

# plan de seguridad informática

## datos

- Armengol Torres
- Consultor homologado idigital.cat
- armengol@torres.net
- 600.485.486

## seguridad de la información en la empresa

### amenazas

- los sistemas información se convierten en un activo fundamental
- amenazas potenciales que pueden provocar problemas en los SI<sup>1)</sup>
- la utilización de internet, la conexión, la multiplicidad de posibilidades de errores, problemas y riesgos
- impulso de la administración en el uso de canales de comunicación

### requisitos

- confidencialidad: solo personal autorizado ha de acceder
  - pública
  - restringida (nóminas)
  - confidencial (contraseñas, secretos industriales)
- integridad: consistencia de la información en diferentes sistemas y que los cambios los hacen las personas autorizadas
  - accidentes fortuitos
  - humanos, internos -error, falta rigor, pasar al lado oscuro- o externos -hackers-
- disponibilidad: que la información se accesible al personal correspondiente, cuando corresponde y de manera segura
  - la lista de clientes que se guardaba bajo llave, la dificultad para acceder a ella
  - exceso de seguridad - muchas contraseñas, llaves → pérdida de eficacia

### areas

- perímetro externo:
  - eBusiness (venta web)
    - especial importancia LSSI
    - relación con terceros frecuente
    - la manipulación de la información es muy importante
      - firma de contratos para mantener la confidencialidad
    - aspectos físicos de la seguridad
    - control de acceso a un sistema directamente expuesto
    - aplican todos los controles e-business
  - trabajador itinerante/teletrabajo → asustar, educar para evitar males mayores
    - la información viaja más allá de las fronteras físicas
    - confidencialidad y uso de la información
    - la manipulación de la información externa es importante
    - operaciones vinculadas con la dependencia de las conexiones

- seguridad física aplicada a entornos móviles
- control ed acceso importante
- vulnerabilidades y riesgos en entornos públicos
- uso de aparatos propios → la empresa incluso propicia o alenta este uso → problemas futuros en caso de final de relación empresa-trabajador
- implementación de un plan de seguridad: 9 / 18 meses
- instalaciones empresa:
  - oficina administrativa
    - alto impacto en política general
    - peso legal importante
    - menor impacto relación con terceros
    - el intercambio de información es clave
    - no se encarga de adquisición y mantenimiento
    - control de acceso importante, escenario intensivo en el uso de la información
    - poca relación con los controles e-business
    - emplazamiento fijo y controlado
  - producción
    - fuertemente vinculado a la organización y política corporativa
    - aplican la mayoría de los controles legales
    - muchas relaciones con terceros
    - la manipulación de la información forma parte nuclear
    - provisión, mantenimiento y desarrollo de sistemas es una parte muy importante, afecta productividad
    - seguridad física importante
    - control acceso importante
  - entornos publicos, carga/descarga
  - SOHO
    - no contratado por la empresa, autónomo, SL, externo
    - formalizar relación aunque sea una relación de confianza
    - implicaciones de manipulación son directametine aplicables
    - medidas físicas son importantes
    - adquisición y mantenimiento de equipos según la configuración
    - los aspectos legales son universales
  - [Ejercicio de Autodiagnóstico, como gestionamos actualmente la seguridad?](#)

1)

Sistemas de Información

From:  
<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:  
<https://miguelangel.torresegea.es/wiki/info:cursos:seguridadinformatica?rev=1352821844>

Last update: **13/11/2012 07:50**

