger el software contra ataques maliciosos de hackers y otros riesgos, de forma que siga funcionando correctamente
- Los defectos de software tienen diversas ramificaciones de seguridad
- Las aplicaciones que tienen salida a Internet presentan además un riesgo de seguridad más alto. Se trata del más común hoy en día. Los agujeros de seguridad en el software son habituales y el problema es cada vez mayor.
- La seguridad de software aprovecha las mejores prácticas de la ingeniería de software e intenta hacer pensar en la seguridad desde el primer momento del ciclo de vida del software.

Seguridad de red

Estas actividades protegen la facilidad de uso, fiabilidad, integridad y seguridad de su red y datos.
¿Cuáles son las amenazas a la red?

- Virus, gusanos y caballos de Troya
- Software espía y publicitario
- Ataques de día cero, también llamados ataques de hora cero
- Ataques de hackers
- Ataques de denegación de servicio
- Intercepción o robo de datos
- Robo de identidad

Hay que entender que no hay una solución única que protege de una variedad de amenazas.

Seguridad de red

Es necesario varios niveles de seguridad.

Un sistema de seguridad de la red se compone de muchos componentes.

Los componentes de seguridad de red incluyen:

- Antivirus y antispyware
- Cortafuegos, para bloquear el acceso no autorizado a su red
- Sistemas de prevención de intrusiones (IPS), para identificar las amenazas de rápida propagación, como el día cero o cero horas ataques

Marco normativo para las TI

* Decreto supremo 1793 para el desarrollo de las TIC y Software Libre (nov 2013)
* Ley General de Telecomunicaciones y TIC (agosto 2011)
* Decreto creación Dirección de Gobierno electrónico (enero 2014)
* Legislación sobre Transparencia (2004)
* Legislación sobre Nombres de Dominio (2002-2003)
* Legislación sobre Telecomunicaciones (2011)
* Proyecto de Ley de Documentos, Firma y Comercio Electrónico (2006)
* Fraude Electrónico Art. 363º Bis y 363º Ter.
* Legislación Habeas Data (2005)