Nuevas Tecnologías:

Riesgos y Amenazas

ERNST & YOUNG

Quality In Everything We Do

ERNST & YOUNG
Quality In Everything We Do

Agenda

- Antecedentes: Sobre la seguridad de la información
- El mundo del Seguro: Cuestiones a plantear
- El enfoque: Análisis de riesgos
- Esquema general de un Análisis de Riesgos
  - Identificación de activos
  - Amenazas y vulnerabilidades
  - Análisis de impacto y probabilidades
  - Gestión del riesgo
- Nuevas Tecnologías: Actor principal en la seguridad
- Nuevos canales comportan nuevos riesgos
- Cuestiones

Antecedentes: Sobre la seguridad de la información

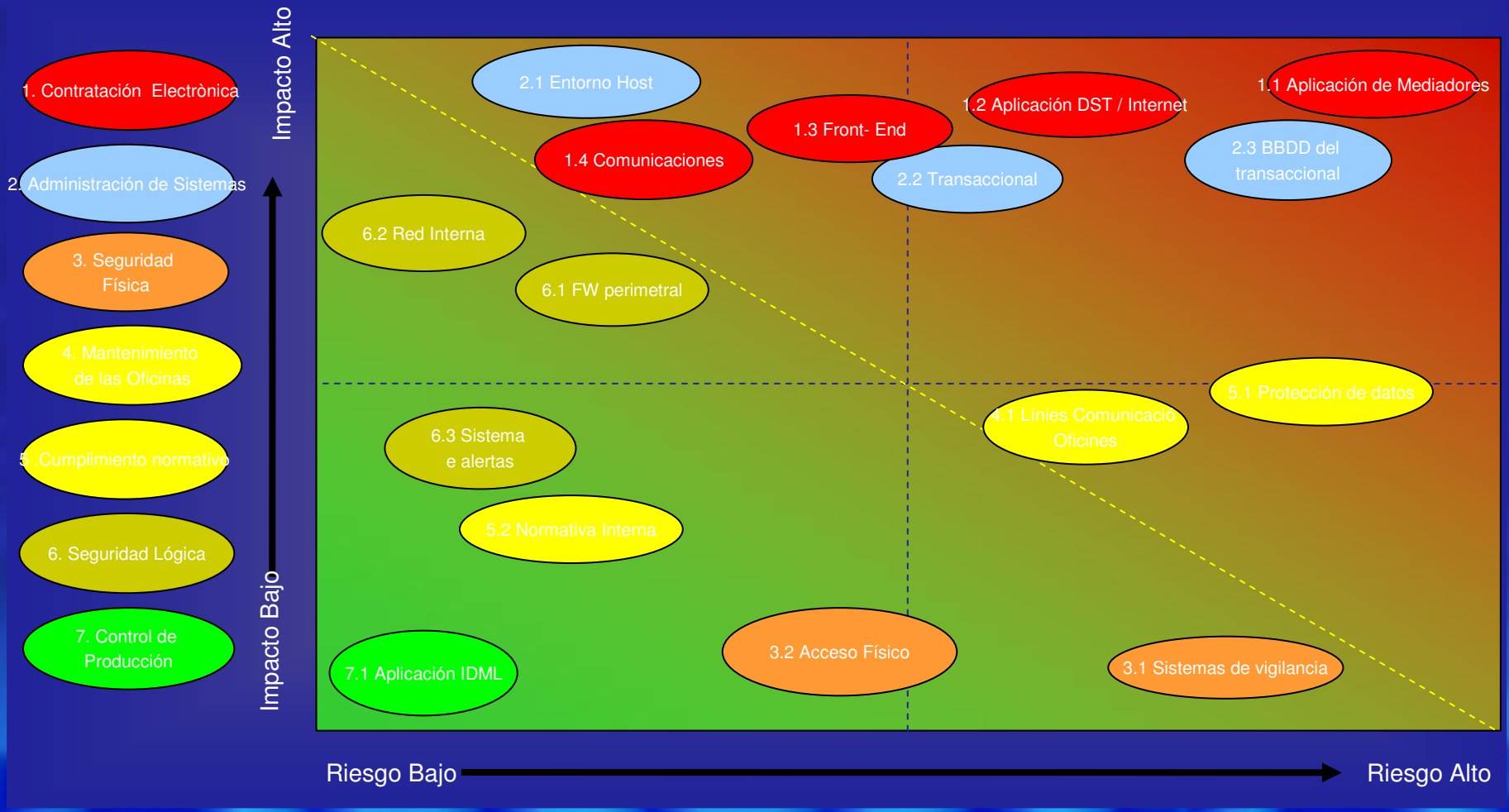
- Tradicionalmente, la seguridad se analiza contemplando tres áreas: Confidencialidad, Integridad y Disponibilidad
  - Confidencialidad: Afecta a la capacidad de establecer mecanismos de control de acceso acordes a los permisos de los usuarios del entorno.
    - Ley de Protección de Datos de Carácter Personal
    - Auditoría de perfiles y entornos / Test de Aplicación
    - Hacking Ético y Test de Intrusión (Interno y Externo)
  - Integridad: Capacidad de mantener un dato confiable y no manipulado
    - Auditoría Informática controles generales (Cobit, SoX, Coso, etc)
    - Análisis de Integridad
  - Disponibilidad: Área que contempla los mecanismos dirigidos al mantenimiento y continuidad del acceso a la información frente a incidentes.
    - Plan de Continuidad del Negocio
    - Análisis de Rendimientes y disponibilidad de Servicios
  - Otras áreas: Auditabilidad, Trazabilidad, Imagen, Normativa, No repudio, etc
    - Análisis de Riesgos Tecnológicos
    - Cumplimiento Normativo (LOPD, SOX, Solvencia II, LSSI, SAS 70, etc.)
    - Plan Director de Seguridad, Políticas y procedimientos de Seguridad de la información
    - Firma Electrónica

El mundo del Seguro: Cuestiones a plantear

- La casuística especial del mundo del seguro, donde la información es el máximo activo del negocio, requiere un análisis especial del impacto de la seguridad en este sector:
  - ¿Cómo me afectan e impactan las actuales leyes y normativas?
    - LOPD: Ley muy restrictiva, ya que los datos son de alto nivel (Partes, siniestros, etc.)
    - SOX: Gran incidencia en un sector caracterizado por multinacionales
    - Solvencia II: Requerimientos de un entorno de control y calidad de la información
  - ¿Cómo me afecta la seguridad en mis procesos de negocio?
    - Red de mediadores y agentes:
      - El rendimiento de las comunicaciones impacta en la cuenta de resultados
      - Firma electrónica y no repudio: Una solución al servicio de la Entidad
    - Consolidación de la información:
      - Los datos residen en el mainframe, hay que establecer controles adicionales en este entorno
      - Desarrollos ad-hoc: Suelen ir dirigidos a la funcionalidad vs seguridad
    - Infraestructura de comunicación:
      - Criterios de visibilidad entre agentes / oficinas / Sistemas Centrales / partners / proveedores

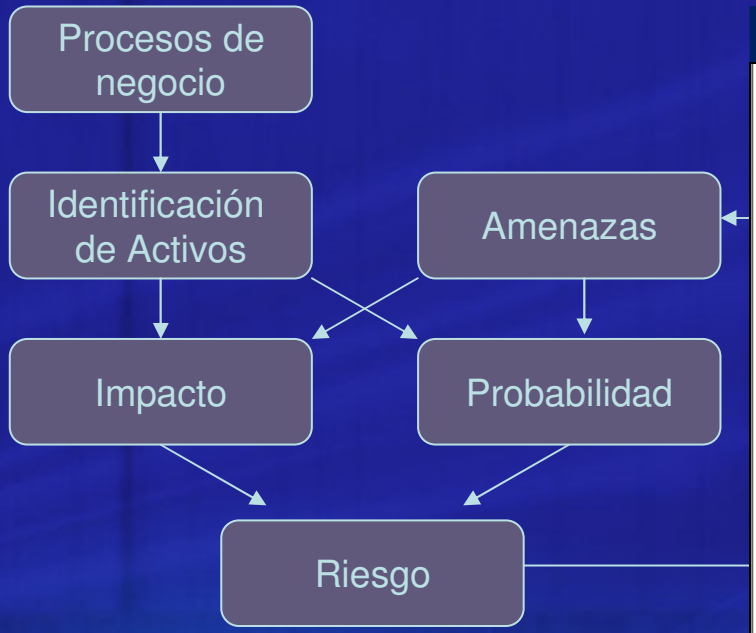
ERNST & YOUNG
Quality In Everything We Do

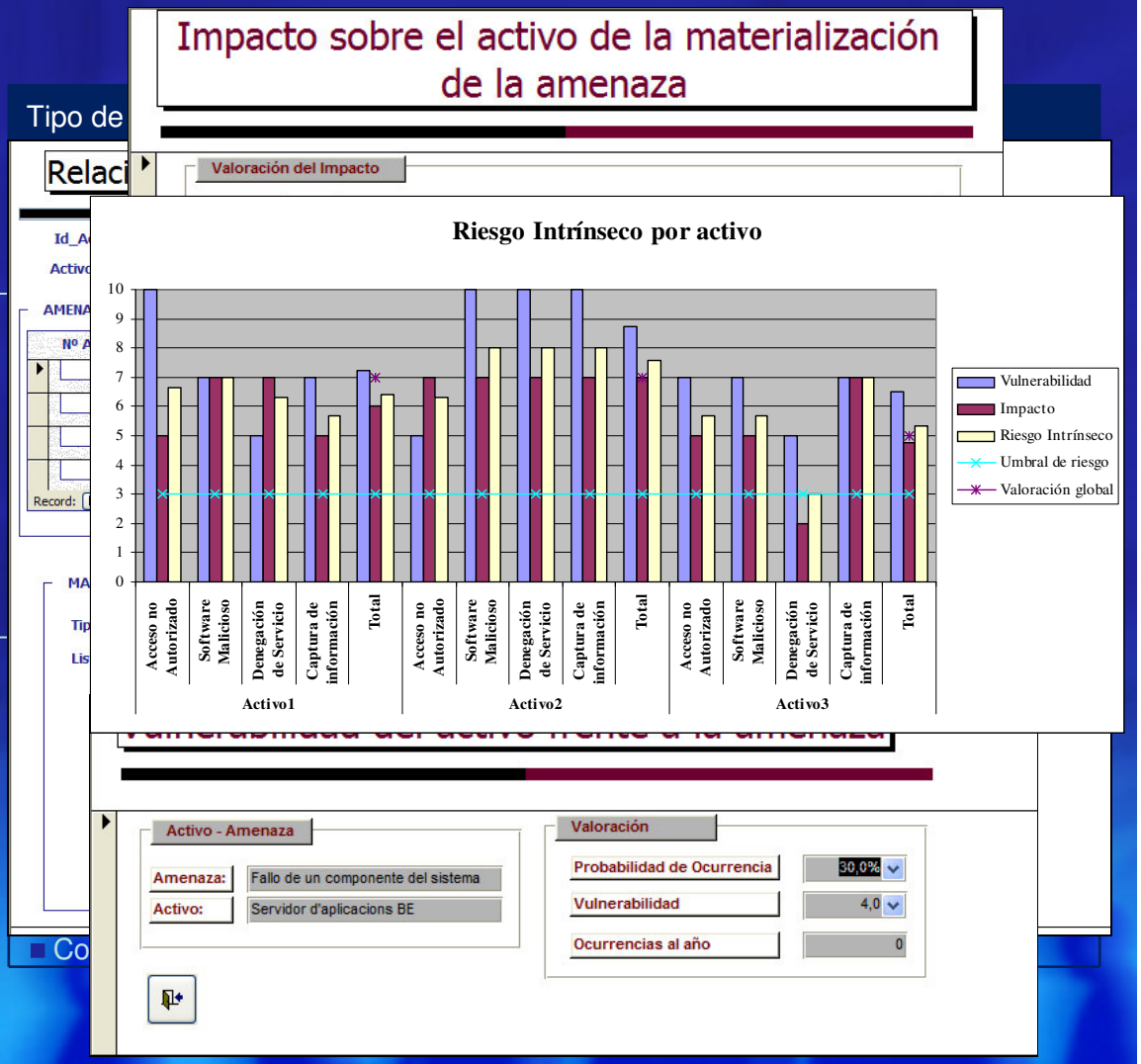
El enfoque: Análisis de Riesgos



ERNST & YOUNG
Quality In Everything We Do

Esquema general de un Análisis de Riesgos

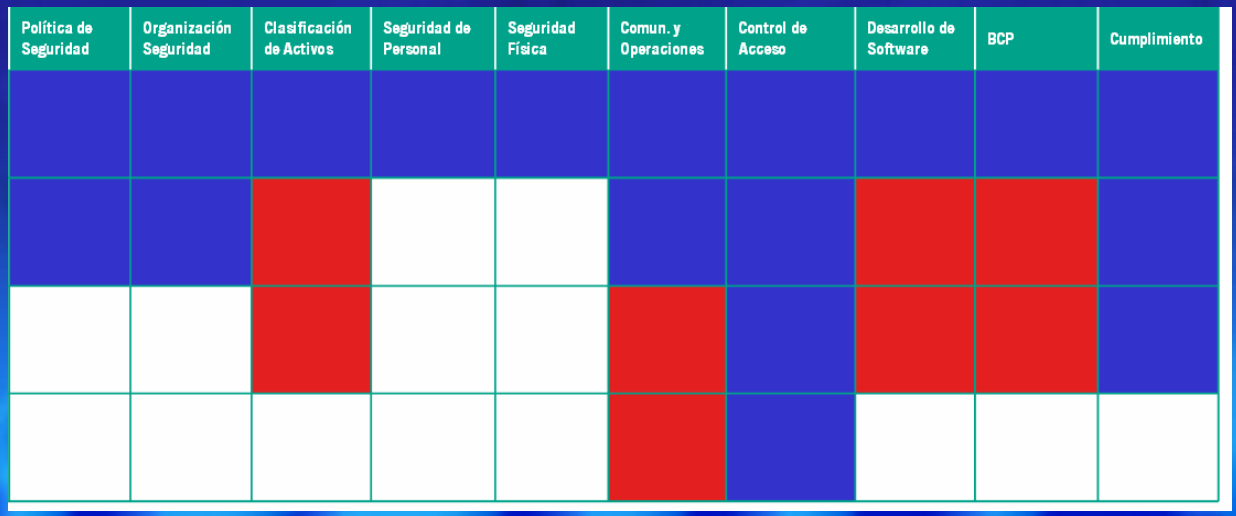




ERNST & YOUNG
Quality In Everything We Do

Enfoque y alcance de un Análisis de Riesgos

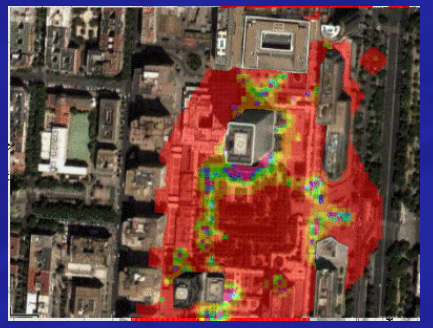
- La granularidad para alcanzar una visión general de los riesgos tecnológicos de una Entidad depende en gran medida del ámbito que quiere analizarse.
- En este sentido, el alcance se acrecienta conforme al empleo de tecnologías más novedosas o emergentes, donde el carácter técnico asume gran importancia.
- A modo de ejemplo, sirva el siguiente gráfico basado en las diferentes áreas de seguridad de la ISO 17799, donde puede observarse que en un enfoque top-down, el nivel al que se llega en las áreas técnicas es el más detallado.

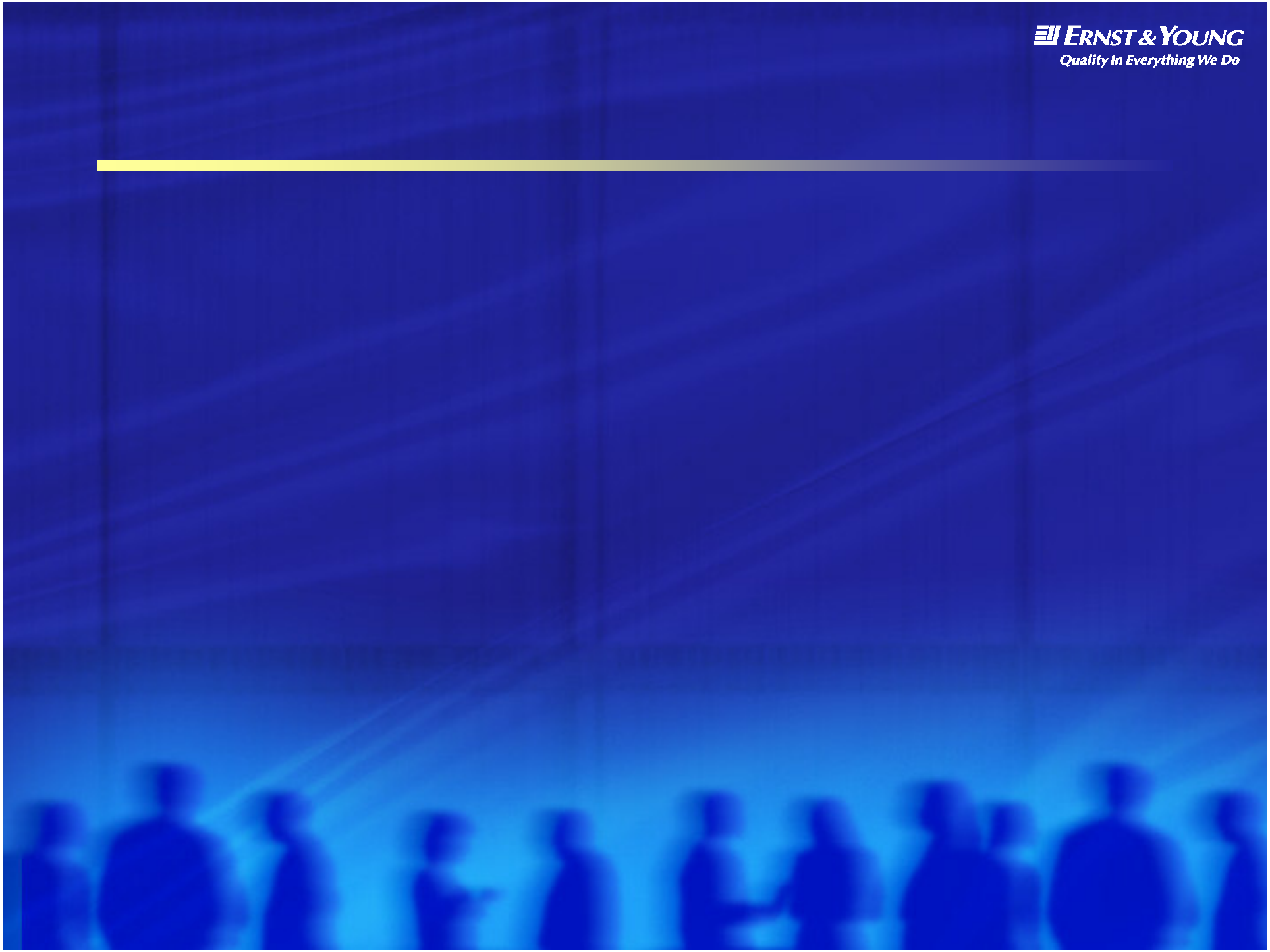


ERNST & YOUNG
Quality In Everything We Do

Nuevas tecnologías, actor principal en la seguridad

- Nuevas tecnologías emergentes y su facilidad de uso ofrecen un nuevo escenario de riesgo. Cuanto mayor es la facilidad y funcionalidad de un sistema, más se incrementa este riesgo.
  - Internet, Intranet, Extranet: Riesgos a un click de distancia.
    Hacking Ético – Test de visibilidad de activos
  - Comunicaciones inalámbricas: Acceso privilegiado a un usuario anónimo.
    Análisis wifi / bluetooth
  - Aplicaciones web: Vía de intercomunicación directa con el host.
    Análisis de flujo de datos - Test de Intrusión de entorno Host
  - Infraestructura de comunicaciones: O como ofrecer accesos a partners, externos y clientes VIP a nuestro core business.
    Diseño de Arquitecturas – Análisis de Infraestructuras




ERNST & YOUNG
Quality In Everything We Do