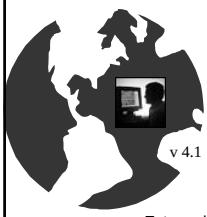
Capítulo 5
Introducción a la Gestión de la Seguridad

Seguridad Informática y Criptografía



Material Docente de
Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 46 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

Protección lógica y física de los datos

Los datos deben protegerse aplicando:

- Seguridad Lógica
  - Uso de herramientas de protección de la información en el mismo medio en el que se genera o transmite.
  - Protocolos de autenticación entre cliente y servidor.
  - Aplicación de herramientas de seguridad en redes.
  - Se incluyen también medidas de prevención de riesgos y la instauración de políticas de seguridad, de planes de contingencia, de recuperación ante desastres, aplicación de normativas, la legislación vigente, etc.
- Seguridad Física
  - Procedimientos de protección física del sistema: acceso personas, incendio, agua, terremotos, etc.

La seguridad física en entornos de PCs

- Anclajes a mesas de trabajo.
- Cerraduras en puertas.
- Tarjetas con alarma.
- Etiquetas con adhesivos especiales.
- Bloqueo de unidades externas.
- Protectores de teclado.
- Tarjeta de control de acceso al hardware.
- Sistema de suministro continuo de corriente.
- Toma de tierra.
- Eliminación de la estática... etc.

Temas a tener en cuenta en un entorno de PCs

Análisis de riesgo: plan estratégico

- Es el proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo que significaría la prevención de este suceso.
- Su análisis no sólo nos lleva a establecer un nivel adecuado de seguridad, sino que permite conocer mejor el sistema que vamos a proteger.

- Le recomiendo descargar estas herramientas de libre distribución para el análisis de riesgo desde las direcciones que se indican:

Magerit V 2 http://www.csi.map.es/csi/pg5m20.htm

Chinchon V 1.3 http://www.criptored.upm.es/software/sw_m214_01.htm

Información del análisis de riesgo

- Información que se obtiene en un análisis de riesgo:
  - Determinación precisa de los recursos sensibles de la organización.
  - Identificación de las amenazas del sistema.
  - Identificación de las vulnerabilidades específicas del sistema.
  - Identificación de posibles pérdidas.
  - Identificación de la probabilidad de ocurrencia de una pérdida.
  - Derivación de contramedidas efectivas.
  - Identificación de herramientas de seguridad.
  - Implementación de un sistema de seguridad eficiente en costes y tiempo.

Ecuación básica del análisis de riesgo

$$¿\ B > P * L\ ?$$

- B: es la carga o gasto que significa la prevención de una pérdida específica debido a una vulnerabilidad.
- P: es la probabilidad de que se vea afectada dicha vulnerabilidad y ocurra esa pérdida específica.
- L: es el impacto o coste total que significa la pérdida específica debido a esa vulnerabilidad que ha sido afectada por una amenaza.

¿Cuándo y cuánto invertir en seguridad?

Si $B \leq P * L$

Hay que implementar una medida de prevención.

Si $B > P * L$

No es necesaria una medida de prevención.

... al menos matemáticamente. No obstante, siempre puede ocurrir una desgracia que esté fuera de todo cálculo como las consecuencias informáticas en algunas empresas tras el 11 de septiembre. Lo que sí es cierto, es que no tiene sentido alguno invertir más dinero en la protección del bien que el propio valor de éste.

Efectividad del coste de la medida

- Las medidas y herramientas de control han de tener menos coste que el valor de las posibles pérdidas y el impacto de éstas si se produce el riesgo temido.
- Ley básica: el costo del control ha de ser menor que el activo que se protege. Algo totalmente lógico y que tanto los directivos como los responsables de seguridad de la empresa deberán estimar de forma adecuada a su realidad. En varios casos, el verdadero problema está en la dificultad de calcular de forma más o menos precisa el impacto económico que puede suponer el hecho de que ocurra ese riesgo.

El factor L en la ecuación de riesgo

Factor L (en $B \leq P * L$)

- El factor de impacto total L es difícil de evaluar. Incluye daños a la información, a los equipos, pérdidas por reparación, por volver a levantar el sistema, pérdidas por horas de trabajo, etc.
- Siempre habrá una parte de valoración subjetiva.
- La pérdida de datos puede llevar a una pérdida de oportunidades por el llamado efecto cascada.
- En la organización debe existir una comisión especializada interna o externa que sea capaz de evaluar todas las posibles pérdidas y cuantificarlas.

El factor P en la ecuación de riesgo

Factor P (en $B \leq P * L$)

- El factor P está relacionado con la determinación del impacto total L y depende del entorno en el que esté la posible pérdida. Como este valor es difícil de cuantificar, dicha probabilidad puede asociarse a una tendencia o frecuencia conocida.
  - Una vez se conoce P para un L dado, se obtiene la probabilidad de pérdida relativa de la ocurrencia $P*L$ que se comparará con B, el peso que nos supondría implantar la medida de prevención respectiva.

El factor B en la ecuación de riesgo

Factor B (en $B \leq P * L$)

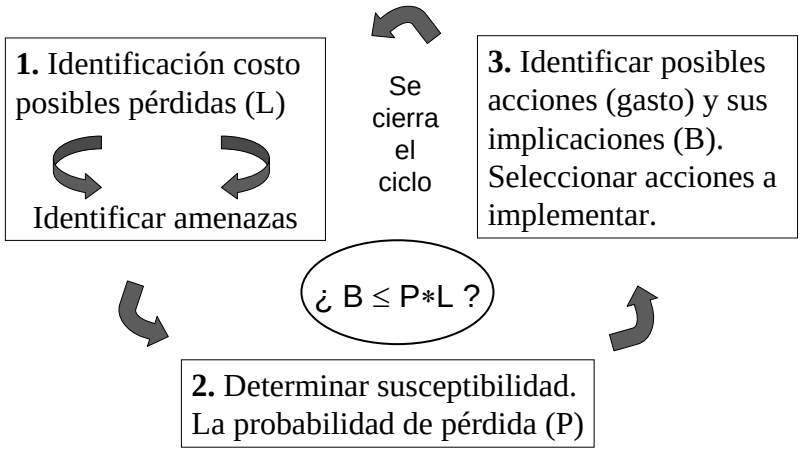
- Indica qué se requiere para prevenir una pérdida. Por ejemplo, puede ser la cantidad de dinero que vamos a disponer para mitigar la posible pérdida.
  - Ejemplo: la carga de prevención para que un sistema informático minimice el riesgo de que sus servidores sean atacados desde fuera incluye la instalación de software y hardware adecuado, un cortafuegos, un sistema de detección de intrusos, una configuración de red segura, una política de seguimiento de accesos y de passwords, personal técnico cualificado, etc. Todo ello importa una cantidad de dinero específica.

Cuantificación de la protección

¿ $B \leq P * L$?

- ¿Cuánta protección es necesaria?
  - En nuestro ejemplo: qué configuración de red usar, en qué entorno trabajar, qué tipo de cortafuegos, etc. Eso dependerá del nivel de seguridad que nuestra empresa desee, crea oportuno o que nos imponga el mercado.
- ¿De qué forma nos protegeremos?
  - Una casa puede protegerse con puertas, cerraduras, barras de hierro en ventanas, sistemas de alarmas, etc.
  - En un sistema informático podemos aplicar protecciones físicas, políticas de seguridad, control de accesos, planes de contingencia y de recuperación, cortafuegos, IDs, uso de cifrado, autenticación, firmas, pasarelas seguras, etc.

Pasos en un análisis de riesgos



Algunas políticas de seguridad

- Políticas administrativas
  - Procedimientos administrativos.
- Políticas de control de acceso
  - Privilegios de acceso del usuario o programa.
- Políticas de flujo de información
  - Normas bajo las cuales se comunican los sujetos dentro del sistema.

Aspectos administrativos

- Políticas administrativas
  - Se establecen aquellos procedimientos de carácter administrativo en la organización como por ejemplo en el desarrollo de programas: modularidad en aplicaciones, revisión sistemática, etc.
  - Se establecen responsabilidades compartidas por todos los usuarios, cada uno en su nivel.
  - Se procede a la etapa de concienciación.

Control de accesos

- Políticas de control de acceso
  - Política de menor privilegio
    - Acceso estricto a objetos determinados, con mínimos privilegios para los usuarios.
  - Política de compartición
    - Acceso de máximo privilegio en el que cada usuario puede acceder a todos los objetos.
  - Granularidad
    - Número de objetos accesibles. Se habla entonces de granularidad gruesa y fina.

Control de flujo

- Políticas de control de flujo
  - La información a la que se accede, se envía y recibe por:
    - ¿Canales claros o canales ocultos? ¿Seguros o no?
  - ¿Qué es lo que hay que potenciar?
    - ¿La confidencialidad o la integridad?
    - ¿La disponibilidad? ... ¿El no repudio?
    - Según cada organización y su entorno de trabajo y servicios ofrecidos, habrá diferencias. En algunos sistemas primarán unos más que otros, en función de lo secreta que sea la información que procesan.

Modelos de seguridad

- Modelo de Bell LaPadula (BLP)
  - Rígido. Confidencialidad y con autoridad.
- Modelo de Clark-Wilson (CW)
  - Orientación comercial: integridad.
- Modelo de Take-Grant (TG)
  - Derechos especiales: tomar y otorgar.

Se definirán brevemente en próximas diapositivas

- Otros: modelo de Goguen-Meseguer (no interferencia entre usuarios); modelo de Matriz de Accesos (estados y transiciones entre estados: tipo Graham-Dennig; tipo Harrison-Ruzzo-Ullman), Biba, Chinese Wall, etc.

Modelo de Bell y LaPadula

- La escritura hacia abajo está prohibida.
- La lectura hacia arriba está prohibida.
- Es el llamado principio de tranquilidad.

Lectura hacia arriba prohibida	Secreto máximo
Usuario dado de alta con un nivel de secreto	Secreto
Escritura hacia abajo prohibida	No clasificado

http://en.wikipedia.org/wiki/Bell-LaPadula_model

Modelo de Clark Wilson CW

- Está basado en políticas de integridad
  - Elementos de datos restringidos.
    - sobre éstos debe hacerse un chequeo de consistencia.
  - Elementos de datos no restringidos.
  - Procedimientos de transformación.
    - trata los dos elementos.
  - Procedimientos de verificación de integridad.

http://www.criptored.upm.es/guiateoria/gt_m248c.htm

Modelo de Take Grant TG

- Se describe mediante grafos orientados:
  - el vértice es un objeto o sujeto.
  - un arco es un derecho.
- Se ocupa sólo de aquellos derechos que pueden ser transferidos.

http://www.criptored.upm.es/guiateoria/gt_m248b.htm

➢ Documentos de lectura recomendada:

Biba	http://www.criptored.upm.es/guiateoria/gt_m248a.htm
Harrison, Ruzzo y Ullman	http://www.criptored.upm.es/guiateoria/gt_m248e.htm
Chinese Wall	http://www.criptored.upm.es/guiateoria/gt_m248d.htm
Sea View: bases de datos	http://www.criptored.upm.es/guiateoria/gt_m248f.htm

Criterios y normativas de seguridad

- Criterio de evaluación TSEC
  - Trusted Computer System Evaluation Criteria, también conocido como Orange Book.
- Criterio de evaluación ITSEC
  - Information Technology Security Evaluation Criteria.
- Criterio de evaluación CC
  - Common Criteria: incluye los dos anteriores.
- Normativa internacional 17799
  - Desarrolla un protocolo de condiciones mínimas de seguridad informática de amplio espectro.

➢ Encontrará una interesante lectura sobre aplicación de criterios de seguridad en el documento que se indica

http://www.csi.map.es/csi/criterios/seguridad/index.html

Leyes de seguridad informática en España

- En el Real Decreto 994/1999 (11 junio) sobre "Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal" se definen las funciones del Responsable de Seguridad.
- Ley Orgánica de Protección de Datos LOPD se desarrolla en España en diciembre de 1999 y comienza a aplicarse ya en el año 2002.
- Se crea una Agencia Española de Protección de Datos AEPD que debe velar por el cumplimiento de esta ley mediante la realización de auditorías, al menos cada dos años. La AEPD la forman 9 personas.
- Se definen las funciones y obligaciones del Responsable de Fichero y del Encargado de Tratamiento.
- Las infracciones se clasifican como leves, graves y muy graves con sanciones de 60.000 €, 300.000 € y 600.000 € respectivamente.
- Establece un conjunto de procedimientos de obligado cumplimiento de forma que además de proteger la privacidad de los datos, se cumplan los principios de la seguridad informática física y lógica.

http://www.agpd.es/index.php?idSeccion=77

Cadena de responsabilidades en seguridad

- Responsable de Fichero: es la entidad, institución o persona jurídica que posee datos de carácter personal y que por tanto debe velar por la seguridad de ellos.
- Responsable de Tratamiento: es posible que la entidad anterior sea quien manipule los datos (gestión, copias de seguridad, etc.) o bien esta tarea la ejecute otra empresa. De ahí que se diferencie entre estos dos responsables.
- Responsable de seguridad: persona o personas en las que el responsable de fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.8%29%20Real%20Decreto%20994-1999.pdf

Operaciones de responsabilidad en LOPD

- Artículo 9: Seguridad de los datos.
  - El responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Temas como estar en el "estado de la tecnología" y conocer todo tipo de "riesgos" son un dolor de cabeza para el responsable de seguridad.

https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf

Niveles de seguridad en el RD 994/1999

- Nivel Básico: todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
- Nivel Medio: los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros ..., deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
- Nivel Alto: los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas como de nivel alto.

Las medidas a que se hace mención en estos textos puede verlas en:

https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.8%29%20Real%20Decreto%20994-1999.pdf

LOPD: algunas infracciones leves

- No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
- No proporcionar información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
- No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente ley.

LOPD: algunas infracciones graves

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el “Boletín Oficial del Estado” o diario oficial correspondiente.
- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.
- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste se exigible.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determine.

LOPD: algunas infracciones muy graves

- La recogida de datos de forma engañosa y fraudulenta.
- La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
- La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

La norma ISO 17799 (27001)

- Presenta normas, criterios y recomendaciones básicas para establecer políticas de seguridad.
- Éstas van desde los conceptos de seguridad física hasta los de seguridad lógica.
- Parte de la norma elaborada por la BSI, British Standards Institution, adoptada por International Standards Organization ISO y la International Electronic Commission IEC.
- Documento de 70 páginas no de libre distribución.

☞ Desde finales de 2005 estas normas se están revisando y cambiando de numeración a partir del número 27001.

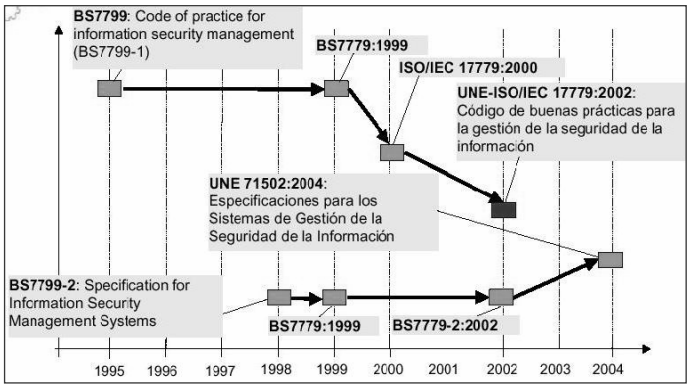
http://www.aenor.es/desarrollo/normalizacion/normas/resultadobuscnormas.asp?campobuscador=17799

Entornos de la norma ISO 17799

Se trata de un código de buenas prácticas para la Gestión de la Seguridad de la Información.

- Antecedentes
- Introducción
- Objeto y campo de la aplicación
- Términos y definiciones
- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de los archivos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad del negocio
- Conformidad

Historia de la norma ISO 17799



Ref.: "Gestión de Seguridad de la Información: UNE 71502, ISO17799", A. Villalón.

http://www.criptored.upm.es/guiateoria/gt_m209b.htm

Planes de contingencia

- Un Plan de Contingencia consiste en un estudio y análisis pormenorizado de las áreas que componen la organización y que nos servirá para establecer una política de recuperación ante un desastre.
  - Es un conjunto de datos estratégicos de la empresa y que se plasma en un documento con el fin de protegerse ante eventualidades.
- Además de aumentar su seguridad, con un plan estratégico la empresa también gana en el conocimiento de sus fortalezas y sus debilidades.
- Pero si no lo hace, se expone a sufrir una pérdida irreparable mucho más costosa que la implantación de este plan.

Acciones a realizar en un SGSI

El Plan de Contingencia será una herramienta imprescindible en un Sistema de Gestión de la Seguridad Informática (SGSI). Acciones:

- Planificar: estudiar la implantación de la política de seguridad adoptada, alcances que tendrá la gestión, análisis de riesgos que se harán, establecimiento de controles que activaremos, etc.
- Hacer: implantar el sistema de gestión, poner y activar los controles, registros e indicadores. Toma de datos del estado de la seguridad.
- Verificar: realizar una auditoría interna para comprobar el grado de cumplimiento de nuestro sistema.
- Actuar: realizar el seguimiento de la gestión y tomar las medidas correctivas así como las acciones preventivas correspondientes.

Se cierra el ciclo ajustando las acciones planificadas si fuera el caso.

Ciclo más conocido por las siglas PDCA (Plan - Do - Check - Act) ⇨

Ciclo PDCA

Plan

Política y Alcance del sistema
Análisis de riesgos
Selección de controles

Do

Implantación del SGSI
Implantación controles
Implantación indicadores

Check

Auditoría interna
No conformidades
Grado de cumplimiento

Act

Acciones correctivas
Acciones preventivas
Modificación Plan

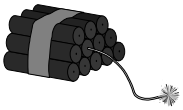
Desastres naturales y su prevención

- Desastres naturales
  - Huracán
  - Tormenta
  - Inundación
  - Tornado
  - Vendaval
  - Incendio
  - Terremoto
  - Otros

- Medidas prevención
  - Emplazamientos adecuados
  - Protección fachadas, ventanas, puertas

Vandalismo informático y su prevención

- Terrorismo
- Sabotaje
- Robo



- Virus
- Chantaje informático
- Programas malignos

- Medidas de prevención
  - Fortificación de entradas
  - Guardia Jurado
  - Patrullas de seguridad
  - Circuito cerrado TV
  - Control físico de accesos
  - Protección de software y hardware con antivirus, cortafuegos, detección de intrusos, etc.
  - Seguimiento de las políticas de seguridad de la empresa.

Amenazas del agua y su prevención

- Amenazas
  - Inundaciones por causas propias de la empresa
  - Inundaciones por causas ajenas
  - Pequeños incidentes personales (la típica botella de agua o taza con café que se cae sobre el teclado...)

- Medidas prevención
  - Revisar conductos de agua
  - Emplazar la sala con los equipos más caros en un sitio libre de estos problemas
  - Instalar sistemas de drenaje de emergencia
  - Concienciar a nuestros empleados

Amenazas del fuego y su prevención

- Amenazas
  - Una mala instalación eléctrica
  - Descuidos personales como puede ser fumar en sala de ordenadores
  - Papeleras mal ubicadas en la que se tira un cigarrillo no apagado
  - Vulnerabilidades del sistema ante el humo
- Medidas prevención
  - Detector humo y calor
  - Materiales ignífugos
  - Almacén de papel separado de máquinas
  - Estado del falso suelo
  - Extintores revisados

Es la amenaza más temida por su rápido poder destructor.

¿Qué sucede si se produce un desastre?

- Las empresas dependen hoy en día de los equipos informáticos y de todos los datos que hay allí almacenados (nóminas, clientes, facturas, ...).
- Dependen también cada vez más de las comunicaciones a través de las redes de datos.
- Si falla el sistema informático y éste no puede recuperarse, la empresa puede desaparecer porque no tiene tiempo de salir nuevamente al mercado con ciertas expectativas de éxito, aunque conserve a todo su personal.

Tiempos de recuperación ante desastres

- Según diversos estudios el período máximo de inactividad que puede soportar una empresa sin poner en peligro su supervivencia es de:
  - Sector seguros: 5,6 días
  - Sector fabricación: 4,9 días
  - Sector industrial: 4,8 días
  - Sector distribución: 3,3 días
  - Sector financiero: 2,0 días
- Si nos han dicho que nuestro banco tiene problemas de seguridad y no podemos mover nuestras cuentas, lo más seguro es que cambiemos de banco al día siguiente.

Pérdidas por no contar con plan estratégico

- Pérdida de clientes.
- Pérdida de imagen.
- Pérdida de ingresos por beneficios.
- Pérdida de ingresos por ventas y cobros.
- Pérdida de ingresos por producción.
- Pérdida de competitividad en el mercado.
- Pérdida de credibilidad en el sector.

Medidas básicas ante un desastre

- Plan de emergencia
  - Vidas, heridos, activos, evacuación personal.
  - Inventariar recursos siniestrados.
  - Evaluar el coste de la inactividad.
- Plan de recuperación
  - Acciones tendentes a volver a la situación que existía antes del desastre.

http://recovery-disaster.info/index.htm

Alternativas del plan de continuidad

- Instalaciones alternativas
  - Oficina de servicios propia
  - Acuerdo con empresa vendedora de HW y SW
  - Acuerdo recíproco entre dos o más empresas
  - Arranque en frío: sala vacía propia
  - Arranque en caliente: centro equipado
  - Sistema Up Start: caravana, unidad móvil
  - Sistema Hot Start: centro gemelo

Algunas soluciones pueden resultar de muy alto costo. Su elección dependerá entonces de las características de nuestra empresa y qué tan crítico debe ser ese plan de continuidad acorde con ello.

Fin del capítulo

Cuestiones y ejercicios (1 de 2)

1. ¿Qué es y qué significa hacer un análisis de riesgos?
2. Explique el sentido de las ecuaciones $B > P*L$ y $B \leq P*L$.
3. Tras un estudio, obtenemos $B > P*L$, ¿podemos estar totalmente tranquilos al no utilizar medida alguna de prevención?
4. Explique qué significan los factores L y P en la ecuación $B > P*L$.
5. ¿Cuáles son los pasos a seguir en un análisis de riesgo de acuerdo a los factores de la ecuación de $B > P*L$?
6. En algunos sistemas de gestión de información a veces prima más el elemento confidencialidad, en cambio en otros más el de integridad. Dé algunos ejemplos en que pueda cumplirse al menos en parte este escenario. ¿Qué opina respecto a una transacción electrónica?
7. Comente el modelo de seguridad de Bell Lapadula. ¿Por qué se le llama el modelo de la tranquilidad?

Cuestiones y ejercicios (2 de 2)

8. Ud. es el responsable de seguridad y detecta que un empleado está robando información confidencial, ¿cómo reaccionaría?
9. ¿Cuáles pueden ser las pérdidas en una empresa si no se cuenta con un adecuado Plan de Contingencia y sucede un desastre?
10. ¿Qué es un Plan de Contingencia y por qué es importante?
11. Nuestra empresa está a medias entre el rubro distribución y el de las finanzas. ¿Resulta estratégico tener aquí un Plan de Contingencia?
12. ¿Qué soluciones tenemos para que un banco no se vea afectado por un desastre y pueda seguir trabajando con sus clientes con un tiempo de recuperación bajo o mínimo? ¿Cómo sería su coste?
13. ¿Se pueden prever situaciones extremas como lo acontecido con las torres gemelas? ¿En que tipo de empresas o instituciones no deben descartarse estos extremos? ¿En una empresa que vende coches?