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[1)]
- 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
    - púbica
    - 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 vincualdas con la dependencia de las conexiones

        - seguridad física aplicada a entornes móbiles
        - 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 directametne 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,e tc...
    - servicios
- http://www.inteco.es
- http://www.slideshare.net/mib/el-plan-estratgico-de-sistemas-de-informacin
- http://ca.wikipedia.org/wiki/Planificaci%C3%B3_de_sistemes_inform%C3%A0tics

planificación estratégica

- previsión de decrecimiento e implicaciones
- analisis
    - organizativo
    - de procesos
    - de recursos (infraestructura)
    - ...
- fases

    - determinar estrategia y contecto actual
    - identificar los requerimientos de negocio en SI[2)]
    - estado actual
    - analisis
    - ...
- Normas y buenas prácticas en gestión TI[3)]
    - ITIL = Informatiion Technology Infraestructure Library
    - COBIT = Control OBjectives for Information and related Technology
    - normas internacionales, algunas certificables
    - normas ISO elaboradas por comité técnico JTC1
        - 27001
        - 9000
- Areas gestión ITIL
    - perspectiva orientada a procesos
    - 3 áreas principales
        - tecnología/negocio
        - perspectiva negocio, panificación 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 - backout
        - versiones
            - software y hardware
        - gestión financiera
            - evaluación y control de costes asociados a TI
            - ROI[4)]
        - 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
        - ...
    - Gestión de la seguridad
        - disponibilidad sea donde sea: segurida perimetral, test de intrusión, politica de seguridad
        - mobilidad de empresa: acceso sin hilo/móvil, seguridad perimetral
        - evitar robos o mal uso: seguridad perimetral, auditoria seguridad, test de intrusión, politica

de seguridad, seguridad de directorio, ...
        - colaboración interpersonal y entre empresas
        - continudad de negocio
        - cumplimiento de requisitos legales
        - confianza en la veracidad de la información
    - ejemplos grado coste de inversiones y matenimiento
        - tabla con solución, coste inicial, mantenimiento
    - cálculo ROSI = Retorno sobre la Seguridad Informática
        - (Valor Perdidas - Coste Seguridad) / Coste Seguridad
        - Si ROSI > 0 es aceptable
        - Valor perdidas: perdidas por incidendes sin tratar - perdidas por incidentes evitados
        - Coste Seguridad: inversión inicial + inversión periodica
        - Perdidas: frecuencia anual de ocurrencias x imacto 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

[1]
Sistemas de Información
[2]
Sistemas ed Información
[3]
tecnologias de información
[4]
retorno de la inversión