Industria y Comercio
SUPERINTENDENCIA

LOS NUEVOS RETOS DE LA SEGURIDAD EN LA INFORMACIÓN CLÍNICA.
LOS SERVICIOS DE CLOUD COMPUTING EN EL CAMPO DE LA SALUD

María Claudia Caviedes Mejía
Asesora Delegatura para la Protección de Datos Personales

Bogotá, 23 de octubre de 2014

MinComercio
Ministerio de Comercio, Industria y Turismo

PROSPERIDAD PARA TODOS

Industria y Comercio
SUPERINTENDENCIA

Computación en la nube

http://blog.dataprius.com/wp-content/uploads/2013/05/security-on-cloud.jpg

Responsable = Cliente

↕

Encargado = Proveedor

Industria y Comercio
SUPERINTENDENCIA

Servicios en salud

Gestión global médica

Agenda médica – Citas - Programaciones
Registro y atención de pacientes
Historial Clínico
Cirugías – Hospitalizaciones - Urgencias
Laboratorios - Farmacia
Atención de pacientes
Admisiones - Remisiones
Autorizaciones en línea

Gestión financiera

Procesos de facturación

Gestión administrativa

Administración del talento humano
Manejo de múltiples contratos

Industria y Comercio
SUPERINTENDENCIA

Reto

Cloud como negocio vs.
Seguridad de la información y protección de datos personales

Negocio:

- ✓ Interoperabilidad entre organizaciones del sistema de salud, usuarios, gobierno
- ✓ Historia clínica unificada e integrada
- ✓ Reducción de costos

Seguridad de la información y protección de datos personales:

- ✓ Custodia
- ✓ Seguridad
- ✓ Disponibilidad
- ✓ Confiabilidad
- ✓ Integridad
- ✓ Confidencialidad
- ✓ Continuidad del negocio y recuperación de desastres
- ✓ Accesibilidad a la información del paciente durante los tiempos de ventanas de mantenimiento programadas y no programadas.

- ❖ Conocer la localización del proveedor del servicio y de sus recursos, para anticipar un nivel adecuado de protección de datos.

Industria y Comercio
SUPERINTENDENCIA

Dictamen 05/2012 sobre la computación en la nube: GT Art. 29

Industria y Comercio
SUPERINTENDENCIA

Riesgos

Falta de control:

- ✓ Falta de disponibilidad (falta de interoperabilidad y dependencia de un proveedor)
- ✓ Falta de integridad (recursos compartidos)
- ✓ Falta de confidencialidad (requerimientos entidades competentes)
- ✓ Falta de intervención (complejidad en la cadena de tercerización y falta de medidas necesarias para asistir al responsable ante el ejercicio de los derechos de los titulares)
- ✓ Falta de aislamiento (múltiples arrendatarios)

Industria y Comercio
SUPERINTENDENCIA

Riesgos

Falta de transparencia (frente a Responsables y Titulares):

- ✓ Cadenas de sub-encargados
- ✓ Zonas geográficas donde se tratan los datos (ley aplicable)
- ✓ Transferencias internacionales (niveles de protección)

Responsable debe informar a titulares:

- ✓ Identidad del responsable/encargado
- ✓ Finalidades del tratamiento

Industria y Comercio
SUPERINTENDENCIA

Contratos de Cloud (1)

- Deberes de las partes (**cliente = responsable** y **del proveedor = encargado**)
- Apoyo al cliente en el ejercicio de los derechos de los titulares.
- Alcance, forma y finalidad del tratamiento.
- Actualización y rectificación de la información.
- Transparencia en el tratamiento de los datos.
- Devolución y/o destrucción de datos (eliminación simultanea en servidores redundantes y garantizarse con subcontratistas).
- Cláusula de confidencialidad vinculante para el proveedor, sus empleados y cadena de subcontratistas.
- Prohibición de circulación de datos a terceros salvo que se pacte la posibilidad de subcontratar.

Industria y Comercio
SUPERINTENDENCIA

Contratos de Cloud (2)

- Acuerdos sobre nivel de servicio y sanciones por incumplimiento.
- Medidas de seguridad - Integración con la seguridad interna.
- Sujeción de los subcontratistas a los términos y garantías del contrato con el proveedor.
- Obligaciones de notificación al cliente en caso de violaciones de datos.
- Indicación de localización de servidores.
- Procedimiento de auditorías.
- Notificación sobre solicitudes de acceso de entidades competentes.
- Notificación sobre cambios en sus procedimientos.

Industria y Comercio
SUPERINTENDENCIA

Medidas técnicas (1)

- **Disponibilidad**: Acceso oportuno y fiable (prevención de ataques de denegación de servicio, fallos de infraestructura, etc.)
- **Integridad**: Garantía de autenticidad y no alteración de los datos (mecanismos de autenticación de los mensajes, uso de canales seguros).
- **Confidencialidad**: Medidas de cifrado de la información mecanismos de autorización y autenticación, cláusulas para contratistas y empleados.
- **Transparencia**: Medidas técnicas y organizacionales.

Industria y Comercio
SUPERINTENDENCIA

Medidas técnicas (2)

- **Aislamiento:** Segregación de funciones, evitar privilegios excesivos (principio del mínimo privilegio) y medidas técnicas.
- **Posibilidad de intervención**: Evitar los obstáculos excesivos para garantizar el ejercicio de derechos de acceso y supresión.
- **Portabilidad**: Verificación de las facilidades de portabilidad de la información (independencia de hardware y software)
- **Accountability**: Procedimientos de verificación de registros; mecanismos para garantizar acceso; asignación de recursos humanos; certificaciones independientes, etc.

MinComercio
Ministerio de Comercio, Industria y Turismo

PROSPERIDAD PARA TODOS

Industria y Comercio
SUPERINTENDENCIA

Modelos internacionales para Transferencias internacionales

- Declaración de adecuación (UE)
- Principios de Puerto Seguro (*Safe Harbor*)
- Normas Corporativas Vinculantes (NCV)
- Cláusulas contractuales tipo
- Guías sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales (OCDE)
- Cross – Border Privacy Rules (APEC)

MinComercio
Ministerio de Comercio, Industria y Turismo

PROSPERIDAD PARA TODOS

Industria y Comercio
SUPERINTENDENCIA

En Colombia

Industria y Comercio
SUPERINTENDENCIA

Transferencia Internacional de datos
Decreto 1377 de 2013 – arts. 24 y 25

- Distingue entre transferencia y transmisión y señala que si hay transmisión no se requiere informar al titular ni contar con su autorización.

- Establece el deber de celebrar un contrato de transmisión de datos personales entre el Responsable y el Encargado de manera que el control y responsabilidad en el tratamiento de datos esté siempre en cabeza del Responsable.

- En el contrato de transmisión de datos el Encargado se debe comprometer a cumplir con las políticas de tratamiento del Responsable y además se obliga a:

  - Cumplir con los principios de tratamiento de datos.
  - Salvaguarda de la seguridad de la base de datos.
  - Guarda de la confidencialidad.

Industria y Comercio
SUPERINTENDENCIA

Accountability
Decreto 1377 de 2013 – arts. 26 y 27

Los responsables deben ser capaces de demostrar que han implementado medidas apropiadas y efectivas para cumplir con sus deberes legales, de manera que sea proporcional con:

- La naturaleza jurídica del responsable y su tamaño empresarial.
- La naturaleza de los datos personales objeto del tratamiento.
- El tipo de tratamiento.
- Los riesgos potenciales que puede causar el tratamiento.

En caso de ser requeridos, las organizaciones deben describir los procedimientos usados para la recolección de los datos, las finalidades de uso y la relevancia de los datos para ese tratamiento y demostrar medidas de seguridad apropiadas.

Políticas internas efectivas

Las políticas implementadas deben garantizar:

- Existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012.
- Adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.
- Adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos.

La verificación por parte de la SIC de la existencia de medidas y políticas específicas para el manejo adecuado de datos personales que administra un responsable será tenida en cuenta al momento de evaluar la imposición de sanciones.

Industria y Comercio
SUPERINTENDENCIA

Elementos esenciales de los Programas basados en esquemas de Responsabilidad Demostrada

(The Accountability Project, CIPL 2009)

1. Políticas internas efectivas
2. Liderazgo y supervisión
3. Estructura organizacional
4. Educación y concientización
5. Evaluación de riesgos y mitigación
6. Revisión y evaluación constante
7. Manejo de incidentes y quejas
8. Mecanismos internos de cumplimiento
9. Instrumentos de defensa para titulares

OCDE Guías sobre privacidad 2013

TERCERA PARTE. IMPLEMENTANDO *ACCOUNTABILITY*

15. Un responsable del tratamiento de datos debe:

a) Contar con un programa de gestión de la privacidad que:

i. dé cumplimiento a estas Directrices para todos los datos personales bajo su control;

ii. se adapte a la estructura, la escala, el volumen y la sensibilidad de sus operaciones;

iii. prevea salvaguardias adecuadas en función de la evaluación de riesgo para la privacidad;

iv. esté integrado en su estructura de gobierno y establece los mecanismos de supervisión interna;

v. incluya planes para responder a las consultas e incidentes;

vi. esté actualizado en función del seguimiento continuo y evaluación periódica;

b) Estar preparado para demostrar que su programa de gestión de la privacidad es adecuado, en particular, a petición de una autoridad de supervisión competente en materia de privacidad u otra entidad responsable de promover la adhesión a un código de conducta o un acuerdo similar dando efecto vinculante a las presentes Directrices; y

c) Proporcionar notificación, según el caso, a las autoridades de supervisión competente en materia de privacidad u otras autoridades pertinentes donde se ha producido un fallo de seguridad importante que afecte a los datos personales. Cuando el fallo probablemente afecte a los interesados, un responsable del tratamiento de datos debe notificar a los interesados afectados.

Industria y Comercio
SUPERINTENDENCIA

Ciclo de vida del dato

La Gestión de la Información, es un conjunto de procesos por los cuales se controla el “ciclo de vida del dato”.

El objetivo de la Gestión de la Información es propender por la seguridad de la información, garantizando su integridad, disponibilidad y confidencialidad.

Industria y Comercio
SUPERINTENDENCIA

Adoptar un el enfoque de “ciclo de vida del dato” significa **reconocer cómo se produce el flujo de información en sus procesos y actividades**.

Identificar los procesos de Tratamiento de la información:

- Recolección
- Transformación, uso, almacenamiento y transferencia.
- Eliminación o archivo

Industria y Comercio
SUPERINTENDENCIA

Recolección

¿En qué parte del procedimiento o actividad se obtienen los datos (por creación o captura, manual o sistematizados)?

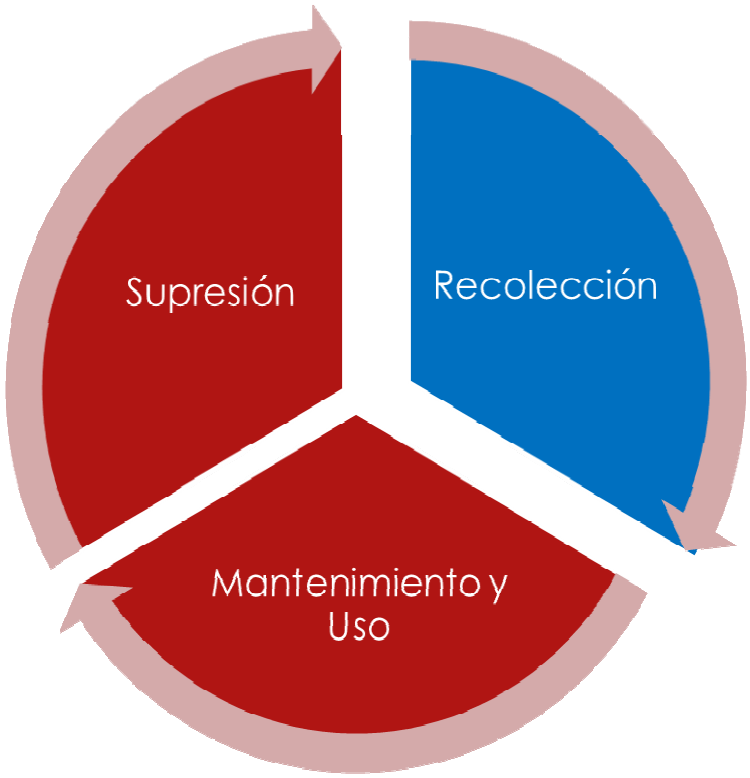
¿Es necesaria la recolección?

¿Qué información se debe recolectar?

¿Cómo se debe recolectar la información?

¿Se asegura la calidad de los datos a la hora de la captura de los mismos?

¿Se está informando la finalidad?



Industria y Comercio
SUPERINTENDENCIA

Mantenimiento y uso

¿En qué procedimientos o actividades internas se procesan los datos y cuales de ellos requieren ser transferidos?

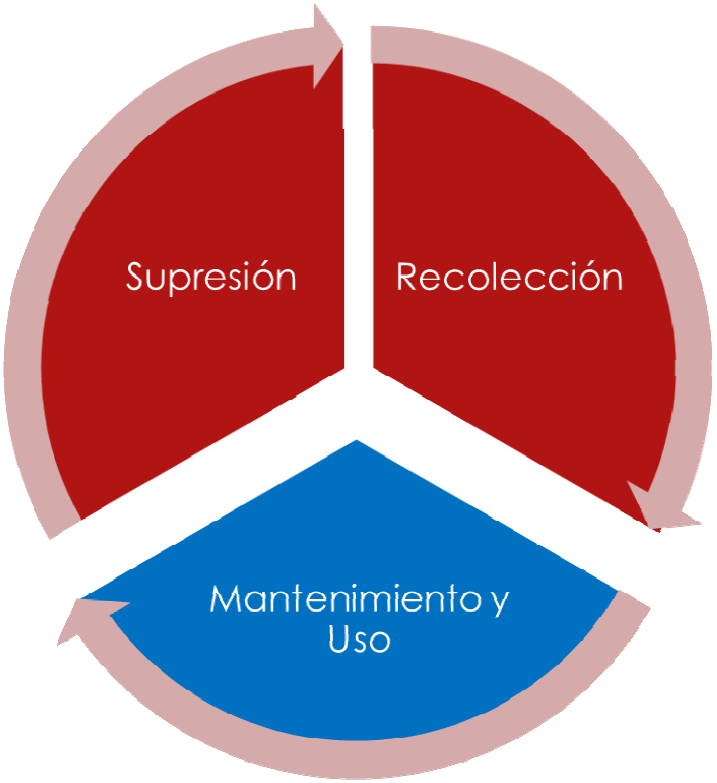
¿Cuál es el procedimiento para realizar oportunamente la actualización y rectificación de los datos?

¿Se depuran, consolidan e integran los datos?

¿Se tiene medidas de seguridad y políticas de acceso?

¿Se actualizan y respaldan los datos?

¿Aseguran la calidad?



Industria y Comercio
SUPERINTENDENCIA

Disposición Final

¿Cuánto tiempo se conservan los datos en la organización y cuáles son los medios para su disposición final?

¿Existen procedimientos de archivo documental con medidas de seguridad?

¿Se deben almacenar los datos eliminados con el fin de tomar medidas de prevención de solicitudes posteriores?

¿Existen procedimientos para atender la solicitud de revocar la autorización y/o solicitud de la supresión del dato?

Gestión de incidentes documentada.

Industria y Comercio
SUPERINTENDENCIA

http://www.cepal.org/cgi-bin/getProd.asp?xml=/prensa/noticias/comunicados/8/52118/P52118.xml&

Industria y Comercio
SUPERINTENDENCIA

¡Muchas gracias!

mcaviedes@sic.gov.co

www.sic.gov.co