NORMA DE ASIGNACIÓN DE RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

GASES DEL CARIBE, en su compromiso con la protección de la información que se gestiona en los Servicios o Procesos que soporta su operación, considera de importancia vital establecer los parámetros que deben tenerse presentes a la hora de asignar roles y responsabilidades frente al deber de seguridad derivado de las normas legales aplicables y buenas prácticas con el fin de fortalecer la seguridad de la información en esta organización, en particular las normas sobre protección de datos personales, sin perjuicio de las demás que se expidan.

1. CONSIDERANDOS

a) Qué GASES DEL CARIBE adoptó una Política de Seguridad de la Información mediante la cual expresa un serio compromiso respecto de la gestión segura de los activos de información de su propiedad y/o entregados por terceros para su gestión, sea resultado de normas legales, contractuales y/o estatutarias.
b) Qué la mencionada política de Seguridad de la Información se desarrolla a través de un conjunto de normas internas, las cuales tienen como objetivo articular y alinear los objetivos empresariales con los objetivos de seguridad y los intereses de los grupos de interés impactados por la seguridad de la información.
c) Que, como marco de referencia en materia de Seguridad de la Información, esta organización acogerá las buenas prácticas incorporadas en la norma NTC-ISO/IEC 27002; sin perjuicio de otras normas de industria y/o legales que complementen o fortalezcan este objetivo.
d) Que la seguridad de la información implica organizar el gobierno de esta a nivel interno, considerando la estructura funcional que habrá de liderar este objetivo, así como los roles y responsabilidades requeridos para fortalecer y controlar la gestión segura de los activos de información en la organización.
e) Qué la seguridad respecto de los activos de información es un aspecto esencial en la estrategia corporativa, no solo por los aspectos regulatorios, sino también por la importancia que estos tienen en el siglo XXI, los datos, información y conocimientos, como creadores de valor para los diferentes grupos de interés con los cuales se relaciona esta organización.
f) Qué la estrategia de seguridad de la información debe ser revisada de forma periódica de acuerdo con los riesgos, tendencias, riesgos, incidentes de seguridad y aspectos regulatorios.
g) Que la seguridad de la información implica la necesidad de establecer canales de comunicación y cooperación adecuados con autoridades, industria, expertos y demás grupos de interés que contribuyan a la protección de los activos en poder de la organización y/o entregados para su custodia por terceros.
h) Que la rendición de informes a la Alta Dirección y al responsable de la seguridad de la información en la organización es un deber de todo colaborador y/o proveedor involucrado en la prestación de un Servicio en relación con la gestión de los activos de información a los que accede y trata en virtud de la relación contractual y/o legal.

Qué la Seguridad de la Información es un imperativo incorporado en los deberes de los administradores de toda organización, entendiendo por estos quienes ejercen funciones de representación legal; lo que no excluye el deber de todos los colaboradores de contribuir de forma proactiva a la seguridad de los activos de información gestionados por esta organización.

2. OBJETO

Definir la estructura funcional encargada de liderar la seguridad de la información, así como establecer los parámetros para asignar los roles y las responsabilidades que propendan por la

seguridad de los activos de información gestionados por los Servicios o Procesos que soportan la operación de GASES DEL CARIBE.

Para ello se requiere un enfoque sistémico, cooperativo y multidisciplinario que involucre no solo a la Alta Dirección sino también a Jefes de Área de la organización.

3. DESTINATARIOS

Esta norma aplica a todos los colaboradores, 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.

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.

4. ROLES EN LA SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información en la organización tiene dos tipos de roles, uno estratégico y otro operativo.

4.1. ROLES ESTRATÉGICOS

Los roles estratégicos en esta materia están en cabeza de la **Alta Dirección**.

4.2. ROLES OPERATIVOS

Los roles operativos están en cabeza de:

4.2.1. PROPIETARIO DEL ACTIVO DE INFORMACIÓN

Hace referencia al líder de cada Servicio que soporta la operación de esta organización; quien tiene la capacidad de decidir respecto de los activos de información relacionados directamente con el Servicio bajo su responsabilidad, así como de propender que la información y los activos asociados con los servicios de procesamiento de información se clasifiquen adecuadamente según los criterios adoptados por esta organización[1].

4.2.2. CUSTODIO DEL ACTIVO DE INFORMACIÓN

Hace referencia al colaborador que gestiona en su actividad diaria los activos de información entregados para el desempeño de las funciones contratadas en el marco de una relación laboral.

[1] Norma de clasificación de activos e inventario de activos de información

También, tendrán el carácter de custodios de la información, los proveedores y colaboradores de estos, que en virtud de la relación contractual de orden comercial y/o civil gestionan activos de información para la ejecución de la actividad contratada.

Son los responsables de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, respeto a los privilegios de acceso, modificación, entre otros.

4.2.3. AUTORIDADES USUARIAS DEL ACTIVO DE INFORMACION

Hace referencia a las autoridades competentes, que, con fundamento en una norma legal y solicitud escrita motivada, acceden y/o tratan activos de información. El acceso a un activo de información, como pueden ser los datos personales u otros, otorga a la autoridad la condición de responsable del tratamiento respecto del activo, caso en el cual debe cumplir con las obligaciones dispuestas en la normativa colombiana aplicable en cada caso.

5. ESTRUCTURA FUNCIONAL DE LA SEGURIDAD

La seguridad de la información, como aspecto esencial de la estrategia de esta organización, está en cabeza de la Alta Dirección.

La Alta Dirección, asigna la responsabilidad de liderar la estrategia de seguridad en el 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.

Según las necesidades de seguridad de la información en la organización se podrá designar un equipo que apoye este objetivo estratégico; mientras tanto las funciones en esta materia estarán a cargo de la Alta Dirección de esta organización.

A continuación, se indican las responsabilidades a cargo de la Alta Dirección y demás áreas involucradas respecto de la seguridad de la información en su dimensión estratégica.

5.1.ALTA DIRECCIÓN

Son responsabilidades de la Alta Dirección en relación con la seguridad de la información las siguientes:

a) Establecer los objetivos estratégicos en materia de seguridad de la información.
b) Aprobar la Política de Seguridad e incorporar a su juicio las mejoras propuestas presentadas por el responsable de la seguridad de la información.
c) Aprobar las normas que desarrollan la Política de Seguridad de la Información
d) Monitorear y evaluar de forma periódica el logro de los objetivos estratégicos vinculados a la seguridad de la información.
e) Asignar los recursos necesarios para el logro de los objetivos estratégicos e implementación de controles, previo análisis de riesgos y plan de acción.
f) Aprobar las declaraciones de aplicabilidad[2] de acuerdo con el análisis de riesgos en relación con aquellas situaciones riesgosas que justifiquen asumir estas.

[2] Es la evaluación que se realizan frente a la aceptación del riesgo, después de un análisis respecto del mismo.

g) Promover una cultura de seguridad de la información al interior respecto de los activos de información gestionados por la organización.
h) Dar lineamientos y adoptar las decisiones empresariales pertinentes en caso de incidentes de seguridad que comprometan uno a varios activos de información.
i) Designar los miembros del equipo de apoyo a la Seguridad de la Información que llegue a crearse para la gestión segura de la información propiedad de esta organización y/o entregadas por terceros para su custodia.

5.2. EQUIPO DE APOYO A SEGURIDAD DE LA INFORMACIÓN

Este equipo de apoyo a la Seguridad, funcional o formal según el caso, tendrá las siguientes responsabilidades, sin perjuicio de las funciones de otros que puedan existir en esta organización.

a) Desarrollar las directrices generales impartidas desde la Alta Dirección en materia de seguridad de la Información.
b) Aprobar la asignación de roles y responsabilidades respecto del tratamiento de los activos de información.
c) Revisar los cambios en la Política de Seguridad de la Información y/o de las normas que la desarrollan, con el fin de dar concepto favorable o no, para que la Alta Dirección apruebe o no; así como solicitar aclaraciones y/o ajustes a los cambios propuestos.
d) Conceptuar sobre el plan de riesgos en materia de seguridad de la información presentado por la Coordinación SGI-Sistema de Gestión Integral o la Dirección Digital, según sus funciones como responsables de esta materia.
e) Analizar el plan de inversiones en materia de seguridad de la información, teniendo como criterio el mapa de riesgos predicables respecto de esta materia, con el fin de dar concepto favorable o no, para que la Alta Dirección apruebe; así como solicitar ajustes al mismo para someterlo a la aprobación de la Alta Dirección.
f) Coordinar la adopción de los controles necesarios y pertinentes para dar seguridad a los activos de información en poder de la organización, conforme la gestión de riesgos existente en materia de seguridad de la información.
g) Coordinar la adecuada gestión de los incidentes de seguridad de la información conforme las definiciones adoptadas en la norma respectiva[3].
h) Hacer seguimiento al estado de la seguridad de la información.
i) Liderar el fortalecimiento de la seguridad de la información en la organización.
j) Construir, evaluar y mejorar el marco normativo de seguridad de la información y someterlo a la aprobación de la Alta Dirección.
k) Crear y mantener actualizado un esquema de riesgos respecto de los activos de información; abordando entre ellos el esquema en materia de protección de datos personales, sin perjuicio de otros activos.

l) Proponer a la Alta Dirección, la creación de roles y responsabilidades respecto del tratamiento de los activos de información.
m) Exigir a los servicios que soportan la operación de esta organización y colaboradores que sigan los parámetros consagrados en la Política de Seguridad de la información y normas que la desarrollan ésta.
n) Monitorear el estado de los controles de seguridad.

[3] Norma de gestión de incidentes de seguridad de la información

o) Informar a la Alta Dirección los incumplimientos graves a la política de seguridad de la información, marco normativo y/o controles adoptados; en casos de menor gravedad los incidentes serán informados a Relaciones laborales y/o al Servicio que gestione la relación con proveedores para la toma de decisiones.
p) Informar a Auditoría los incumplimientos respecto de la seguridad de la información.
q) Informar a la Alta Dirección los incidentes que comprometan de forma grave los activos de información respecto de los cuales exista obligación legal de reportarlos a las autoridades correspondientes.
r) Velar por el cumplimiento regulatorio que impacte el rol y responsabilidades asignadas en materia de seguridad de la información, incluida la protección de datos personales y demás regímenes legales que apliquen en esta materia.
s) Preparar el plan de inversiones en materia de seguridad de la información considerando el estado de los riesgos respecto de los activos de información., incluidos los datos personales.
t) Realizar evaluaciones y ajustes a la Política de Seguridad de la Información y normas que la desarrollan para someterla a la revisión del equipo de apoyo a la Seguridad para la aprobación por parte de la Alta Dirección.
u)

5.3.OFICIAL DE CUMPLIMIENTO

v) Coordinar la definición e implementación del programa de tratamiento de datos personales.
w) Gestionar el cumplimiento de las obligaciones legales en materia de protección de datos personales en relación con aquellas asignadas al Oficial de Cumplimiento establecidas en la ley y conexas con estas.
x) Liderar el cumplimiento del régimen de protección de datos personales, la estrategia de privacidad y el programa integral de datos personales basado en riesgos.
y) Establecer contacto con las autoridades colombianas que deban intervenir en la gestión de los incidentes de seguridad que por disposición legal deban ser notificados a estas.

5.4.PROPIETARIO DEL ACTIVO DE INFORMACIÓN

El líder funcional[4] de cada Servicio de esta organización será el propietario respecto de los activos de información, dentro de ellos las bases de datos con información personal inventariadas, quien asume las siguientes responsabilidades en relación con la seguridad de la información.

a) Identificarlos activos de información respecto de los cuales tiene la condición de Propietario y en compañía del Oficial de Cumplimiento los activos de información que incluyan datos personales.
b) Clasificar los activos de información de acuerdo con los criterios establecidos en la norma de clasificación de activos.
c) Establecer las necesidades de acceso del personal bajo su subordinación con el fin de definir los niveles de acceso, consulta y modificación de los activos de información.
d) Informar al Departamento involucrado las características de los controles de seguridad a nivel físico, administrativo y tecnológico que deben adoptarse por la organización para su implementación.

[4] Hace referencia en principio al Jefe de Departamento, sin perjuicio de las obligaciones que corresponde al superior de este.

e) Presupuestar anualmente su contribución a los controles que deban adoptarse respecto de los activos de información en relación con los cuales tiene la condición de propietario en los términos de esta norma.
f) Gestionar ante l Coordinación SGI- Sistema de Gestión Integral las novedades para habilitar los accesos, restricciones, suspensiones y/o cese en los mismos respecto de los activos de información por parte de los custodios de la información bajo su subordinación.
g) Velar porque el personal bajo su subordinación en calidad de custodio de la información aplique los controles adoptados para garantizar que los niveles y roles autorizados estén cumpliéndose.

h) Informar al área correspondiente (Dirección Digital, Coordinación SGI- Sistema de Gestión Integral, Coordinación de Seguridad Física, Servicios Generales, Gestión Documental u Oficial de cumplimiento) cualquier situación, comportamiento y/o sospecha que ponga en peligro los activos de información a cargo de los custodios de la información.
i) Realizar evaluación de riesgos de seguridad de la información respecto de los niveles de autorización para el acceso de los custodios a los activos de información respecto de los cuales tiene la condición de Propietario del Activo.
j) Permitir las revisiones periódicas por parte de Auditoría que se realicen a los accesos, roles y responsabilidades respecto de los activos de información por parte de los Custodios de la Información que están bajo su subordinación.
k) Informar a la Dirección Digital ,, Coordinación SGI (en caso de accesos) u Oficial de Cumplimiento (en caso de datos personales) los requisitos de seguridad requeridos en su operación y/o proyectos de mejora o innovación que involucren datos personales.
l) Monitorear al cumplimiento de los requisitos de seguridad respecto de los activos de información que tiene en condición de propietario.

5.5.CUSTODIO DEL ACTIVO DE INFORMACIÓN

Cada colaborador que hace parte de la estructura orgánica, líder de la prestación de uno de los Servicios de esta organización, que accede y/o trata un activo de información en virtud de las funciones contratadas es considerado Custodio del Activo. Esta misma condición la tendrá toda persona que en calidad de prestador de servicios acceda y/o trate los activos de información. Son responsabilidades del custodio las siguientes:

a) Conocer, cumplir y velar por el cumplimiento de la política de seguridad de la información y normas que la desarrollan, con el fin de lograr que el activo de información se preserve seguro.
b) Proteger el activo de información entregado para el desempeño de las funciones contratadas, sea que la relación sea laboral o civil.
c) Impedir que terceros accedan y/o traten los activos de información sin autorización previa y expresa otorgada por el Propietario del Activo.
d) Comunicar, una vez tenga conocimiento, toda situación, sospecha o incidente que atente contra la seguridad del activo de información bajo su custodia y responsabilidad.
e) Colaborar en la investigación y entendimiento de todo incidente de seguridad que comprometa la seguridad del activo de información, como puede ser entre otros los siguientes: Fuga de información, acceso no autorizado; alteración de la información, destrucción del activo, entre otros.

6. AUTORIZACIONES DE ACCESO Y TRATAMIENTO DE LOS ACTIVOS DE INFORMACIÓN

El acceso y tratamiento de los activos de información por parte de los Custodios de estos se debe realizar mediante la solicitud que realiza el Propietario del Activo a la Dirección Digital , Coordinación de SGI- Sistema de Gestión Integral y/o gestión documental, según aplique, para que el colaborador o prestador de servicios en calidad de custodio acceda y trate los activos de información para el desempeño exclusivo de las funciones contratadas.

Es responsabilidad del Propietario del Activo solicitar e informar por los medios de atención establecidos, la fecha de inicio y terminación del derecho de acceso y tratamiento; así mismo debe informar la fecha de inicio y terminación del período de vacaciones, suspensiones, incapacidades y/o enfermedades.

7. DOCUMENTACIÓN DE LA SEGURIDAD

Para el logro de los objetivos estratégicos asociados a la seguridad de la información se requiere fortalecer la documentación de los procesos de seguridad, realizando una revisión periódica tanto a nivel de proceso de seguridad como a nivel de los controles. Para esta finalidad es conveniente, según las necesidades de seguridad, considerar los aportes que los diferentes marcos de referencia realizan en materia de seguridad y adoptar las mejores prácticas.

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