NORMA DE RIESGOS EN PROTECCIÓN DE DATOS PERSONALES

CONTENIDO

1. OBJETO

Este Norma que desarrolla la Política de Seguridad de la Información de GASES DEL CARIBE tiene como objetivo describir el esquema de riesgos que adopta esta organización en materia de protección de datos personales.

2. 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.

3. ENFOQUE DE RIESGOS

En este documento se describen los momentos y consideraciones para realizar la gestión de riesgos al evaluar la operación de la organización para el caso puntual de la Protección de Datos Personales teniendo presente el principio de Responsabilidad Demostrada.

Un esquema de gestión de riesgo debe incorporar una visión sistémica que comprenda el ciclo PHVA; por tanto, se tendrán presentes las siguientes etapas:

i. Planificar la Gestión de Riesgos
ii. Identificación de Riesgos
iii. Análisis de Riesgos
iv. Tratamiento de los Riesgos
v. Implementación de los planes de acción
vi. Monitoreo de los riesgos y procesos de gestión

A continuación, se describen el alcance y consideraciones de cada uno de ellos.

4. PLANIFICAR LA GESTIÓN DE RIESGOS

Esta etapa consiste en que los involucrados en el gobierno de la protección de Datos Personales en la organización definan los parámetros de la gestión del programa integral de datos personales, teniendo en consideración, entre otras cosas: Personas que participaran en el proceso de riesgos en materia de protección de datos personales, así como sus roles y responsabilidades

- La tolerancia a los riesgos que tiene la organización y consideraciones al respecto
- Las conclusiones serán documentadas por el oficial de cumplimiento y el jefe del área de riesgo.

5. IDENTIFICAR LOS RIESGOS

En este proceso se identifican los riesgos que puedan derivarse del tratamiento de datos personales en la operación empresarial considerando estos en relación con el cumplimiento del régimen de protección de datos personales teniendo presente el principio de Responsabilidad Demostrada.

Estos riesgos se documentarán dejando de presente las eventuales consecuencias o efectos negativos en caso de materializarse el riesgo para la organización.

Como primera medida se debe realizar una primera Identificación de riesgos, con los riesgos más evidentes y posteriormente en las reuniones de seguimiento se revisarán estos para analizar si siguen vigentes, si se han transformado y/o si se deben incluir nuevos.

Al documentar los riesgos se tendrá presente lo siguiente:

A continuación, se describen los campos que debe contener cada riesgo y las consideraciones para su análisis:

- ID: Se asignará un código con un número consecutivo, cada riesgo debe tener su identificador individual, el propósito de este identificador es poder tener una referencia para hacer mención a él en actas o documentos de control.

- Descripción: En este campo se realiza una descripción clara del riesgo, se recomienda que contenga tres elementos en la descripción, la causa, la consecuencia y el efecto concreto para la organización.

- Proceso empresarial: Especificar el Proceso Empresarial o área que estará encargada de este riesgo y la implementación de sus planes de acción

6. ANALIZAR LOS RIESGOS

En esta etapa se realizará un análisis de cada uno de los riesgos identificados, los criterios principales para establecer la prioridad o criticidad del riesgo serán la probabilidad y el impacto.

En el análisis del riesgo se tendrá presente respecto de cada riesgo lo siguiente:

- Probabilidad de ocurrencia: Asignar un valor de probabilidad. La determinación de la probabilidad de ocurrencia exacta de un riesgo puede ser difícil de cuantificar o requerir métodos estadísticos avanzados, por esta razón se establece una escala para clasificar las probabilidades:

- Escala de probabilidad: Esta podrá ser

    - Casi inminente
    - Muy probable
    - Medianamente probable
    - Poco Probable
    - Difícil ocurrencia

- Impacto: De la misma manera que la probabilidad, el impacto también tiene un carácter cualitativo.

Es pertinente asignar un valor de impacto conforme a la siguiente escala:

    - Crítico: Además de afectar la reputación y de requerir una gestión, puede llegar a implicar una multa, indemnización, cierre, suspensión o denuncia penal
    - Medio Alto: Puede afectar la imagen (Reputacional), implica una gestión, sin embargo, NO implica multa, indemnización, cierre, suspensión o denuncia penal

- Medio: Implicaría una gestión interna o externa, resultado de una investigación o requerimiento judicial
- Leve: Se crearía un incidente con el titular del dato que implica una gestión detallada pero no compleja
- Muy leve: Puede causar inconformidades con el titular del dato, sin embargo, no supone una gestión importante

- Calificación: Este campo deberá ser determinado y es resultado de multiplicarla escala de probabilidades por la escala de impacto.

Conforme a la calificación de riesgos se podrá establecer el nivel de criticidad del riesgo conforme los siguientes criterios:

- Categorías: Establecer las categorías en materia de protección de datos considerando los criterios que permitan evaluar el cumplimiento del régimen de protección de datos personales a la luz del Principio de Responsabilidad Demostrada.

- Subcategoría: De cada categoría podrán establecerse subcategorías que permitan a un mayor nivel de análisis evaluar el cumplimiento del régimen de protección de datos personales a la luz del Principio de Responsabilidad Demostrada.
- Sanciones: De acuerdo con el tipo de situación de riesgo que pudiere presentarse se establecerá si la misma puede dar lugar a multas económicas, operativas (Suspensión o cierre de bases de datos) y/o reputacional; sin perjuicio de otros efectos derivados del incumplimiento del régimen de protección de datos personales, como pueden ser incumplimientos contractuales.

7. TRATAMIENTO DE LOS RIESGOS

En esta etapa se procede con base en cada riesgo a diseñar uno o varios planes de acción según la criticidad del riesgo.

- Plan de Acción: Se deben especificar las acciones que se definen con el fin de escalar, evitar, mitigar, transferir o aceptar el riesgo y en caso de que se vaya a realizar un plan de contingencia cuáles serán las acciones que se ejecutarán para prepararlo.

- Técnica: Se debe especificar si el plan de acción corresponde a escalar, evitar, mitigar, transferir o aceptar el riesgo

- Responsable: Se debe asignar un responsable dentro de la organización, el cual será el "propietario" del riesgo, esta persona tiene la responsabilidad de que se lleven a cabo los planes de acción y a informar cualquier cambio en la probabilidad o impacto del mismo.

- Fecha: Se debe especificar la fecha en la que se ejecutaran las acciones que hacen parte del plan de acción.

8. IMPLEMENTACIÓN DE LOS PLANES DE ACCIÓN

Esta etapa consiste en implementar los planes de acción acordados para afrontar los riesgos, el principal beneficio de este momento es garantizar que tales planes se lleven a cabo y así minimizar o eliminar las amenazas propias del riesgo.

Cada uno de los responsables definidos para cada riesgo deben comprometerse con asegurar todos los recursos para ejecutar los planes de acción y coordinar todas las actividades asociadas.

De igual manera debe informar cualquier inconveniente que encuentren en esta misión.

Para la implementación de los planes de acción se recomienda tener en cuenta:

- Lecciones aprendidas de la organización
- Los planes registrados para gestionar los riesgos identificados
- La gestión del presupuesto
- Los umbrales y tolerancia de riesgos en cada proceso o servicio organizacional
- Registrar los incidentes que se presenten en la implementación de los planes
- Actualizar la información respecto de los riesgos identificados según la realidad de estos

9. MONITOREO DE LOS RIESGOS Y PROCESOS DE GESTIÓN

Periódicamente durante la gestión deben revisarse los riesgos y actualizar la información propia del riesgo según su dinámica, así mismo adicionar o retirar riesgos y mantener actualizados los planes de acción.

- Seguimiento: Documentar la evolución del riesgo a lo largo del tiempo, dejando una trazabilidad de la gestión, la cual es de gran utilidad para el monitoreo y para presentar reportes a la Alta Dirección y a la autoridad de protección de datos personales.

- Estado Actual: Especificar la situación actual del riesgo se encuentra Abierto, Eliminado, Materializado, Cancelado o Suspendido

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