NORMA DE SEGURIDAD DE LA INFORMACIÓN DEL RECURSO HUMANO

CONTENIDO

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 las personas físicas en condición de colaboradores y de los roles que desempeñan, en virtud de una relación contractual de orden laboral, civil, comercial o legal, deban acceder a determinados activos de información en poder de esta organización.

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.7. relativo a la Seguridad del Recurso Humano establece como objetivo asegurar que todos los colaboradores y contratistas sean conscientes de las responsabilidades y deberes respecto de la obligación de protección de los activos de información a los que acceden en virtud de una obligación contractual y/o legal.
d) Que es necesario gestionar los riesgos de seguridad de la información en el marco de la gestión humana antes, durante y después de la relación laboral; necesidad que se extiende a las personas físicas contratadas a través de agencias de empleo o personas que laboral para terceros proveedores en las instalaciones de la organización y/o que acceden a activos de información de forma remota.
e) Que en el perfil de cada cargo existente en la organización deben identificarse los activos de información, las responsabilidades en materia de seguridad de la información y deberes de protección respecto de tales activos; lo cual deberá documentarse para fines de evidencia sobre la debida diligencia y demostración de tales responsabilidades.
f) Que los activos de información tendrán dentro de esta organización un "Propietario" responsable del mismo a quien corresponde identificar los derechos de acceso a los activos requeridos para el desempeño del cargo, los cuales estarán identificados en el perfil del cargo desempeñado. Las dudas en materia de seguridad de la información serán consultadas con el área responsable esta

materia. Así mismo, el "Propietario" del activo 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 en poder de esta organización que las personas que deban desempeñar las funciones contratadas en el marco de una relación laboral, civil o comercial, sean idóneas en términos de sus competencias profesionales y su escala de valores éticos; aspectos que deberán ser considerados en el proceso de selección, sea que se trate de una nueva vinculación o de un ascenso laboral.
h) Que es fundamental que la organización mantenga sensibilizado al personal sobre los riesgos de seguridad respecto de los activos de información, así como respecto de la existencia del marco de seguridad de la información y la normatividad adoptada en materia de protección de datos personales y demás regulaciones aplicables a la gestión de activos de información; para esto es fundamental la formación y educación, la cual puede ser obligatoria o voluntaria, según las normas legales que apliquen.
i) Que los terceros proveedores de esta organización que suministren personal y/o en ejecución de un contrato civil o comercial accedan a activos de información en poder de esta organización se obligan a seguir los parámetros aquí consignados para la gestión del recurso humano asignado a la ejecución de las obligaciones contractuales que existan con esta organización.

Con base en las anteriores consideraciones se procede a fijar las reglas aplicables a la gestión del recurso humano en el ámbito de la seguridad de la información, la cual comprende los datos personales, sin perjuicio de otros activos de información identificados en el respectivo perfil del cargo.

2. OBJETO

Este 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, en el marco de la gestión humana, la cual comprende el antes, la ejecución y el después de la relación laboral.

3. DESTINATARIOS

Son destinatarios de esta norma los colaboradores de todo nivel de esta organización quienes tienen el deber de gestionar de forma segura los activos de

información entregados por GASES DEL CARIBE para el desempeño de las funciones contratadas.

Es obligatorio cumplir con las obligaciones que en materia de seguridad de información tienen los colaboradores de esta organización respecto de los activos de información que gestionan, incluidos los datos personales, los bienes protegidos por la propiedad intelectual, la información empresarial, entre otros.

También son destinatarios los prestadores de servicios que suministren personal, los prestadores de servicios en el marco de un contrato civil, los colaboradores y/o contratistas de terceros proveedores que en la ejecución del contrato respectivo gestionen activos de información en poder de esta organización. Finalmente, quedan obligados en lo que aplique las personas con las cuales exista una relación de orden estatutario y/o legal que accedan, traten y gestionen uno o varios activos de información.

4. RESPONSABILIDAD EN LA GESTION SEGURA DE LA INFORMACION EN LAS RELACIONES LABORALES

Además de las funciones propias de cada cargo o rol existente en la estructura orgánica es necesario que en cada uno de ellos se identifiquen, definan, documenten y capaciten sobre las obligaciones de protección y gestión segura de los activos de información a los que se acceda en virtud del cargo y función contratada.

Cada Jefe de Área de los servicios que presta la organización deberá en compañía del departamento de Gestión Humana, participar en la definición, monitoreo y ajustes periódicos a los perfiles de cargo de sus dependientes, sean colaboradores, practicantes o terceros contratados a través de terceros proveedores.

Antes de crearse y/o modificarse las funciones de un cargo deberá tenerse presente lo aquí establecido. Resultado de esta necesidad organizacional en las relaciones laborales deberá cumplirse al menos con los siguientes requisitos:

i. En los casos que aplique según las funciones del cargo, perfil con un acápite especifico relacionado con: (i) Identificación de los activos de Información necesarios para el desempeño de las funciones contratadas, entre ellos bases de datos de información personal; y (ii) Obligaciones que aplican en materia de seguridad respecto de los activos de información identificados.
ii. Cláusula laboral de protección de datos en el contrato laboral.
iii. Acuerdo de Confidencialidad y Protección de datos personales, a partir del cual se entienden entregados los activos de información propios del cargo.

iv. Constancia de devolución de los activos de información, sea resultado de la terminación de la relación laboral o sea resultado del cambio en el cargo desempeñado.
v. Parámetros respecto del uso de los recursos informáticos asignados para el desempeño de las funciones contratadas.
vi. Constancia escrita de las actividades de sensibilización y/o capacitación en materia de seguridad de la información durante la relación laboral, como puede ser la referida a las políticas de seguridad; políticas de protección de datos personales y marco normativo; políticas en materia de propiedad intelectual; políticas en otros aspectos regulatorios vinculados a la seguridad de la información y/o tratamiento de información.

5. SEGURIDAD DE LA INFORMACION EN LOS TRES MOMENTOS DE UNA RELACION DE CARÁCTER LABORAL

En cada momento de la relación laboral a saber: antes de la contratación o proceso de selección, durante la ejecución del contrato laboral y terminado el contrato laboral, es importante seguir las siguientes reglas:

5.1. ANTES DE LA RELACIÓN LABORAL O DURANTE EL PROCESO DE SELECCIÓN DE PERSONAL

Antes de dar inicio al proceso de selección de personal para un cargo en la organización, sea que se busque proveer por externos o personal interno, deberá verificarse que el perfil del cargo del respectivo cargo tiene identificados los activos de información necesarios para el desempeño del cargo a contratar, así como las obligaciones que en materia de seguridad de la información sean aplicables, incluidos los roles y nivel de acceso, consulta, modificación, eliminación, según el caso.

Esta es una tarea inicial responsabilidad del jefe del Área o Departamento que requiere seleccionar la persona para la vacante o cargo existente. Verificado que el perfil del cargo esta actualizado así lo informará en el formulario de solicitud de selección de personal al Área de Desarrollo Humano para que inicie el proceso.

En caso de no estar actualizado el perfil del cargo lo informará al departamento de Gestión Humana, para la correspondiente actualización.

En la selección de personal esta organización deberá, en términos de las necesidades de seguridad de la información y protección de los activos de información relacionados con el cargo a desempeñar, tenerse presente las siguientes pautas:

- Cumplir con los requisitos de contratación de personal establecidos en el Procedimiento de Selección y Desarrollo (PD-A-12).
- Realizar pruebas profesionales para evaluar la idoneidad para el desempeño del cargo, en relación con la seguridad de la información y la protección de activos de información, cuando se considere necesario por la organización.
- Solicitar a terceros proveedores del proceso de selección y/o subproveedores del proceso de selección que cumplan lo aquí dispuesto por ser parte de la política de seguridad de la información.

Estas pautas deben ser exigidas igualmente a aquellos terceros proveedores que suministren personal y/o asignen a personal bajo su dependencia para ejecutar el respectivo contrato en el ámbito de esta organización.

El inicio de todo proceso de selección debe estar precedido por la firma del Aviso de Privacidad y Autorización de tratamiento de datos que gestiona el Oficial de Cumplimiento, como responsable de la privacidad de los datos.

Antes de celebrar el contrato laboral, la persona seleccionada deberá ser informada por la organización de las obligaciones de seguridad de la información y obligaciones de protección de los activos de información, así como de las consecuencias de una gestión negligente o inadecuada en esta materia.

5.2. DURANTE LA EJECUCIÓN DEL CONTRATO LABORAL

Celebrado el contrato de trabajo con la persona seleccionada para la vacante, sea una persona nueva externa a la organización o un colaborador que haya sido promovido, deberá en el proceso de inducción tenerse presente lo relativo a las responsabilidades y obligaciones que en materia de seguridad de la información aplican para la correcta gestión de activos de información como pueden ser los datos personales, la información protegida por la propiedad intelectual, la información estratégica y demás información que tenga representación económica o importancia para la organización o para terceros, entre otros.

5.2.1. RESPONSABILIDADES Y OBLIGACIONES EN LA EJECUCIÓN DE LAS FUNCIONES CONTRATADAS

Para todos los colaboradores de esta organización es obligatorio el cumplimiento del conjunto de normas que desarrollan la política de seguridad de la información.

Así mismo, el obligatorio el cumplimiento de la Política de Privacidad y la normativa interna adoptada para dar cumplimiento a las Leyes Estatutarias 1581 de 2012 sobre Protección de Datos Personales y 1266 de 2008 sobre Habeas Data Financiero.

Los colaboradores de esta organización quedan obligados a cumplir toda la normatividad interna que adopte esta organización para dar cumplimiento a regulaciones legales en materia de propiedad intelectual, lavado de activos, gestión documental, transparencia y/o estándares de industria que se adopten conforme las necesidades del negocio. En tal sentido, tales normas hacen parte de la relación laboral con los colaboradores de esta organización.

Esta normatividad, según el análisis de cada caso, aplicará a aquellas personas vinculadas por normas estatutarias a esta organización.

Previsiones en este sentido deberán ser exigidas a las empresas de servicios temporales y los proveedores cuyos colaboradores deban gestionar activos de información en ejecución de la relación contractual con estos. Esto deberá ser verificado antes de la contratación o inicio de la prestación del servicio por estos proveedores, correspondiendo al Área o Departamento que presta el Servicio, realizar esta actividad.

5.2.2. SENSIBILIZACIÓN

El Departamento de Gestión Humano durante el proceso de inducción al cargo de la persona contratada deberá sensibilizar respecto de las obligaciones, roles y responsabilidades derivadas de la Política de Seguridad de la Información, Protección de Datos Personales, Respuesta de incidentes de seguridad de la información, lavado de activos, prevención de fraudes y demás normatividad aplicable a la organización.

Desde el inicio de la relación con los colaboradores y colaboradores la organización deberá informar, sensibilizar y concientizar a estos respecto de la propiedad, derechos y/o custodia que tiene esta organización sobre los activos de información en su poder; los cuales, en ningún caso, podrán ser objeto de apropiación por parte de estos, incluso después de terminada la relación laboral.

5.2.3. EDUCACIÓN

En aras de crear una cultura de seguridad de la información en esta organización es conveniente formar a los colaboradores y demás

colaboradores en temas vinculados a la seguridad de la información, la protección de datos personales, respuesta de incidentes de seguridad de la información, lavado de activos, prevención de fraudes, entre otros.

La formación que se imparta a los colaboradores y colaboradores deberá ser periódica en la medida que los riesgos en materia de seguridad de la información cambian según las tendencias que atentan contra los activos de información.

En materia de protección de datos personales es necesario un proceso de formación general, específico y permanente, que sea evaluable, de forma que permita evidenciar la adecuada formación[1] de los colaboradores en esta materia, componente que hace parte de las instrucciones de la Superintendencia de Industria y Comercio contenidas en la Guía de Responsabilidad Demostrada.

Promover la formación de los colaboradores y colaboradores en otras regulaciones que apliquen a la organización es conveniente con el fin de mitigar los riesgos de infracción, como expresión de la debida diligencia de la Alta Dirección.

5.2.4. INCIDENTES DE SEGURIDAD

Es obligación de los colaboradores de esta organización reportar al departamento de Gestión Humana o superior inmediato cualquier sospecha de violación o incumplimiento de las responsabilidades, obligaciones y/o deberes vinculados a la seguridad de la información y/o de la protección de datos personales.

Para el efecto se tendrá presente lo dispuesto en la Norma sobre Gestión de Incidentes de Seguridad[2] adoptada por esta organización.

[1] Guía para la implementación del principio de responsabilidad demostrada, 2.5 Requisitos de formación y educación: "Un componente fundamental para implementar un programa de Gestión de Datos personales está en la educación y formación de todos los colaboradores de la organización."

[2] Guía para la implementación del principio de responsabilidad demostrada, 2.6 Protocolos de respuesta en el manejo de violaciones e incidentes: "… Es necesario que los sujetos obligados cuenten con 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."

5.2.5. CESIÓN DE LOS DERECHOS PATRIMONIALES DE AUTOR SOBRE CREACIONES INTELECTUALES

Durante la relación laboral deberá documentarse de forma periódica la cesión de los derechos patrimoniales de autor[3] que haya creado o en los que haya participado el colaborador durante la relación laboral.

5.2.6. PROCESO DISCIPLINARIO

Los incumplimientos de los colaboradores y/o colaboradores de esta organización respecto de las políticas de seguridad de la información y/o del régimen de protección de datos personales podrán ser objeto de procesos disciplinarios; para ello se aplicará lo dispuesto en la legislación laboral vigente.

Cuando el incumplimiento sea causado por colaborador contratado a través de una empresa de servicios temporales o sea colaborador de un proveedor de esta organización, se comunicará y notificará al colaborador de estos del incumplimiento para que estos apliquen lo dispuesto en el régimen laboral colombiano.

5.2.7. SUSPENSIÓN DE LA RELACIÓN LABORAL

Es aconsejable que, durante la suspensión de la relación laboral, sea originada en el período de vacaciones o licencias o en situaciones disciplinarias, se notifique de forma oportuna al Área de Sistemas por el superior del colaborador o colaborador esta situación, con el fin de restringir los accesos a los sistemas de información. En igual forma, deberá comunicarse el reintegro del colaborador a sus actividades con el fin de habilitar los accesos a los sistemas de información nuevamente.

5.3. DESPUÉS DE TERMINADO EL CONTRATO LABORAL

La terminación de la relación laboral con los colaboradores impone a estos responsabilidades, deberes y obligaciones en materia de seguridad de la información, protección de datos personales, propiedad intelectual, entre otras.

La terminación de la relación laboral implica que la organización, previo a ese momento, cumpla con los siguientes requisitos:

[3] Formato de cesión de derechos patrimoniales de autor.

- Identificar el inventario de activos de información entregado al colaborador para el desempeño de sus funciones.
- Documentar mediante acta la devolución de los activos de información entregados por la organización para el desempeño de sus funciones.
- Restringir el acceso al colaborador a los sistemas de información y/o recursos informáticos entregados para el desempeño de las funciones contratadas.
- Verificar que el colaborador cesó el uso de los recursos informáticos asignados para el desempeño de las funciones.
- Documentar la cesión de los derechos patrimoniales de autor respecto de las creaciones intelectuales desarrollas por los colaboradores en el marco de las relaciones laborales.

6. PERJUICIOS POR INFRACCIONES A LA SEGURIDAD DE LA INFORMACION

Es de importancia manifiesta que los colaboradores sean conscientes de las responsabilidades, obligaciones, cargas y deberes que asumen al acceder y/o gestionar activos de información en el desempeño de las funciones contratadas, los cuales son propiedad de esta organización o están bajo su custodia. La gestión de tales activos está sometida a lo dispuesto en las normas adoptadas en materia de seguridad de la información, protección de datos, gestión documental y demás regulaciones o normatividad interna que aplique a esta organización.

En materia de protección de datos personales, la ley prevé la posibilidad de imponer sanciones a las organizaciones y/o a las personas que realizan algún tratamiento de datos personales violando los principios previstos en el régimen de protección de datos personales; sanciones que pueden ser de orden económico hasta dos mil (2.000) Salarios Mínimos Mensuales Vigentes. Lo anterior, sin perjuicio de los daños causados a esta organización y/o titulares de los datos personales resultado de un incumplimiento de la ley.

La legislación penal en Colombia establece sanciones restrictivas de la libertad y económicas a las personas que incurren en la conducta denominada violación de datos personales consagrada en el artículo 269 F de la Ley 1273 de 2009 que reformo el Código Penal.

7. MONITOREO, REPORTE Y AUDITORÍA

Esta organización en calidad de Propietario de los activos de información o Responsable o Encargado de los activos de información entregados por terceros para su custodia tiene la obligación, deber y facultad de monitorear de forma periódica la forma como los colaboradores gestionan los activos de información,

así como la facultad de auditar el cumplimiento de las normas adoptadas por esta organización en materia de Seguridad de la Información, Protección de Datos Personales, Gestión Documental, Propiedad Intelectual, entre otras regulaciones legales y/o internas adoptadas para cumplir con la ley o buenas prácticas en materia de seguridad de la información.

Los resultados del monitoreo o auditoria deberán ser documentados. Las situaciones que puedan configurar violaciones a la ley, incidentes de seguridad de la información y/o incumplimientos de las políticas de seguridad de la información, protección de datos, gestión documental, propiedad intelectual, u otras, serán informadas a la Alta Dirección, a Desarrollo Humano, a Auditoria y a Sistemas.

GASES DEL CARIBE podrá auditar el cumplimiento de los requisitos de seguridad aplicables a la relación con colaboradores y/o colaboradores, sea realizando tal actividad de forma directa o a través de los terceros, usando medios físicos o automatizados.

8. TRANSPARENCIA Y ACCESO A LA INFORMACION PÚBLICA

Las disposiciones legales que apliquen en virtud del régimen de transparencia y acceso a la información pública contenido en la Ley Estatutaria 1712 de 2015 se interpretarán de forma armónica y sistemática con lo dispuesto en materia de protección de datos personales y seguridad de la información, de acuerdo con las directrices contenidas en la Sentencia de Constitucionalidad 274 de 2013.

8. INTERPRETACION SISTÉMICA

Lo dispuesto en la Política de Seguridad de la Información, la Política de Privacidad que desarrolla el régimen legal de protección de datos personales, las disposiciones de gestión documental y los demás regímenes legales que apliquen a esta organización deberán ser interpretados de forma armónica y sistémica teniendo presentes los derechos fundamentales que estén presentes, las normas legales y las necesidades de seguridad de la información de esta organización.

9. COLABORADORES EXTERNOS

Lo dispuesto en materia de Seguridad de la Información y Protección de Datos Personales para los colaboradores de esta organización será aplicable a las personas contratadas a través de empresas que suministran personal, así como a los colaboradores de terceros proveedores que ejecutan lo contratado a nombre de sus colaboradores en las instalaciones y/o infraestructura de esta organización.

En cada caso, el Propietario[4] del Activo de Información deberá analizar la pertinencia de lo dispuesto en materia de seguridad de la información y protección de datos personales en las relaciones con estos colaboradores externos.

Igual consideración se tendrá presente con aquellos colaboradores externos vinculados a la organización por los estatutos, como pueden ser miembros del Consejo Directivo, Auditores y Revisores Fiscales.

10. CONTROL

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

11. 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.

12. 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

[4] Norma de asignación de responsabilidades de seguridad de la información: "Hace referencia al lider de cada Servicio que soporta la operación de esta organización; quien tiene la capacidad de decidir y tomar decisiones 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 clasifican adecuadamente según los criterios adoptados por esta organización".