

TIC en la Gestión de Emergencias

Xavier Serrano Cossío
Director de Seguridad de la Información
y Continuidad Operativa Grupo Banc Sabadell



Madrid, 22 de febrero de 2011

-
1. Introducción

 2. Contexto Actual. Algunos ejemplos

 3. La identificación de los Procesos Críticos

 4. Metodología general y cálculo de Riesgo Operacional

 5. Monitorización, Respuesta y Coordinación con otras áreas

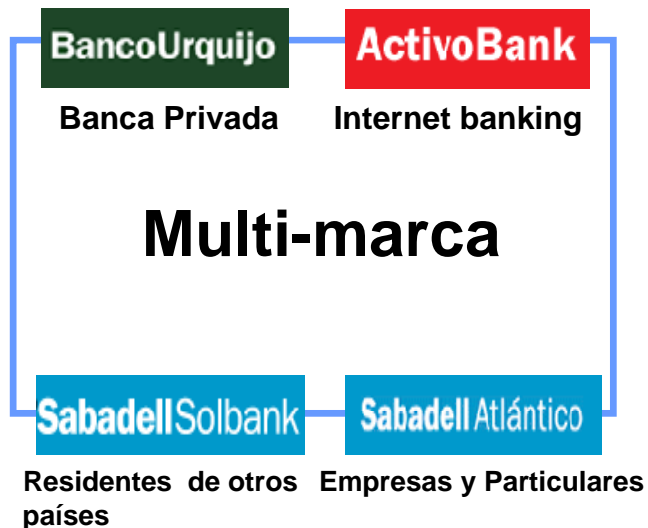
1.- Introducción: Grupo BancSabadell

- 4o. grupo bancario por tamaño en España (en el IBEX-35 desde 2004)
- 2a. Institución Banca Privada en España
- 1.467 oficinas, 10.777 empleados



• 19 países

Oficinas

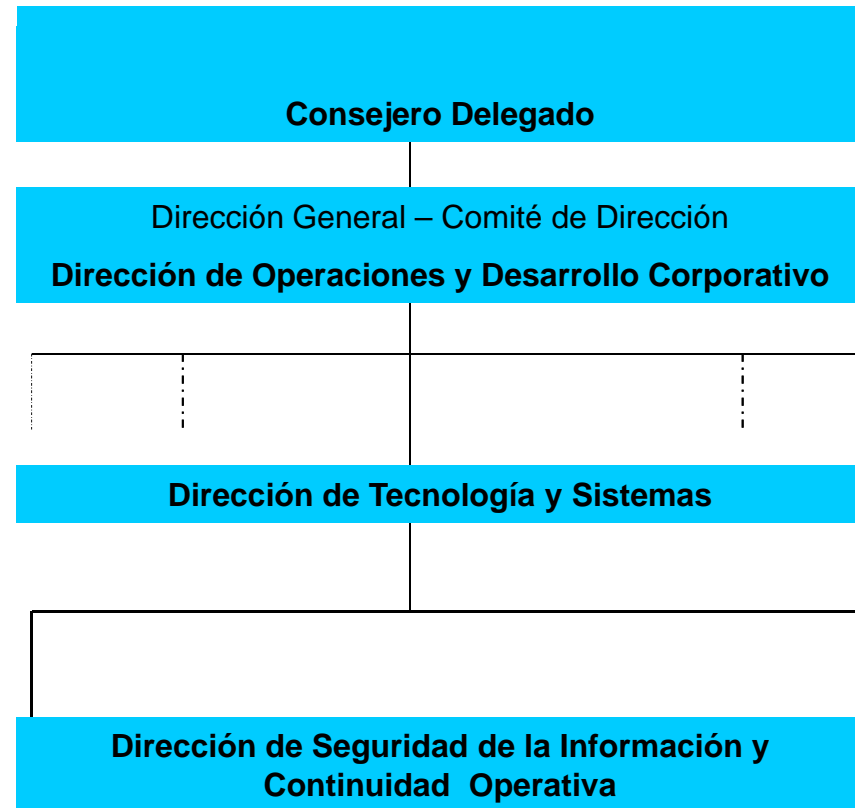


1.- Introducción: Grupo BancSabadell

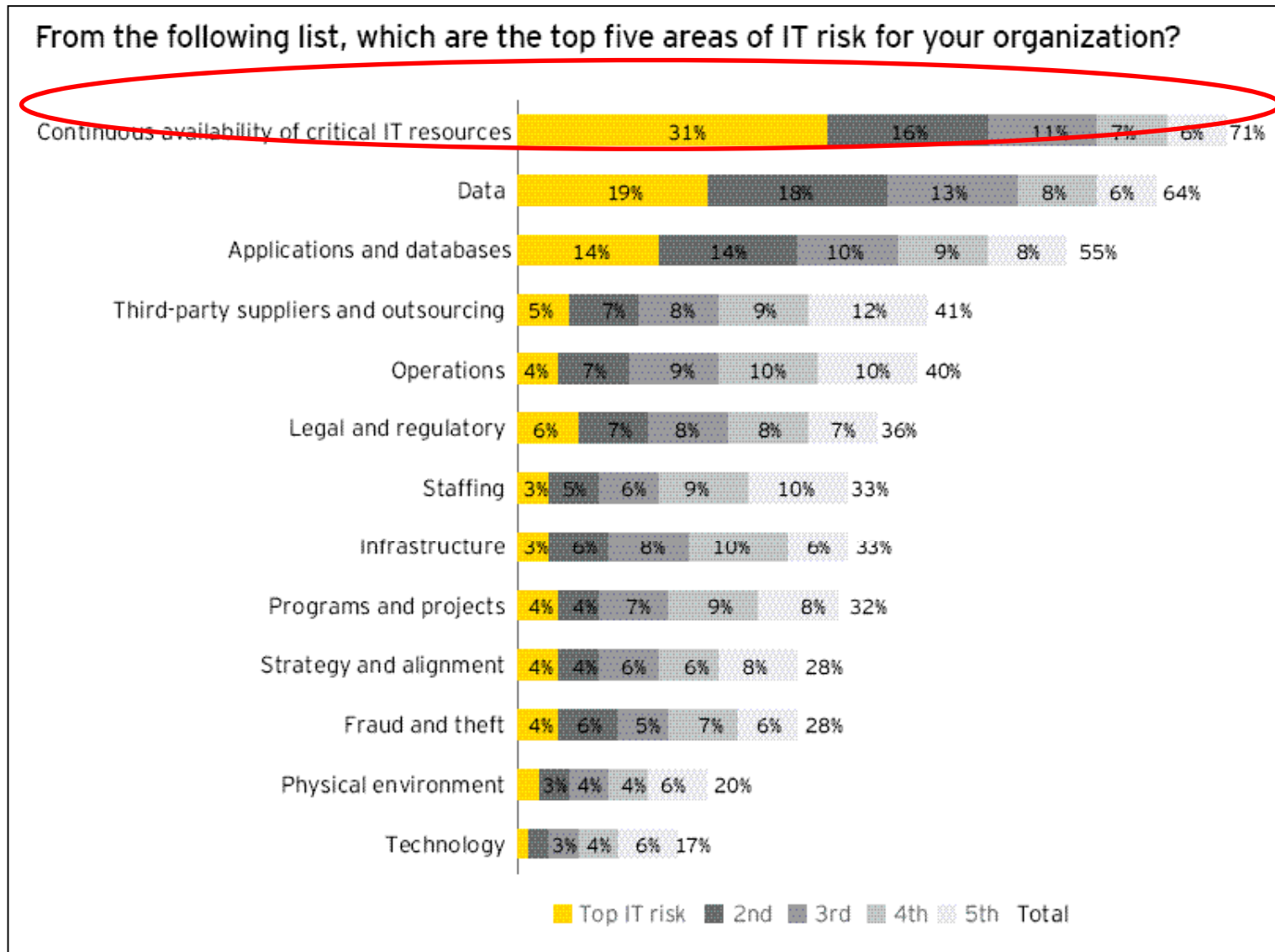
Relevancia del área en el plan
estratégico y operativo de la
empresa



Emplazamiento dentro del
Comité de Dirección

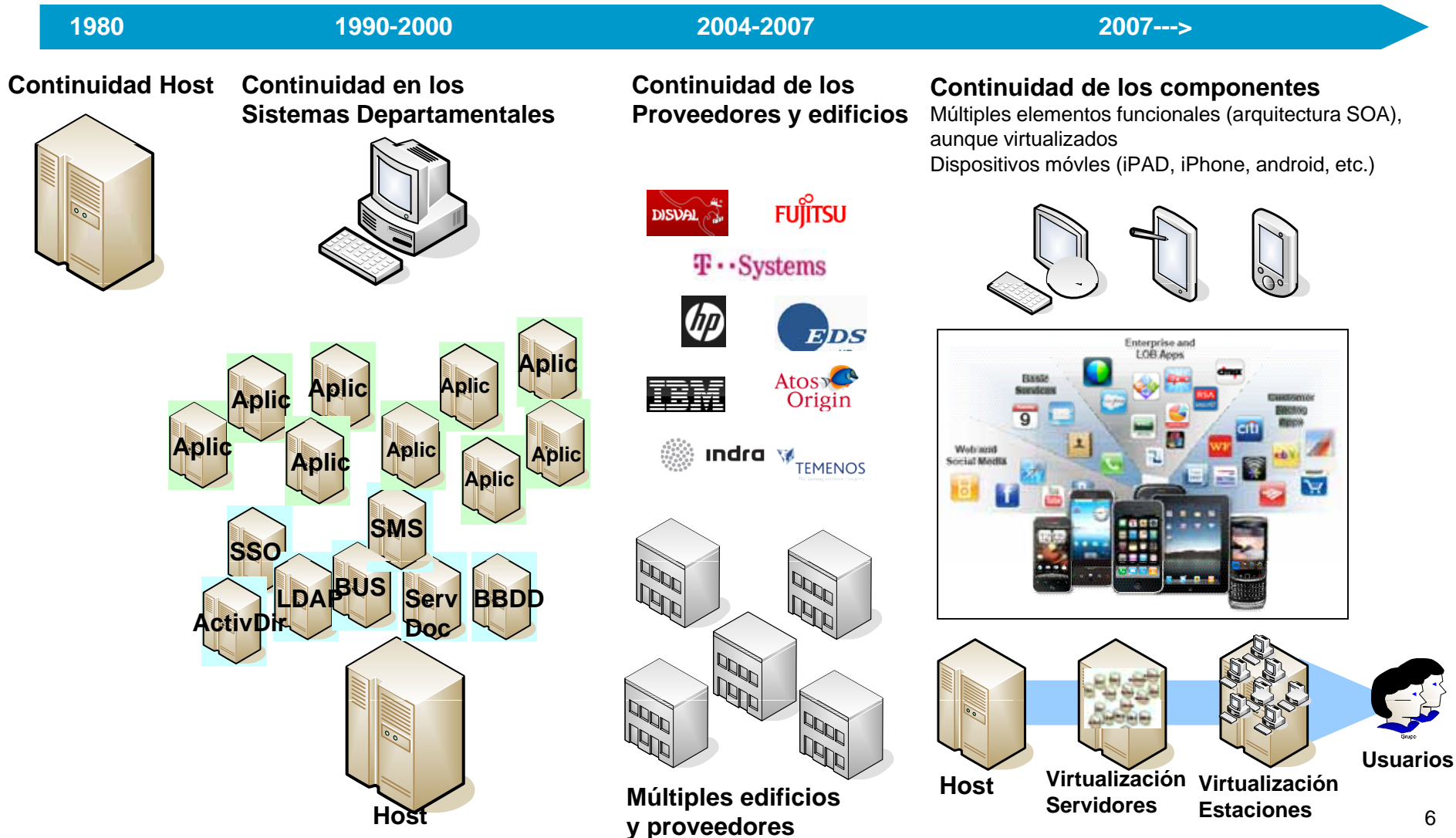


2.- Contexto actual. Algunos ejemplos



2.- Contexto actual. Algunos ejemplos

Evolución: de la Continuidad del Host a la Continuidad de los componentes



2.- Contexto actual. Algunos ejemplos

CAUSAS INTERNAS:

15 September, 2010 - 11:21

Chase Web crash locks out 16.5 million online customers

Chase CEO Jamie Dimon issued a public apology to the bank's 16.5 million online banking customers after a computer glitch knocked out the site for more than a day.

4943 views 0 comments

The Chase Website went down late Monday evening, forcing the bank to put up a holding page indicating that the downtime was due to "scheduled maintenance".

Oddly, the bank hadn't forewarned customers of any maintenance issues and by Tuesday morning had replaced the message with a simple notice saying merely that the site was "temporarily unavailable".

In the afternoon, Chase CEO Jamie Dimon apologised to customers for the outage at a banking conference in New York.

The lights eventually came back on on Tuesday evening, although the bank has yet to provide an explanation for the source of the problems, leading to rampant speculation on online message boards and Twitter.

Chase is the latest top tier bank to have problems with its online outlet following in the wake of DBS Bank of Singapore and Barclays which have both experienced extended downtime in recent weeks.

Update The Chase Website crashed again Wednesday afternoon before power was restored later that evening. Bank spokesman Thomas Kelly told the New York Times that the fault was caused by third-party database software that corrupted information in its systems and prevented users from logging on.

Network failure halts London Stock Exchange trading

Exchange hit with connectivity issue on potentially one of its busiest trading days



by Mike Simons Comments Recommended Share

September 8, 2008 (Computerworld UK) LONDON – The London Stock Exchange suffered a breakdown today on what looked set to be one of the busiest trading days of the year.

The exchange suspended trading as dealers reacted to the dramatic economic news that the U.S. government had taken over control of mortgage groups **Freddie Mac** and **Fannie Mae**, in the biggest financial bailout in world history.

Trading was halted at 8:45 a.m. London time. According to **Reuters**, it was not restored until shortly before close of the trading day, which is 4 p.m.

The LSE said the system had been hit by a "connectivity issue" and

14 July, 2010 - 11:10

IBM employee fingered as culprit in massive DBS outage

An IBM employee has been fingered as the culprit behind a seven-hour system-wide outage that knocked out all consumer and business banking services and ATM and POS transactions at Singapore's DBS Bank on Monday.

8464 views 4 comments

In a letter posted on the bank's Website, DBS Ceo Piyush Gupta, says the outage was triggered during a routine repair job on a component within the disk storage subsystem connected to the bank's mainframe.

"So far, we understand from IBM that an outdated procedure was used to carry out the repair," says Gupta. "In short, a procedural error in what was to have been a routine maintenance operation subsequently caused a complete system outage."

IBM and BDS entered into a \$5.1.2bn agreement in 2002 in which the bank outsourced IT services and infrastructure in Singapore and Hong Kong to IBM.

Gupta says that all payments and transactions that were scheduled to be made on 5 July were completed. "Nothing was held over and full data integrity was maintained at all times," he says.

He continues: "I am treating this matter with utmost priority and the full scale investigation that we initiated last week is still underway. This investigation is being done with the support of IBM's labs in the US and their engineering teams in Asia.

In a statement, IBM says it has taken steps "to enhance training of our personnel related to current procedures and brought in experts from our global team to provide further assistance."

In addition, IBM and DBS are taking "additional actions to increase the resiliency and redundancy of this part of DBS' infrastructure."

2.- Contexto actual. Algunos ejemplos

CAUSAS EXTERNAS:

Washington Post: Bank of America ATM's affected by Internet Virus

Tags » [ATM](#), [Bank of America](#) »

0 [tweet](#)

[f](#) Me gusta

Reuters reports that Bank of America's ATM network was affected Saturday by a malicious Internet worm that affected Internet traffic worldwide.

“ Bank of America spokeswoman Lisa Gagnon said by phone from the company's headquarters in Charlotte, North Carolina, that many, if not a majority of the No. 3 U.S. bank's ATMs were back online and that their automated banking network would recover by late Saturday.

Why? I'll bet that a number of folks will want to understand how such an Internet outage could have affected the largest ATM network in the US.

Posted: [Jan 26, 2003 07:37 AM Pacific](#) | [Permalink](#) | [Share This](#) | [Tweet This](#)

Extortion via DDoS on the rise

Money extraction - not fun - is the new motivation for DDoS attacks.

By Denise Pappalardo and Ellen Messmer, Network World | [Network World US](#)

Published: 11:00 GMT, 17 May 05



Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.

Those targeted are increasingly deciding to pay the extortionists rather than accept the consequences, experts say. While reports of this type of crime have circulated for several years, most victimized companies remain reluctant to acknowledge the attacks or enlist the help of law enforcement, resulting in limited awareness of the problem and few prosecutions.

Extortion is "becoming more commonplace," says Ed Amoroso, chief information security officer at AT&T. "It's happening enough that it doesn't even raise an eyebrow anymore."

"In the past eight months we have seen an uptick with the most organized groups of attackers trying to extort money from users," says Rob Rigby, director of managed security services at MCI. "We try to do our best to get (customers) through it, but we leave it up to them to bring such attacks to the attention of law enforcement."

While MCI has been asked to help with prosecutions in other cybercrime cases, Rigby says he does not recall a service provider being subpoenaed in a distributed DoS extortion case.

Quantifying the extortion problem is difficult because the FBI, ISPs and third-party research firms can't provide figures on the number of distributed DoS attacks that include demands for money. The FBI aggressively works daily on cases involving distributed DoS attacks and extortion, says bureau spokesman Paul Bresson.

"Almost all of them have an international connection," he says. "There aren't many cases where people doing this are from the U.S., and many times it is a juvenile subject to the laws of another country."

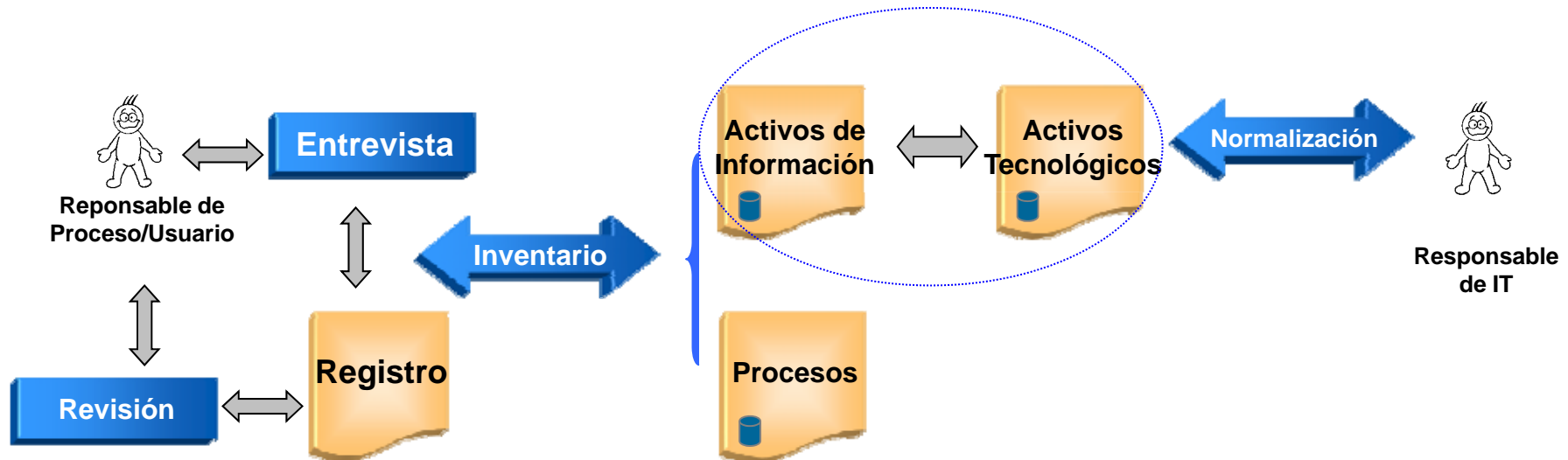
3.- La identificación de los Procesos Críticos

- En **2005** se dio un **nuevo impulso** a la **prevención y gestión** de emergencias, con la creación de la **Unidad de Continuidad Operativa** y realización de un **nuevo Plan**
- **Objetivo: garantizar el correcto funcionamiento de todos los procesos críticos del Grupo** ante cualquier tipo de **eventualidad** que pudiera producirse
- Un **proceso crítico** es aquel que **no puede dejar de funcionar durante un corto intervalo de tiempo** (unos pocos **minutos u horas**) sin que ello implique un **muy elevado impacto** en el Grupo. El impacto puede ser **económico, reputacional, legal**, etc

De los todos los procesos diferentes identificados en el Grupo, **352 procesos están catalogados como críticos** por sus propietarios

3.- La identificación de los Procesos Críticos

- Actividades para la **identificación** de los **Procesos Críticos** y sus recursos asociados. **BIA** (Business Impact Analysis)

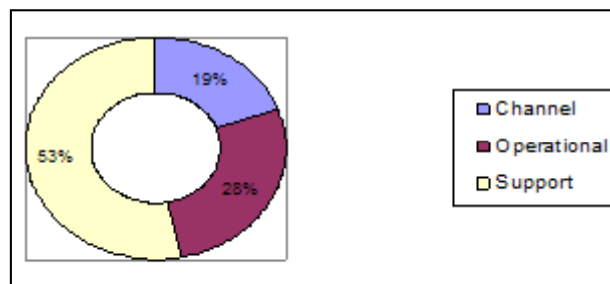


- El **Responsable de Proceso** marca sus procesos críticos dentro de la **aplicación de mapa de procesos** del Grupo
- Dicha aplicación se integra con la **aplicación** para la **gestión** del Plan de Continuidad (gestiona **procesos críticos**, **recursos** asociados y **planes**)

3.- La identificación de los Procesos Críticos

→ Ejemplos de Unidades con procesos críticos declarados:

| Ámbito | Unidad |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------|
| Operaciones | • Administración Centralizada |
| Mercados Financieros | • Tesorería y Mercado de Capitales |
| Canales | • Servicios Operativos y Canales • Oficinas |
| Tecnología | • Producción |
| Servicios | • Logística |
| Gestión de Fondos y Valores | • Inversiones de Gestión de Activos • Control, Procesos y Servicios de Gestión de Activos • Dirección de Soporte |



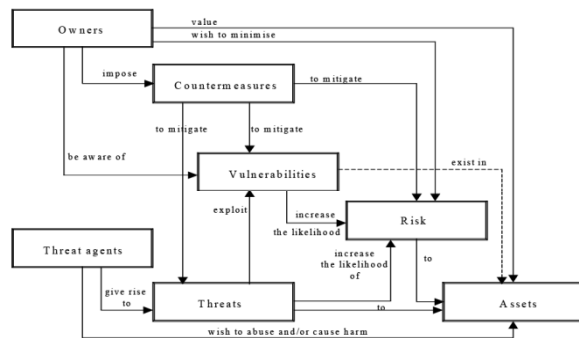
Canales: Procesos de negocio que interactúan directamente con Clientes. (Ej.: Oficinas, Contact Center, Internet, Cajeros aut.)

Operacional: Procesos de negocio que interactúan directamente con procesos de canales (Ej.: Gestión de Inversiones, Comercio Exterior).

Soporte: (Ej.: RRHH, Admin. Centralizada, Compras)

4.- Metodología general y cálculo de Riesgo Operacional

→ Se entiende por **Continuidad Operativa** el conjunto de **metodologías y tecnologías** que **identifican la exposición** de la organización a los riesgos sobre la continuidad de los **procesos críticos**, y **determinan los recursos imprescindibles** para proporcionar una **prevención y recuperación** eficaz



ISO 15408 (Common Criteria)

Análisis tradicional de riesgos

- Pérdida parcial/completa de un **edificio** (o la posibilidad de acceder al mismo), por incendio, inundación, fallo eléctrico, accidente químico o físico externo, cierre vías de acceso, huelgas, amenaza de bomba, etc

- Fallos en la **tecnología**

- Fallos en operadores de **telecomunicaciones** y en **servicios globales**: Internet, GPS, etc

- Fallos de larga duración en servicios "**utilities**": electricidad, agua, gas

- Pérdidas de **personal**, incluso en periodos cortos o medios: pérdida de personas críticas o de gran número de personas no críticas, como consecuencia de **accidente, epidemia**, etc.

- **Vandalismo** o terrorismo

- Y en general, cualquier **riesgo** que afecte a los **activos imprescindibles** para el funcionamiento de los procesos críticos, ya sean estos activos edificios, tecnología, servicios externos o personas

Riesgos específicos de Continuidad

4.- Metodología general y cálculo de Riesgo Operacional

→ Son muchas las áreas y **departamentos que participan** en la prevención y actuación ante emergencias

| Participante | Responsabilidades |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Propietario del proceso crítico | <ul style="list-style-type: none"> • Identifica su proceso como crítico, define los parámetros de tiempo máximo admisible de recuperación (RTO) y pérdida máxima de información admisible (RPO) en contingencia. • Redacta y prueba los procedimientos de gestión de la contingencia para el caso en que la Tecnología y otros recursos no estén disponibles |
| Responsables de Tecnología | <ul style="list-style-type: none"> • Encargados de los sistemas, aplicaciones y comunicaciones redundantes que dan servicio a los procesos críticos • Diseñan e implantan mecanismos que soporten múltiples fallos, prueban y ponen en marcha los sistemas de contingencia |
| Comunicación Interna y Externa | <ul style="list-style-type: none"> • Coordinación del flujo de información interna y externa |
| Seguridad Corporativa | <ul style="list-style-type: none"> • Identifica a tiempo amenazas externas relacionadas con la seguridad y dota de protección extraordinaria para los recursos y personas en caso de contingencia |
| Gestión de espacios y edificios | <ul style="list-style-type: none"> • Proporcionan espacios alternativos para la ejecución de los procesos críticos según necesidad |
| Logística, Organización, RRHH, etc. | <ul style="list-style-type: none"> • Dependiendo del tipo de riesgos y situaciones, son muchas otras áreas las que pueden participar |
| Oficina de Control y Monitorización (OCM) | <ul style="list-style-type: none"> • Identifica o recibe notificación de contingencia, comunica de forma simultánea y activa mecanismos de contingencia |

4.- Metodología general y cálculo de Riesgo Operacional

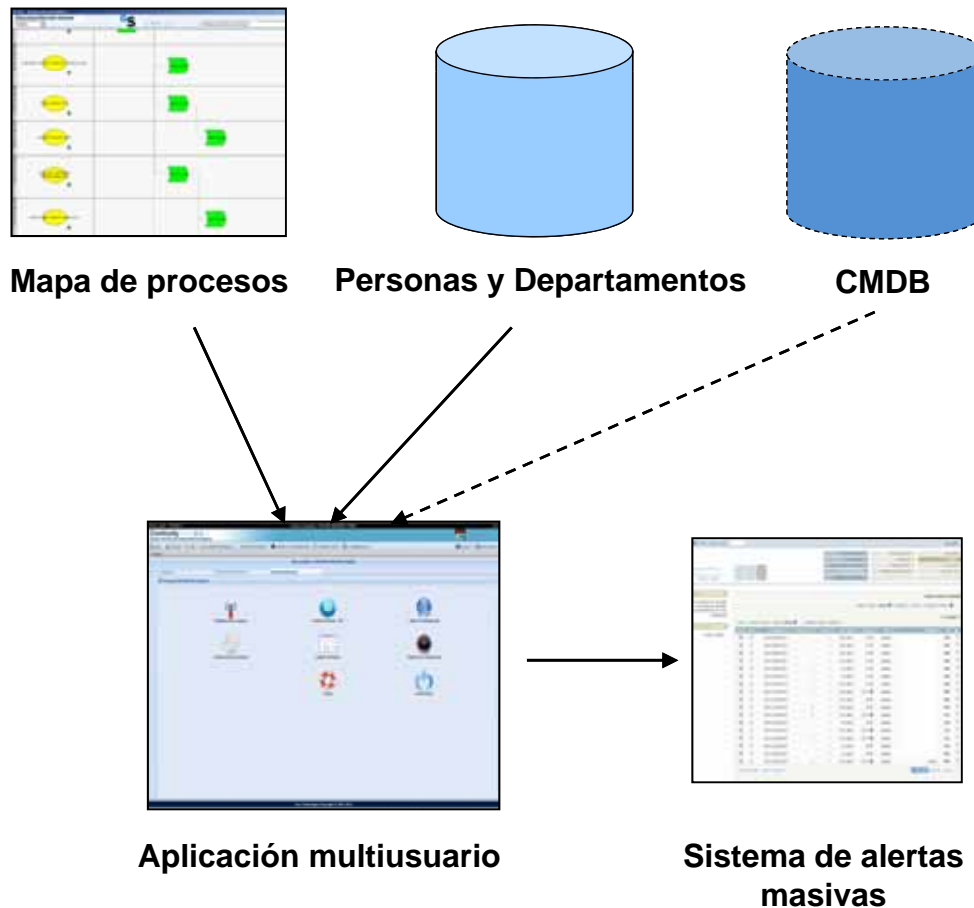
- Ciclo de **Revisión y Mejora**: Se destaca el hecho que la Continuidad Operativa **no es un proyecto que se realiza en una ocasión** sino que, muy al contrario, es un **proceso continuado** que obliga al **mantenimiento, pruebas y mejora continuada**



- **Mantenimiento** continuado de **procesos, recursos, propietarios y planes**
- **Importancia fundamental** de la realización de las **pruebas y entrenamientos periódicos**
- Dado que los **riesgos** asociados con la continuidad operativa únicamente se **materializan** en **contadas ocasiones**, es **importantísimo** realizar **pruebas y entrenamientos periódicos** para **garantizar** que los mecanismos establecidos funcionarán perfectamente cuando sean necesarios

4.- Metodología general y cálculo de Riesgo Operacional

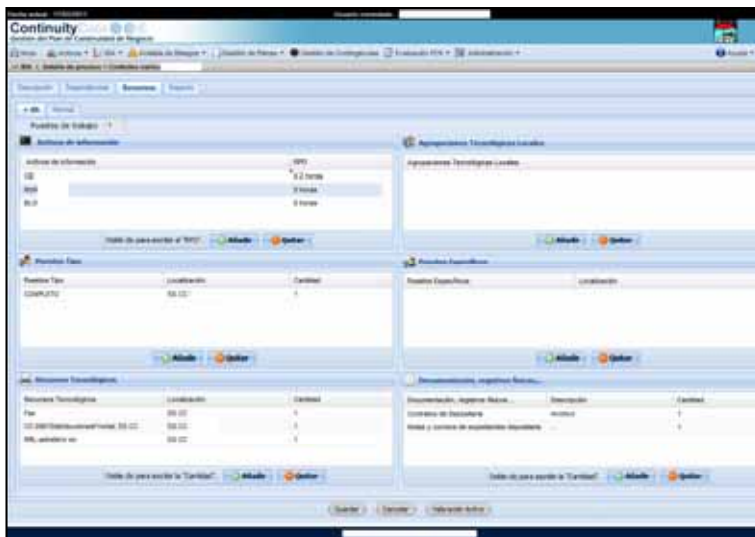
→ **Aplicación** para la gestión:



- La aplicación se nutre de los **movimientos** realizados en el mapa de **procesos** corporativo y en los datos de **personas** y **departamentos**
- Está previsto que se nutra también de la nueva **CMDB** (Configuration Management DataBase), que se está desplegando
- Reflejo en el **sistema de alertas**

4.- Metodología general y cálculo de Riesgo Operacional

→ Aplicación para la gestión:



Datos reales con información confidencial eliminada

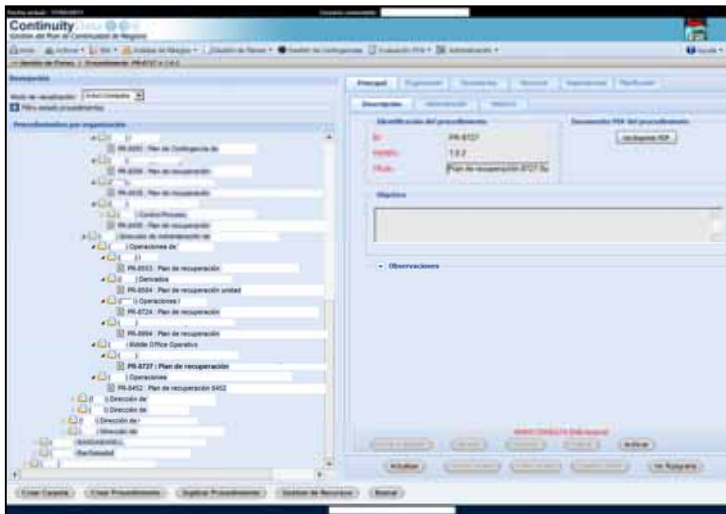
→ Para cada **proceso crítico**, se relacionan sus **recursos**, su **RTO** (Recovery Time Objetivo) y su **RPO** (Recovery Point Objetivo)

→ Como **recursos** aparecen:

- Aplicaciones,
- Puestos de trabajo,
- Recursos tecnológicos,
- Documentación y
- Otros registros físicos

4.- Metodología general y cálculo de Riesgo Operacional

→ Aplicación para la gestión:

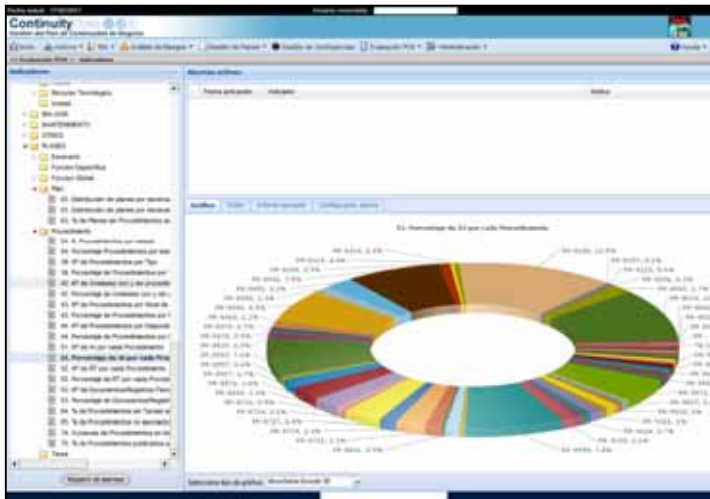


Datos reales con información confidencial eliminada

- Relación de **planes** de contingencia **específicos** de cada **departamento** con procesos críticos
- Se gestionan las diferentes **versiones** e **históricos** de los **planes**

4.- Metodología general y cálculo de Riesgo Operacional

→ Aplicación para la gestión:



Datos reales con información confidencial eliminada

- Módulo de **informes, indicadores y gráficos avanzados**
- **Informes predefinidos y a medida** para poder realizar toda clase de consultas
- Forma de ver rápidamente **qué recursos afectan a más procesos críticos**, **qué procesos y recursos están afectados** ante la contingencia **en un edificio**, **cuántos puestos de trabajo se necesitan reubicar** en caso de incidente, etc.

4.- Metodología general y cálculo de Riesgo Operacional

- Desde 2007, los riesgos de Continuidad Operativa se cuantifican de igual forma que el **Riesgo Operacional**
- **Lenguaje común**, todo el mundo entiende la necesidad de **cuantificar** económicamente y asignarle una **probabilidad** a los riesgos
- A partir de la cuantificación de todos los riesgos, Basilea II obliga a los Bancos a realizar **mayores o menores provisiones económicas**
- **Riesgo Operacional**: El riesgo de pérdida resultante de procesos internos inadecuados y/o erróneos, personas, sistemas o sucesos externos



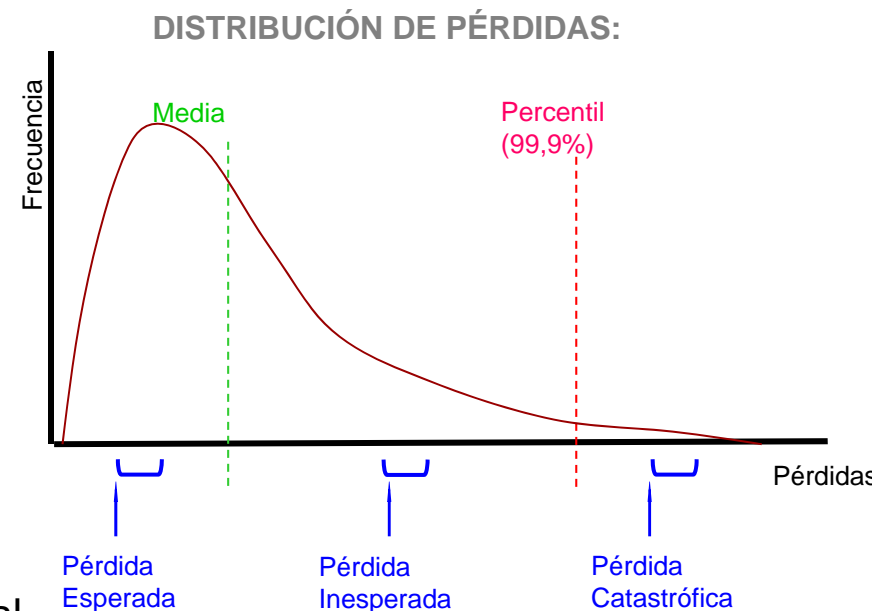
4.- Metodología general y cálculo de Riesgo Operacional

- **Una vez al año**, todos los responsables de Unidad deben **reevaluar** el valor de las variables significativas para **recalcular** los resultados del cálculo del riesgo operacional de **todos sus procesos con riesgo significativo**
- Dentro del modelo de **objetivos personales**, los responsables de los procesos tienen como objetivo la gestión (**minimización**) y **control** del riesgo operacional
- La **justificación** de un **proyecto** se compara con la reducción del **valor del riesgo operacional que implica**.
- La **metodología** se basa en un **modelo estadístico**, **comparando los resultados estimados con los resultados reales de pérdida**, cuando existe materialización de los riesgos en periodos anteriores

4.- Metodología general y cálculo de Riesgo Operacional

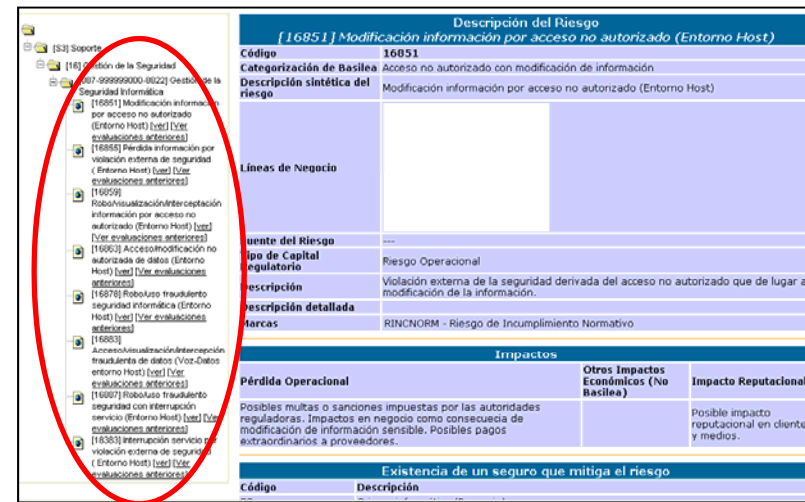
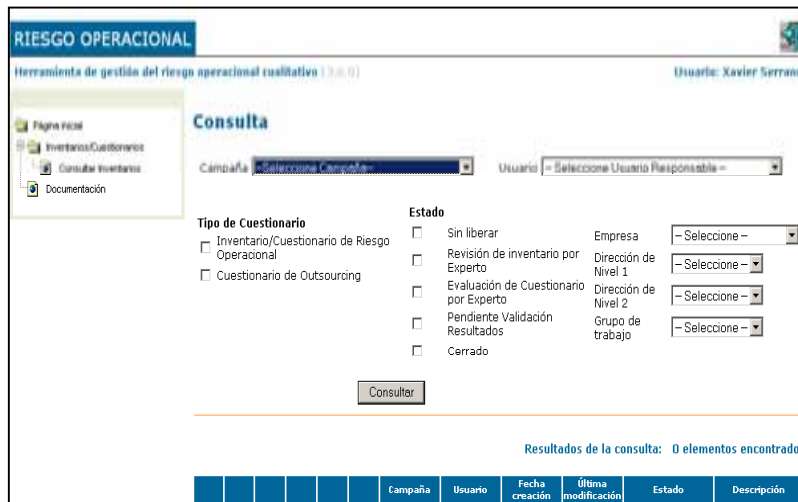
CONCEPTOS

- **Pérdidas Esperadas:** Coste del negocio, reflejan lo que se espera perder de media (valor medio de las pérdidas)
- **Pérdidas Inesperadas:** Medida de riesgo (volatilidad de pérdidas), que surge a consecuencia de que las pérdidas reales pueden ser superiores a las esperadas
- **Pérdidas Catastróficas:** Las que se incurren en situación de stress y de grandes pérdidas (situaciones de crisis)
- **Valor en Riesgo:** (VaR) Máxima pérdida potencial por este riesgo operacional en un año. Muestra la agregación de pérdidas esperadas e inesperadas, calculada con un intervalo de confianza del 99,9% en un horizonte de un año.



4.- Metodología general y cálculo de Riesgo Operacional

HERRAMIENTAS



- ➔ Aplicación **multiusuario**, conectada con el mapa de **procesos**
- ➔ Para cada proceso, se debe gestionar **vulnerabilidades** y **cuantificar** potenciales **impactos**
- ➔ Se debe indicar: **frecuencia** de la **amenaza**, del **impacto**, impacto **económico medio**, **peor escenario** sobre riesgo residual y calificar **cualitativamente** el impacto **reputacional**

- ➔ Se deben especificar todos los **controles** mitigantes **aplicados**, indicando **periodicidad** de aplicación, **justificación**, **efectividad** y **efectividad conjunta** de todos los controles
- ➔ Como **resultado** se obtiene: valor económico de **pérdida esperada**, **VaR** y **multiplicador**
- ➔ Existen **herramientas complementarias**

5.- Monitorización, Respuesta y Coordinación con otras áreas

→ **Monitorización** e Identificación de una Incidencia o Emergencia: **la OCM**

Misión: *Garantizar un nivel de servicio optimo de los sistemas y de los proveedores tecnológicos*

→ **Monitorización** (24 x 7)

- Plataformas tecnológicos (HW, Comunicaciones,...)
- Servicios (Teleproceso, Cajeros, Internet, Swift,...)
- Procesos (On-line, Batch)

→ **Coordinación y comunicación**

- Alerta a proveedores y equipos técnicos de situaciones de posible impacto en el nivel de servicio
- Comunicación a usuarios de impactos en el nivel de servicio
- Coordinación, con la Unidad de Continuidad Operativa, de situaciones de contingencia

→ **Control SLA's** proveedores y equipos internos

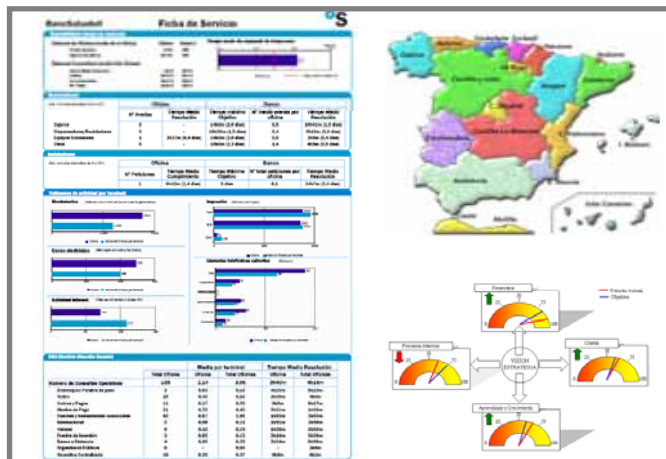
- Cumplimiento objetivos para la retribución

5.- Monitorización, Respuesta y Coordinación con otras áreas

“COCKPIT”



Ficha de Servicio On-line



OCM (Oficina Control y Monitorización)

- “Ready for Business”
- Nivel de Servicio
- Continuidad Operativa

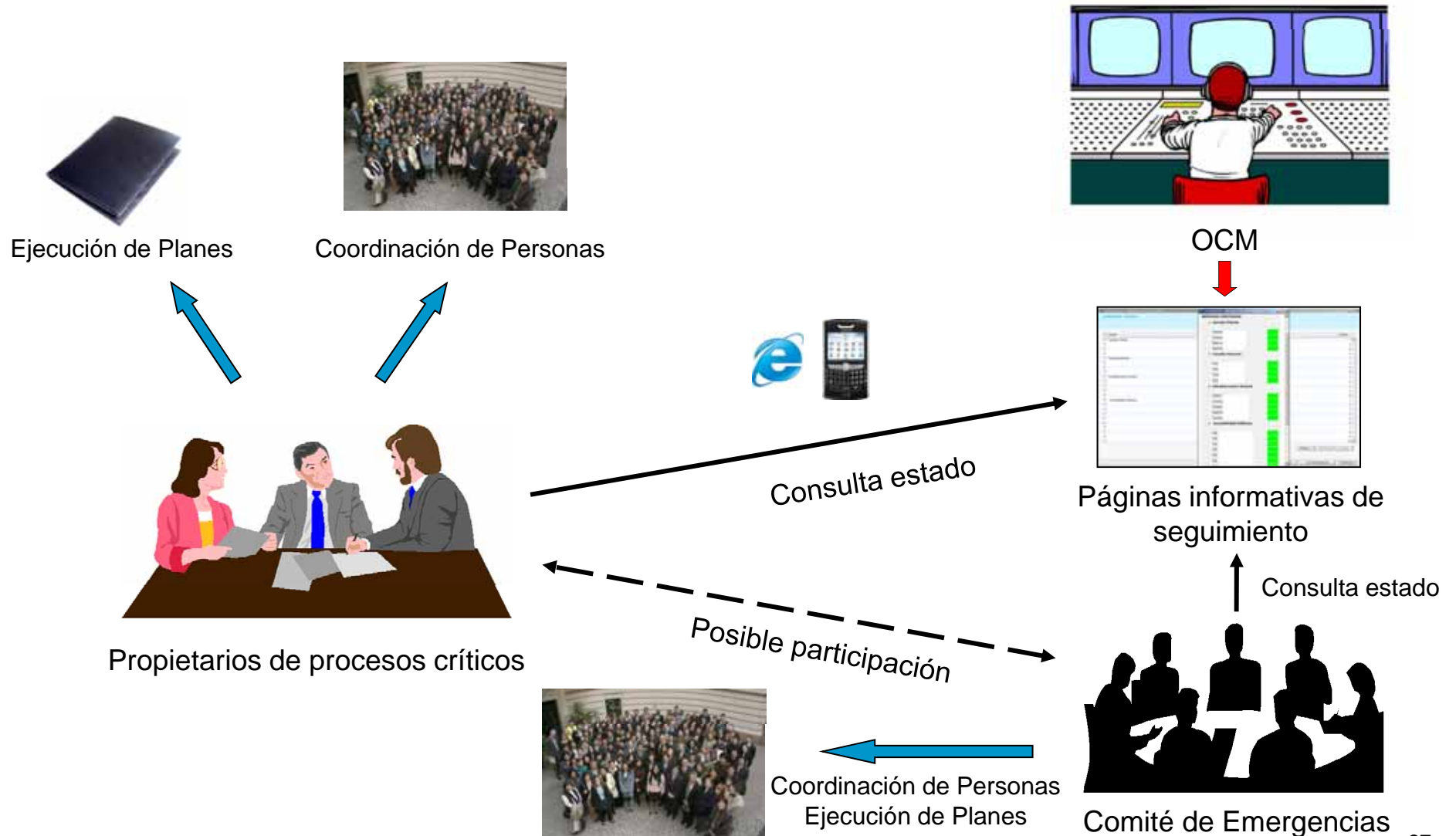
5.- Monitorización, Respuesta y Coordinación con otras áreas

→ Notificación y gestión de una Emergencia



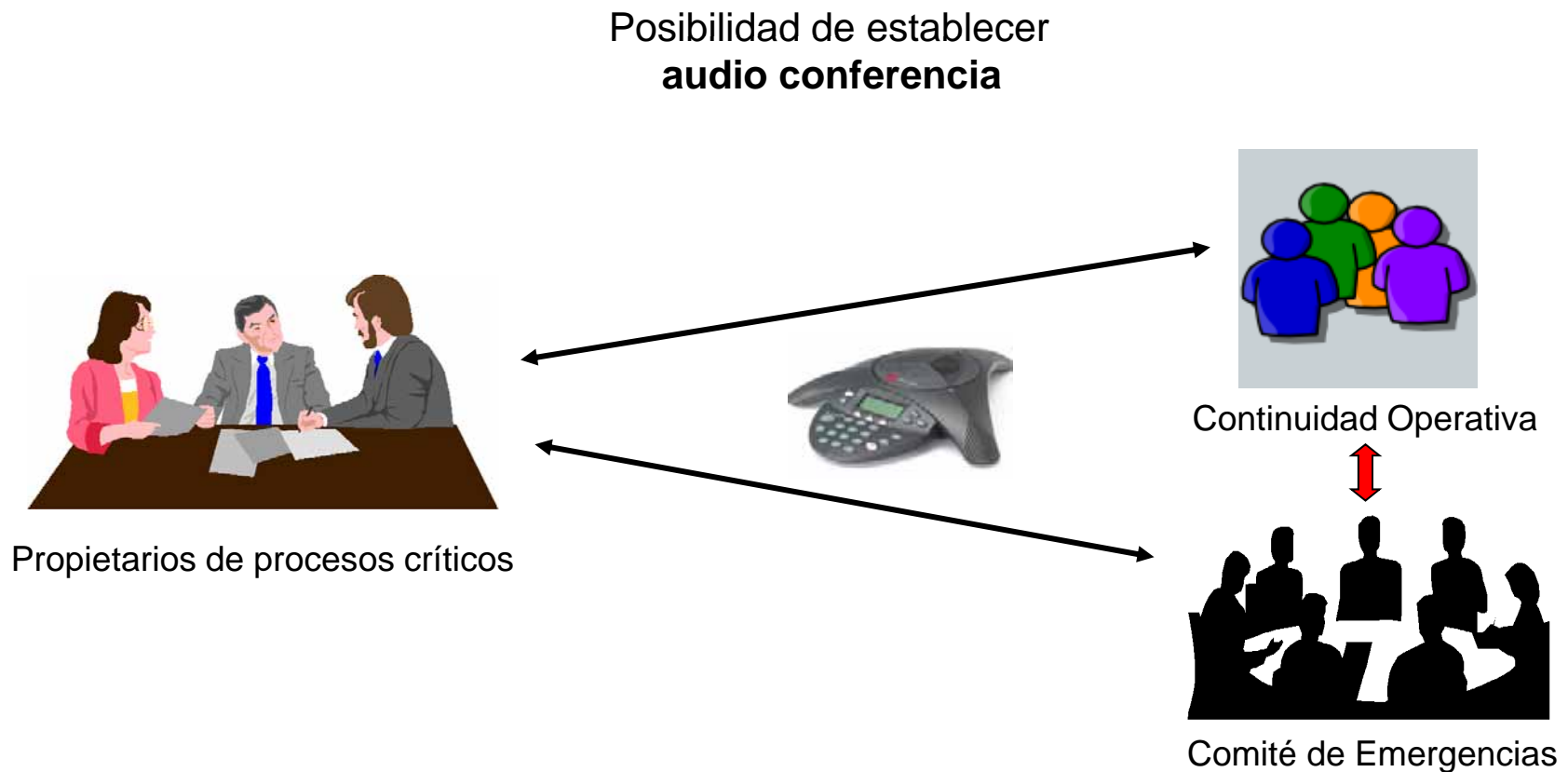
5.- Monitorización, Respuesta y Coordinación con otras áreas

→ Notificación y gestión de una Emergencia



5.- Monitorización, Respuesta y Coordinación con otras áreas

→ Notificación y gestión de una Emergencia



5.- Monitorización, Respuesta y Coordinación con otras áreas

El Comité de Emergencias

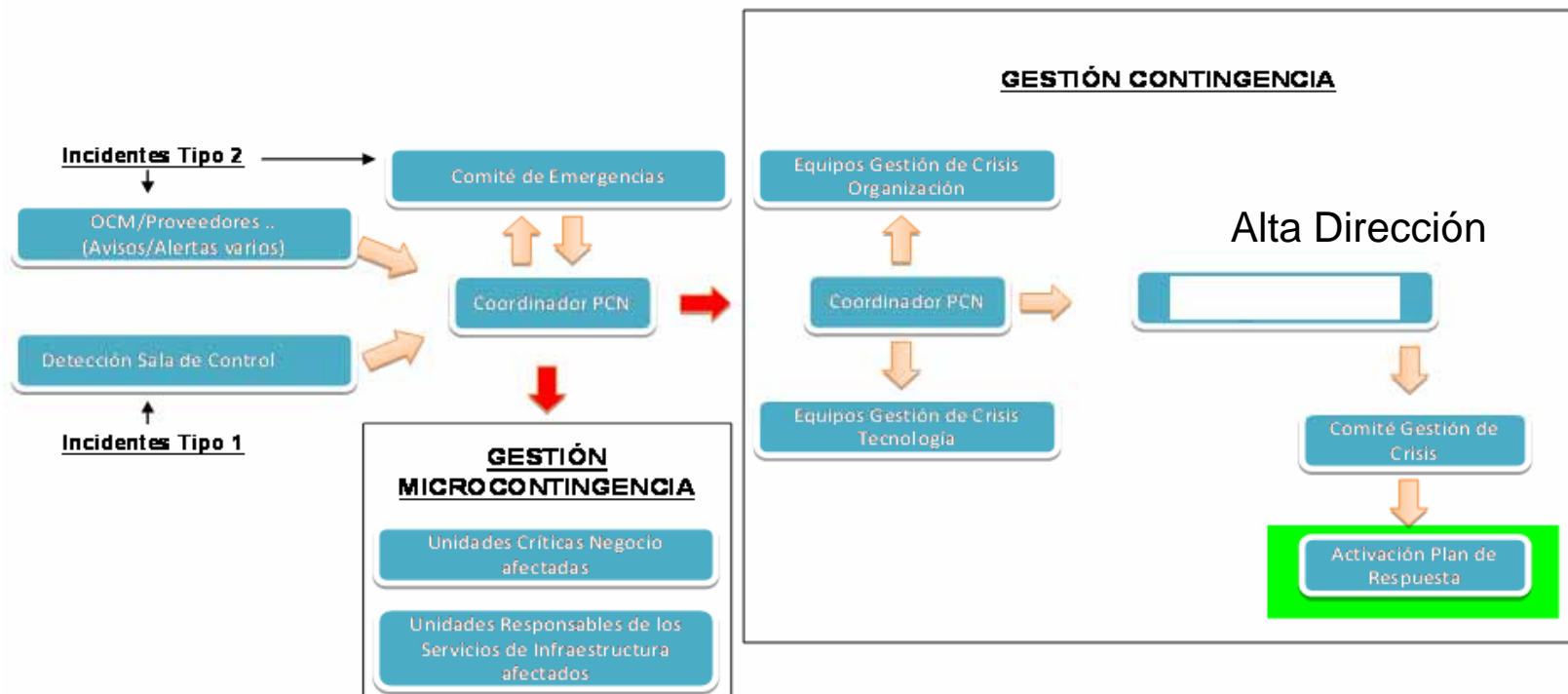
- Creado con el objetivo de conseguir mayor coordinación ante **Emergencias de todo tipo**
- Comité **ejecutivo multidisciplinar**, que se convoca para dar respuesta coordinada a situaciones de emergencia que afectan tanto a procesos críticos como no críticos
- Formado por un grupo de **miembros fijos**: RRHH, Seguridad, Organización, Comunicación, Servicios Generales, Continuidad Operativa, etc.
- Según la emergencia, el Comité **puede convocar a otros miembros**: otras Unidades de Negocio, unidades Operativas, de Servicios, etc.



5.- Monitorización, Respuesta y Coordinación con otras áreas

→ El Comité de Emergencias

- Los **incidentes menores** se gestionan **sin la intervención** del Comité de Emergencias
- Los **incidentes de impacto medio** se gestionan **por** el Comité de Emergencias, que **informa** a la Alta Dirección
- En los incidentes de **impacto muy elevado** se **convoca** el **Comité de Gestión de Crisis**, en el que participa de forma activa la Alta Dirección



Muchas gracias por su atención

Xavier Serrano

www.bancosabadell.com

B Sabadell

SabadellAtlántico BancoHerrero SabadellSolbank BancoGuipuzcoano

