



RETO

Transformación Organizacional
Sistemas de Gestión

www.reto.com.co

Servicios de Consultoría

**Atención a la medida
de sus necesidades**



**Cuando Usted necesite
estar seguro...**

Usted cuenta con nosotros



RETO


Transformación Organizacional
Sistemas de Gestión

www.reto.com.co



RETO

transformacion organizacional



Consultoría Especializada Seguridad de la Información Personal

2016



Se ha preguntado...

- Está su Empresa asegurada frente al cumplimiento regulatorio?
- Su Empresa estaría cubierta frente a una visita de la Superintendencia de Industria y Comercio -SIC?
- En la situación actual, de cara a la normatividad, su Empresa está exenta de tener que pagar multas, sanciones y/o suspensiones temporales o permanentes?
- Su Empresa ha considerado apoyarse en un servicio efectivo de Consultoría especializada para cumplir la regulación de la SIC?
- Su Empresa considera que este proceso es Jurídico? De Ingeniería? De Gestión?



Por favor, le invitamos a revisar el documento y podrá obtener la respuesta a estas cinco (5) preguntas ...

Para las nuevas preguntas que le llegaren a surgir sobre este asunto, del **SG SIP**, con gusto le atenderemos.



1. Seguridad de la Información Personal

- ❖ ¿Tiene un documento de seguridad de la información personal o general aprobado?
- ❖ ¿Ha realizado documentación de procesos en torno a la seguridad de la información personal?
- ❖ ¿Tiene procedimientos de asignación de responsabilidades, acuerdos de confidencialidad y autorizaciones en el tratamiento de la información personal?
- ❖ ¿Tiene controles de seguridad en la tercerización de servicios para el tratamiento de la información personal?
- ❖ ¿Tiene integradas las medidas legales, técnicas y administrativas requeridas para asegurar el derecho de Habeas Data de los titulares de la información personal?



2. Sistema de Gestión de la Seguridad de la Información Personal

❖ ¿Tiene implementado un Programa en Gestión Integral de Datos Personales?

Con esta implementación se debe tener en cuenta el tratamiento de los siguientes datos:

- ❖ Datos de los trabajadores
- ❖ Datos de los clientes
- ❖ Datos sensibles
- ❖ Manejo de datos captados por lectores biométricos
- ❖ Manejo de redes sociales
- ❖ Datos de los proveedores
- ❖ Datos de los terceros
- ❖ Datos de los accionistas
- ❖ Videovigilancia
- ❖ Cloudcomputing



3. Seguridad de la Información Personal entorno al Recurso Humano

¿Tiene implementados controles de seguridad de la información personal para el recurso humano antes de la vinculación y una vez finalizado el contrato laboral?



4. Control de Acceso a la Información Personal

- ❖ ¿Tiene una política de control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico?
- ❖ ¿Cuenta con un procedimiento para la gestión de usuarios con acceso a la información personal?
- ❖ ¿Ha implementado una política específica para el acceso a la información personal de las bases con información personal sensible?
- ❖ ¿Tiene una política implementada de copia de respaldo de la información personal?
- ❖ ¿Ha implementado una política de protección para el acceso remoto a la información personal?



5. Procesamiento de Información Personal

- ❖ ¿Cuenta con una política implementada para el correcto tratamiento de la información personal en las diferentes etapas del ciclo de vida del dato (recolección, circulación y disposición final)?
- ❖ ¿Cuenta con un procedimiento implementado para la validación de datos de entrada y procesamiento de la información personal, para garantizar que los datos recolectados y procesados sean correctos y apropiados, como información de tipos, formatos, longitudes, pertinencia, cantidad, uso, etc.?
- ❖ ¿Cuenta con control de seguridad de información para la validación de datos de salida?
- ❖ ¿Cuenta con una política implementada para el intercambio físico o electrónico de datos (como por ejemplo durante el comercio electrónico para la compra y venta de productos o servicios), transporte y/o almacenamiento de información personal?
- ❖ ¿Tiene un procedimiento o control implementado para la disposición final de la información personal (supresión, archivo, destrucción, etc.)?



6. Gestión de Incidentes de Seguridad de la Información Personal

- ❖ ¿Cuenta con una política y procedimientos implementados de gestión de incidentes de seguridad de la información personal?
- ❖ ¿Tiene implementada una política para mejorar la seguridad de la información personal a partir de los incidentes o vulnerabilidades detectados?



7. Auditorías de Seguridad de la Información Personal

- ❖ ¿Tiene una política de auditorías de seguridad de la información personal?
- ❖ ¿Dentro de las auditorías de seguridad de información personal, tiene en cuenta el cumplimiento de requisitos, políticas y normas que específicamente le apliquen a la base de datos?



Ventajas de la implementación del Programa para la empresa

- Control sobre el manejo de la información al interior y por fuera de la empresa.
- Identificar los diferentes tipos de información personal.
- Maximizar el uso de la información.
- Generar buenas practicas al interior de la empresa sobre el uso de la información .
- Minimizar el riesgo en la información que se transmite y transfiere a terceros.
- Aumentar la reputación corporativa frente a todas las contrapartes.



La implementación del Programa de Protección de Datos Personales debe cumplir con los 10 fundamentos básicos definidos en la **Guía de Responsabilidad Demostrada** de la SIC.

1. Compromiso de alta gerencia y asignación de responsabilidades	6. Sistema de Administración de riesgos asociados al tratamiento de los datos personales
2. Presentación de informes	7. Requisitos de formación y educación
3. Procedimientos Operacionales	8. Protocolo de respuestas en el manejo de violaciones e incidentes
4. Inventario de Base de Datos	9. Gestión de los encargados del tratamiento en las transferencias y/o transmisión internacional de datos personales
5. Políticas efectivas	10. Comunicación externa



Registro Nacional Base de Datos - RNBD

- El RNBD es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.
- Las empresas tienen 1 año para inscribir sus bases de datos en el RNBD, la SIC fijó los siguientes plazos teniendo en cuenta los 2 últimos dígitos del NIT:

Del 00 a 24

Del 9/11/2015 a 08/02/2016

Del 25 a 49

Del 9/02/2016 a 10/05/2016

Del 50 a 74

Del 06/05/2016 a 08/08/2016

Del 75 a 99

Del 09/08/2016 a 08/11/2016



**... y su Empresa,
cómo está
utilizando los
Recursos?**



RETO

Transformación Organizacional
Sistemas de Gestión

Jaime Rodriguez Pacheco
Cel: 310 229 35 94
jrpacheco@reto.com.co

www.reto.com.co

Carrera 7 No. 71- 21
Torre B Oficina 1301
Teléfono +57 1 325 11 48
Bogotá, D.C., Colombia

**Quando Usted necesite
estar seguro...**

Usted cuenta con nosotros

www.reto.com.co



SPO	Sistema de Planeamiento Organizacional	SARLAFT	Sistema para la Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo
SGP	Sistema de Gestión por Procesos	SASI	Sistema para la Administración de la Seguridad de la Información
SGI	Sistema de Gestión de la Información	SARM	Sistema para la Administración del Riesgo de Mercado
SCI	Sistema de Control Interno	SARL	Sistema para la Administración del Riesgo de Liquidez
SGH	Sistema de Gestión Humana	SARC	Sistema para la Administración del Riesgo de Crédito
SARO	Sistema para la Administración del Riesgo Operativo	SARG	Sistema para la Administración del Riesgo de Garantías
SACN	Sistema para la Administración de la Continuidad del Negocio		

15
Años



Servicios de Consultoría
Atención a la medida de sus necesidades