POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. CONSIDERANDOS

a) Que la legislación colombiana (Ley Estatutaria 1581 de 2012[1] y Ley Estatutaria 1266 de 2008[2], en lo que sea aplicable esta última) en materia de protección de datos personales exige a los responsables y Encargados del tratamiento de datos personales identificar e inventariar el conjunto organizado de datos o bases de datos[3] que contienen información personal, sea que su tratamiento sea físico y/o automatizado.

b) Que en el caso particular de GASES DEL CARIBE, existe la obligación legal de realizar ante la Superintendencia de Industria y Comercio (SIC) como autoridad de control una declaración sobre las bases de datos que contienen información personal respecto de las cuales se realiza cualquier tratamiento[4] de datos, sea físico y/o automatizado; sea que esta se realice directamente por esta organización como Responsable[5] del Tratamiento y/o de forma indirecta a través de terceros proveedores que actúan en calidad de Encargados[6] respecto de tales bases de datos.

c) Que como consecuencia de la declaración obligatoria de las bases de datos con información personal tratadas a cargo del Responsable, en el Registro Nacional de Bases de Datos (RNBD) se solicita a la organización que declare el marco interno de políticas, normas y procedimientos adoptados para materializar el principio de seguridad de la información[7], el cual es uno de los principios de mayor importancia para hacer efectivo y real el Derecho Fundamental a la Protección de Datos Personales[8] que tiene el Titular[9] de este tipo de dato o activo.

d) Que esta organización en la definición del marco de cumplimiento del principio de seguridad podrá adoptar como referente las buenas prácticas de seguridad de la información contenidas en las normas

---

[1] Congreso de Colombia. (17 de octubre de 2012). Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

[2] Congreso de Colombia. (31 de diciembre de 2008). Ley de Habeas Data y manejo de información financiera. [Ley 1266 de 2008]. DO: 47.219.

[3] Congreso de Colombia. (17 de octubre de 2012). Artículo 3 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

[4] IBID.

[5] IBID.

[6] IBID.

[7] Congreso de Colombia. (17 de octubre de 2012). Artículo 4 [Título II]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

[8] Congreso de Colombia. (17 de octubre de 2012). Artículos 1 y 2 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

[9] Congreso de Colombia. (17 de octubre de 2012). Artículo 3 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

estándar ISO 27001:2013, ISO 27002:2015 e ISO 27005:2018, ISO 27032:2012, NIST 800-53 rev4:2013; sin perjuicio de acudir a otras normas estándar de industria aplicables a la gestión de datos, información, conocimientos y/o gobierno de estos. Lo anterior, considerando la prevalencia de las normas legales sobre las normas estándar de industria.

e) Que, teniendo presente el contexto anterior, esta organización entiende que los datos personales en poder de esta exigen que, una vez estos sean identificados, sean gestionados y protegidos con el fin de dar cumplimiento al régimen legal de protección de datos personales.
f) Que el estándar de la norma ISO 27001 y demás de esta familia antes mencionadas, incorpora el dominio de cumplimiento (A.18.1)[10] respecto de los requisitos de ley y contractuales que deben tenerse presente en la gestión de la seguridad de la información; uno de ellos es la "Privacidad y Protección de la Información Personal"[11].
g) Que como expresión del compromiso de la Alta Dirección de esta organización y evidencia de la responsabilidad con la que se asume el cumplimiento del régimen de protección de datos personales se adopta esta Política; esto considerando lo dispuesto en la Guía de Responsabilidad Demostrada[12] expedida por la SIC que señala los parámetros para cumplir con el Principio de la Responsabilidad Demostrada.
h) Que esta organización además es consciente de la importancia de identificar, proteger y gestionar otros tipos de activos de información que también son creadores de valor en la ejecución de la estrategia como son los datos, información, conocimientos y/o derechos que tenga bajo su custodia; motivo por el cual los lineamientos aquí indicados y la estrategia de seguridad de la información se extenderá no sólo a los datos personales, sino también a los demás activos de información[13] en propiedad de esta organización y/o bajo sus custodia.
i) Que mediante esta política se pretende fortalecer de forma más robusta e integral las prácticas de seguridad de la información existentes en la organización que han sido desplegadas de forma razonable y diligente por la organización.

---

[10] Organización de Estándares Internacionales. (2013). Anexo A Dominio 18.1 Cumplimiento de los requisitos legales y contractuales. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].
[11] IBID.
[12] Superintendencia de Industria y Comercio. Guía para la implementación del principio de responsabilidad demostrada. Recuperado de http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf.
[13] Organización de Estándares Internacionales. (2013). Articulo 3 Términos y definiciones. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].

j) Que esta Política será desarrollada a través de normas, procedimientos y/o instructivos, los cuales serán objeto de revisión y mejoramiento permanente, acorde con los requisitos de seguridad de esta organización y dinámica de los objetivos estratégicos de la misma, en la medida que los datos, información y conocimientos tienen el potencial de crear valor para la organización y grupos de interés con los cuales se relaciona.

2. OBJETO

El objetivo o propósito de esta Política de Seguridad de la Información aplicable a los datos personales y demás activos de información es declarar que estos de acuerdo con su naturaleza son creadores de valor para la organización; razón por la cual, de acuerdo con los objetivos estratégicos y requisitos del negocio, se adoptará un esquema sistemático de gestión segura basado en riesgos con el fin de preservar los atributos de Integridad, confidencialidad y disponibilidad para fortalecer la confianza con sus grupos de interés.

3. DESTINATARIOS

Esta Política da alcance a todas las líneas de negocio, procesos, sedes y activos de información de la empresa Gases del caribe S.A. E.S.P. y aplica a las relaciones que esta tiene con sus grupos de interés; a saber:

- Accionistas
- Junta Directiva.
- Empleados colaboradores
- Proveedores.
- Clientes.
- Gobierno
- Autoridades
- Comunidades
- Asociaciones
- Agremiaciones.

4. ÁMBITO DE APLICACIÓN

Esta política de seguridad de la información será criterio rector de carácter obligatorio aplicable por los colaboradores en los procesos administrativos que soportan diferentes servicios que presta esta organización a los clientes, comunidad, así como en el relacionamiento con los grupos de interés.

Igualmente será exigible en las relaciones estatutarias, contractuales y/o legales con terceros, proveedores y/o autoridades; sin perjuicio de lo aplicable a otros destinatarios de esta política.

5. ENFOQUE DE LA SEGURIDAD DE LA INFORMACIÓN

Acorde a la naturaleza de la organización, los riesgos contra la seguridad de la información adquieren mayor relevancia cuando un alto porcentaje de la operación y prestación de los servicios están soportados en Tecnologías de Información y Comunicaciones (TIC) lo que incrementa de forma importante los riesgos en relación con el logro de los objetivos estratégicos, especialmente el de potenciar nuevos negocios y lograr eficiencias por medio de la transformación digital.

Esta realidad no sólo es predicable de esta organización, sino que constituye una preocupación a nivel público y privado presente también a nivel internacional; lo que ha determinado la expedición a nivel mundial de normas legales y de industria orientadas a proteger a las personas y organizaciones respecto de los riesgos cibernéticos originados en la presencia incremental de las TIC en la vida social.

Consecuencia de ello, el régimen de protección de datos personales vigente en Colombia incorpora el principio de Responsabilidad Demostrada[14] mediante el cual se exige la adopción de un programa integral de protección de datos personales basado en riesgos. Este programa integral de protección de datos personales gradualmente irá siendo extendido en esta organización a otros activos de información como datos, información, conocimiento y derechos no relacionados con datos personales.

Por tanto, el esquema de riesgos que a continuación se enuncia será considerado en la prestación de los servicios actuales de esta organización, así como en la mejora de estos y en la incorporación de los nuevos servicios, sea que involucren o no datos personales.

El enfoque de riesgos aplicable a la gestión de la seguridad de la información, que incorpora la protección de datos personales, comprende los cuatro (4) momentos fundamentales de todo sistema de gestión, como son:

[14] Superintendencia de Industria y Comercio. Guía para la implementación del principio de responsabilidad demostrada. Recuperado de https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf

Planear: Esta etapa comprende la identificación de los activos de información, entiéndase datos personales o no, información, conocimientos y/o derechos que representen un valor estratégico para la organización en relación con los objetivos estratégicos de esta y los respectivos servicios que presta a terceros, para así identificar los riesgos en relación con el cumplimiento de las obligaciones legales, estatutarias y contractuales teniendo como referencia la normatividad legal y las normas de industria o buenas prácticas aplicables según el caso. A partir de estos se establecerán los objetivos de control, controles y análisis sobre la declaración de aplicabilidad[15].

Hacer: En esta etapa, previa identificación de los riesgos y definición de la declaración de aplicabilidad, se desplegarán los planes de acción orientados a prevenir, mitigar, eliminar y/o aceptar el riesgo, previo análisis y justificación de las razones por las cuales se asume este. En el plan de acción para gestionar los riesgos se determinará el responsable de la gestión, acciones a desplegar, los controles, los recursos asignados de acuerdo con su impacto y probabilidad, métricas, sin perjuicios de demás aspectos relevantes para la gestión de los riesgos vinculados.

Verificar: En esta etapa se evaluará el resultado de la gestión de la seguridad de la información respecto de los activos de información, sean datos personales o no, aplicando para ello técnicas de auditoría razonables que permitan identificar debilidades en la gestión, recomendaciones y nuevos riesgos, para así fortalecer la gestión segura de la información en la organización.

Actuar: En esta etapa a partir de los hallazgos y recomendaciones se actualizará el plan de acción para gestionar los riesgos identificados respecto de los activos de información en poder y/o custodia de esta organización.

Documentación: Es importante en términos de evaluar la debida diligencia de la Alta Dirección y demás colaboradores responsables[16] de la gestión segura de la información la documentación y conservación de las evidencias físicas y/o electrónicas que permitan establecer que la organización ha cumplido y gestionado de forma eficaz los activos de

[15] Definición de la ISO 27000 referido al documento que describe los objetivos de control, controles pertinentes y aplicables en materia de un sistema de gestión de seguridad de la información.
[16] Organización de Estándares Internacionales. (2013). Anexo A Dominio 6.1 Organización Interna de la seguridad de la información. Sistemas de Gestión de Seguridad de la Información. [ISO 27001 de 2013].

información como datos personales o no, información, conocimientos y/o derechos.

Comunicación: Para la gestión segura de los activos de información es un elemento fundamental la comunicación interna y externa con el fin de crear, promover, mantener y fortalecer la cultura de seguridad respecto de los activos de información en poder y/o bajo custodia de la organización.

Educación y formación: El logro del objetivo de crear una cultura de seguridad de la información alrededor de los activos de información en poder y/o bajo custodia de la organización exige que la formación considere la dimensión de los riesgos que a nivel personal pueda experimentar cada colaborador y/o prestador de servicios para construir al interior de la organización una cultura colectiva respecto de la protección de los datos personales y demás activos de información objeto del programa de gestión de la seguridad de la información.

6. COMPROMISO DE LA ALTA DIRECCIÓN

El régimen colombiano de protección de datos personales al dar instrucciones sobre la aplicación del Principio de Responsabilidad Demostrada establece como primer elemento para hacer realidad el Derecho Fundamental a la Protección de Datos Personales el compromiso de la Alta Dirección. Este deber legal está alineado con el deber de diligencia establecido en la normas de Código de Comercio aplicables a los administradores de la organización, el cual también está contenido en la norma de industria ISO 27001 sobre gestión segura de la información la cual señala como parte de ese deber la definición de una política que guía la gestión segura de la información basada en riesgos, la que habrá de incorporar los requisitos de cumplimiento y articular estos con el logro de los objetivos estratégicos trazados por la organización.

7. RENDICIÓN DE INFORMES

Un componente fundamental en la seguridad de la información es mantener un proceso de comunicación efectivo que permita mantener informada a la Alta Dirección. En este orden de ideas, desde la Dirección Digital, Coordinación SGI, Coordinación de seguridad física, Coordinación de Gestión Documental y Oficial de cumplimiento, en lo que a sus funciones corresponde, como responsables de la seguridad de la información, de

forma periódica y/o excepcional, se rendirán informes respecto del estado de la seguridad de la información.

De igual forma, deberá existir una comunicación fluida desde los Departamentos que soportan los servicios que presta esta organización hacia la Dirección Digital, Coordinación SGI, Coordinación de seguridad física y Oficial de cumplimiento con el fin de informar sobre las necesidades de seguridad que deben ser consideradas por la organización para su operación.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Gerencia General de esta organización mediante esta Política declara a los grupos de interés el firme compromiso que tiene respecto del deber legal de proteger los activos de información de su propiedad y/o entregados para su custodia en virtud de una obligación legal, estatutaria y/o contractual.

Resultado del valor estratégico que tienen para esta organización los datos personales o no, datos, información, conocimientos y derechos, se precisan los parámetros generales que deben tenerse presentes en el logro de los objetivos estratégicos en relación con la integridad, disponibilidad y confidencialidad, sin perjuicio de los otros atributos que se predican respecto de la información.

En virtud de esta Política los procesos empresariales que soportan los servicios prestados por esta organización, cuando traten datos personales, deberán aplicar los principios relativos a la protección de datos personales señalados en la ley, jurisprudencia y/o buenas prácticas internacionales, según cada caso.

9. OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27001 y las demás que hacen parte de este estándar para la gestión segura de la información definen un conjunto de objetivos específicos que contribuyen de forma armónica y sistémica a la protección de los datos, información, conocimientos y derechos ya mencionados.

En el cumplimiento de la gestión segura de la información se dará prioridad a los objetivos específicos exigidos por la normatividad legal vigente en materia de datos personales, sin que ello signifique que dejarán de

atenderse aquellos otros que de forma indirecta contribuyan al objetivo general señalado en esta Política.

9.1. Organización de la Seguridad de la Información

La Alta Dirección de Gases del Caribe S.A. E.S.P. vela por la existencia, implementación, funcionamiento e incorporación de buenas prácticas de seguridad de la información en todos los procesos de la organización.

La Coordinación de Gestión Integral, lidera y vela por la incorporación de las buenas prácticas de seguridad de la información y para ello, con apoyo en otros procesos organizacionales, se encarga en relación con el objetivo de esta política de: establecer y mantener esta política, sus objetivos, roles, límites y responsabilidades respecto del tratamiento[17] de los activos de información;

La Dirección Digital vela por la implementación y funcionamiento de los procedimientos establecidos sobre los activos de información digitales; establecer los controles que protejan la información durante la operación y en los proyectos en ejecución vinculados a esta materia; velar porque los recursos informáticos a través de los cuales se gestionan activos de información y datos personales, entre otros, sean seguros.

Así mismo, Gestión documental y cada departamento vela por la seguridad de los activos de información bajo su custodia.

Adicionalmente la organización ha definido otros roles y responsabilidades específicos como en la *norma de asignación de responsabilidades para la seguridad de la información*.

9.2. Seguridad de los Recursos Humanos

La gestión segura de la información es una obligación que debe estar presente en todos los procesos organizacionales que soportan los servicios que se prestan a los clientes y a la comunidad, lo cual constituye una obligación para todo colaborador y/o tercero que participa en la operación de los servicios.

Gases del Caribe S.A. E.S.P. busca lograr que la seguridad de la información se gestione en los siguientes momentos: antes de la relación laboral, durante la relación laboral y después de la relación laboral.

En cualquiera de los tres momentos antes descritos, gestión humana, la Coordinación de Gestión Integral, la Dirección Digital, Coordinación

[17] Congreso de Colombia. (17 de octubre de 2012). Artículo 3 [Título I]. Ley de Protección de Datos Personales. [Ley 1581 de 2012]. DO: 48.587.

de Gestión Documental y el oficial de cumplimiento , en lo que a sus funciones corresponde, definirá los lineamientos que contribuyan a la seguridad de la información y a la protección de los datos personales con el fin de mitigar riesgos y asegurar que en estos se cumplen los requisitos legales, estatutarios y contractuales vinculados al logro de los objetivos empresariales.

Así mismo, es un propósito promover y fortalecer la cultura de la seguridad con respecto a los activos de información, incluidos los datos personales, considerando las necesidades de la organización y/o requerimientos de ley.

9.3. Gestión de Activos

La seguridad de los activos de información, incluidos los datos personales, requiere de la creación y mantenimiento de un inventario de estos, con el fin de gestionarlos de forma segura de acuerdo con las necesidades del negocio y/o requerimientos de ley.

Corresponde a cada propietario del activo de información realizar las siguientes acciones: identificar e inventariar los activos de información, incluidos los datos personales; establecer los criterios de clasificación de estos; adoptar controles para su protección cualquiera que sea la forma de su tratamiento, considerando el ciclo de vida de los recursos en los cuales se gestionan estos.

9.4. Control de acceso

La gestión segura de la información, así como la protección de la información personal, exige que los activos de información solo sean tratados por personas autorizadas siendo para ello necesario limitar el acceso de estos a los sistemas de información, instalaciones de procesamiento y centros de gestión documental física.

Corresponderá a la organización a través del área responsable de la gestión de accesos establecer los parámetros y/o directrices para crear usuarios y contraseñas; asignar derechos de acceso y tratamiento a estos; otorgar derechos de acceso privilegiado bajo el principio del mínimo necesario; adoptar mecanismos de autenticación y validación de usuarios; revisar y validar los derechos de acceso de forma periódica; y restringir y/o cancelar los accesos resultantes de la suspensión o

terminación de la relación contractual, respectivamente. Estos son descritos en instructivos y normas internas aplicables.

El acceso a los sistemas de información se gestionará cualquiera que sea el ambiente existente para soportar los sistemas de información, sea desarrollo, pruebas, pre productivo o productivo.

El derecho de acceso a los sistemas de información cualquiera que sea su naturaleza y centros de procesamiento de datos implica una seria responsabilidad por parte del personal autorizado, por tanto, el derecho concedido es intransferible y por tanto prohibido otorgar este derecho a otra persona.

Se informa que en Colombia el acceso a los sistemas de información sin autorización y/o por fuera de lo acordado puede ser considerado un delito informático según lo dispuesto en la Ley 1273 de 2009[18].

9.5. Seguridad Física

La gestión segura de la información, así como la protección de la información personal, involucra el componente físico y ambiental con el fin de prevenir el acceso no autorizado a la información tratada de forma manual, así como el daño y/o destrucción activos de información.

Corresponderá a la organización, a través de la Coordinación de Seguridad Física el respectivo propietario del activo de información, establecer los parámetros y/o directrices para establecer controles de acceso, tránsito y salida de las instalaciones de la organización; adoptar controles para proteger los equipos y los activos de información en las oficinas, salones e instalaciones de la organización; definir perímetros de seguridad con el fin de proteger los activos de información sea que se trate estos de forma manual y/o automatizada; adoptar mecanismos que impidan la salida de equipos informáticos u otra naturaleza sin autorización; definir medidas que eviten el deterioro de los activos de información por factores ambientales.

Es responsabilidad de cada usuario de un activo de información aplicar las medidas de seguridad físicas adoptadas por la organización. Debe tenerse presente que los derechos de acceso a la información física se otorgan a título personal y por tanto son intransferibles.

9.6. Adquisición, desarrollo y mantenimiento de sistemas de información

La seguridad de los activos de información digitales y de los datos personales debe ser un requisito fundamental en los procesos de adquisición, desarrollo y mantenimiento de los sistemas de información, en los cuales debe garantizarse la integridad, disponibilidad y confidencialidad de los activos de información durante todo el ciclo de vida de estos; sea que la gestión la realice directamente la organización y/o se contrate con un tercero proveedor.

Corresponderá a la organización, a través de la Dirección Digital y Oficial de cumplimiento , en lo que a sus funciones se refiere, y el respectivo o futuro propietario del activo de información, señalar parámetros para establecer en cada caso los requisitos de seguridad y protección de datos personales que deben estar presentes en el sistema de información; incorporar mecanismos que validen y verifiquen los datos de entrada, salida y procesamiento completo de las transacciones; adoptar prácticas seguras de desarrollo de sistemas de información; implementar prácticas seguras de control de cambios; definir esquemas de pruebas; definir los mecanismos de monitoreo con el fin de que los accesos sean autorizados y/o detectar irregularidades; y diseñar estrategias de salida en producción que no comprometan la operación de los servicios de la organización.

Es responsabilidad de todo líder de proceso empresarial y/o servicio involucrado en la adquisición, desarrollo y mantenimiento de sistemas de información definir al inicio del proyecto los requisitos que permitan garantizar la seguridad de los activos de información y datos personales tratados en el respectivo sistema de información.

Es indispensable que toda adquisición, desarrollo y/o mantenimiento de un sistema de información incluidas las redes, incorpore como requisito la seguridad de los activos de información y protección de datos personales en cualquier de los momentos del proyecto, independiente de que este lo ejecute directamente la organización y/o se contrate con un tercero.

No son aceptables sistemas de información que adolezcan de funcionalidades que omitan la seguridad de los activos mencionados, incluidos los datos personales.

9.7. Relaciones con los proveedores

La seguridad de la información es un deber que involucra a los terceros proveedores que, en razón de las relaciones precontractuales, contractuales o postcontractuales acceden y/o realizan cualquier tratamiento respecto de los activos de información, incluidos los datos personales, que están en poder y/o bajo la custodia de esta organización.

Corresponde a esta organización adoptar directrices internas en materia de seguridad de la información las cuales fortalecerán los criterios a tener presentes en la selección y contratación de proveedores que deban acceder y/o tratar activos de información, incluidos los datos personales.

9.8. Gestión de incidentes de seguridad de la información

La seguridad de la información y de los datos personales imponen a la organización la obligación de gestionar de forma adecuada los incidentes de seguridad que comprometan algún activo de información; siendo obligación reportar ante la SIC aquellos que hayan comprometido cualquier tipo de dato personal.

Corresponde a la Dirección Digital y al Oficial de Cumplimiento , en lo que a sus funciones corresponde, en relación con la gestión de los incidentes de seguridad de la información liderar la adopción del procedimiento para la gestión de estos y consecuente respuesta, así como desplegar un plan de acción que de forma periódica evalúe las debilidades de la seguridad de la información a nivel físico e informático; clasificar y analizar los eventos de seguridad para definir si han alcanzado el nivel de incidentes; gestionar el conocimiento a partir de los incidentes para adoptar controles que mejoren la seguridad de la información y fortalezcan las competencias para responder a los incidentes de seguridad de la información, sea que incluyan datos personales o no.

Es responsabilidad de la Dirección Digital, así como a el Oficial de Cumplimiento en lo que a sus funciones corresponde, responsable de la Protección de Datos Personales, gestionar de forma adecuada todo incidente de seguridad de la información que comprometa datos personales. El Informe del incidente de seguridad, realizado a partir del procedimiento de atención a este, será presentado a la Alta Dirección con el fin de informar sobre la situación, para efectos del reporte que debe realizarse a la SIC como autoridad de control en el término establecido en la ley.

La gestión del incidente de seguridad respecto de un activo de información y/o datos personales debe ser pactado como obligación de los proveedores involucrados de forma directa o indirecta en el incidente de seguridad; tal como lo exige el régimen de Protección de Datos vigente en Colombia.

Es obligación de todo destinatario de esta política informar sobre la sospecha de una situación que pueda comprometer la seguridad de un activo de información, incluidos los datos personales, reporte que se realizará a la Dirección Digital al correo soporteciberseguridad@gascaribe.com y al Oficial de Cumplimiento habeasdata@gascaribe.com, por medio de los canales establecidos para tal fin.

9.9. Controles criptográficos

La gestión segura de la información y la protección de datos personales exige el uso de sistemas y técnicas criptográficas como mecanismos de protección de acuerdo con una adecuada gestión de riesgos con el fin de preservar los atributos de integridad, confidencialidad y disponibilidad.

Corresponde a la organización, a través de la Dirección Digita, la implementación de controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberían ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y los avances en el estado del arte en materia de criptografía.

9.10. Gestión de las operaciones

La gestión segura de los sistemas de información que soportan los procesos empresariales hace necesario monitorear, documentar y adoptar controles de diferente índole considerando la dinámica de las

amenazas y riesgos empresariales en materia de seguridad de la información y ciberseguridad.

Corresponde a la Dirección Digital evaluar el posible impacto operativo de los cambios previstos en la infraestructura tecnológica crítica, sistemas de información, redes y demás activos, siendo necesario como medida preventiva evaluar la capacidad de estos, realizar copias de respaldo y adoptar los controles requeridos para la seguridad de los datos y servicios conectados a las redes de la organización.

9.11. Controles en las comunicaciones

La gestión segura de las redes requiere de una cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección, acorde a los objetivos estratégicos de la organización.

Corresponde a la Dirección Digital asegurar la protección de la información que se transmite a través de la infraestructura tecnológica crítica, sistemas de información y redes. Así mismo, es necesario evaluar e implementar los controles adicionales que se requieran para la protección de la información que se trasmite en otros medios tecnológicos, cumpliendo con la legislación vigente y atendiendo la actividad empresarial de esta organización.

9.12. Gestión de la continuidad tecnológica

Preservar la seguridad de la información durante las fases de activación, desarrollo de procesos, procedimientos y planes para la continuidad de negocio y retorno a la normalidad, implica integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información, ciberseguridad y datos personales con atención especial a la legislación, las características de la actividad empresarial, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual.

Corresponde al Dirección Digital desarrollar e implementar planes de contingencia para asegurar que los sistemas de información se pueden restablecer en los plazos requeridos por los procesos de negocios, manteniendo las consideraciones en seguridad de la información y

ciberseguridad utilizada en los planes de continuidad y función de los resultados del análisis de riesgos, minimizando los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

9.13. Cumplimiento de los requisitos legales

Es deber de la organización en materia de seguridad de la información, ciberseguridad, protección de datos personales, propiedad intelectual entre otros, monitorear y evaluar de forma periódica en cumplimiento de la normatividad legales, así como el cumplimiento de las obligaciones contractuales con terceros proveedores que participen en la ejecución de la actividad empresarial.

En este sentido, los requisitos normativos y contractuales pertinentes a cada sistema de información impactado en materia de seguridad de la información, ciberseguridad y protección de datos personales deberían estar debidamente definidos y documentados.

10. DESARROLLO DE ESTA POLÍTICA

Esta Política se desarrolla a través normas, manuales, instructivos, manuales, formatos y/o Instrumentos normativos adoptados por Gases del Caribe SA ESP.

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