CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Aprendiendo de las Sanciones

Esteban Jaramillo Aramburo
(ejaramillo@summa-consultores.com)

Daniel Fernández Bleda
(@deferble / dfernandez@isecauditors.com)

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- El Artículo 3 de la Ley incluye las de definiciones básicas de términos que emplearemos en las presentaciones:
  a) **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
  b) **Base de Datos**: Conjunto organizado de datos personales que sea objeto de Tratamiento.
  c) **Dato personal**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
  d) **Encargado del Tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

e) **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento.
f) **Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Presentación

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- En esta presentación vamos a analizar resoluciones de la SIC en casos de incumplimiento de la Ley 1581/2012 desde un punto de vista **técnico y jurídico**.
- No mencionaremos los nombres de las empresas ni detalles identificativos, no resulta relevante.
- Lo relevante de las resoluciones en esa presentación es:
  - Qué generó la investigación.
  - Qué se pudo haber incumplido.
  - Cómo actuó la empresa ante los aspectos de cumplimiento.
  - Qué se puede aprender para no cometer los posibles “errores” que se hubieran producido.

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Ficha del Caso

- Fecha: **Febrero 2015**
- Sector de la Empresa: **Alimentación**
- Importe de la Sanción: **150 slmmv ($96.652.500)**
- Origen del Proceso: **Denuncia Cliente**
- Tipos de incumplimientos: **Técnicos, Jurídicos, Procedimentales**
- Terceros Implicados: **Proveedores TIC/desarrollo SW, asesores en Prot. Datos, asesores en Seguridad TIC.**

Resumen del caso

- La empresa sancionada lleva a cabo un envío por correo electrónico de información sobre una campaña de mercado.
- El correo electrónico, realizado por un proveedor de servicios de mercadeo, incluye un enlace a un sitio web.
- El sitio web aloja una BD con Datos Personales.
- Estos datos personales resultan ser accesibles sin limitación ni control de acceso ninguno.
- No existen contratos con ciertos proveedores de servicio que permitan descargas de responsabilidades de la investigada.

Caso 1

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- A algunos de los requerimientos de la SIC, las respuestas y alegaciones de la sancionada no tienen el contenido y detalle técnico adecuado que atienda la petición.
- Estas respuestas hacen mención a que su asesor en seguridad avaló las medidas implementadas, cuando estas quedan claramente en entredicho por las revisiones realizadas por el propio personal de la SIC. También se mencionan controles de acceso incoherentes o medidas de seguridad inexistentes.
- Las respuestas y alegaciones de la investigada a la SIC empeoran la valoración de la SIC de dichas respuestas defectuosas.

Caso 1

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- La empresa resulta sancionada por incumplir (Art. 4):

  f) El Principio de acceso y circulación restringida: […] el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente Ley.
  Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

g) **El Principio de seguridad**: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o **acceso no autorizado** o fraudulento.

Caso 1

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Conclusiones:
  1. El uso de información obtenida debe ser usada para aquello para lo que se informó al Titular. Si se va a ha hacer otro uso, deberá informarse.
  2. Es imprescindible almacenar y gestionar la custodia de las autorización de Tratamiento del Titular.
  3. Todo sitio web que contenga Datos Personales debe ser revisado desde el punto de vista de cumplimiento jurídico y contar con las medidas técnicas de seguridad adecuadas.
  4. Cuando se produce un requerimiento de la SIC es imprescindible tener un asesor experto en incidentes, seguridad TIC y protección de datos.

5. Las respuestas ante la ejecución de los derechos de los Titulares deben coordinarse técnica y legalmente cuando sea necesario: en caso contrario se darán respuestas antes de corregir problemas o las razones que hayan generado la petición.
6. Una respuesta defectuosa a un Titular tiene el efecto contrario.
7. Una respuesta defectuosa a la SIC genera descrédito y mayor desconfianza: el investigador querrá más información.
8. Todos los proveedores de servicios que impacten en el cumplimiento legal deberán trabajar bajo contratos de prestación de servicio adecuados.

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Ficha del Caso

- Fecha: **Febrero 2015**
- Sector de la Empresa: **Servicios**
- Sanción: **Bloqueo Temporal de BBDD**
- Origen del Proceso: **Denuncia de 2 Clientes**
- Tipos de incumplimientos: **Técnicos, Jurídicos, Procedimentales**
- Terceros Implicados: **N/A.**

Resumen del caso

- El equipo investigador atiende dos denuncias de dos clientes con el mismo objeto. Se persona en las instalaciones de la empresa para realizar la investigación.
- La empresa no facilita ni política de Tratamiento de la Información ni del Manual de Políticas y Procedimientos.
- Además, la representante legal intenta impedir de forma activa la investigación.
- La acción de bloqueo es tan infructuosa que el investigador tiene acceso en el ordenador sobre el que actúa, un documento con datos personales en una hoja de cálculo abierta.

Caso 2

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- La empresa sobre la que se actúa de forma cautelar está obteniendo datos identificativos, de ubicación y crediticios de forma ilegítima.
- En el Call Center de la compañía, el personal que realiza el tratamiento no conoce la existencia de ningún tipo de cláusulas de confidencialidad.
- La investigación confirma que la compañía no tiene documentado ni implementado un procedimiento para la atención de reclamos y consultas de los Titulares.

Caso 2

En el curso de la investigación, esta obtiene indicios que infieren la posible recopilación de información de forma ilegal.

Los indicios son los siguientes:

(i) Al momento de proceder a tomar la información de los equipos que se encontraron en la empresa, la: representante legal obstruyó la labor de investigación de la entidad negando el acceso a los mismos, razón por la cual esta Dirección le puso de presente las consecuencias legales de tal obstrucción. Aun así la representante legal persistió en la negativa;

(ii) al momento de proceder a revisar las medidas de seguridad del equipo de cómputo que maneja la representante legal, está Dirección pudo constatar que se encontraba abierto un archivo Excel que contenía datos de identificación (nombres e identificaciones) asociados con datos de ubicación (direcciones, teléfonos) y datos financieros (nombres de entidades bancadas, números de tarjetas de crédito), sin embargo al momento de proceder a verificar dicha información la representante legal de la empresa impido nuevamente el acceso, persistiendo en la obstrucción a la labor de investigación de la Dirección y;

(iii) al ser requerida la represente legal para que aportara las autorizaciones previas, expresas e informadas de los reclamantes y de todos los clientes de la empresa informó que no solicita autorización de tratamiento de datos personales, tal como quedó consignado en acta".

Caso 2

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Se procede al bloqueo temporal de la base de datos personales, medida necesaria para proteger el derecho fundamental de los titulares, teniendo en cuenta que, las evidencias encontradas en la inspección permiten inferir que el tratamiento de información personal se realiza con pleno **desconocimiento** del régimen general de protección de datos personales.
- Esto implica que se le prohíbe el uso de las bases de datos de clientes y prospectos de clientes de la sociedad, lo cual implica, por ejemplo, que no se podrá acceder, consultar, actualizar, modificar, eliminar, transmitir, transferir, etc. la información contenida en las mismas.

Caso 2

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Las acciones de la reguladora hacen especial atención a la violación de los principios del Art. 4:
  - **a) Principio de legalidad**: El Tratamiento a que se refiere la presente leyes una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.
  - **c) Principio de libertad**: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
  - **g) Principio de seguridad** y **h) Principio de confidencialidad**.

Caso 2

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- La sociedad sancionada finalizó sus actividades 4 meses después de esta resolución. Desconocemos si por la imposibilidad de seguir operando tras ver como no puede seguir haciendo uso de su Base de Datos clave en procesos de negocio con clientes y potenciales clientes.
- Aspectos de gradación que hubieran aplicado en caso de haberse producido sentencia:
  (i) se encontró que la investigada obtenía beneficio económico alguno por la comisión de la infracción.
  (iii) hubo resistencia y obstrucción a la acción investigativa de la Superintendencia.

- Conclusiones:
  1. La ausencia de capacitación se verá reflejada en el caso de una investigación. Es necesario preparar al personal y que sus contratos cubran estos aspectos.
  2. Resistirse a la acción investigativa no aportará ningún beneficio y redundará en la sanción preliminar o definitiva. Se debe contar con un soporte asesor adecuado en el ese momento (interno o externo) en lugar de ejercer un bloqueo.
  3. Es necesario revisar los procesos internos del Tratamiento de información para emplear herramientas y medidas de seguridad acordes con los requerimientos de la Ley.

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Ficha del Caso

- Fecha: **Abril 2014**
- Sector de la Empresa: **Financiero**
- Importe de la Sanción: **35 slmmv ($21.560.000)**
- Origen del Proceso: **Denuncia Cliente**
- Tipos de incumplimientos: **Procedimentales**

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Resumen del caso

- La empresa sancionada lleva a cabo un envío por correo electrónico de una campaña en la que aparecen los datos del Titular y un familiar, menor de edad.
- 16 días después, el Titular presenta reclamo solicitando:
  - i) copia de su autorización para el uso y tratamiento de sus datos personales y los del menor,
  - ii) así como información respecto de cuáles datos personales se encontraban alojados en las bases de datos de Protección,
  - iii) la finalidad de su tratamiento,
  - iv) protocolo y nivel de seguridad para conservación de los mismos y, finalmente,
  - v) la suspensión de los datos del menor de edad.

Caso 3

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- 18 días más tarde, la empresa sancionada se comunica con el Titular anunciando la recepción de la petición y diciendo que la atenderán a la mayor brevedad.
- 24 días después, no recibiendo noticia alguna, el Titular presenta reclamo al servicio de Defensor del cliente de la entidad.
- 34 días tras el último reclamo, sin recibir respuesta de la entidad, presenta denuncia ante la SIC.

Caso 3

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- En el proceso de la investigación y atendiendo a los requerimientos de esta, la sancionada presentará de forma completa:
  - Evidencia de que la obtención de los datos del menor se realizaron mediante un formulario diligenciado por el Titular y que el único dato empleado del menor es naturaleza pública.
  - Evidencia de las autorizaciones de Tratamiento por medio de correos electrónicos que incluían la autorización expresa de este al Tratamiento.
  - Evidencia de que la información del menor fue eliminada atendiendo a la petición del Titular.
  - Muchas más evidencias de las comunicaciones, procedimientos de Seguridad, etc. de la Entidad.

Caso 3

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Se aplicarán criterios de gradación que atenuarán la sanción recogidos en el Art. 24 de la Ley:
  f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

- La investigada, en una comunicación al Titular, reconoció la comisión de la infracción respecto de su omisión en responder dentro del término previsto en la ley la petición presentada por el reclamante, por lo que **procederá a reducir la sanción impuesta en 5 smlmv.**

Caso 3

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Las sanciones que se aplicarán en este caso no están relacionadas con la vulneración de ninguno de los Principios recogidos en ella si no en que la empresa incumplió con los deberes contemplado en los literales j) y m) del articulo 17 de la Ley 1581 de 2012, pues:
  i) no dio respuesta a la reclamación radicada por el titular en su totalidad ni dentro del plazo otorgado por la ley,
  ii) así como tampoco informó el uso dado a los datos personales suministrados por el reclamante, luego de que éste lo solicitará en su derecho de petición.
- También se le instruye a la sancionada a que en un plazo máximo de un mes presente un informe detallado de las medidas físicas adoptadas para dar cumplimiento a las políticas de seguridad de la información implementadas.

Caso 3

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Conclusiones:
  1. La empresa sancionada no atendió correctamente a los tiempos de respuesta.
  2. Atendió parcialmente las peticiones del Titular en cuando a la eliminación de información pero no en facilitar la información de este, aunque sí disponía de ella y tenía la capacidad de obtenerla.
  3. Gestionó internamente de forma correcta la custodia documental relacionada con el Tratamiento y contaba con la documentación exigida por la Ley en referencia a las Medidas de Seguridad.
  4. Justificó en la coyuntura interna la imposibilidad de atender la petición pero no se comunicó con el Titular sobre su intención de atender su petición.

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Ficha del Caso

- Fecha: **Junio 2016**
- Sector de la Empresa: **Salud**
- Importe de la Sanción: **1.500 slmmv ($1.034.182.500)**
- Origen del Proceso: **Denuncia Cliente**
- Tipos de incumplimientos: **Técnicos, Procedimentales**

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Resumen del caso

- Tras una búsqueda de un cliente de su nombre a través del buscador de Google encuentra que uno de los primeros resultados es un enlace a un sitio web de la empresa objeto del caso.
- A través de dicho enlace, observa que, sin ningún tipo de control de acceso, hay expuesta información de carácter personal que incluye información de salud.
- Comunicándose son la sancionada, esta le facilita un usuario y contraseña para acceder al sitio web tras implementar control de acceso (que durante un período superior a un año) parecía no estar implementado.

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Tras la denuncia a la SIC de la Titular, esta inicia una investigación que incluye:
  - La búsqueda de datos médicos que todavía pudieran estar accesibles sin control de acceso.
  - La búsqueda de datos médicos en la caché del buscar que todavía pudieran estar accesibles por haber sido libremente accedidos y almacenados por el buscador en fechas previas.
- Se corrobora que ya no existe información personal accesible en el sitio web.
- Se corrobora que existe información personal (incluyendo datos de salud) en la caché de Google, no sólo del denunciante si no de más personas, incluyendo menores. Esto confirma la publicación sin control de acceso durante un período estimado de más de 1 año.

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Tras los resultados preliminares de la investigación, el responsable de esta dispone el bloqueo temporal de datos personales durante 3 días en el sitio web en cuestión. Éste es el portal principal de la empresa.
- Este bloqueo acaba no efectuándose por el perjuicio tan importante que podría causar a la empresa se interpone un aplazamiento a dicho bloqueo.
- Se presentan múltiples alegaciones ante la demanda a fin de anular dos de los aspectos clave de la demanda:
  - No se produjo una falta de medidas de Seguridad.
  - No se realizó una notificación a las SIC del incidente, por no ser supuestamente tal la situación.

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Un aspecto relevante es que la SIC establece que un incidente de seguridad es:

  Los incidentes se refieren a ***cualquier evento*** *en los sistemas de información* o *bases de datos manuales* o *sistematizadas,* ***que atente contra la seguridad*** *de los datos personales en ellos almacenados. La Ley 1581 de 2012 no hace distinción alguna respecto de los incidentes que deben ser reportados a la Superintendencia, por lo que,* ***independientemente de su impacto****, deben reportarse* a *esta entidad todos los incidentes ocurridos.* Como *mínimo, debe informarse el tipo de incidente, la fecha en que ocurrió y la fecha en la que se tuvo conocimiento del mismo, la causal, el tipo de datos* ***personales comprometidos*** *y la cantidad de titulares afectados.*

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Y ante cualquier incidente, independientemente de su naturaleza, la SIC enuncia que:

  Basta con la simple configuración del incidente -bien sea por una falla propia o ajena- que ponga en riesgo la administración de los datos personales para que surja el deber de informar a la autoridad de control dicho evento.

- Esta interpretación llevaría a informar ante incidentes de cualquier tipo sobre sistemas que incluyeran Datos Personales, independientemente de si afectan a la confidencialidad, integridad o disponibilidad. Aunque en la definición anterior finalmente sólo considera el "compromiso".

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Las acciones de la reguladora hacen especial atención a la violación de los principios del Art. 4:
  f) El Principio de acceso y circulación restringida y;
  g) El Principio de seguridad en lo que refiere a la publicación sin control de acceso adecuado y medidas de seguridad, máxime cuando la información está clasificada como datos sensibles (por incluir datos médicos) y datos de menores.
- A este incumplimiento se aplicará una sanción de 1.200 smmlv ($827.346.000)

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- También se hace referencia al hecho de la ausencia de notificación a la SIC cuando el Art. 17 de Deberes de los Responsables del Tratamiento y la obligatoriedad establece la necesidad de:

  n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

- A este incumplimiento se aplicará una sanción de 300 smmlv ($206.836.500).

Caso 4

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

- Conclusiones:
  1. La sanción castiga en especial el hecho de considerar que con un plazo de 20 meses durante los cuales los datos eran accesibles libremente queda patente que no se siguió la diligencia debida en cuanto a la validación de las medidas de seguridad presuntamente implementadas.
  2. Esto se multiplica por el hecho que las Bases de Datos contienen datos sensibles (salud y menores).
  3. La SIC es especialmente enfática con el hecho que la sancionada no comunicara del incidente. Esto puede sentar un precedente a notificar cualquier incidente en su interpretación más “amplia” a la SIC, sin interpretaciones.

¿Tienes Preguntas?

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

Gracias

CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO
www.ccce.org.co

www.isecauditors.com
www.summa-consultores.com