

valoración y suscripción del Ciberriesgo



30 de Mayo 2013



Antonio Moreno
Antonio.Moreno@acegroup.com

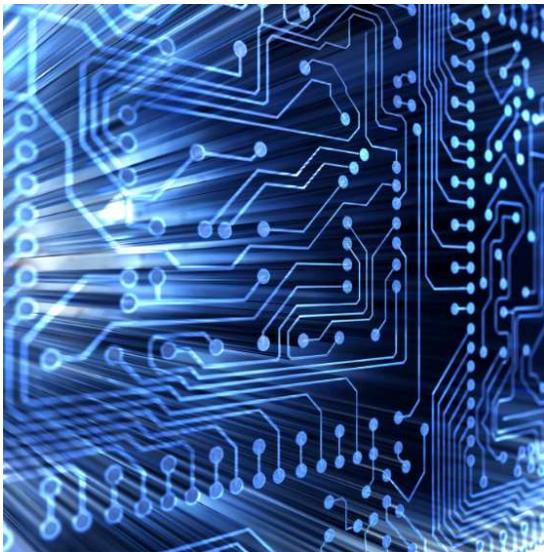
ENCUESTA REALIZADA POR ACE

**Fecha: Abril 2012.
Muestra: 606 Gerentes
de Riesgos.
Países: España, Italia,
Francia, Alemania,
Benelux, UK.**



- Principales conclusiones:
- **Cyber risk** es considerado por un 26 % como el riesgo de mayor importancia o relevancia de su empresa.
- Un 52 % confiesa que sus empresas no están nada o poco preparadas para **Cyber risk**.
- Un 43 % declara haber sufrido una Denegación de Servicio (DOS).
- Un 36 % confirma haber sufrido un ataque de hacker.
- Un 30 % declara haber tenido fallos en el sistema por corrupción de la información.
- Un 19 % dice haber tenido fallos en sus sistemas de información por errores humanos.
- Un 9 % declara haber tenido pérdidas económicas por infección de virus.

INFORME ANUAL DE LA SEGURIDAD EN ESPAÑA 2012



Fuente: Esys



- Principales conclusiones:
- Un 36 % de las grandes empresas tiene hecho análisis de riesgos.
- Un 50 % de las recomendaciones incluidas en los análisis de riesgos se implementan.
- Un 75 % de las grandes empresas tiene BCP (Plan de continuidad del negocio) elaborado.
- Un 68 % de las grandes empresas que tienen BCP lo prueban antes de implantarlo.
- Un 80 % obtiene un resultado correcto en la prueba del BCP.

DATA BREACH INVESTIGATION REPORT 2012



Fuente: Verizon



- Principales conclusiones:
- El 62 % de las brechas de seguridad tardaron meses en descubrirse. El 4 % superó el año.
- El 69 % de las brechas de seguridad fueron descubiertas por terceros ajenos a la empresa.
- El 86 % de las brechas tienen un origen externo a la empresa.
- El 75 % de los ataques son oportunistas.
- El 78 % de las brechas tiene tácticas de dificultad baja o muy baja.

QUÉ LIMITES SON ADECUADOS – ASPECTOS A CONSIDERAR

- 1.- Análisis de riesgos.
- 2.- Países donde opera nuestra organización.
- 3.- Arquitectura IT en cada país o sociedad
- 4.- Número y tipo de registros totales sobre empleados y clientes. (particulares/empresas).
- 5.- Gastos en los que podemos incurrir:
 - - Gastos de investigación.
 - - Gastos de notificación.
 - - Gastos de respuesta.
 - - Perdida de negocio.
- 6.- Coste medio por registro: USA (190 USD), Europa (105 €).
- 7.- Margen bruto a 3 meses.



PRINCIPALES PARAMETROS PARA EL CALCULO DE LA PRIMA

- 1.- Límite de cobertura.
- 2.- Actividad.
- 3.- Implantación geográfica.
- 4.- Volumen de facturación y número de empleados.
- 5.- Medidas de seguridad y nivel de protección.
- 6.- Número de registros y tipología.



PUNTOS CLAVES A VALORAR

- Proveedores de sistemas y servicios informáticos – Incluidos.
- Definición amplia de Empleado: a tiempo parcial, freeland, becario.
- Consultores o asesores que tengan una relación contractual con el asegurado.
- Brechas de seguridad producidas a través de cualquier dispositivo móvil (Ej. teléfono 3G, Tablet, Portátil) con acceso a la red deben estar cubiertas.
- Virus y sus réplicas, un solo siniestro las producidas en intervalos de 7 días.
- Datos propios y datos de terceros en poder del asegurado.



ANÁLISIS DEL CIBERRIESGO Y VALORACIÓN DEL RIESGO

- 1.- ORGANIZACIÓN DE LOS SISTEMAS DE INFORMACION
- 2.- PROTECCIÓN DE LA INFORMACIÓN Y CONTROL DE ACCESO
- 3.- PROTECCIÓN DE LOS SISTEMAS Y ANTIVIRUS
- 4.- COPIAS DE SEGURIDAD
- 5.- SEGURIDAD Y FUNCIONAMIENTO DE RED
- 6.- PLAN DE CONTINUIDAD DEL NEGOCIO
- 7.- SEGURIDAD FÍSICA CPD'S
- 8.- EXTERNALIZACIÓN
- 9.- PROTECCIÓN y POLÍTICA DATOS CARÁCTER PERSONAL



CONCLUSIÓN

Si está esperando tener su primera brecha o incidente de seguridad para asegurarse, ese momento ya pasó.....

