

## Protección de Datos

### Prevención del robo de información

Los crecientes incidentes de seguridad en las organizaciones involucrando tanto datos personales como también información confidencial de la organización acaparan la atención tanto de los responsables de la seguridad informática como de los organismos reguladores.

Por otra parte, el nuevo panorama económico presiona a las empresas a tomar nuevos desafíos. Todo esto, sumado a las nuevas tecnologías van borrando las fronteras de la organización y dificultan la gestión de la información. Outsourcing, integración con nuevos socios de negocios, usuarios móviles y la apertura del negocio a Internet son prueba de ello. Esta realidad lleva a las organizaciones a compartir cada vez más información, sin embargo es

clave proteger adecuadamente los datos para que no caigan en las manos equivocadas.

Entre los organismos reguladores que abordaron este tema está la Dirección Nacional de Protección de Datos Personales, la cual, a través de la ley 25.326 y sus disposiciones obliga a las organizaciones a proteger los datos personales a través de medidas de seguridad alineadas con las mejores prácticas del mercado. También las administradoras de tarjetas de crédito (PCI), a través de su estándar de seguridad de datos obliga a las Organizaciones que utilizan esta vía de pago a utilizar estrictos niveles de seguridad para proteger los datos de los clientes.

Es clave proteger adecuadamente los datos para que no caigan en las manos equivocadas.

#### El Desafío

Pese a ser un problema conocido, mantener adecuados niveles de seguridad y protección de los datos, sigue siendo un desafío para todas las organizaciones dado que:

- La complejidad de las organizaciones es creciente, resultando en un enorme volumen de información que es almacenada, transmitida y procesada.



Esto complica el proceso de conocer el detalle de los datos existentes, dónde se almacenan, cómo se usan y quién los accede.

- El acceso de terceros a la información, que en muchos casos deben transmitirla a sus propios sistemas fuera de la organización.
- La información, especialmente la financiera, es cada vez más apetecible para las organizaciones criminales.
- Concientizar a toda la organización de los riesgos y las medidas de protección a tomar es un esfuerzo enorme y constante.

### Nuestra Visión

Las iniciativas para la protección de la información deberían incluir al menos los siguientes pasos:

- 1 Conocimiento de los datos**  
Es crítico saber qué información es valiosa, dónde está y quién debería accederla lícitamente.
- 2 Identificación de los flujos de datos**  
La identificación de las áreas, los sistemas y las personas a través de las cuales circulan los datos, dentro y fuera de la organización.
- 3 Clasificación de la información**  
Participando a los verdaderos dueños de la información y

considerando los riesgos para la organización y los requerimientos internos y regulaciones externas (ej: habeas data, PCI).

- 4 Ciclo de vida de los datos**  
Con la información obtenida es posible establecer el ciclo de vida de los datos, desde su punto de origen, a través de su procesamiento, mantenimiento, almacenamiento y destrucción, identificando los controles existentes en cada estado. Como resultado se obtiene una clara visión de los riesgos en cada caso.

- 5 Definición de las políticas de protección de datos**  
Los resultados de los pasos anteriores permiten diseñar una política para la protección de los datos ajustada a las necesidades de la organización, involucrando a los responsables en cada caso y ajustando la complejidad y costo de los controles de acuerdo al verdadero riesgo asociado.

- 6 Monitoreo y evolución de las capacidades de protección**  
Es imprescindible dar seguimiento al correcto uso de las políticas y controles definidos y ajustarlos a medida que el negocio y la organización evoluciona.

### El diferencial de Deloitte

Tenemos una metodología probada para ayudar a nuestros clientes a cumplir estos pasos detallados. Seguimos un enfoque basado en los riesgos, lo cual resulta en recomendaciones y soluciones ajustadas a los riesgos del negocio. Asimismo, todas las deficiencias de seguridad identificadas durante nuestro trabajo son consolidadas y priorizadas, de manera de resaltar los temas más importantes para ser tratados por la gerencia de la organización y definir los pasos a seguir para solucionarlos.

Contáctenos:

#### Martín Carmuega Socio

Líder Risk Advisory  
+54 11 4320 4003  
mcarmuega@deloitte.com

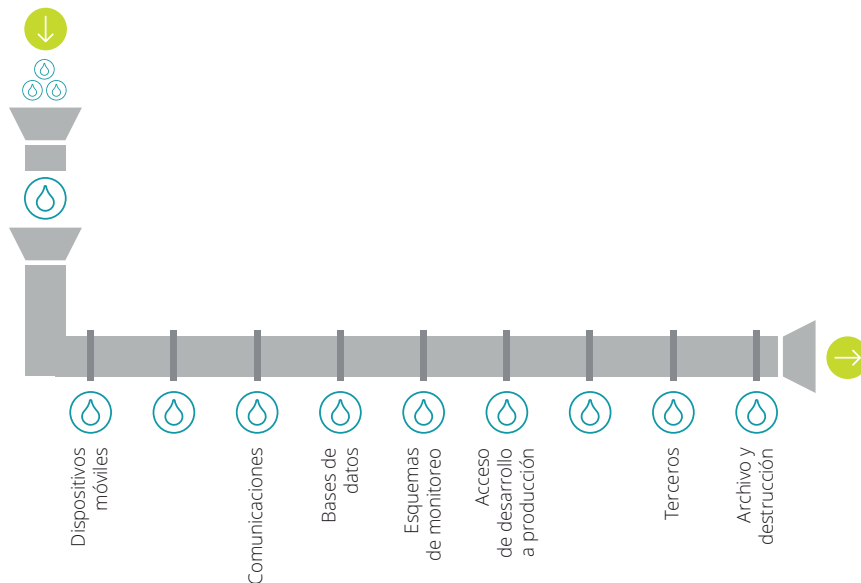
#### Andrés Gil Socio

Líder Cyber Risk Services  
+54 11 4320 2779  
angil@deloitte.com

#### Facundo Jamardo Socio

Cyber Risk Services  
+54 11 4320 4067  
fjamardo@deloitte.com

### Pérdida de Datos



Si su dispositivo móvil lo permite, escanee el código y acceda a nuestra web.

Deloitte se refiere a una o más de las firmas miembro de Deloitte Touche Tohmatsu Limited, una compañía privada del Reino Unido limitada por garantía ("DTTL"), su red de firmas miembro, y sus entidades relacionadas. DTTL y cada una de sus firmas miembro son entidades únicas e independientes y legalmente separadas. DTTL (también conocida como "Deloitte Global") no brinda servicios a los clientes. Por favor acceda a [www.deloitte.com/about](http://www.deloitte.com/about) para conocer más sobre nuestra red global de firmas miembro.