

# NORMA DE RELACIÓN CON PROVEEDORES

## CONTENIDO

1.	CONSIDERANDOS .....	2
2.	OBJETO.....	3
3.	DESTINATARIOS.....	3
4.	PROVEEDOR Y TERCEROS QUE PARTICIPAN EN LA RELACION CONTRACTUAL .	4
5.	SEGURIDAD DE LA INFORMACION EN LA RELACION CON PROVEEDORES.....	4
6.	MONITOREO, REPORTE Y AUDITORIA .....	10
7.	CONTROL.....	11
8.	USO EXCLUSIVO .....	11
9.	APROBACION DE ESTA POLITICA.....	11

---

	<b>NORMA DE RELACIÓN CON PROVEEDORES</b>	<b>CÓDIGO:</b>	OD-04-PD-A-35
		<b>VERSIÓN:</b>	1
		<b>FECHA:</b>	24/04/2023
		<b>PÁGINA:</b>	2 de 11

GASES DEL CARIBE, en su compromiso con la protección de la información que gestiona considera de importancia esencial establecer las reglas que permitan mantener el esquema de seguridad de la información adoptado por esta Organización cuando terceros proveedores, en virtud de una relación contractual o legal, deban acceder a determinados 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.15. relativo a la Relación con Proveedores establece como objetivo Asegurar la protección de los activos de información que necesariamente sean requeridos por terceros proveedores como contratistas u otros terceros.
- d) Que es necesario identificar los riesgos que sobre la información y/o los sistemas de información cuando terceros proveedores accedan a estos en el marco de un contrato; salvo que se justifique de manera objetiva omitir tal previsión.
- e) Que una vez identificados los riesgos sobre tales activos de información deben evaluarse estos con el fin de adoptar los controles necesarios para su protección, los cuales deberán ser acogidos de forma obligatoria por el proveedor de GASES DEL CARIBE que deba acceder a estos.
- f) Que los activos de información tendrán dentro de esta Organización un “Propietario” responsable de garantizar que los terceros proveedores que provean servicios a sus procesos cumplan con las obligaciones consignadas en este anexo y las demás plasmadas en el respectivo contrato; así mismo será responsable de identificar nuevos riesgos, evaluarlos y proponer los controles requeridos para preservar la seguridad sobre los mismos.
- g) Que es fundamental para la debida protección de los activos de información de GASES DEL CARIBE que los terceros proveedores que accedan a estos en virtud de la relación contractual tengan las competencias para gestionar los incidentes que puedan comprometer su seguridad, teniendo presente el tipo de activo comprometido de acuerdo con la clasificación de la información definida por GASES DEL CARIBE.



## NORMA DE RELACIÓN CON PROVEEDORES

<b>CÓDIGO:</b>	OD-04-PD-A-35
<b>VERSIÓN:</b>	1
<b>FECHA:</b>	24/04/2023
<b>PÁGINA:</b>	2 de 11

- h) Que los terceros proveedores de GASES DEL CARIBE deben garantizar el cumplimiento de las disposiciones legales aplicables a los activos de información en poder de GASES DEL CARIBE, así como aquellas normas internas adoptadas en materia de seguridad de la información por esta Organización.
- i) Que lo dispuesto en materia de seguridad de la información y consecuentes obligaciones que surgen para los proveedores que traten activos de información como datos personales u otros, deberán ser considerados y alineados en el manual de contratación de la organización.

Con base en las anteriores consideraciones se procede a fijar las reglas aplicables a la relación con terceros proveedores que en calidad de contratistas acceden a activos de información propiedad de GASES DEL CARIBE o entregados para su custodia.

### 2. OBJETO

Esta Norma que desarrolla la Política de Seguridad de la Información de GASES DEL CARIBE tiene como objetivo asegurar la protección de los activos de información propiedad de GASES DEL CARIBE y/o entregados para su custodia, por parte de aquellos terceros contratistas que deben acceder y/o realizar cualquier tratamiento o gestión de estos en el marco de una relación contractual o legal.

### 3. DESTINATARIOS

Son destinatarios de esta norma todos los empleados de todo nivel quienes, respecto de los activos de información, serán considerados custodios de estos, en la medida que acceden y tratan activos de información para el desempeño de las funciones contratadas.

Igual serán considerados custodios, aquellos terceros que, en condición de proveedores, accedan y traten activos de información en poder de esta organización; así como aquellos terceros que, en virtud de una relación legal, estatutaria y/o contractual, deban tratar tales activos.

Los custodios tienen la responsabilidad de gestionar de forma segura los activos de información que traten de forma temporal o permanente en virtud de la relación legal y/o contractual existente.

	<b>NORMA DE RELACIÓN CON PROVEEDORES</b>	<b>CÓDIGO:</b>	OD-04-PD-A-35
		<b>VERSIÓN:</b>	1
		<b>FECHA:</b>	24/04/2023
		<b>PÁGINA:</b>	2 de 11

#### **4. PROVEEDOR Y TERCEROS QUE PARTICIPAN EN LA RELACION CONTRACTUAL**

En cada relación jurídica con un tercero que involucre activos de información como datos personales u otros, sea durante la fase precontractual o contractual, es conveniente establecer si existen otros terceros que en condición de Sub Encargados del tratamiento de datos participen o llegaren a participar.

En estos casos, tales terceros deberán ser identificados de forma plena y a ellos les será exigible lo dispuesto para los terceros proveedores en materia de protección de datos personales y/o en seguridad de la información, según la criticidad de los activos de información que estos gestionen.

#### **5. SEGURIDAD DE LA INFORMACION EN LA RELACION CON PROVEEDORES**

Para fines de mantener la seguridad de la información en la relación con terceros proveedores deberán seguirse las siguientes reglas:

##### **5.1. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN NECESARIOS PARA LA CELEBRACIÓN Y EJECUCIÓN DEL CONTRATO.**

En la fase previa de planeación de un contrato con un proveedor deberán identificarse por esta organización los activos de información involucrados en la ejecución del mismo. Esto con el fin de identificarlos, documentar y controlar la debida gestión por parte del proveedor que debe necesariamente acceder y/o tratar estos para la correcta ejecución del objeto contratado. En la definición de los activos a involucrar en la ejecución se aplicará el principio del mínimo necesario.

##### **5.2. IDENTIFICACIÓN DE RIESGOS Y ADOPCIÓN DE CONTROLES SOBRE LOS ACTIVOS DE INFORMACIÓN ACCESIBLES POR TERCEROS**

Identificados los activos de información necesarios para la ejecución del contrato se procederá por el Propietario del activo y el Departamento beneficiario del contrato a identificar y evaluar los riesgos que puedan comprometer la seguridad de estos; a partir de tales riesgos se adoptaran las medidas de seguridad de naturaleza administrativa, física y/o tecnológicas que permitan preservar la seguridad del activo de información. Estas medidas de seguridad deberán ser documentadas y harán parte de la documentación contractual.



## NORMA DE RELACIÓN CON PROVEEDORES

<b>CÓDIGO:</b>	OD-04-PD-A-35
<b>VERSIÓN:</b>	1
<b>FECHA:</b>	24/04/2023
<b>PÁGINA:</b>	2 de 11

Los riesgos se evaluarán de acuerdo con la metodología que defina GASES DEL CARIBE, atendiendo la naturaleza del activo y su respectiva clasificación. En principio se abordarán los riesgos en materia de información y de forma gradual se extenderá a los demás activos de información que se consideren necesarios acorde con los objetivos estratégicos de la organización.

Dentro de los riesgos a identificar deberán considerarse si el tercero proveedor respecto del activo de información requiere:

- a) Acceso físico.
- b) Acceso a los sistemas de información y las características del mismo.
- c) Conexión en sitio a la red de GASES DEL CARIBE.
- d) Conexión remota a los sistemas de GASES DEL CARIBE.

De conformidad con tales riesgos el tercero proveedor deberá especificar en detalle, según la naturaleza del activo de información clasificado acorde a los parámetros definidos por GASES DEL CARIBE, lo relacionado con:

- Medios y controles que aplicará para la protección
- Prácticas y procedimientos para gestionar eventuales incidentes de seguridad, incluyendo la minimización del impacto y la recuperación de la normal operación.
- Compromiso de cumplir con los requisitos legales o internos que deben aplicarse según el activo de información identificado
- Forma como responderá por los eventuales perjuicios a terceros afectados por un eventual incidente de seguridad de la información.

### **5.3. ABORDAJE DE LA SEGURIDAD EN LOS CONTRATOS CON LOS PROVEEDORES**

En las relaciones contractuales con terceros proveedores que impliquen acceso, procesamiento, comunicación, gestión o cualquier otro tratamiento respecto de los activos de información necesarios para la ejecución del contrato, deberán considerarse regular los siguientes aspectos:

- a. Comunicación y entrega de política de seguridad de la información que aplica el tercero al interior de su organización.
- b. Conocimiento y cumplimiento de los anexos del contrato, especialmente el anexo C14 – Condiciones de Seguridad y Ciberseguridad.
- c. Medidas de seguridad informática a aplicar a nivel de hardware, software y redes
- d. Identificación plena de los empleados del proveedor que accederán a los activos de información y/o terceras partes en calidad de subcontratistas



## NORMA DE RELACIÓN CON PROVEEDORES

<b>CÓDIGO:</b>	OD-04-PD-A-35
<b>VERSIÓN:</b>	1
<b>FECHA:</b>	24/04/2023
<b>PÁGINA:</b>	2 de 11

- e. Establecimiento de acuerdos de confidencialidad por parte de empleados del proveedor y/o subcontratistas, según la clasificación del activo de información en GASES DEL CARIBE, cuando así se requiera. La extensión de la obligación de confidencialidad aplicar no solo respecto del activo de información al que se accede sino también a todos aquellos otros activos como papeles de trabajo, versiones intermedias o borradores del objeto del contrato y/o del activo de información.
- f. Exigencia de realizar análisis periódicos para identificar y neutralizar vulnerabilidades.
- g. Uso de software debidamente licenciado.
- h. Prohibición de conceder acceso a los activos de información a personas no autorizadas, trátase o no de empleados del proveedor.
- i. Capacitación del personal del tercero proveedor, empleados o subcontratistas, en materia de seguridad de la información.
- j. Prohibición de compartir las credenciales de acceso a los sistemas de información asignadas a persona determinada.
- k. Garantizar que la ejecución del contrato debe caracterizarse por aplicar las buenas prácticas internacionalmente aceptadas asociadas al objeto contratado según el estado del arte. Para efectos de precisión el tercero proveedor deberá especificar en el contrato cuales son las buenas prácticas que aplicará. La inaplicación de tales prácticas será considerada una causal de incumplimiento grave del contrato.
- l. Regular la propiedad intelectual y/o inmaterial del activo de información desde la concepción del proyecto y documentarlo en el respectivo contrato hasta la formalización de los derechos sobre estos.
- m. Dar respuesta a las solicitudes de información en materia de seguridad que sean exigidas por GASES DEL CARIBE, cumpliendo con los requisitos solicitados y en los tiempos fijados.
- n. Definir las obligaciones generales y específicas que asumirá el tercero proveedor en materia de seguridad de la información, las cuales se consideran esenciales para la ejecución del contrato y respectiva protección de activo de información involucrado.
- o. Definir mecanismo mediante el cual el tercero proveedor se incorpora a los procesos de gestión del cambio y la configuración de sistemas, incluida la gestión de vulnerabilidades, las actualizaciones de seguridad (parches) y la verificación de los controles de seguridad del sistema antes de su conexión a las redes de producción de la empresa.
- p. Definir el derecho que tiene la empresa a supervisar y monitorear todo el acceso y uso de las instalaciones, redes, sistemas, entre otros y auditar el cumplimiento del contrato por parte del proveedor.

	<b>NORMA DE RELACIÓN CON PROVEEDORES</b>	<b>CÓDIGO:</b>	OD-04-PD-A-35
		<b>VERSIÓN:</b>	1
		<b>FECHA:</b>	24/04/2023
		<b>PÁGINA:</b>	2 de 11

- q. Determinar los acuerdos para la continuidad de negocio que incluyan la gestión de crisis e incidentes, resiliencia, copias de seguridad y recuperación de desastres.

#### **5.4. SELECCIÓN DEL PROVEEDOR**

El Área líder del servicio o producto contratado, de acuerdo con el análisis de riesgos realizado, determina la necesidad de verificación de antecedentes de los proveedores que participen en el proceso y los métodos que deben aplicarse. Para ello se puede tener en cuenta los siguientes criterios:

- a) Reputación y antecedentes de la organización.
- b) Nivel de Experticia y Conocimiento.
- c) Calidad del servicio prestado a otros clientes.
- d) Estabilidad financiera de la organización y registro comercial.
- e) Buenas prácticas en materia de calidad y/o seguridad que se encuentran en cumplimiento por la empresa (ISO 9001, ISO 27001, entre otros).
- f) Otros, de acuerdo con el análisis de riesgos.

#### **5.5. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

Es obligación de todo tercero proveedor que acceda a activos de información de GASES DEL CARIBE notificar de forma inmediata, una vez tenga conocimiento, de la materialización o sospecha de un incidente que comprometa la seguridad de la información de tales activos.

El incidente de seguridad deberá ser gestionado por el tercero proveedor siguiendo la Norma de gestión de incidentes de seguridad de la información que adopte esta organización, salvo que GASES DEL CARIBE autorice el uso de políticas propias del proveedor; las cuales en ningún caso podrán ser inferiores a las definidas por esta organización.

#### **5.6. RESPONSABILIDAD CIVIL**

Es de importancia manifiesta que el tercero proveedor sea consciente de las responsabilidades que asume al acceder y/o gestionar activos de información propiedad de GASES DEL CARIBE o bajo su custodia.

Por tanto, debe regularse con el proveedor la responsabilidad civil contractual respecto de aquellos casos en los cuales este pueda causar un perjuicio a los activos de información propiedad de GASES DEL CARIBE; y responsabilidad



## **NORMA DE RELACIÓN CON PROVEEDORES**

<b>CÓDIGO:</b>	OD-04-PD-A-35
<b>VERSIÓN:</b>	1
<b>FECHA:</b>	24/04/2023
<b>PÁGINA:</b>	2 de 11

civil extracontractual respecto de aquellos activos de información propiedad de terceros bajo custodia de GASES DEL CARIBE, como pueden ser los datos personales, la propiedad intelectual o inmaterial, entre otros.

El tercero proveedor será responsable de todos los daños indemnizables que experimente GASES DEL CARIBE como resultado de su falta de pericia, negligencia y/o imprudencia en la gestión de los activos de información y/o servicios de procesamiento de información involucrados en la ejecución del contrato. Así mismo, el proveedor será responsable de los daños indemnizables que cause a terceros.

Las multas, sanciones o condenas que impusieran a GASES DEL CARIBE como consecuencia de la falta de diligencia por parte del tercero proveedor en la gestión de activos de información, como pueden ser los datos personales de terceros, deberán ser asumidas por el proveedor.

No es aconsejable cláusulas de exclusión de la responsabilidad o limitación de esta por parte de terceros proveedores que en la ejecución del contrato accedan y/o traten activos de información propiedad de GASES DEL CARIBE o entregados para su custodia. Corresponderá al Propietario del Activo y al Área Jurídica evaluar el riesgo.

### **5.7. PÓLIZAS**

Los riesgos asociados a la seguridad de la información deberán estar cubiertos por las pólizas de seguros que los terceros proveedores otorguen a GASES DEL CARIBE, siempre que en la ejecución del contrato estos accedan y/o traten activos de información.

La criticidad del activo de información constituye un criterio para establecer el porcentaje de cobertura sobre el valor del contrato.

De acuerdo con la evaluación del riesgo en cada caso, podrá liberarse al proveedor del otorgamiento de una póliza de seguros.

Se comunicará al futuro proveedor y/o interesado en participar en el proceso de selección sobre la exigencia o no de pólizas de seguro, lo cual se realizará en la fase de invitación a contratar o proceso licitatorio.

### **5.8. ACUERDOS DE CONFIDENCIALIDAD**

En las relaciones contractuales con terceros en los cuales sea indispensable el acceso y/o gestión de activos de información se pactarán las obligaciones en materia de confidencialidad.





## **NORMA DE RELACIÓN CON PROVEEDORES**

<b>CÓDIGO:</b>	OD-04-PD-A-35
<b>VERSIÓN:</b>	1
<b>FECHA:</b>	24/04/2023
<b>PÁGINA:</b>	2 de 11

Este deber aplica durante la fase precontractual, contractual y postcontractual.

El tercero proveedor que accede a activos de información propiedad de GASES DEL CARIBE o entregados por terceros para su custodia debe ser informado y entender que la propiedad sobre tales activos no cambia por el transcurso de tiempo; lo cual deberá quedar pactado de forma expresa y clara en los contratos.

### **5.9. ENTREGA Y DEVOLUCIÓN DEL ACTIVO DE INFORMACIÓN**

Antes, durante y después de la ejecución del contrato, GASES DEL CARIBE documentará mediante acta la entrega o acceso por parte del tercero proveedor a los activos de información requeridos; así mismo a la finalización del contrato se deberá documentar mediante acta la devolución de los activos de información entregados a lo largo de la ejecución del contrato. Esta devolución deberá estar acompañada por una certificación del representante legal del tercero proveedor en que indique que ha devuelto los activos de información y que no existe copia de los mismos en su poder.

### **5.10. CUMPLIMIENTO**

Las obligaciones originadas en la ley colombiana y en aquellas originadas en las políticas internas adoptadas por esta organización en materia de seguridad de la información, sin limitarse a aquellas relacionadas con la protección de datos personales, obligan a los proveedores que gestionen activos de información propiedad de esta organización o entregados por terceros para su custodia. En materia de protección de datos personales tales terceros proveedores asumen el rol de encargados como les denomina la ley.

Lo dispuesto en materia de seguridad de la información constituye obligaciones esenciales de la relación con todo proveedor que gestione activos de información, como puede ser la información personal u otra.

### **5.11. PROTECCIÓN DE DATOS PERSONALES**

Si en la relación con terceros proveedores estos acceden y/o tratan activos de información que contengan datos personales estos serán considerados Encargados del tratamiento de información personal. Por tanto, estos Encargados deben cumplir con lo dispuesto en el artículo 18 de la Ley Estatutaria 1581 de 2012; independiente de si están domiciliados dentro del territorio colombiano o fuera de Colombia.

	<b>NORMA DE RELACIÓN CON PROVEEDORES</b>	<b>CÓDIGO:</b>	OD-04-PD-A-35
		<b>VERSIÓN:</b>	1
		<b>FECHA:</b>	24/04/2023
		<b>PÁGINA:</b>	2 de 11

Por disposición legal todo proveedor Encargado del tratamiento de datos ubicado fuera del territorio colombiano deberá suscribir un contrato de transmisión internacional de datos personales.

Todo proveedor que trate datos personales deberá certificar por escrito a través del representante legal y revisor fiscal que cumple la Ley Estatutaria de Protección de Datos Personales 1581 de 2012 y Ley Estatutaria 1266 de 2008, si esta última fuere aplicable, y que gestiona un Programa Integral de Datos Personales conforme la instrucción de la SIC contenida en la Guía de Responsabilidad Demostrada.

Este es un requisito esencial para ser proveedor de esta organización, el cual será exigido si la relación contractual con el proveedor implica el tratamiento de datos personales por cuenta de este respecto de los activos de información de esta organización.

#### **5.12. FACULTAD DE AUDITORIA**

En las relaciones con los terceros proveedores que traten información personal en poder y/o bajo custodia de esta organización se deberá pactar en los contratos de forma clara la facultad de auditoría que puede desplegar esta organización con el fin de verificar el cumplimiento de las obligaciones en materia de protección de datos personales y seguridad de la información.

### **6. MONITOREO, REPORTE Y AUDITORIA**

El Propietario del activo de información y/o el jefe del Área del Servicio beneficiario de la relación contractual con el tercero proveedor debe establecer la periodicidad con que realizará la revisión del cumplimiento de las obligaciones que en materia de seguridad de la información fueron pactadas en el respectivo contrato.

De acuerdo con la naturaleza del activo de información, clasificación del activo y riesgos identificados deberán establecerse los aspectos que serán objeto de monitoreo, sin perjuicio de aquellos otros que durante la ejecución del contrato puedan adicionarse.

Los resultados del monitoreo deberán ser documentados en los formatos definidos por esta organización, los cuales harán parte de la documentación del contrato respectivo.

GASES DEL CARIBE podrá auditar el cumplimiento de los requisitos de seguridad aplicable a la relación con terceros proveedores, sea realizando tal actividad de forma directa o a través de los terceros.

	<b>NORMA DE RELACIÓN CON PROVEEDORES</b>	<b>CÓDIGO:</b>	OD-04-PD-A-35
		<b>VERSIÓN:</b>	1
		<b>FECHA:</b>	24/04/2023
		<b>PÁGINA:</b>	2 de 11

## **7. CONTROL**

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

## **8. 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.

## **9. 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