NORMA DE AUDITORIA EN PROTECCION DE DATOS PERSONALES

CONTENIDO

GASES DEL CARIBE, en su compromiso con la protección de la información que gestiona considera de importancia vital establecer los parámetros que deben seguirse en materia de preauditoria aplicable a la Protección de Datos Personales en poder de la organización, la cual tendrá como criterios el Principio de Seguridad y de Responsabilidad Demostrada, sin perjuicio de otros que sean pertinentes desde la perspectiva de la auditoria.

1. CONSIDERANDOS

a) Que la legislación colombiana (Ley Estatutaria 1581 de 2012 y Ley Estatutaria 1266 de 2008, en lo que sea aplicable esta última) en materia de protección de datos personales impone el deber a los Responsables y Encargados del tratamiento de datos personales de "implementar planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de datos personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a sus códigos de seguridad o detecten riesgos en la administración de la información de los Titulares"[1].

b) Que, del Principio de Responsabilidad Demostrada e instrucción de la SIC contenida en la guía expedida en 2015, en relación con la gestión de encargados de datos personales, se impone a los sujetos obligados el deber de adoptar las medidas necesarias para asegurar la protección de datos personales, sea que este se realice de forma directa o a través de terceros proveedores como encargados del tratamiento. En este sentido, el numeral 2.7 de la citada guía establece como deber: "Realización de auditorías internas y externas", las cuales se podrán realizar tanto a nivel de información tratada de forma física y/o tratada automatizada, es decir, en sistemas de informáticos en sentido amplio.

c) Que de la mencionada Guía de Responsabilidad Demostrada se establece como mecanismos de evaluación y monitoreo de los controles del Programa Integral de Protección de Datos Personales que se verifique si "¿Los controles del programa están teniendo en cuenta las nuevas amenazas y reflejando las quejas más recientes o los hallazgos de las auditorías, o las orientaciones de la autoridad de protección de datos?"[2].

d) Que, respecto de las funciones del Oficial de Protección de Datos Personales en Colombia, así como en otros países[3], corresponde a este revisar los resultados de las evaluaciones o auditorias respecto del tratamiento de datos que realice de forma directa esta organización en condición de responsable o a través de terceros proveedores en condición de Encargados, esto con el fin de realizar

[1] Guía de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio, Numeral 1.3., 2015

[2] Guía de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio, Literal B, Capitulo IV, pág. 22, 2015

[3] Literal b, Articulo 39. Reglamento Europeo de Protección de Datos Personales. No. 679/2018

mejorar y mitigar los riesgos naturales derivados del tratamiento de la información personal.

e) Que es necesario mantener informada a la Alta Dirección de esta organización de las estrategias, planes de auditoría, resultados, riesgos y mejoras resultantes del deber de auditoría impuesto por la ley con el fin de garantizar la protección de los derechos de los titulares de los datos personales gestionados.
f) Que con ocasión de las obligaciones alrededor del Registro Nacional de Bases de Datos se establece la obligación de disponer de una política de auditoría de seguridad de la información personal[4]. En el caso de esta organización, considerando la existencia de una política de seguridad de la información se procede mediante esta norma a cumplir tal obligación, entendiendo que la misma cumple con la finalidad exigida por la autoridad al desarrollar la Política de Seguridad de la Información y Política de Privacidad adoptadas con esta organización.
g) Que es de suma relevancia en la celebración de contratos entre esta organización como Responsable y terceros proveedores en condición de Encargados del Tratamiento de datos personales, en los casos en que esto ocurra, que se pacte la obligación de auditoría que la ley exige a esta organización; debiendo tales terceros permitir y contribuir a la realización de las auditorias, incluidas las inspecciones en sitio que se consideren, sea que la auditoria la realice directamente o a través de un auditor externo autorizado por esta organización.
h) Que lo dispuesto en esta norma de auditoria en protección de datos, en lo que sea pertinente, constituye también criterios para que esta organización, a través del Oficial de Cumplimiento y área de auditoría, despliegue las funciones de investigación alrededor de los incidentes de seguridad de la información que involucre datos personales, sea que el mismo se presente bajo en control de esta organización como responsable o bajo el control de un Encargado del tratamiento de datos.
i) Que esta organización considerará relevante poner de presente a los destinatarios de esta norma que las autoridades de protección de datos a nivel internacional, en sus funciones de investigación realizan estas en forma de auditoría[5], tendencia que seguramente será adoptada por la SIC como autoridad de protección de datos personales.
j) Que es deber de todo colaborador de esta organización y/o prestador de servicios participar y coadyuvar en las auditorias que en materia de protección de datos personales se realicen de forma directa o a través de auditores

4 Manual de Usuario del Registro Nacional de Bases de Datos – RNBD. Numeral 5.9, pág. 61Versión 6.1. agosto de 2018
5 Literal b, Numeral 1, Articulo 58. Reglamento Europeo de Protección de Datos Personales. No. 679/2018

externos, nivel de cooperación que deberá quedar documentado en el informe de auditoría que sea presentado a la Alta Dirección de esta organización.

k) Que las prácticas de auditoría sirven como medida para evidenciar el cumplimiento y las mejoras continuas, en este caso aplicables a la protección de datos personales.

l) Que esta norma se adopta considerando las buenas prácticas en materia de auditoría, Guía de Responsabilidad Demostrada y estándares de seguridad de la información; las cuales constituyen criterios para fortalecer el compromiso en materia de protección de datos personales adoptado por esta organización.

2. OBJETIVO

Esta norma que desarrolla la Política de Seguridad de la Información de esta organización regula lo relacionado con la preauditoria y/o auditoria en materia de protección de datos personales, la cual tiene como objetivo determinar si la operación de esta organización cumple con las regulaciones derivadas del régimen de protección de datos personales como son las normas legales, principios aplicables al tratamiento de datos personales, prácticas de seguridad de la información establecidas en el Registro Nacional de Bases de Datos, normatividad interna adoptada por la organización a nivel de políticas y normas que desarrollan estas. El contexto mínimo desde el cual se debe analizar el cumplimiento debe tener en cuenta la Guía de Responsabilidad Demostrada que exige la adopción y funcionamiento de un Programa Integral de Datos Personales.

Este objetivo tiene como génesis la contribución y cooperación de la auditoria para que la organización gestione los riesgos de cumplimiento, de ahí la necesidad de que la auditoria aporte al fortalecimiento de las prácticas seguras en materia de protección de datos personales.

3. DESTINATARIOS

Son destinatarios de esta norma los colaboradores de todo nivel quienes respecto de los activos de información serán considerados custodios de estos en la medida que acceden y traten activos de información para el desempeño de las funciones contratadas. Igualmente, serán destinatarios todos aquellos que de acuerdo con la ley tengan el rol de Encargados del tratamiento de datos personales.

4. ELEMENTOS ESENCIALES

Las preauditorias y auditoria, internas y/o externas, en la instancia de responsable y/o del Encargado del tratamiento de datos personales deberán realizarse teniendo presente todos y cada uno de los elementos que a continuación se establecen:

4.1. OBJETIVIDAD

Los resultados de toda preauditoria y/o auditoria deben estar soportados en evidencia objetiva. El pre auditor y/o auditor deberá fundar sus resultados en evidencia objetiva; por tanto, no serán aceptables los informes que contengan hallazgos o conclusiones si la objetividad no está soportada y demostrada.

Es conveniente tener presente los siguientes conceptos:

Evidencia Objetiva. Aspectos probados mediante hechos que dan veracidad, obtenidos mediante observación, documentación, ensayo, medición, entrevista u otros medios que permitan contrastar lo afirmado con la realidad.

Hallazgos de preauditoria y/o auditoría. Son los resultados de la evidencia recolectada, analizada y evaluada durante la preauditoria y/o auditoria.

No Conformidad. Incumplimiento parcial o total de las normas legales vinculadas al régimen de protección de datos personales.

Recomendación. Es el consejo experto que entrega el pre auditor y/o auditor a la organización para fortalecer el cumplimiento en materia de protección de datos personales y/o mejorar el programa integral de datos personales adoptado, teniendo presente los principios de seguridad, legalidad y responsabilidad demostrada.

Lo anterior, sin perjuicio de otros criterios sobre objetividad que se desprendan de las técnicas de auditoría que adopte quien realice la auditoria.

4.2. INDEPENDENCIA

Quien realice la preauditoria y/o auditoria debe mantener independencia respecto de los auditados durante el proceso de preauditoria y/o auditoría, esto con el fin de preservar la objetividad.

Tratándose de auditorías internas o preauditorias, si existe alguna situación que genere duda a la organización o a terceros sobre la independencia en la actividad a realizar, es conveniente que se informe tal situación para efectos de mantener el compromiso con la objetividad y la independencia. En este sentido, es aconsejable documentar la declaración de independencia.

4.3. VISIÓN SISTÉMICA

Las preauditorias o auditorias, si bien pueden realizarse sobre asuntos puntuales en materia de protección de datos personales según las necesidades de la organización no puede omitir la visión sistémica de la protección de datos personales en la organización a la luz del principio de responsabilidad demostrada.

4.4. DOCUMENTACIÓN

La documentación de las preauditorias y auditorias es un requisito esencial que permite evidenciar y soportar los informes, requisito que debe tenerse presente desde la planeación, ejecución, cierre y seguimiento de la preauditoria y/o auditoría realizada; de allí la necesidad de conservar la información documental para efectos de demostrar no solo la realización de estas sino también el proceso de mejoramiento adoptado a partir de las recomendaciones resultantes de la preauditoria y/o auditoria.

4.5. PERIODICIDAD

Realizar preauditoria y/o auditorías en materia de cumplimiento en protección de datos personales es un deber legal como se expone en las consideraciones de esta norma. Si bien no se establece una periodicidad en la ley si es conveniente que se realice al menos una vez al año.

Esto sin perjuicio de las preauditorias que considere el Oficial de Cumplimiento, responsable de la Protección de Datos, realizar con el fin de mantener la mejora continua del Programa Integral de Datos Personales.

La periodicidad también podrá estar determinada por la gestión de los incidentes de seguridad de la información que involucren datos personales.

5. AMBITO DE APLICACIÓN DE LA PREAUDITORIA Y/O AUDITORIA

Las preauditorias y/o auditorias en materia de cumplimiento del régimen de protección de datos y del Programa Integral de Datos Personales aplicables a esta organización se realizarán respecto de los tratamientos de información personales que se realicen en los diferentes procesos organizacionales, sea que tales tratamientos se realicen solo por esta organización en condición de responsable y/o se realicen con apoyo de terceros proveedores en condición de Encargados del Tratamiento.

Así mismo, la preauditoria y/o auditoria en esta materia se realizará respecto de aquellos tratamientos que se realicen dentro del territorio nacional o fuera del territorio.

6. ELEMENTOS A AUDITAR

Serán objeto de preauditoria y/o auditoria en materia de cumplimiento del régimen de protección de datos personales la información personal tratada en:

- Instalaciones Físicas. Hace referencia a las instalaciones y/o archivos en los cuales se almacena la información en papel.

- Formato físico. Hace referencia a la información contenida en soporte papel.

- Sistemas de información. Hace referencia a los sistemas de información en los cuales se recolecta, procesa, trata y/o almacena información en soporte electrónico, como puede ser el software, hardware, redes y/o periféricos.
- Centro de datos. Hace referencia a las instalaciones en las cuales están ubicados los servidores que soportan los sistemas de información que tratan datos personales.

Para efectos de esta norma la preauditoria y/o auditoría tendrá como contexto el inventario de las bases de datos existente en la organización declaradas ante la SIC como autoridad de protección de datos personales.

Debe tenerse presente que la obligación de cumplimiento en materia de bases de datos personales también se extiende a las bases de datos tratadas por la organización en calidad de Encargado del tratamiento de datos personales.

7. SUJETOS INTERVINIENTES

7.1. RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES

GASES DEL CARIBE como responsable del tratamiento de datos personales tiene la obligación de dar cumplimiento al régimen legal vigente en esta materia, así como el deber de adoptar y mantener vigente el Programa Integral de Datos Personales basado en riesgo que surge del Principio de Responsabilidad Demostrada.

Esta organización, a través del Oficial de Cumplimiento, coordinará con los procesos que tratan datos personales las preauditorias a realizarse, siguiendo las fases indicadas en la guía de auditoria en materia de protección de datos personales.

Las auditorias serán coordinadas de forma conjunta entre el Departamento digital, el Oficial de Cumplimiento y el Departamento de Auditoria.

7.2. RESPONSABLE DE LA SEGURIDAD Y DE LA PROTECCIÓN DE DATOS

En esta organización la seguridad de la información y de la protección de datos personales está en cabeza del equipo de apoyo conformado por la Coordinación de SGI- Sistema de Gestión Integral, la Dirección Digital, Oficial de Cumplimiento, Coordinación de Gestión Documental y Coordinación de Seguridad Física, en lo que a sus funciones corresponde.

7.3. ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES

Los terceros proveedores que, por cuenta de esta organización, en virtud de una relación contractual y/o legal, traten datos personales en poder de esta organización como responsable del tratamiento de datos, en virtud de la obligación de auditoria pactada en los contratos u ordenes de servicios originadas en ofertas, tienen el deber de facilitar la realización de las preauditorias y/o auditorias.

Es obligatorio que respecto de cada proveedor que como Encargado trata datos personales se mantenga actualizado el nombre del Oficial de Privacidad por ellos designado o en su defecto la persona de esa organización que tenga a cargo las funciones de líder de la protección de datos personales. En caso de no existir, el contacto con el Encargado debe darse directamente con el representante legal o empresario.

Esta organización entiende que, cuando actúa como Encargado del tratamiento de datos personales que realice bajo este rol, queda obligada al deber de auditoría que tienen los responsables del tratamiento de datos personales con los cuales exista una relación contractual y/o legal con GASES DEL CARIBE.

7.4. AUDITOR EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Según los objetivos y el alcance de la auditoria a realizarse podrá determinar que exista un equipo de auditoría a cargo de esta; caso en el cual, deberán estructurarse las funciones del equipo que intervenga en esta actividad.

Quien realice la auditoria en materia de protección de datos deberá, en aras de la objetividad, visión sistémica y responsabilidad demostrada, tener conocimientos suficientes y experiencia acreditada en los siguientes campos:

- Ámbito Jurídico de la Protección de Datos Personales. Conocimiento del régimen legal en materia de protección de datos personales, jurisprudencia constitucional y buenas prácticas internacionales en materia de protección de datos personales.
- Ámbito Informático. Conocimientos en sistemas de información y en seguridad de la información.
- Ámbito de la Auditoria. Conocimientos y/o experiencia en fundamentos y técnicas auditoria aplicables a los temas objeto de estas.

Estos requisitos serán exigidos en menor medida para quien realice de forma interna las preauditorias, pero si tal labor es contratada con un tercero este deberá cumplir con las competencias mencionadas en este numeral.

Acreditar tales competencias es vital en la medida que la auditoria solo será eficaz siempre que exista un conocimiento de esta actividad en materia de protección de datos personales.

7.5. ENTREVISTADOS

Las personas entrevistadas en la preauditoria y/o auditoria constituyen una de las principales fuentes de información para establecer el cumplimiento del régimen de protección de datos personales. De ahí la importancia de que el preauditor y/o auditor tenga objetivos concretos y previos a la realización de esta con el fin de conducir una conversación orientada al objetivo definido de la auditoria.

Es importante en la selección de los entrevistados involucrar a personal de los diferentes niveles de la organización que realicen diferentes tratamientos de datos personales.

7.6. USUARIOS

Otra fuente de información relevante para el preauditor y/o auditor se encuentra en los usuarios, diferentes a los entrevistados, de la organización que realizan diversos tratamientos de datos personales en formato físico y/o automatizado; de quienes a partir de técnicas como la observación y/o muestreo de la aplicación de las medidas de seguridad administrativas, físicas y/o tecnológicas permiten al auditor obtener evidencia objetiva sobre el cumplimiento del régimen de protección de datos personales y de la eficacia del Programa integral de datos personales adoptado por la organización.

8. FASES DE LA AUDITORIA

En la planificación de toda actividad de preauditoria y/o auditoria es necesario que la misma involucre cinco (5) momentos claramente diferenciables, a saber:

i. **Inicio.** Esta fase parte de la decisión de realizar una preauditoria y/o auditoria. En este sentido, se establecerán los parámetros a considerar en la auditoria a encargar y/o contratar.
ii. **Planeación**. Esta fase comprende la planificación estratégica, administrativa y técnica de la preauditoria y/o auditoria a ejecutar.
iii. **Ejecución.** Esta fase comprende la ejecución del plan de la preauditoria y/o auditoria, la recolección de la evidencia y despliegue de las técnicas de auditorías determinadas por el responsable de la ejecución de estas.

iv. **Conclusión y Revisión.** Esta fase comprende la revisión del plan de preauditoria y/o auditoria ejecutado, organización de la información, análisis de la evidencia, determinación de las recomendaciones, construcción del informe a presentar y distribución del informe.

v. **Cierre.** Esta fase comprende la aprobación del informe presentado, almacenamiento y conservación histórica de las auditorias desarrolladas para fines de responsabilidad demostrada del deber de auditoría.

9. SEGUIMIENTO A LAS RECOMENDACIONES

La importancia de la preauditoria y/o auditoria no se agota en esta y en el respectivo informe que contiene las recomendaciones. La trascendencia de la preauditoria y/o auditoria es, a partir del estado de cumplimiento identificado, incorporar las recomendaciones del auditor con el fin de fortalecer el cumplimiento en materia de protección de datos personales y el programa integral de datos personales existente en la organización.

10. CONSERVACION DE INFORMES

Como parte de la aplicación del principio de responsabilidad demostrada corresponde a esta organización conservar prueba de las preauditorias y/o auditorías realizadas incluidos sus soportes, así como de la adopción de las recomendaciones formuladas. Esta información hará parte de la información gestionada por las respectivas áreas responsables de la protección de datos personales en esta organización. Esta información se conservará bajo los criterios de retención documental que defina la organización considerando que la misma hace parte de la información empresarial.

11. CONTROL

Este documento deberá revisarse de manera periódica con el fin de realizar las actualizaciones que se consideren necesarias cuando surja un cambio importante.

12. USO EXCLUSIVO

Este documento es de uso exclusivo de Gases del Caribe S.A. E.S.P. y se prohíbe su uso a terceros no autorizados.

13. APROBACION DE ESTA POLITICA

Este documento fue aprobado teniendo en cuenta las actividades descritas en el procedimiento de Normalización y Control de Documentos y Registros PD-A-11 y se encuentra publicado en la Red de Documentos de Gases del Caribe SA ESP