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[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

2. Gestión de los sistemas de información

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
        - ...

3.Gestión de la seguridad de la información

- 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
  - Mejorar seguridad de la información de la empresa
  - Mejorar los sistemas productivos
  - optimizar recursos de la empresa
  - incorporar a la empresa en la filosofia 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 requirimientos 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
  - analisis 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 estandard 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, técnivos y personales que entre todos garantizan los niveles
  - 3 etapas
    - determinar las necesidades de protección de lso 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[5)]
    - e-Pulpo: http://www.e-pulpo.es
- auditorias seguridad:
  - si queremos la certificación, empresa externa
- seguridad como servicio
  - analisis de log
  - servidores correo
  - servidores web
  - encriptación de comunicaciones / ordenadores
  - backup gestionado
    - servidores: recuperación de desastres, continuidad de opreación, copia externa
    - ordenadores: servidor almacenamiento local, copia externa
  - supervisión y análisis de web
    - supervisión remota de webs
    - analisis 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

- Analisis: 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 limite
- 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

Expresión gráfica del sistema de seguridad diseñado

1. caracterización del SI
2. resultado del analisis de riesgos
3. politicas de seguridad de la información
4. responsabilidad de los participantes
5. descripción detallada del sistema de seguridad
    - medios: humanos, materiales, técnicos
    - medidas y procedimientos de seguridad: fisico, técnico, lógico

nos ha de permitir prevenir, detectar y responder a las posibles amenazas

5.1.caracterización

- ordenadores: servidores/clientes
- sistemas de seguridad: hard y soft
- dispositos auxiliares: impresoras, escaners, dispostivos de almacen portatil)
- procedimientos: de tratamiento de la información
- recursos y procesos subcontratados: listado de externos
- formas de acceso: a y desde el exterior
- topologia de red
- dispositivos de red
- sistemas operativos
- aplicaciones

5.2.resultado del analisis de riesgos

- riesgos más probables y de mayo impacto
- aspectos centrados en la seguridad de sistema
- detallar:
    - acciones a realizar
    - quien las realiza
    - en que momento se ralizan
    - ...

5.3.politicas de seguridad

- normas que ha de cumplir el personal
- adecuados a la legislación vigente
- sencillo, el ABC
- homogeneizar con respecto a normativa vigente:
    - LOPD para el uso de usuarios/contraseñas, p.e.
- ...

5.4.responsabilidad de los particiapnetes

- personal involucrado
- responsabilidad de cada uno
- comunicar adecuadamente
- ...

descripción del sistema de seguridad

- forma de implementar las políticas de seguridad y resto de medidas de protección
- elaborar:
    - programa de seguridad
    - planificación temporal
    - acciones necesarias para llegar a niveles de seguridad superior
- detallar:
    - asignación de medios humanos en las tareas de seguridad
    - lista de medios técnicos y su configuración

medidas y procedimientos de protección física

- amenazas de daños a equipos o infraestructuras: incendios, inundaciones, agya, terremotos, sabotaje
- en función de la probabilidad:
    - CPD (interno/externo) con protección de incendios, inundaciones, acceso restringido
    - Duplicar infraestructuras críticas (servidores y similares) en diferentes localizaciones
    - duplicidad de la red interna (por ejemplo, cable y red)
    - duplicidad de red externa (dos proveedores)
    - estoc de seguridad de equipos y componentes para cambios rápidos
    - no permitir uso de USBs y similares

medidas y procedimientos de protección lógica

- protección de la información por medio de programas o dispositivos específicos
    - identificación y autentificación de usuario
    - métodos de contro de acceso: mínimo privilegio necesario
    - métodos para garantizar la integridad de los ficheros y los datos: sistemas de alta disponibilidad, copias de seguridad, logs

medidas y procedimientos de protección en operaciones

- procedimientos que permitan minimizar los riesgos
    - metodologia de las copias de seguridad
        - periodicidad
        - responsables
        - números de versiones
        - tipos de copias
    - gestión de las claves de acceso
    - control de los equipos
        - con información sensible y la entrada/salida de tecnología
    - seguridad de las coneciones en la red interna (desde el exterior)
    - almacenar y analizar los logs
    - control de mantenimiento y reparación de los equipos
    - autorización y denegación de los servicios a usuarios

medidas y procedimientos de recuperación ante contigencias

- cualquier eventualidad que pueda parar total o parcialmente la actividad

relaciones entre el plan de seguridad y el de continuidad de negocio

- ...

Plan de seguridad: metodologia ISO 27001

- cuatro áreas de especialización
    1. Gestión
    2. Control de acceso
    3. ...
    4. ...

plan de seguridad, actores implicados

- dirección general
- profesionales de la seguridad de los sistemas de información
- propietarios de activos concretos
    - asegurarse de que se implementa la seguridad adecuada
    - niveles de sensibilidad de la información
    - determinar privilegios de acceso
- administradores
- ...
- personal de los sistemas de información
- auditor de los sitemas de información

práctica

- deficiencias detectadas:
    - sin control acceso físico
    - sin sistema de backup
    - sistema de refigeración
    - software:
        - windows vista → obsoleto?
        - office pirata → funcional?
        - antivirus → obligado? centralizado?
        - administradores

1)
Sistemas de Información
2)
Sistemas ed Información
3)
tecnologias de información
4)
retorno de la inversión
5)
Security as a Service