

# plan de seguridad informática

## datos

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

## 1. 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

- condidencialidad: 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 directamente 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?](#)

## webs de seguridad

- <http://www.cesicat.cat>
  - alertas virus, peligros, etc...
  - servicios
- <http://www.inteco.es>
- <http://www.slideshare.net/mib/el-plan-estratégico-de-sistemas-de-información>
- [http://ca.wikipedia.org/wiki/Planificaci%C3%B3n\\_de\\_sistemas\\_inform%C3%A1ticos](http://ca.wikipedia.org/wiki/Planificaci%C3%B3n_de_sistemas_inform%C3%A1ticos)

## 2. Gestión de los sistemas de información

### planificación estratégica

- previsión de decrecimiento e implicaciones
- análisis
  - organizativo
  - de procesos

- de recursos (infraestructura)
- ...
- fases
  - determinar estrategia y contexto actual
  - identificar los requerimientos de negocio en SI<sup>2)</sup>
  - estado actual
  - análisis
  - ...
- Normas y buenas prácticas en gestión TI<sup>3)</sup>
  - ITIL = Information Technology Infrastructure Library
  - COBIT = Control Objectives for Information and related Technology
  - normas internacionales, algunas certificables
  - normas ISO elaboradas por comité técnico JTC1
    - 27001
    - 9000
- Áreas gestión ITIL
  - perspectiva orientada a procesos
  - 3 áreas principales
    - tecnología/negocio
    - perspectiva negocio, planificación para implementación, gestión de la infraestructura TI
    - gestión de servicios
    - ...
  - Soporte al servicio
    - disponibilidad
    - gestión incidencias
      - resolución rápida y eficaz
      - restauración del servicio, no causas.
      - asignación personal
    - gestión de problemas
      - recurrentes o de gran impacto
      - determinar causas
      - reactiva, proactiva
    - configuraciones
      - registros actualizados
    - cambios
      - planificación y evaluación de procesos de cambio
      - testeo previo en entorno de pruebas
      - plan vuelta atrás - backup
    - versiones
      - software y hardware
    - gestión financiera
      - evaluación y control de costes asociados a TI
      - ROI<sup>4)</sup>
    - gestión de capacidad
      - todos los servicios TI están apoyados por una capacidad de procesos y almacenaje suficiente y correctamente dimensionada
      - VIRTUALIZACION, CLOUD COMPUTING
    - gestión de continuidad del servicio
      - factores de riesgo en los entornos de los SI y evaluarlos en función de su probabilidad de suceder y su grado de impacto
      - combinar reactivo y proactivo
    - gestión de disponibilidad (SLA)
      - ...
    - gestión de niveles de servicio
      - ...

### 3. Gestión de la seguridad de la información

- Gestión de la seguridad
  - disponibilidad sea donde sea: seguridad perimetral, test de intrusión, política de seguridad
  - movilidad de empresa: acceso sin hilo/móvil, seguridad perimetral
  - evitar robos o mal uso: seguridad perimetral, auditoria seguridad, test de intrusión, política de seguridad, seguridad de directorio, ...
  - colaboración interpersonal y entre empresas
  - continuidad de negocio
  - cumplimiento de requisitos legales
  - confianza en la veracidad de la información
- ejemplos grado coste de inversiones y mantenimiento
  - tabla con solución, coste inicial, mantenimiento
- cálculo ROSI = Retorno sobre la Seguridad Informática
  - $(\text{Valor Perdidas} - \text{Coste Seguridad}) / \text{Coste Seguridad}$
  - Si ROSI > 0 es aceptable
  - Valor perdidas: perdidas por incidentes sin tratar - perdidas por incidentes evitados
  - Coste Seguridad: inversión inicial + inversión periodica
  - Perdidas: frecuencia anual de ocurrencias x impacto económico, legal u otro
- SGSI = Sistema de Gestión de Seguridad de la Información
  - ISO/IEC 27001
  - gestión de la seguridad de la información de manera ordenada y diligente
  - en ciertas empresas puede ser una exigencia comercial o legal
  - aplicar una inversión en seguridad balanceada - no seguir modelos o presiones comerciales o a impulsos a causa de un accidente aislado
  - dificultades o desventajas:
    - primer año de implementación
    - cambios de procedimientos
    - documentación
    - automatización de tareas
    - impacto en el personal
  - Mejorar seguridad de la información de la empresa
  - Mejorar los sistemas productivos
  - optimizar recursos de la empresa
  - incorporar a la empresa en la filosofía PDCA o de mejora continuada
  - obtener los niveles exigidos en los pliegos de la Administración relativos en los servicios TIC
  - dispone de sistemas certificados por terceros de confianza
  - la ISO genera confianza internacional
  - cumplir requerimientos legales (LOPD, LPI, LSSICE, ...)
  - mejora la imagen de la empresa respecto a la competencia (solo 300 empresas con normativa 27001)
  - implantación por capas o niveles, no apretar el acelerador (27002, compendio de buenas prácticas)
  - herramientas de gestión para soportar el SGSI
  - análisis de riesgos y atacar los puntos más calientes
  - controlar falsa sensación de seguridad
- objetivos de la gestión de la seguridad
  - diseñar políticas de seguridad - una hoja, no es una normativa
  - garantizar que los niveles estandar de seguridad se cumplen
  - minimizar los riesgos de seguridad
  - la gestión de seguridad:
    - es responsabilidad de todos
    - no es una prioridad en su misma
  - supervisar la inclusión en las SLA y garantizar su cumplimiento

- tener un comportamiento proactivo
- sistemas de seguridad
  - conjunto de medios administrativos, técnicos y personales que entre todos garantizan los niveles
  - 3 etapas
    - determinar las necesidades de protección de Iso SI
      - identificar amenazas y estimación de riesgos
      - evaluación del estado actual de la seguridad
    - definir e implementar el sistema de seguridad que garantice minimizar riesgos
      - definir las políticas de seguridad
      - definir las medidas y procedimientos a implementar
    - evaluar sistemas de seguridad
  - no se pueden eliminar todos los riesgos
- <http://www.ISO27000.es>
- PDCA = Plan+Do+Check+Act = Ciclo de Deming
  - P = establecer SGSI
  - D = Mantener y mejorar
  - C = verificar y evaluar
  - A = puesta en explotación y ejecución
  - es una rueda, siempre vuelve a empezar, cada vuelta puede ser de 1 año
- Herramientas útiles:
  - inventarios y gestión documental:
    - surveymonkey, excel para recuperar información
    - sharepoint: gestión documental
  - 27001:
    - PILAR: <http://www.pilar-tools.com>
    - GlobalSuite
    - ERA
    - GovRic
    - AGGIL: <http://www.aggil.es> SaaS<sup>5)</sup>
    - e-Pulpo: <http://www.e-pulpo.es>
- auditorias seguridad:
  - si queremos la certificación, empresa externa
- seguridad como servicio
  - análisis de log
  - servidores correo
  - servidores web
  - encriptación de comunicaciones / ordenadores
  - backup gestionado
    - servidores: recuperación de desastres, continuidad de operación, copia externa
    - ordenadores: servidor almacenamiento local, copia externa
  - supervisión y análisis de web
    - supervisión remota de webs
    - análisis de logs y transacciones
  - <http://www.catrian.com>
  - <http://www.segall.es>
  - idigital.cat
    - generación de informes de recomendaciones
    - coste 400 euros
    - empresas catalanas

## 4. plan de continuidad de empresa

## riesgos

- Análisis: tipos de riesgos
  - amenazas: externas
  - vulnerabilidades: internas
  - probabilidad de ocurrir
  - impacto que tiene el suceso
  - evaluar coste económico
    - coste evitar un suceso
    - coste de minimizar los efectos
    - coste de recuperarse
    - coste de asumir el suceso
- Gestión: diseño planes para evitar
  - minimizar el riesgo: controles
  - transferir el riesgo: externalizar
  - aceptar el riesgo: sin medidas, ser consciente
  - evitar el riesgo: acabar con la actividad que la origina

## interrupciones en los procesos de negocio

- criticidad de los recursos
- periodo de tiempo de recuperación límite
- sistema de clasificación de riesgos

## recuperación

- punto de recuperación: determinar % de funcionamiento
- tiempo de recuperación: tolerancia

## estrategias de recuperación

- medidas preventivas, detectivas, correctivas
- ...

## validación del plan

- pruebas de verificación del plan de continuidad
  - parte técnica
  - habilidad del personal
- no tener validado el plan puede ser tan o más peligroso que no tenerlo
- ...

## 5. plan de seguridad

1)

Sistemas de Información

2)

Sistemas ed Información

3)

tecnologías de información

4)

retorno de la inversión

5)

Security as a Service

From:

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



Permanent link:

<https://miguelangel.torresegea.es/wiki/info:cursos:seguridadinformatica?rev=1352832131>

Last update: **13/11/2012 10:42**