



## Monitorización de Alertas

Barcelona, 16 de febrero de 2006



18:30 – 21:30

2 sesiones con descanso

### Aspectos generales de la Auditoría de seguridad

- Introducción a la Auditoría Informática
- Metodología

→ **Enfoques CISA  
y COBIT**

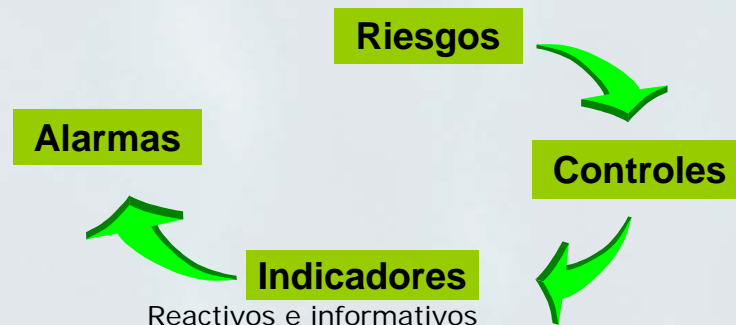
### Algunos trabajos

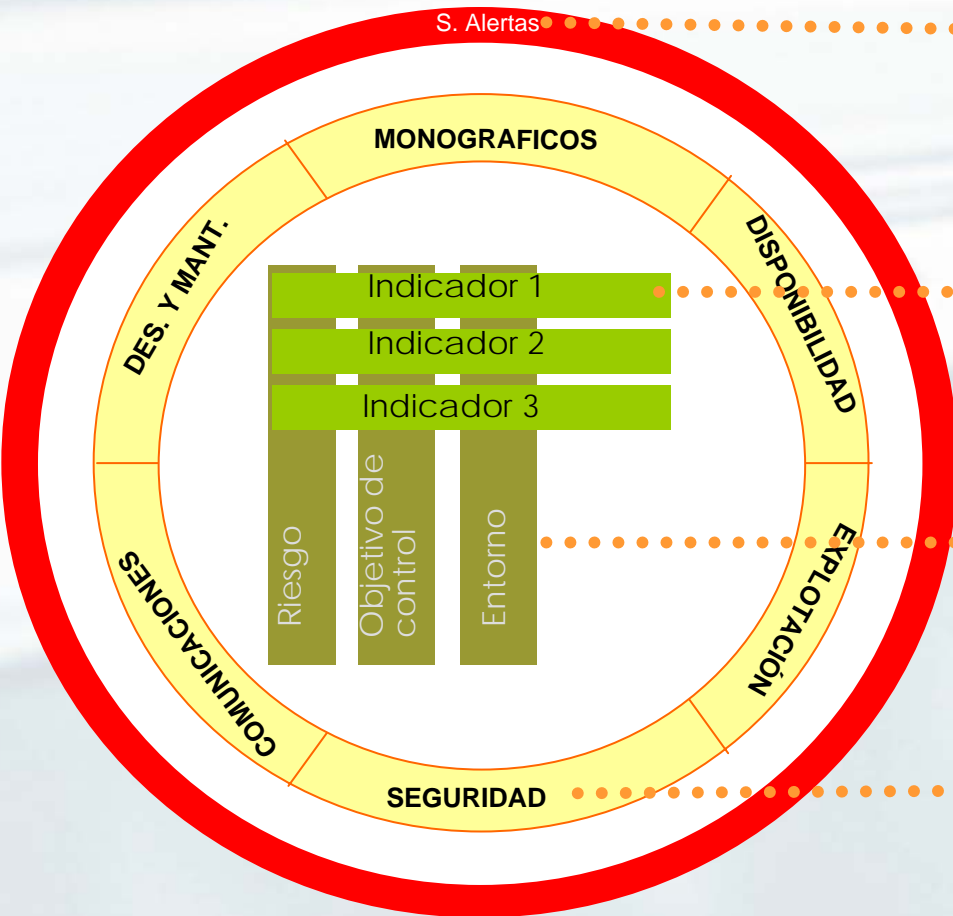
- Auditoría de Seguridad informática
  - Plataforma Internet
  - Seguridad física
  - Aplicaciones Web
- Auditoría de los requerimientos de seguridad estándares en el tratamiento de los PIN
- Auditoría del Reglamento de Medidas de Seguridad de la LOPD
- Sistema de alarmas automatizado

**Requerimientos  
y normativa  
externa**

# Monitorización de alertas

- Un sistema de alertas permite establecer controles automáticos sobre las áreas y procesos de mayor riesgo mediante:
  - Definición de indicadores → Cuadro de mandos para Auditoría informática.
  - Implantación de un sistema de Auditoría informática a distancia que:
    - Proporcione una ayuda a la identificación y priorización de las auditorías a realizar,
    - Permita incrementar el nivel de control de auditoría sobre las áreas técnicas
    - Ayude en la detección de posibles situaciones de riesgo y/o actuaciones de falta eficacia/eficiencia.





**Sistema de Alertas:** Sistema de alertas que permite establecer controles automáticos sobre las áreas y procesos de mayor riesgo.

**INDICADOR:** Métrica definida para dar una magnitud, cuantitativa o cualitativa, a un control.

**RIESGO:** El potencial de que una determinada amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos y causarle pérdidas o daños.

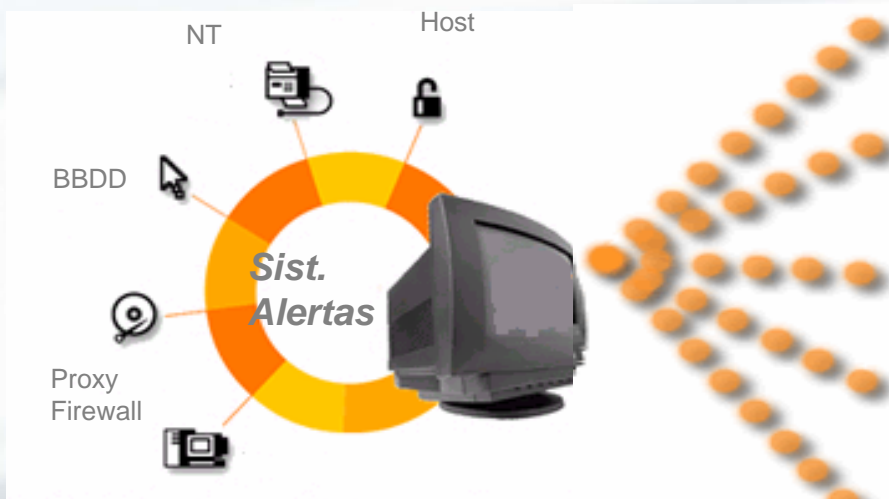
**OBJETIVO DE CONTROL:** Acción que se dispone para mitigar el riesgo

**ENTORNO:** Sistema informático sobre los que se aplican los indicadores para mantener un control ante el riesgo.

**ÁREA:** Área a la que se asocia la métrica.

*Permite incrementar el nivel de control de Seguridad sobre las distintas plataformas técnicas y Ayuda en la detección de posibles situaciones de riesgo y/o actuaciones de falta eficacia/eficiencia.*





## Eventos de varios entornos en una misma consola

### Riesgo

- Objetivo de control

### Acceso al sistema y recursos

- Autenticación
- Administración de autorizaciones
- Operatoria singular

### Cumplimiento de políticas

- Administración de autorizaciones
- Configuración de Sistemas
- Integridad
- Utilización de recursos
- Registros de auditoría
- Administración de usuarios

### Utilización de cajeros

- Control de manipulación

### Acceso desde el exterior

- Acceso al sistema

S  
E  
G  
U  
R  
I  
D  
A  
D

### Rigor en la información de control

- Cumplimentación adecuada de la información de control

### Mantenimiento del software en producción

- Estabilidad de las aplicaciones
- Resolución de incidencias

### Cumplimiento de las previsiones

- Cumplimiento de las estimaciones
- Cumplimiento de los acuerdos contractuales
- Tipología de las peticiones

### Adaptación del desarrollo a las necesidades del usuario

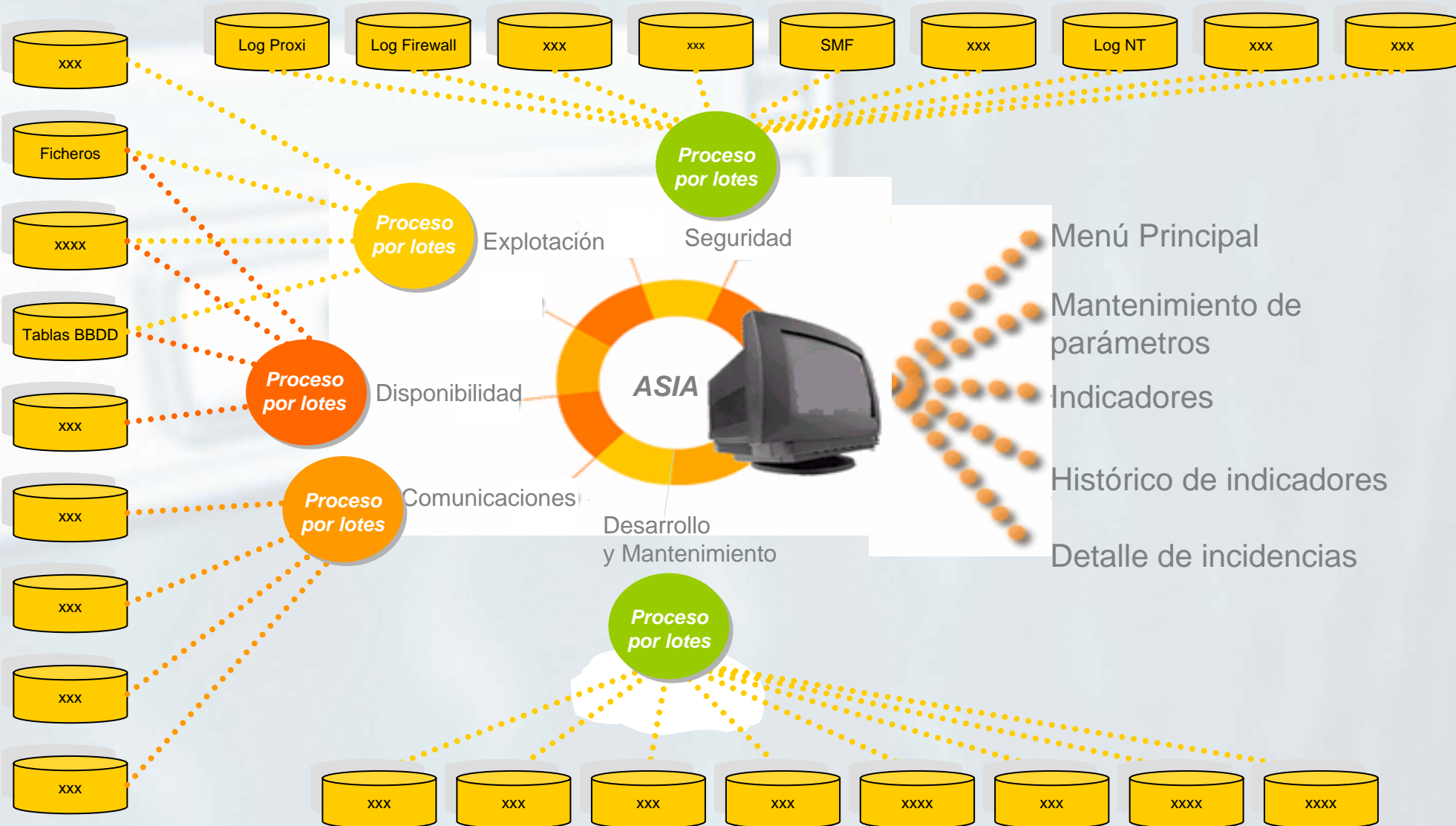
- Correspondencia entre el desarrollo y las necesidades del usuario

### Estancamiento de las peticiones

- Permanencia de las peticiones en las etapas del ciclo de vida

D  
E  
S  
A  
R  
R  
O  
L  
L  
O

| RIESGO  | OBJETIVO DE CONTROL                     |             | INDICADOR   | ENTORNO |   |   |   |   |   |
|---|---|-------------|---|---------|---|---|---|---|---|
|   |   |             |   |         |   |   |   |   |   |
| Acceso al sistema y a recursos                                  | <b>Autenticación</b>                    |             |   |         |   |   |   |   |   |
|   | SEG1                                    | Reactivo    | Intento de suplantación de usuarios específicos   | X       | X |   |   | X |   |
|   | SEG2                                    | Reactivo    | Intentos reiterados de acceso al sistema por usuarios inexistentes desde un mismo terminal. | X       | X |   |   | X |   |
|   | SEG3                                    | Reactivo    | Intentos de acceso a recursos críticos no autorizados .(L. Notes - todos)                   | X       |   |   |   |   | X |
|   | <b>Administración de Autorizaciones</b> |             |   |         |   |   |   |   |   |
|   | SEG4                                    | Reactivo    | Usuarios con fecha de alta y baja en el mismo día y que hayan accedido.                     | X       | X |   |   | X |   |
|   | <b>Operatoria singular</b>              |             |   |         |   |   |   |   |   |
| Cumplimiento de políticas, normas y procedimientos de seguridad | SEG5                                    | Reactivo    | Actividad fuera de horario habitual.  | X       | X |   |   |   |   |
|   | SEG6                                    | Reactivo    | Operatoria simultanea desde distintos centros.  | X       |   |   |   |   |   |
|   | SEG7                                    | Reactivo    | Copia de recursos críticos / File Transfer  | X       |   |   |   |   |   |
|   | <b>Administración de Autorizaciones</b> |             |   |         |   |   |   |   |   |
|   | SEG8                                    | Reactivo    | Cambios en las protecciones sobre ficheros, transacciones y colas TS                        | X       |   |   |   | X |   |
|   | SEG9                                    | Reactivo    | Usuarios desvinculados no dados de baja en el sistema                                       | X       | X |   |   | X |   |
|   | <b>Configuración de Sistemas</b>        |             |   |         |   |   |   |   |   |
|   | SEG10                                   | Reactivo    | Modificación de parámetros de seguridad del sistema y ejecución de comandos críticos        | X       | X | X |   | X |   |
|   | <b>Integridad</b>                       |             |   |         |   |   |   |   |   |
|   | SEG11                                   | Reactivo    | Edición directa de ficheros con datos reales por un usuario no Batch                        | X       |   |   |   |   |   |
|   | SEG12                                   | Reactivo    | Usuarios con autorización de acceso a datos reales a través de TSO                          | X       |   |   |   |   |   |
|   | <b>Utilización de recursos</b>          |             |   |         |   |   |   |   |   |
|   | SEG13                                   | Reactivo    | Virus detectados en un terminal de manera reiterada   |         | X |   |   |   |   |
|   | SEG14                                   | Reactivo    | Navegación internet por usuarios no autorizados   |         |   |   | X |   |   |
|   | SEG15                                   | Reactivo    | Nº de usuarios que reciben mas de n correos diarios   |         |   |   |   |   | X |
|   | SEG16                                   | Informativo | Páginas Web mas visitadas   |         |   |   | X |   |   |
|   | <b>Registros de Auditoría</b>           |             |   |         |   |   |   |   |   |
|   | SEG17                                   | Reactivo    | Edición directa o borrado del log   | X       |   |   |   | X | X |
|   | <b>Administración de usuarios</b>       |             |   |         |   |   |   |   |   |
|   | SEG18                                   | Reactivo    | Usuarios no identificados   | X       | X |   |   |   |   |
| Utilización de cajeros  | <b>Control de manipulación</b>          |             |   |         |   |   |   |   |   |
|   | SEG19                                   | Reactivo    | Operatoria reiterada en off-line en cajeros por parte de una misma persona                  | X       |   |   |   |   |   |
| Acceso desde el exterior  | <b>Acceso al sistema</b>                |             |   |         |   |   |   |   |   |
|   | SEG20                                   | Reactivo    | Intentos de acceso reiterados al sistema desde internet                                     |         |   | X |   |   |   |
|   | SEG21                                   | Reactivo    | Intentos de acceso al sistema. Escaneo de puertos   |         |   | X |   |   |   |
|   | SEG22                                   | Reactivo    | Intentos de acceso al sistema. Suplantación del Firewall                                    |         |   | X |   |   |   |





- Prueba realizada para el indicador **“Intentos de acceso al sistema. Escaneo de puertos”**

| IP-Origen        | Puertos Accedidos |
|------------------|-------------------|
| xxx.xxxx.xxxx.xx | 23                |
| xxx.xxxx.xxxx.xx | 403               |
| xxx.xxxx.xxxx.xx | 14                |
| xxx.xxxx.xxxx.xx | 19                |
| xxx.xxxx.xxxx.xx | 52                |
| xxx.xxxx.xxxx.xx | 38                |
| xxx.xxxx.xxxx.xx | 11                |
| xxx.xxxx.xxxx.xx | 17                |
| xxx.xxxx.xxxx.xx | 18                |
| .....            |                   |

### Detalle:

- IP origen
- Puerto destino
- Total puertos accedidos



|   |   |
|---|---|
| Numero de direcciones externas que superan el umbral del número de puertos escaneados (100) | 1 |
|---|---|

- (1) Se seleccionan los accesos al firewall desde el exterior (campo Orig=fw2-hme02) ,
- (2) Todos aquellos que accedan a mas de SEG21IX puertos distintos o que intenten acceder SEG21IX veces al mismo puerto se consideran seleccionados.
- (3) Contamos el numero de IP seleccionadas y en el caso de que sean SEG21IY o mas se enciende el semaforo rojo.