NORMA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

GASES DEL CARIBE, en su compromiso con la seguridad de la información considera indispensable establecer los parámetros que permitan gestionar los eventos o incidentes que tengan el potencial de comprometer la seguridad de los activos de información gestionados por esta organización, en especial el relativo a la protección de datos personales, sin que ello excluya la gestión de incidentes que afecten otros activos de información

1. CONSIDERANDOS

a) Que de conformidad con lo dispuesto en el numeral 2.1. de la NTC/ISO 27002 sobre buenas prácticas de seguridad de la información se entenderá como Activo "*Cualquier cosa que tenga valor para la organización*".

b) Que el Glosario de Términos de Seguridad de la Información denominado NISTIR 7298 de mayo 2013, promulgado por Instituto Nacional de Estándares y Tecnologías (NIST) de los Estados Unidos, define Información como "*Cualquier comunicación o representación del conocimiento como hechos, datos u opiniones en cualquier medio o forma, incluyendo textual, numérico, gráfico, cartográfico, narrativa, o audiovisual."*

c) Que la norma ISO 27001, versión 2013, en el dominio A.16. relativo a la Gestión de los Incidentes de Seguridad establece como objetivo el reporte de aquellas situaciones de peligro o riesgos que puedan comprometer la seguridad de los activos de información y/o de los sistemas, a través de los cuales se gestionan estos, con el fin de adoptar las acciones correctivas de forma pertinente y oportuna.

d) Que de conformidad con la Ley Estatutaria 1581 de 2012 se estableció la obligación que tienen las organizaciones, públicas y/o privadas, que tratan datos personales en condición de responsables y/o Encargados, de gestionar y notificar a la Superintendencia de Industria y Comercio (SIC) como autoridad de protección de datos personales en Colombia toda violación a los códigos de seguridad que comprometan datos personales, tal como se desprende de los artículos 17 y 18 de la mencionada ley.

e) Que la Guía de Responsabilidad Demostrada expedida por la SIC en 2015 establece la necesidad de que quienes tratan datos en condición de responsables y/o Encargados dispongan de "*un procedimiento y una persona o área responsable de manejar los incidentes o vulneraciones a los sistemas de información donde se gestionan datos personales y a los archivos físicos. Así*

mismo, es preciso que prevean los mecanismos para rendir informes internos y reportar los incidentes a los titulares y a esta Superintendencia".

f) Que de acuerdo con el marco reglamentario del régimen de protección de datos personales es obligatorio reportar como novedades a la SIC la información vinculada a la gestión de incidente de seguridad que comprometa datos personales dentro de los quince (15) días siguientes al conocimiento que tuvo la organización de esta situación.

g) Que es obligación de toda persona como colaborador, prestador de servicio, proveedor y/o dependiente de estos, comunicar a GASES DEL CARIBE a través del área responsable de la protección de datos personales y su respectivo canal formal definido, los eventos y/o incidentes que generen peligro para el cumplimiento del deber de seguridad que tiene esta organización en relación con los activos de información gestionados, en especial con los datos personales tratados en condición de responsable o encargado.

h) Que la protección de los activos de información será posible en la medida que las situaciones de peligro, eventos o incidentes de seguridad sean comunicados a esta organización, una vez se tenga conocimiento de estos, cualquiera que fuere el medio.

i) Que de acuerdo con la mencionada norma ISO, en su dominio A.18, la gestión de la seguridad de la Información debe caracterizarse por el cumplimiento de los requisitos de ley y contractuales, con el fin de evitar violaciones a estos, previniendo así la materialización de riesgos reputacionales, financieros y operativos; así como eventuales perjuicios derivados del incumplimiento del régimen de protección de datos personales y principios aplicables al tratamiento de la información personal.

j) Que considerando las disposiciones legales vigentes en Colombia en relación con los activos de información y seguridad de la información es indispensable considerar tales criterios objetivos con el fin de guiar la gestión de los incidentes de seguridad de la información.

Con base en las anteriores consideraciones se establecen los parámetros que habrán de regular la gestión de los incidentes de seguridad de la información en GASES DEL CARIBE.

2. OBJETO

Este inciso para la gestión de incidentes de seguridad busca regular las situaciones que comprometan datos personales u los activos de información de esta organización respecto los cuales la organización tiene el deber de proteger.

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.

4. DEFINICION DE EVENTOS Y/O INCIDENTES

Para efectos de la gestión de aquellas situaciones que puedan poner en peligro la seguridad de los activos de información que gestiona esta organización deben tenerse en cuenta los siguientes conceptos tomados de la Norma ISO 27000:

- **Evento de Seguridad de la Información**. Consiste en la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles, o una situación previamente desconocida que puede ser pertinente para la seguridad de la información.
- **Incidente de Seguridad de la Información**. Consiste en un solo evento o serie de eventos inesperados o no deseados respecto de la seguridad de la información que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Los incidentes de seguridad de la información que puedan comprometer datos personales u otro tipo de activos de información pueden presentarse a nivel físico y/o digital, siendo necesario dentro de la visión holística abordar ambas dimensiones del incidente.

5. TIPOLOGIA DE EVENTOS Y/O INCIDENTES DE SEGURIDAD

Los eventos e incidentes de seguridad pueden comprender de forma enunciativa situaciones y/o hechos en relación con el hardware, redes, sistemas de información, instalaciones físicas, activos de información o personas. De forma enunciativa los incidentes pueden presentarse en alguna de las siguientes seis (6) dimensiones.

5.1. HARDWARE. El incidente podría presentarse a nivel de:

- Mal Funcionamiento de Hardware
- Perdida de equipos o medios
- Daños en el hardware

5.2. SISTEMAS DE INFORMACIÓN. El incidente podría presentarse a nivel de:

- Violaciones del Acceso
- Códigos maliciosos
- Violaciones a la confidencialidad, integridad o disponibilidad
- Uso inadecuado o no autorizado de los sistemas de información
- Errores producidos por datos incompletos o inexactos
- Mal Funcionamiento a nivel de Software
- Cambios no controlados en los sistemas de información
- Perdida del servicio
- Mal funcionamiento o sobrecargas de los sistemas de información

5.3. REDES. El incidente podría presentarse a nivel de:

- Cambios en la configuración de la arquitectura de seguridad informática.
- Realización de pruebas de penetración sin autorización del área de digital.
- Habilitación de accesos remotos sin autorización.
- Mantener vigentes accesos remotos no existiendo relación jurídica vigente.

5.4. INSTALACIONES FÍSICAS. El incidente podría presentarse a nivel de:

- Violaciones de los acuerdos de seguridad física.
- Accesos no autorizados a los centros de cómputo.
- Accesos no autorizados a áreas de trabajo restringido.
- Accesos no autorizados a las oficinas de personal directivo.

5.5. ACTIVOS DE INFORMACIÓN. El incidente podría presentarse a nivel de:

- Incumplimientos de la Política de Seguridad, incluidas las normas que desarrollan esta política.

- Tratamientos de datos que infringen las medidas de seguridad físicas, lógicas y/o administrativas.
- Infracción a los principios que rigen el tratamiento de datos personales.
- Usos no honestos o contrarios a la ley y/o al contrato respecto de activos de información, entre ellos, datos personales.

5.6. PERSONAS. El incidente podría presentarse a nivel de:

- Errores humanos.
- Ataques de ingeniería social.
- Permisos no autorizados a terceros que comprometan la confidencialidad de la información, disponibilidad o integridad de la información.
- Usos no honestos de la información.

6. SUJETOS A CARGO DE LA GESTION DE INCIDENTES

La obligación de gestionar incidentes de seguridad que comprometan datos personales es una obligación que tiene esta organización cuando realice tratamiento de datos en condición de responsable y/o Encargado.

6.1. ENCARGADOS DEL TRATAMIENTO DE DATOS EN RELACIÓN CON GASES DEL CARIBE COMO RESPONSABLE

Todo proveedor de esta organización que trate datos personales en condición de encargado del tratamiento tiene la obligación legal y contractual de adoptar sus propios protocolos para gestionar los incidentes de seguridad que comprometan información personal para cumplir con lo dispuesto en el régimen de protección de datos personales.

La obligación de gestionar los incidentes de seguridad respecto de activos de información diferentes a datos personales tiene fundamento en el deber de cumplir las obligaciones de ley y los principios generales de buena fe, lealtad contractual, deber de prevención y deber de información exigidos a los empresarios y/o directivos de organizaciones privadas y/o públicas.

El Oficial de Cumplimiento o quien tenga asignada tales funciones deberá coordinar la gestión del incidente dentro de su organización y será la persona de contacto con las áreas responsables del tratamiento de datos personales de GASES DEL CARIBE para estos fines.

6.2. GASES DEL CARIBE COMO RESPONSABLE

La seguridad de la información es una obligación que adquiere y debe cumplir cada colaborador de esta organización que realice en el desempeño de sus funciones cualquier tratamiento de datos personales y/o respecto de otros activos de información.

En esta organización la gestión de incidentes de seguridad de la información estará liderada por el departamento que detecte el incidente de seguridad, el cual será uno de los siguientes, Dirección Digital, Coordinación SGI, Coordinación de seguridad física, Coordinación de Gestión Documental y/o Oficial de cumplimiento, en lo que a sus funciones corresponde y deberá ser apoyada por aquellos Departamentos y/o Servicios a los que este departamento requiera. El área líder del respectivo incidente informará a la Alta Dirección de los resultados de la gestión del incidente con el fin de adoptar las decisiones del caso.

El Oficial de Cumplimiento, responsable del tratamiento de datos personales de esta organización, será notificada de todo incidente de seguridad de la información que comprometa datos personales, quienes además coordinará la investigación, análisis y gestión de este. Igualmente, deberá ser consultado respecto de las respuestas que en materia de Habeas Data deban darse a los titulares de la información personal originadas en consultas y/o reclamos de estos.

6.3. ENTIDADES USUARIAS DE LA INFORMACION PERSONAL

La obligación de gestionar incidentes de seguridad de la información que involucre activos de información tratados por esta organización como responsable y/o Encargado aplica para todas las entidades del sector público a las cuales esta organización haya suministrado información en cumplimiento de obligación de ley.

Estas entidades públicas, que, como usuarias de la información al acceder a los datos personales en poder de esta organización en virtud del principio de legalidad, adquieren la condición de responsable del tratamiento y por tanto quedan obligadas no solo a cumplir el régimen de protección de datos personales sino también a actuar en el marco de la buena fe, deber de prevención y deber de diligencia.

El Oficial de Cumplimiento de la entidad pública o quien tenga asignadas tales funciones deberá coordinar la gestión del incidente dentro de su organización y será la persona de contacto con las áreas responsables del tratamiento de datos personales de GASES DEL CARIBE para estos fines.

7. PERSPECTIVA JURIDICA DEL INCIDENTE DE SEGURIDAD

De conformidad con la obligación legal a cargo de los responsables y/o Encargados del tratamiento de datos de gestionar los incidentes de seguridad de la información que comprometan datos personales resultantes de violaciones a las medidas de seguridad de nivel físico, administrativo y/o tecnológico se deberán tener presentes los siguientes parámetros.

7.1. DEBER DE INFORMACIÓN.

Una vez que cualquier colaborador de esta organización tenga sospecha o sea informado a través de cualquier medio escrito, oral o electrónico de un eventual incidente de seguridad que tenga el potencial o haya generado peligro para el titular de la información personal deberá informar por escrito a través del canal de Habeas Data esta situación con el fin de dar inicio a la gestión del incidente de seguridad. El correo electrónico de protección de datos es: habeasdata@gasesdelcaribe.com.

7.2. DEBER DE COOPERACIÓN.

Todos los colaboradores de cualquier nivel tienen el deber de cooperar con el Oficial de Cumplimiento, responsable del tratamiento de datos personales, con el fin de suministrar a este la información requerida para que esta organización pueda cumplir con la obligación legal de gestionar el incidente.

El Oficial de Cumplimiento coordinará con los Departamentos y/o Servicios de esta organización involucrados con el incidente los aspectos administrativos necesarios para la gestión del incidente de seguridad, independiente de que de forma temprana exista certeza o no del compromiso de datos personales, pues solo será posible al final de la correspondiente gestión del incidente determinar esta situación y el grado de compromiso que resultase.

7.3. DEBER DE SOLIDARIDAD.

Todo Encargado del tratamiento de datos personales respecto de la información personal entregada por esta organización para la ejecución del objeto contratado, tiene el deber de informar al Oficial de Cumplimiento, responsable del tratamiento de datos personales de esta organización, a través de los canales de habeas data y dentro del término de la distancia, la sospecha u ocurrencia de un incidente de seguridad que comprometa o haya comprometido los datos personales entregados para su tratamiento en el

marco del contrato existente. En consecuencia, el proveedor encargado del tratamiento de datos personales deberá gestionar tal incidente por su cuenta y riesgo, debiendo suministrar toda la información del incidente a esta organización con el fin de cumplir con la obligación legal de reportar este ante la Superintendencia de Industria y Comercio como autoridad de protección de datos, siguiendo para ello los pasos indicados en el acápite de Reporte de Novedades contenido en el Manual de Usuario del Registro Nacional de Bases de Datos vigente que puede consultarse en la SIC.

Debe recordarse que el régimen de protección de datos personales vigente en Colombia prevé la solidaridad entre el responsable y el Encargado en materia sancionatoria. El incumplimiento de la obligación legal de gestionar el incidente de seguridad de la información que comprometa datos personales será evaluado por esta organización a la luz del régimen de responsabilidad civil.

7.4. DEBER DE PREVENCIÓN.

Corresponde a esta organización como responsable y/o Encargado del tratamiento de datos personales que realice, así como a los proveedores Encargados del Tratamiento de datos personales, adoptar las medidas de seguridad físicas, administrativas y/o tecnológicas necesarias para mitigar los riesgos y/o perjuicios que puedan causarse a los titulares de los datos personales comprometidos y/o demás terceros afectados por el incidente de seguridad y/o su gestión.

7.5. DEBER DE RENDIR CUENTAS.

El Oficial de Cumplimiento informará a la Alta Dirección de esta organización el inicio, gestión y cierre del incidente de seguridad, esto con el fin de que la Alta Dirección de instrucciones.

7.6. ASPECTOS JURÍDICOS, TECNOLÓGICOS Y CRIMINALÍSTICOS DE LOS INCIDENTES DE SEGURIDAD.

Considerando que un incidente de seguridad de la información puede experimentarse a nivel físico, administrativo y/o tecnológico es necesario considerar en su gestión los aspectos forenses vinculados a la recolección de evidencia digital y/o física, los aspectos criminalísticos orientados a garantizar la integridad, confidencialidad y disponibilidad de los elementos materiales probatorios que lo caractericen siendo para ello necesario tener presentes las buenas prácticas en materia de cadena de custodia.

En este orden de ideas, esta organización gestionará el incidente de seguridad con base en esta norma y los procedimientos que la desarrollan.

7.7. INFORME DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN.

Según las características del incidente de seguridad, el informe de este podrá estar complementado por un dictamen generado por el perito forense que recolectó y analizó la evidencia del mismo, así como por un informe jurídico respecto de las repercusiones legales del incidente, conforme los hallazgos y características del mismo.

Las repercusiones jurídicas del incidente de seguridad podrán ser analizadas a la luz de las normas constitucionales, laborales, comerciales, civiles, administrativas y/o penales.

7.8. DEBER DE REPORTAR EL INCIDENTE ANTE LA AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES.

Si resultado de la gestión del incidente de seguridad de la información se establece que este, conforme a los hallazgos recolectados, investigados y analizados, comprometió datos personales entregados a esta organización para su custodia en ejecución de su objeto, se procederá a preparar el reporte conforme las exigencias establecidas por la Superintendencia de Industria y Comercio como autoridad en esta materia.

Debe tenerse presente que la autoridad de protección de datos tendrá la posibilidad de oficio o a petición de alguna de las partes de evaluar la forma como se gestionó el incidente, así como toda la evidencia recolectada con el fin de verificar si el reporte de este es fiel a los hallazgos, análisis y conclusiones obtenidas de la gestión realizada. En este sentido, debe tenerse presente que la SIC podrá en ejercicio de su facultad de investigación acceder a toda la evidencia recolectada y respectivo análisis, lo cual realizará a través de sus funcionarios y peritos de su departamento de investigación forense.

7.9. REPORTE DEL INCIDENTE ANTE LA SIC.

La organización, con el apoyo de las áreas responsables del tratamiento de datos personales, auditoria y demás departamentos involucrados en el incidente de seguridad, presentarán a la alta dirección el resumen del incidente con el fin de proceder al cumplimiento de esta obligación de ley.

Para efectos de la declaración ante la SIC, este reporte deberá al menos contener lo siguiente: (a) Base de datos personales comprometida; (b) número de titulares o personas en riesgo por el compromiso de sus datos personales; (c) Identificación del Encargado, si esto aplicaré; (d) concepto del incidente; (e) tipo de información personal comprometida; (f) Fecha de reporte; (g) Fecha del conocimiento del incidente; y demás información que sea requerida por la autoridad.

No obstante, los requisitos mínimos del reporte es posible que, dependiendo de las características del incidente, la información vinculada a este sea mayor.

Debe tenerse presente que el término para reportar el incidente de seguridad de la información que ha comprometido datos personales, según el régimen de protección de datos vigente es de quince (15) días.

En este orden de ideas, si dentro del término de los quince (15) días siguientes al conocimiento de un evento de seguridad respecto del cual exista duda razonable sobre un posible carácter de incidente se aplicará lo dispuesto en el siguiente numeral.

Por último debe tenerse presente que respecto de los incidentes de seguridad que comprometan datos personales la ley 1581 de 2012, en sus artículo 17 (literal n) y 18 (literal k) aplicable a Responsables y Encargados respectivamente, indica que los incidentes que deben reportarse deben considerar dos (2) condiciones, a saber: (ii) la violación de los controles de seguridad que afecten los atributos de integridad y/o confidencialidad y/o disponibilidad respecto de datos personales, y (ii) que existan riesgos en la administración de la información de los titulares, caso este último, que establece valorar el riesgo de daño para los titulares de los datos personales cuya información fue comprometida en un incidente de seguridad.

7.10. PROCEDIMIENTO DE REPORTE DEL INCIDENTE ANTE LA SIC

El área responsable de la protección de datos personales que en GASES DEL CARIBE, en este caso el oficial de cumplimiento y el responsable de la seguridad de la información cuando se presente un evento de seguridad de la información que tenga alta potencialidad de adquirir el carácter de incidente, esto es, exista evidencia razonable de compromiso de integridad, disponibilidad y/o confidencialidad de los datos personales de algún titular, procederá en cumplimiento del deber de prevención a reportar ante la SIC tal situación.

Esto deberá hacerlo dentro de los quince (15) días hábiles siguientes al momento en que la organización tuvo conocimiento del evento y razonable

evidencia del potencial carácter de incidente de seguridad, término legal establecido en el régimen de protección de datos personales.

Para el efecto del reporte se deberá ingresar al RNBD de la SIC con el fin de realizar el reporte preventivo del potencial incidente de seguridad de la información que tiene el riesgo de comprometer datos personales. En el campo dispuesto para la descripción del incidente se realizará la descripción de la situación, indicando en la parte final de la descripción, que el reporte que se realiza se predica de un potencial evento que podría adquirir el carácter de incidente de seguridad, adicionando que se realiza el reporte en cumplimiento del deber de prevención. Así mismos, se indicará que se ha iniciado el proceso de investigación con el fin de establecer de manera objetiva si la situación reportada comprometió o no datos personales.

Realizado el reporte aquí mencionado, las conclusiones de la investigación del evento de seguridad cuando este adquiera el carácter de incidente de seguridad, serán informadas a la SIC para confirmar a la SIC la materialización del riesgo respecto de los datos personales. En caso, de que la investigación conduzca a establecer que no hubo compromiso de datos personales, de igual forma en cumplimiento del deber de información se comunicará que el evento no comprometió datos personales.

Lo dispuesto en los incisos anteriores aplicará cuando las conclusiones de la investigación no se puedan obtener dentro de los quince (15) días siguientes al conocimiento del evento.

En caso de que las conclusiones de la investigación respecto de la existencia de un incidente de seguridad se logren obtener dentro del término de quince (15) días se procederá conforme lo dispuesto en el numeral anterior.

7.11. NOTIFICACION A LOS TITULARES

En aquellos incidentes de seguridad de la información que comprometan datos personales de los titulares que hagan parte de cualquiera de los grupos de interés en los cuales GASES DEL CARIBE tenga la calidad de responsable o Encargado deberá evaluarse el riesgo en la administración de los datos de estos, con el fin de establecer la necesidad de notificar a estos el compromiso de datos personales con el fin de que estos adopten las medidas que consideren pertinentes.

Para efectos de evaluar los riesgos para los titulares se tendrá presente, en cada caso particular, el tipo de incidentes de seguridad; el tipo de atributo de información afectado; el tipo de datos personal; el tipo de derecho fundamental afectado; el tipo de daño que pueda experimentar el titular; el tipo de control o código de seguridad vulnerado; las características del titular del datos y/o grupo

familiar; repercusiones jurídicas del incidente, sin perjuicio de otros criterios que deban ser considerados según las característica del incidente.

En caso de existir riesgos deberá informarse de manera particular a cada titular la existencia de un incidente de seguridad que comprometió sus datos personales indicando la información que llegase a ser necesaria para que estos adopten medidas de contención con el fin de mitigar las situaciones dañinas a sus intereses.

La notificación deberá realizarse sin dilación a los titulares, eso sí fundada en razones objetivas, resultantes de la evaluación mencionada.

En caso de que no existan riesgos objetivos en la administración de datos, no se necesitaría la notificación, esto siempre precedido de la debida evaluación del riesgo.

7.12. PLAN DE MEJORAS A PARTIR DEL INCIDENTE DE SEGURIDAD.

La propia dinámica de la presencia de las Tecnología de la Información en la operación empresarial incrementa los riesgos respecto de los activos de información, uno de estos la información personal que gestiona la organización como responsable y/o Encargado. Un efecto natural del incidente es fortalecer la gestión de la seguridad de la información respecto de los activos de información, motivo por el cual, deberá a la luz de los riesgos materializados fortalecer las acciones y medidas de seguridad que hacen parte del Programa Integral de Datos Personales teniendo presente el principio de responsabilidad demostrada.

8. CONTROL

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

9. 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.

10. 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