Manual.

Manual lineamientos en protección y tratamiento de datos personales

RT-Ma04

SISTEMA GESTIÓN DE CALIDAD

SENADO DE LA REPÚBLICA

TABLA DE CONTENIDO

:

1. OBJETIVO

Definir y establecer los lineamientos generales, funciones y obligaciones de los responsables y usuarios de la gestión y tratamiento de la información de carácter personal.

2. ALCANCE

El presente documento será de aplicación a las bases de datos que contienen información de carácter personal que se encuentre bajo la responsabilidad del SENADO DE LA REPÚBLICA DE COLOMBIA y será aplicable a todos los funcionarios, contratistas, proveedores y grupos de interés de la entidad.
Las políticas, metodologías, lineamientos y definiciones incluidas en el presente manual son de obligatorio cumplimiento por parte de todos los grupos de interés y las violaciones a lo dispuesto en el presente documento pueden someter a los funcionarios, contratistas, proveedores y grupos de interés de la entidad, a la imposición de sanciones administrativas, disciplinarias y penales.

3. TÉRMINOS Y DEFINICIONES

- **Aceptación del riesgo**: decisión informada de asumir un riesgo concreto.
- **Activo de información de datos personales**: en relación con la seguridad de la información en datos personales, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, archivos físicos y digital, entre otros) que tenga valor para el SENADO DE LA REPÚBLICA DE COLOMBIA.
- **Amenaza**: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.
- **Análisis del riesgo**: busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.
- **Autorización**: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. Téngase en cuenta que el consentimiento es el eje vertebral de la protección de datos personales y ello exige que como regla general no se puedan tratar datos personales de nadie sin su consentimiento, sin perjuicio de que en ocasiones esta obligación esté exenta. Por ejemplo, cuando los datos se traten en el marco de la relación comercial, laboral o administrativa, cuando exista una Ley que disponga lo contrario.
- **Base de datos**: conjunto organizado de datos personales que sea objeto de Tratamiento. Siempre que exista un conjunto de datos que estén organizados mediante algún criterio, nos encontraremos ante la existencia de una base de datos. Obviamente una aplicación informática de nóminas constituye un ejemplo de base de datos, pero también lo puede constituir una tabla de datos en Word, sin olvidar que también es aplicable este concepto a los datos no automatizados: por ejemplo, un archivo A-Z.
- **Bases de datos descentralizadas**: son aquellas que responden a un mismo contenido, finalidad y propósito, pero pueden responder a distintos tratamientos o encontrarse en repositorios diferentes, pero forman parte integral de la base de datos registrada o inscrita en el RNBD.
- **Bases de datos temporales**: son aquellas que se generan en la operación diaria de tratamiento de los registros de las bases de datos principales y están conformadas por copias de los datos protegidos sobre otras bases de datos o archivos informáticos para tratamientos especiales. Las bases de datos temporales deberán cumplir el nivel de seguridad correspondiente a la tipología de datos tratados y a su nivel de riesgo y serán borrados o almacenados en los servidores una vez que hayan dejado de ser necesarios.
- **Comunicación / cesión de datos:** toda revelación de datos realizada a una persona o entidad distinta del interesado. La cesión de datos debe estar, salvo excepciones, necesariamente consentida por el interesado. Por ello, es importante no comunicar datos de carácter personal a otras personas físicas o jurídicas, salvo que se disponga del consentimiento de dicha persona o se esté ante alguna de las excepciones previstas por la Ley.
- **Comunicación del riesgo**: comunicar o intercambiar la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.
- **Confidencialidad**: la propiedad que esa información esté disponible y no sea divulgada a entidades, personas o procesos no autorizados.
- **Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los

riesgos de seguridad en datos personales por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Es decir, cualquier dato que podamos relacionar con personas físicas. En el ámbito del SENADO DE LA REPÚBLICA DE COLOMBIA esas personas serán normalmente potenciales socios, clientes, proveedores, trabajadores de la entidad, terceros o personas de contacto. En algunos ámbitos concretos de actividad puede que los datos se refieran a otras personas como pacientes, asociados o por ejemplo en el ámbito público dichos afectados son los ciudadanos, contribuyentes entre otros, además de algunos afectados comunes al ámbito privado: por ejemplo, los funcionarios, proveedores, contactos, entre otros. Téngase en cuenta que no sólo se refiere a personas identificadas (cuando tengamos su nombre) sino también cuando esas personas sean razonablemente identificables a través de un identificador: por ejemplo, número de colegiado, CC, IP, correo electrónico y demás información que lo relacione o identifique.
- **Disponibilidad:** la propiedad de estar disponible o utilizable cuando se requiera para personal autorizado.
- **Encargado del tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. El encargado del tratamiento es un tercero (normalmente una empresa, pero no necesariamente) que le presta un servicio al responsable del tratamiento y que para ello requiere acceder a datos del responsable. Ejemplos típicos de encargados lo son la asesoría laboral, contable o fiscal (que accede a los datos de funcionarios, clientes o proveedores de su cliente para asesorarle), empresas de mantenimiento de hardware o software, entre otras.
- **Establecimiento del contexto**: al establecer el contexto, SENADO DE LA REPÚBLICA DE COLOMBIA articula sus objetivos estratégicos y de calidad, define los parámetros externos e internos que se van a considerar en la gestión de riesgos y establece el alcance y los criterios de riesgo.
- **Estimación del riesgo**: proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evaluación del riesgo**: proceso usado para determinar las prioridades de gestión del riesgo mediante la comparación de los resultados de la calificación y el grado de exposición al riesgo.
- **Evitación del riesgo**: decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Gestión del riesgo**: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- **Identificación del riesgo**: proceso para encontrar, numerar y caracterizar los elementos del riesgo.
- **Impacto**: cambio adverso en el nivel de los objetivos del negocio logrado.
- **Integridad**: la propiedad de salvaguardar la integridad y exactitud de los activos.
- **Plan de tratamiento de riesgos**: documento que define las acciones para gestionar los riesgos de seguridad de la información en datos personales inaceptables y determinar los controles necesarios para proteger la misma.
- **Probabilidad**: frecuencia o Factibilidad de ocurrencia del Riesgo.
- **Propietario del riesgo**: persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
- **Reducción del riesgo**: acciones que se toman para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas a un riesgo.
- **Responsable de protección de datos personales**: el responsable del tratamiento designará uno o varios responsables de privacidad o seguridad encargados de coordinar y controlar las medidas definidas en el Manual de Procedimientos. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable de la base de datos.
- **Responsable del tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos o el tratamiento de los datos. El responsable de la base de datos, normalmente coincidirá con la organización: la empresa, asociación, institución, empresarios individual, profesional o entidad y es a quien se le imponen la mayoría de las obligaciones en protección de datos siendo, por tanto, normalmente el responsable de las sanciones que - en su caso - se impongan. Ello sin perjuicio de que el responsable de la base de datos pueda nombrar una persona física que le represente.
- **Riesgo**: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo residual:** el riesgo remanente después del tratamiento del riesgo.
- **Riesgo de seguridad de la información en datos personales**: potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- **Titular**: persona natural cuyos datos personales sean objeto de Tratamiento. Es la persona cuyos datos se tratan, es decir: el cliente, paciente, ciudadano, empleado, proveedor, visitante, contacto, entre otros.
- **Transferencia del riesgo**: compartir con otra de las partes la ganancia o pérdida de un riesgo.
- **Tratamiento**: cualquier operación o conjunto de operaciones realizadas sobre los datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Téngase en cuenta la definición de tratamiento que da la Ley, cualquier operación que se haga con ellos: grabarlos, modificarlos, conservarlos, enviarlos, constituirá tratamiento.
- **Usuarios:** sujeto o proceso autorizado a acceder a datos o recursos. Normalmente un usuario será una persona que accede a datos de la organización. El usuario podrá tener diferentes perfiles de acceso y ser un usuario interno o externo (un usuario de otra organización que accede a nuestro sistema para prestar un servicio, por ejemplo, mantenimiento informático).
- **Valor del Activo**: está determinado por el valor de la confidencialidad, integridad y disponibilidad del activo de información.
- **Valor del Impacto**: está determinado por el responsable del activo de información, quién provee cuanto se vería afectado por incidentes de los activos a cargo.
- **Vulnerabilidad**: debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Fuente: Tomado de **www.funcionpublica.gov.co** y **www.sic.gov.co**

4. DESARROLLO DEL CONTENIDO

4.1. MARCO NORMATIVO

La Constitución Política de Colombia de 1991 consagró en el artículo 15 el derecho de protección de datos personales (núcleo esencial del Habeas Data) definido como el derecho fundamental de toda persona para conocer, actualizar, rectificar o cancelar la información y datos personales que de ella se hayan recolectado y se traten en bases de datos por parte de entidades públicas o privadas. La Corte Constitucional en Sentencia C-748 de 2011 siguiendo los lineamientos jurisprudenciales de esa Corporación define los contenidos mínimos que se desprenden de este derecho así:

1. Derecho de las personas a conocer la información que sobre ellas está recogida en bases de datos.
2. El derecho de incluir nuevos datos con el fin de que se cuente con una imagen del titular.
3. El derecho a actualizar la información.
4. El derecho a que dicha información sea corregida o rectificada, con el fin que concuerde con la realidad.

El derecho a excluir información de una base de datos, o porque se está haciendo un uso indebido de ella, o por la voluntad del titular (salvo las excepciones establecidas en la ley).

Este derecho fundamental fue objeto de regulación por el legislador a través de la Ley Estatutaria 1581 de 17 de octubre de 2012, conocida como el Régimen General de Protección de Datos Personales, reglamentada por los Decretos 1377 de 2013 y 886 de 2014, hoy incorporados en el Decreto 1074 de 2015.

El artículo 19 de la LEPD estableció como máxima autoridad en materia de protección de datos personales a la Superintendencia de Industria y Comercio – SIC.

El decreto 620 de 2020 determina en materia de protección y tratamiento de datos personales, las bases y medidas necesarias que deben adoptar las entidades públicas en el manejo de los datos digitales.

4.2. NIVELES DE RIESGO DE LOS DATOS

Los riesgos de gestión, corrupción y de seguridad digital, en el Senado de la República, tendrán un carácter prioritario y estratégico, fundamentado en el modelo de operación por procesos, conforme a los parámetros del Modelo Integrado de Planeación y Gestión -MIPG-, para lo cual se tendrán en cuenta los procesos estratégicos, misionales, de apoyo y de evaluación. Por tal razón, la identificación, análisis y valoración de los riesgos y controles, se circunscribirá a los objetivos de cada proceso.

4.2.1. Establecimiento del contexto: El objetivo de esta etapa es conocer a la organización para determinar lo que puede afectarla a nivel interno y externo en cuanto a la protección de datos personales y su impacto.

Para el establecimiento del contexto, la entidad identifica y revisa las condiciones internas y externas del entorno que pueden generar eventos que afecten su capacidad para lograr los resultados previstos de seguridad en datos personales.

La evaluación del contexto interno y externo de la organización puede incluir entre otros:

• El ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local.

• Los medios de tratamiento y de las tecnologías que se utilizan en la organización y, en particular, aquellas que introduzcan mayores riesgos para la privacidad.

• Las categorías de datos personales que se deben tratar, finalidades para las que se usan cada una de ellas, necesidad de su utilización y colectivos afectados.

• Quién accede a cada categoría de datos personales y los motivos y justificaciones para ello.

• Sistemas de información, flujos de información: recogida, circulación dentro de la organización, cesiones fuera de la misma y recepciones de datos personales procedentes de otras organizaciones, y toma de decisiones.

• Identificación de personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos.

• Política(s) de protección de datos existente o mecanismos de planificación, implantación, verificación y corrección eficaces.

• Recursos humanos, físicos, tecnológicos, financiero y de tiempo asignados para la protección de datos personales.

La identificación de los riesgos se realizará de acuerdo con lo definido en la política de datos personales y en los procedimientos y lineamientos referentes a la seguridad de la información adoptados por la entidad. Sin embargo, el Responsable de tratamiento de datos, podrá implementar medidas o procedimientos adicionales cuando así considere oportuno.

4.2.2. Valoración del riesgo (Guía para la administración del riesgo y el diseño de controles en entidades públicas-Función Pública, 2018): La valoración del riesgo en datos personales describe cualitativa y cuantitativamente el riesgo y permite a los líderes de procesos priorizar los riesgos de acuerdo con la gravedad percibida u otros criterios establecidos.

La valoración del riesgo determina el valor de los activos de información de datos personales, identifica los causales de riesgo que existen (o que podrían existir), identifica el impacto en los riesgos identificados, determina las consecuencias potenciales, y finalmente prioriza los riesgos derivados y los clasifica frente a los criterios de evaluación del riesgo determinados en el contexto establecido.

• **Análisis del riesgo:** Esta etapa busca establecer la probabilidad de ocurrencia de los riesgos en datos personales y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

• **Identificación del riesgo**: Es el proceso para encontrar, numerar y caracterizar los elementos del riesgo. El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Para llevar a cabo esta actividad es importante contar con la información que se relaciona a continuación:

• **Identificación de los activos de información en datos personales**: Teniendo claro cuál es el alcance y los límites de la gestión de riesgos, se identifican los activos de información en datos personales teniendo claro que un Activo es todo aquello que tiene valor para la entidad. Estos activos se listan incluyendo:

- Nombre del proceso
- Activo de información de datos personales

- Cargo Responsable
- Custodio
- Medio de Almacenamiento
- Clasificación de la información (Privado, Semiprivado, Público o sensible)
- Encargado del tratamiento
- Responsable del tratamiento
- Ubicación
- Estado del Activo
- Propiedades del activo de información: Confidencialidad, integridad, Disponibilidad
- Valor del Activo

• **Identificación de la Causas de riesgo**: Se realiza la identificación de las vulnerabilidades y amenazas de los activos de información en datos personales. A continuación, se detalla una descripción general de los conceptos y las responsabilidades:
• Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Algunas amenazas pueden afectar a más de un activo de datos personales. En tales casos puede causar diferentes impactos dependiendo de los activos que se vean afectados.

• Es responsabilidad de los líderes de procesos realizar la identificación de las Amenazas.
• Se deben identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos de información en datos personales o al SENADO. Es importante anotar que un control implementado de manera incorrecta o que funcione mal, o un control que se utiliza de modo incorrecto podrían por si solos constituir una vulnerabilidad.
Es responsabilidad de los líderes de procesos realizar la identificación de las Vulnerabilidades.
• Identificación del riesgo: Consiste en la identificación del riesgo en datos personales a raíz de las amenazas y vulnerabilidades asociadas. Se realiza una descripción puntual del riesgo asociado a los activos de información.
Se especifica una base estándar de riesgos como se especifica en la figura 1, pero queda abierto para la inserción de nuevos riesgos:

TABLA DE RIESGOS
Fuga de información
No disponibilidad de la información
Incumplimientos Legales
Acceso no autorizado
Perdida total de la información
Violaciones de la confidencialidad de los datos personales

• **Identificación del dueño del riesgo**: Se realiza la identificación del dueño del riesgo para la definición de responsabilidades y planes de mitigación.
• **Identificación tipo de Impacto**: Se definen los siguientes tipos de impactos de acuerdo a los requerimientos del SENADO DE LA REPÚBLICA:

- Financiero
- Continuidad Operativa
- Imagen/Reputación
- Legal

Los tipos de impactos están relacionados directamente con los tipos de riesgo. Esto permite que basado en el tipo de riesgo identificado se realice una asociación al tipo de impacto que este riesgo genera y se pueda realizar su calificación. Esta relación se evidencia a continuación:

- Tipo de impacto
- Continuidad Operativa
- Legal
- Imagen
- Financiero

• **Estimación del riesgo**: El propósito de la estimación del riesgo es determinar los valores cuantitativos y cualitativos del Impacto y la Probabilidad de Ocurrencia del Riesgo. Los rangos y los valores cualitativos son establecidos por la entidad de acuerdo a las necesidades del negocio.
Se realizan las siguientes estimaciones para el riesgo:
• **Identificación de controles:** Se realiza la identificación de los controles implementados en el SENADO DE LA REPÚBLICA para tratar los riesgos. Puede que no existan controles para el tratamiento del riesgo, esto afectara el resultado del riesgo residual e indicara, según los niveles de probabilidad de ocurrencia e impacto, que deberán tener un tratamiento mediante la implementación de controles. La identificación de los controles permite hacer un seguimiento a la eficacia de las implementaciones y poder así realizar ciclos de mejora continúa a los mismos.
• **Estimación de Riesgo Residual**: Se evalúa el valor del impacto y la probabilidad de ocurrencia del riesgo residual, es decir, se tienen en cuenta los controles existentes en la entidad para el tratamiento de los riesgos identificados. El resultado es el nivel de riesgo residual controlado mediante salvaguardas.
Para esto se realizan las siguientes etapas:
• **Valoración del impacto**

El impacto se determina teniendo en cuenta los criterios de impacto definidos según se identifica en las siguientes figuras:

NIVEL	VALOR	FINANCIERO	CONTINUIDAD OPERATIVA
		La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la Organización.	Tiempo en que se ve afectada la operación de los procesos de la Organización.
Insignificante	1	Si el hecho llegara a presentarse, la Organización no tendría consecuencias económicas que impacten el funcionamiento, por tanto se asumirán las perdidas.	Si el hecho llegara a presentarse, el proceso de la Organización no se vería afectado en su continuidad.
Menor	2	Si el hecho llegara a presentarse, la Organización tendría bajas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera mínima.
Moderado	3	Si el hecho llegara a presentarse, la Organización tendría medianas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera moderada.
Mayor	4	Si el hecho llegara a presentarse, la Organización tendría altas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera considerable interrumpiendo periódicamente el proceso y otros.
Catastrófico	5	Si el hecho llegara a presentarse, la Organización tendría nefastas consecuencias económicas.	Si el hecho llegara a presentarse, el proceso de la Organización se vería afectado en su continuidad de manera total.

NIVEL	VALOR	IMAGEN	LEGAL
		Afectación sobre la imagen y reputación de la Organización.	Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones.
Insignificante	1	Si el hecho llegara a presentarse, tendría consecuencias o efectos sobre un grupo de funcionarios de manera interna.	Si el hecho llegara a presentarse, la organización tendría multas.
Menor	2	Si el hecho llegara a presentarse, tendría un impacto leve en la Organización que sería reparable a corto plazo	Si el hecho llegara a presentarse, la organización tendría demandas.
Moderado	3	Si el hecho llegara a presentarse, tendría un impacto medio en la Organización de manera local.	Si el hecho llegara a presentarse, la organización tendría una investigación disciplinaria.
Mayor	4	Si el hecho llegara a presentarse, tendría un impacto alto en la Organización a nivel gremial.	Si el hecho llegara a presentarse, la organización tendría una investigación fiscal.
Catastrófico	5	Si el hecho llegara a presentarse, tendría un impacto catastrófico en la Organización a nivel nacional/ internacional.	Si el hecho llegara a presentarse, la organización tendría sanciones legales. Podría generar el cierre definitivo de la Organización.

Figura 1. Valor del impacto.

Es responsabilidad de los líderes de procesos realizar la identificación de las consecuencias y nivel de impacto que puede tener la pérdida de confidencialidad, integridad y disponibilidad de los activos de información de datos personales.

• **Nivel de probabilidad del riesgo**

NIVEL DE PROBABILIDAD		DESCRIPCIÓN
1	Raro	El riesgo ocurre rara vez en la Organización.
2	Improbable	El riesgo ocurre en ocasiones especificas en la Organización.
3	Posible	El riesgo ocurre con cierta periodicidad en la Organización.
4	Probable	El riesgo ocurre frecuentemente en la Organización.
5	Casi Seguro	El riesgo ocurre inminentemente en la Organización.

Figura 2. Nivel de probabilidad del riesgo.

• **Evaluación del riesgo**

Para el cálculo del valor del riesgo se considera la siguiente ecuación:

VALOR DEL RIESGO = Valor Impacto * P(r)

En donde:

Valor del Impacto: Está determinado por el responsable del activo de información o el dueño de los riesgos del proceso quienes determinan los niveles de impacto de manifestarse un riesgo sobre los activos de información en datos personales.

P(r): Es determinada por el responsable del activo de información o el dueño de los riesgos del proceso quienes determinan la probabilidad de ocurrencia del riesgo identificado.

Como salida de éste cálculo se obtiene una lista con los niveles de tolerancia según el rango de valores en que se encuentre y el tratamiento que se debe realizar a los riesgos identificados. Se evidencian en la siguiente figura:

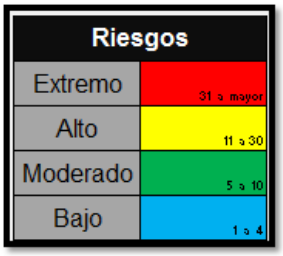

Figura 3. Valoración del riesgo.

Conforme a lo establecido en la política integral de gestión del riesgo; Para el Senado de la República el nivel de aceptación del riesgo está sujeto al tratamiento, manejo y seguimiento a los riesgos que afectan el logro de los objetivos institucionales y son considerados para cada uno de los procesos.
Los riesgos calificados en la zona como bajo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y este puede ser aceptado, y estar sujetos a monitoreo.
El riesgo en zona moderada, se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo y se hace seguimiento del mismo.
En caso de que el riesgo identificado se considere alto o extremo se debe incluir en el matriz de riesgo Institucional y se establecen acciones de control preventivas que permitan mitigar la materialización del riesgo y se debe hacer seguimiento.
En los riesgos de seguridad digital identificados como alto o extremo, se consolidará el plan de tratamiento de riesgos de Seguridad de la Información.
Los riesgos de corrupción son inaceptables siempre deben conducir a un tratamiento por parte de la entidad.

4.3. INVENTARIO BASES DE DATOS PERSONALES

El SENADO DE LA REPÚBLICA DE COLOMBIA, ha estipulado para identificar, inventariar y actualizar sus bases de datos, de acuerdo con lo establecido en la legislación nacional, especialmente lo definido en la ley 1581 de 2012 y demás normas vigentes y concordantes, los siguientes criterios generales:

• Finalidad

El SENADO DE LA REPÚBLICA ha identificado las bases de datos de acuerdo con su finalidad. Lo anterior bajo el entendido que una base de datos central e inscrita puede segregarse en otras descentralizadas que responden a un mismo contenido y propósito, pero responde a distintas formas de tratamiento o encontrarse en repositorios diferentes a la base central.

• Forma de tratamiento:

a. Base de datos automatizada : EL SENADO DE LA REPÚBLICA identifica como base de datos automatizada aquella que se almacena y administra con la ayuda de herramientas informáticas o sistemas de información automatizados; comprende las siguientes características: (i) Recoge datos que sean uniformes, en el sentido de ser orientados a un determinado fin; (ii) Que esté organizada, esto es que sus contenidos estén dispuestos de una forma determinada de acuerdo con la decisión tomada para el efecto por el responsable de la información. En definitiva, se define como un conjunto de datos tratados de forma unitaria o uniforme, relacionados entre sí y referidos a una misma cuestión, asunto, aspecto o tema, asociados a una persona y que pueden ser tratados para fines determinados de forma descentralizada.

b. Base de datos física (papel): EL SENADO DE LA REPÚBLICA identifica una base de datos física o manual cuando contiene archivos cuya información se encuentra organizada y almacenada de manera física. Estos archivos o carpetas pueden estar compuestos por cualquier tipo de soporte o conjunto documentos físicos vinculados a las personas y organizados por criterios específicos relativos a las personas; el tratamiento de estos documentos responde a una finalidad común y determinada.

4.4. FUNCIONES Y OBLIGACIONES

Se definen dentro de la entidad unas funciones y obligaciones específicas:

4.4.1. Dirección General Administrativa

• Propender por el cumplimiento de la protección de datos personales a todo nivel en el SENADO a través de la asignación de los recursos necesarios para tal fin y de la aprobación de políticas generales que faciliten la implementación y capacitación de los funcionarios del SENADO en cuanto a los mecanismos de control necesarios para el cumplimiento de la protección de datos personales.
• Designar la persona que asumirá el rol de oficial de protección de datos personales dentro de la organización.
• Destinar recursos suficientes para la gestión integral de protección de datos personales.
• Informar a la Jefatura de la División de Planeación y Sistemas cada vez que se presenten novedades en el ingreso y retiro de contratistas bajo la modalidad de prestación de servicios.
• Verificar que los contratos formalizados con terceros que tengan la consideración de encargados de tratamiento de datos, cuenten con todos los requerimientos legales.

4.4.2. División de Planeación y Sistemas.

• Mantener permanentemente informados a los responsables de cada proceso de la organización, el estado del cumplimento de las normas y las políticas implementadas para la Protección de Datos Personales y evidenciar las debilidades detectadas en el desarrollo de la labor.
• Diseñar mecanismos de control, indicadores de gestión y de prevención de riesgos, con el fin de garantizar la correcta evaluación y seguimiento de las reglas y políticas de Protección de Datos Personales.
• Implementar buenas prácticas con relación a la seguridad de la información.
• Adoptar las medidas necesarias para que los usuarios del SENADO conozcan las políticas de seguridad de la información, así como las consecuencias en que pudieran incurrir en caso de incumplimiento de las mismas.
• Diseñar dentro del “Plan de continuidad” los procesos que sean considerados críticos en cuanto al manejo de la información, de manera que permitan recuperar y restaurar de manera confiable y veraz la información que sea vulnerable en casos de desastre o de debilidad del sistema. Se incluye la implementación de servidores espejo para respaldo de la información.

• Definir y mantener políticas sobre la seguridad de la información que es almacenada en los medios electrónicos, magnéticos y físicos de la entidad.
• Verificar que, con anterioridad a la implementación o modificación de los sistemas de información, las pruebas no se realicen con datos reales, salvo que se garantice el nivel de seguridad correspondiente al tipo de base de datos tratada.
• Elaborar y dar cumplimientos a las políticas de auditorías de seguridad de la información de la Entidad relativas a información personal.
• Establecer controles sobre servicios tercerizados que almacenen información personal. Tanto a nivel técnico como de seguridad física.
• Verificar que los procedimientos de retiro de usuarios de los sistemas de información estén coordinados con la División de Recursos Humanos y la Dirección General Administrativa.

4.4.3. Oficial de Protección de Datos Personales

El SENADO DE LA REPÚBLICA designara una persona para desempeñar el Rol de Oficial de tratamiento de datos personales, con el propósito de velar y garantizar el uso adecuado de la información suministrada en las bases de datos. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al Responsable del Tratamiento de una determinada base de datos.

Adicionalmente, cada una de las áreas del SENADO DE LA REPÚBLICA DE COLOMBIA, apoyarán la gestión del Oficial de Protección de datos.

Las responsabilidades asignadas al oficial de protección de datos personales, además de todas aquellas que generalmente establecen las leyes de protección de datos personales vigentes son las siguientes:

• Establecer los lineamientos mínimos requeridos para garantizar una adecuada administración y protección de la información contenida en las bases de datos.
• Monitorear y hacer seguimiento a la normatividad expedida en materia de protección de la información y hacer recomendaciones de ajustes al interior de la entidad.
• Efectuar la inscripción de las bases de datos actuales en el Registro Nacional de Bases de Datos, así como los cambios y actualizaciones que se requieran.
• Detectar y, en su caso, notificar a la Superintendencia la creación o modificación de nuevas bases de datos del SENADO DE LA REPÚBLICA DE COLOMBIA.
• Revisar y actualizar periódicamente las políticas que deben ser implementadas en la entidad para la protección de los datos personales, las cuales deben ser aprobadas por el director(a) General Administrativo(a).
• Promover entre los funcionarios de la entidad y contratistas, la importancia del cumplimiento de la protección de datos personales y realizar evaluaciones que permitan medir el grado de conocimiento de la legislación al interior de la entidad.
• Supervisar el cumplimiento en materia de Protección de Datos Personales del SENADO DE LA REPÚBLICA DE COLOMBIA.
• Atender las consultas e inquietudes relacionadas con el tratamiento de información personal que titulares, funcionarios, personas o entidades con los que se comparte la información soliciten.
• Atender requerimientos de las autoridades, así como procesos administrativos o judiciales en materia de protección de datos personales, en conjunto con las áreas y asesores que considere adecuados para el efecto.
• Actualizar el manual interno de lineamientos de protección de datos personales e implementar los nuevos que se elaboren.
• Valorar los incidentes de seguridad de la información relacionados con información personal con el fin de establecer las medidas correctivas que ameriten y su posterior comunicación a la Superintendencia de Industria y Comercio, en caso de considerarlo necesario.
• Monitorear el procedimiento de consultas y reclamos, establecido para que los Titulares puedan ejercer sus derechos al habeas data, verificando que estén disponibles y acordes con lo establecido por la regulación vigente.
• Participar en el desarrollo de nuevos procesos y la documentación que les sirve de soporte con el fin de verificar el cumplimiento de la normatividad de protección de datos personales vigente.
• Comprobar si se producen transferencias o transmisiones internacionales de datos y si las mismas son efectuadas de acuerdo a lo prescrito en la normatividad legal vigente.
• Servir de enlace y coordinar con las demás áreas el cumplimiento en materia de protección de datos personales.
• Verificar que se han implementado acuerdos de confidencialidad y Protección de Datos Personales con los funcionarios y terceros que tienen acceso a información personal o puedan tener un acceso potencial.
• Revisar que los contratos y acuerdos con terceros encargados de tratamiento cumplan con los estándares de clausulados implementados o a implementar por la entidad.

4.4.4. División de Recursos Humanos

• Obtener de los funcionarios y candidatos las autorizaciones pertinentes para el manejo de su información personal antes y durante la relación reglamentaria.
• Establecer planes de formación transversales en materia de protección de datos personales para todos los funcionarios y cargos del SENADO DE LA REPÚBLICA DE COLOMBIA.
• Comunicar de forma oportuna a la Jefatura de la División de Planeación y Sistemas, la vinculación, la desvinculación de los funcionarios y, de igual forma, cuando se presente un traslado o novedad en sus cargos.
• Verificar que en todos los procesos de bienestar donde se capturen o puedan capturar datos de menores, se recaba de padres y tutores la debida autorización para su tratamiento.
• Solo se recibirán hojas de vida en formato físico o automatizado por los canales habilitados por el SENADO DE LA REPÚBLICA DE COLOMBIA.
• Establecer los controles para que únicamente el personal autorizado en el área tenga acceso a la información sensible.
• Verificar que los traslados de documentación de carácter sensible hacia el Archivo central que se establezca o archivos tercerizados se realiza bajo medidas de seguridad y confidencialidad apropiadas, GA-It06 y GA-It03.
• Verificar que la información sensible que pueda ser almacenada en equipos locales es eliminada de los mismos o almacenada en servidores una vez ha concluido el uso para la que fue recabada en esos equipos.
• Las cesiones de datos de carácter sensible, se realizan bajo los lineamientos de procedimientos de envíos canales automatizados o telemáticos de las políticas de seguridad de la información de la organización.

4.4.5. División Jurídica

• Asesorar al Oficial de Protección de Datos Personales en las respuestas a las solicitudes presentadas en los diferentes medios habilitados por el SENADO DE LA REPÚBLICA DE COLOMBIA, que se pueden derivar del ejercicio de los derechos de los titulares en materia de Protección de Datos Personales.

4.4.6. Áreas y Colaboradores de la Entidad en General

• Colaborar con el Oficial de Protección de datos en el seguimiento a las actividades relacionadas con manejo de información personal dentro de sus áreas de responsabilidad.

• Realizar acciones adecuadas para qué, en cada uno de los procesos, se implementen la totalidad de mecanismos necesarios para la protección de datos personales, recomendados por el Oficial de Protección de datos o cualquier organismo de vigilancia y control.

• Garantizar que, ante cambios en procesos y nuevos proyectos o programas, estos cuenten con los requisitos necesarios para la protección de datos personales antes de su puesta en operación, presentándolos al Oficial de Protección de datos para que este aporte recomendaciones, si fuere el caso, cuando se vaya a manejar información personal.

• Proteger los activos de información personal del SENADO a través del cumplimiento de la Política General de Seguridad y Privacidad de la Información. Así mismo, deben reportar cualquier incumplimiento de normas o procedimientos establecidos que pongan en riesgo la información personal.

Los responsables del tratamiento de la información que administren bases de datos con información personal, son encargados de definir el valor y la criticidad de la información personal que se custodia, procesa o transporta de acuerdo con el procedimiento de identificación de activos de información y, con base en esta valoración, realizar la identificación de riesgos de seguridad de la información para definir los controles que garanticen las condiciones mínimas de seguridad y mitigación de los riesgos asociados a los mismos.

4.5. FUNCIONES, OBLIGACIONES Y PROHIBICIONES DE LOS USUARIOS

El personal que, para el correcto desarrollo de su labor, tiene autorizado acceso a datos personales, tiene las siguientes obligaciones:

a. Obligaciones Generales:

• Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la organización.

• Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.

• En caso de ser necesario el traslado de cualquier soporte, con datos de carácter personal sensible, en los que se almacene información personal titularidad de la organización fuera de las sedes de la misma, se deberá cumplir con las medidas de seguridad de la información.

• Bases de Datos de carácter temporal, como, listados, informes o copias de documentos que sean generados de manera temporal, para el cumplimiento de una necesidad determinada, deben ser borrados o eliminados una vez hayan dejado de ser necesarios para los fines que motivaron su creación. Mientras estén vigentes, deberán cumplir con los niveles de seguridad adecuados en función de la tipología o riesgo de los datos.

• Únicamente las personas autorizadas podrán introducir, modificar o anular los datos contenidos en las Bases de Datos o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por la Jefatura de la División de Planeación y Sistemas para bases de datos automatizadas y, en lo que tiene que ver con documentos objetos de protección, por la Jefatura de la División de Recursos Humanos. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a Bases de Datos o documentos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del Oficial de Protección de datos o responsable del área correspondiente.

b. Obligaciones respecto a Bases de Datos Automatizadas:

• Cambiar las contraseñas de acuerdo a los lineamientos establecidos en los procedimientos de gestión de usuarios y acceso de la organización.

• Recomendar a los usuarios cerrar o bloquear todas las sesiones al término de la jornada laboral o en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos no autorizados.

• No copiar la información contenida en las Bases de Datos en los que se almacenen datos de carácter personal (en especial sensibles) en el ordenador personal, portátil, memorias USB o a cualquier otro soporte sin autorización expresa del área responsable.

• Los usuarios tienen prohibido el envío de información de carácter personal sensible o de nivel de riesgo alto, salvo autorización expresa del Oficial de Protección de datos o área que tenga asignada esta tarea. En todo caso, este envío únicamente podrá realizarse si se adoptan los mecanismos establecidos en los lineamientos de intercambio de información con terceros de la organización para evitar que la información no sea inteligible ni manipulada por terceros.

• Los usuarios no podrán, salvo autorización expresa de la Jefatura de la División de Planeación y Sistemas, instalar cualquier tipo de programa informático o dispositivo, en los servidores centrales ni en el ordenador empleado.

c. Queda prohibido:

• Emplear identificadores y contraseñas de otros usuarios para acceder al sistema.

• Intentar modificar o acceder al sistema de información donde se almacenen datos personales, sin la autorización.

• Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a Bases de Datos o programas cuyo acceso no le haya sido permitido.

• Realizar envíos masivos de correos (spam) empleando la dirección de correo electrónico corporativa.

• Y en general, el uso de la red corporativa, sistemas informáticos y cualquier medio puesto al alcance del usuario, vulnerando el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

d. Obligaciones respecto a Bases de Datos Físicas - No Automatizadas:

• Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con la entidad.

• Mantener debidamente custodiadas las llaves de acceso a las instalaciones, oficinas, a sus despachos y a los armarios, archivadores u otros elementos que contenga bases de datos físicas - no automatizadas con datos de carácter personal, debiendo poner en conocimiento del Oficial de Protección de datos o responsable del área cualquier hecho que pueda haber

comprometido esa custodia.
• Cerrar con llave las puertas de los despachos al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
• Comunicar al Oficial de Protección de datos, las incidencias de seguridad sobre datos personales de las que tenga conocimiento, a través de correo electrónico: tratamiento.datospersonales@senado.gov.co.
• Guardar todos los soportes físicos o documentos que contengan información con datos de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente fuera de la jornada laboral.
• Garantizar que no quedan documentos impresos que contengan datos protegidos, en la bandeja de salida de la impresora.
• Únicamente las personas autorizadas para ello en el listado de accesos podrán introducir, modificar o anular la información contenida en las bases de datos objeto de protección. Los permisos de acceso de los usuarios a las diferentes bases de datos son concedidos por el área responsable. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a bases de datos a cuyo acceso no está autorizado, deberá ponerlo en conocimiento de la persona encargada que para este caso sería la persona que cumple el rol de Oficial de protección de datos personales o responsable de área.

e. Obligaciones respecto a Bases de datos de carácter temporal:

• Son aquellas en los que se almacenan datos de carácter personal, generados para el cumplimiento de una necesidad determinada, siempre y cuando su existencia no sea superior a la necesidad temporal del tratamiento para la que fue creada.
• Las bases de datos de carácter temporal deben ser destruidas de forma segura impidiendo la recuperación una vez hayan dejado de ser necesarias para los fines que motivaron su creación y, mientras estén vigentes, deberán contemplarse las medidas de seguridad contenidas en este documento.
• Las bases de datos temporales son responsabilidad del usuario que las creó y es responsabilidad suya la salvaguarda.

4.6. LINEAMIENTOS GENERALES PARA LA AUTORIZACIÓN EN EL TRATAMIENTO DE PROTECCIÓN DE DATOS PERSONALES

A continuación, se establecen los lineamientos generales aplicados por el SENADO DE LA REPÚBLICA DE COLOMBIA con el fin de cumplir con sus obligaciones en cumplimiento de los principios para la administración de datos personales.
Estos lineamientos son complementarios a las políticas, procedimientos o instructivos generales actualmente existentes e implementados y en ningún momento pretenden remplazarlas o desconocerlas.

a. Captura de información:

Si la captura se hace en un medio físico, la autorización cuenta con la firma del titular de los datos; si se utiliza un medio tecnológico o verbal, se implementan mecanismos eficientes que permitan la conservación de su aceptación al tratamiento de los datos por parte de la entidad.
En los casos en que el SENADO DE LA REPÚBLICA actúe como responsables de las bases de datos y sin importar el medio de captura, se obtiene autorización del Titular de la información y se guarda prueba de la misma, a menos que dicha autorización se haya otorgado por parte del titular por medio de acciones inequívocas, tales como aceptar comunicaciones por parte de la entidad y responderlas.
NOTA: La ley 1581 de 2012 artículo 10 establece: La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública; c) Casos de urgencia médica o sanitaria; d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) Datos relacionados con el Registro Civil de las Personas.
Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

b. Autorización:

De conformidad con las normas vigentes, el consentimiento del Titular de los datos debe cumplir con las siguientes características:

1. **Ser previo:** Debe otorgarse antes de la incorporación del dato a la base de datos.
2. **Ser expreso**: Otorgarse de forma inequívoca, explícita y concreta para la finalidad que requiere.
3. **Ser informado**: El Titular del dato debe conocer la finalidad de la base de datos y el tratamiento que se le va a dar a sus datos; así como ser consciente de los efectos de su autorización. En concreto, es obligatorio informar al titular de los datos: (i) El tratamiento que se hará sobre sus datos y la finalidad del mismo; (ii) el carácter facultativo de las respuestas a las preguntas que versen sobre datos sensibles; (iii) los derechos que tiene; (iv) la identificación, dirección física o electrónica del responsable del tratamiento.

Para obtener la autorización se siguen las siguientes instrucciones:
En primer lugar, antes de que la persona autorice se le informará de forma clara y expresa lo siguiente:
• El tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
• El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas hacen referencia expresa sobre datos sensibles o sobre los datos de niñas, niños o adolescentes.
• Los derechos que le asisten como titular previstos en el artículo 8 de la ley 1581 de 2012.
En segundo lugar, obtiene el consentimiento del titular a través de cualquier medio que pueda ser objeto de consulta posterior. Los mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al titular su manifestación automatizada.
Se entiende, como se indicó anteriormente, que la autorización cumple con estos requisitos cuando se manifiesta por:

1. **Escrito:** Se deja prueba del cumplimiento de la obligación de informar y del consentimiento. Si el titular solicita copia, deberá suministrársele.
2. **Verbalmente**: A través de llamadas telefónicas en las cuales el titular es informado de sus derechos y las finalidades de tratamiento de la información dándole la oportunidad a continuación de manifestar su aceptación. De dichas comunicaciones, y si se cuenta con los medios, se dejará prueba a través de grabaciones conservadas de manera que puedan ser objeto de posterior consulta.
3. **Conductas inequívocas del titular**: La autorización también puede obtenerse a partir de conductas inequívocas del Titular del Dato que permitan concluir de manera razonable que éste otorgó su consentimiento para el tratamiento de su información.

En ningún caso, el silencio del Titular podrá considerarse como una conducta inequívoca.

c. Autorización para tratamiento de datos sensibles:

EL SENADO solo puede realizar operaciones o tratamientos de los datos sensibles con autorización expresa del titular de dichos datos personales, siempre y cuando se haya informado al titular:
Cuando se trate de la recolección de datos sensibles se deben cumplir los siguientes requisitos:

- La autorización debe ser explícita.
- Se debe informar al Titular que no está obligado a autorizar el tratamiento de dicha información.
- Se debe informar de forma explícita y previa al Titular cuáles de los datos que serán objeto de tratamiento son sensibles y la finalidad su uso.

d. Autorización de tratamiento de datos de niños, niñas o adolescentes (NNA):
Cuando se trate de la recolección y tratamiento de datos de niños, niñas o adolescentes se deben cumplir los siguientes requisitos:

• La autorización debe ser otorgada por personas que estén facultadas para representar los NNA. El representante de los NNA deberá garantizarles el derecho a ser escuchados y valorar su opinión del tratamiento teniendo en cuenta la madurez, autonomía y capacidad de los NNA para entender el asunto.
• Se debe informar que es facultativo responder preguntas sobre datos de los NNA.
• El tratamiento debe respetar el interés superior de los NNA y asegurar el respeto de sus derechos fundamentales.
• SENADO DE LA REPÚBLICA DE COLOMBIA solamente usará, almacenará y realizará tratamiento de datos personales de menores de edad que sean hijos, descendientes o que dependan o estén a cargo de los funcionarios o contratistas y que sus datos sean de naturaleza pública, y de los menores de edad que participen en las visitas guiadas. La finalidad de dicho tratamiento será administrar y verificar bases de datos referentes a las actividades realizadas por los miembros de la entidad en el ejercicio de sus funciones.

e. Prueba de la autorización:
Con el fin de que posteriormente se pueda consultar la autorización, EL SENADO conservará prueba de la misma.

4.7. TRANSMISIÓN DE INFORMACIÓN

El intercambio o transmisión electrónica o física de datos personales se realiza de acuerdo a los lineamientos de manejo de información previstos en las Políticas de Seguridad de la Información implementadas.
Por norma general se establece que:

1. La información sensible, confidencial o privada que se transmita a través de las redes debe ser protegida.
2. La Jefatura de la División de Planeación y Sistemas, debe definir qué controles de seguridad se deben implementar para los servicios de red.
3. Para la transmisión de información personal sensible de nivel de riesgo alto, se deberán adoptar medidas de seguridad reforzadas.

4.7.1. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES:

Salvo autorización expresa del Titular de los datos personales y las demás excepciones previstas en la ley 1581 de 2012 está prohibida la transferencia de datos a terceros países que no proporcionen niveles adecuados de protección de datos.

4.7.1.1. Transmisión de datos a un encargado para que haga el tratamiento de los datos personales:

EL SENADO DE LA REPÚBLICA DE COLOMBIA podrá transmitir o entregar los datos personales de sus bases de datos a un tercero en Colombia o en el exterior para que este tercero, en calidad de encargado, realice el tratamiento de los datos personales.
Suscribir un contrato con dicho tercero en el que:
• Se señalará los alcances del tratamiento, las actividades que el encargado realizará para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el responsable.
• El encargado se comprometerá a dar aplicación a las obligaciones bajo la política de Tratamiento de datos personales y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables.

4.8. ACCESO Y CONTROL DE LA INFORMACIÓN PERSONAL

La División de Planeación y Sistemas ha implementado controles tecnológicos y de monitorización que permiten la trazabilidad y control de los usuarios que acceden a la información. (Véase RT-Ma02/ Manual de Políticas de seguridad de Información)
A nivel de instalaciones físicas y acceso a la documentación física no automatizada cada una de las áreas asume una responsabilidad por la información que es mantenida en sus archivos de gestión, de acuerdo con la ley 594 de 2000.

4.8.1. USO DE LA INFORMACIÓN

La información de carácter personal contenida en las bases de datos debe ser utilizada y tratada de acuerdo a aquellas finalidades sobre las que los titulares otorgaron su consentimiento.
Cualquier uso de la información diferente al establecido será previamente consultado con el Oficial de Protección de datos o área responsable. Enviando solicitud a la Jefatura de la División de Planeación y sistemas donde se decidirá que tratamiento deberá tener.
Únicamente los funcionarios autorizados pueden introducir, modificar o anular los datos contenidos en las bases de datos o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por la DIVISIÓN PLANEACIÓN Y SISTEMAS de acuerdo a los perfiles establecidos por cargo.
La Entidad a través de la División de Planeación y Sistemas, debe garantizar que se cuente con los recursos tecnológicos mínimos requeridos para el desarrollo de las actividades que establece el programa en cuanto al uso de herramientas tecnológicas para el alcance de los objetivos propuestos.

4.8.2. ALMACENAMIENTO DE INFORMACIÓN

El almacenamiento de la información automatizada y física se realiza en medios o ambientes que cuentan con controles para la protección de los datos. Esto involucra controles seguridad, tecnológicos y de tipo ambiental en áreas restringidas en instalaciones propias o centros de cómputo o centros documentales gestionados por terceros. De acuerdo con lo establecido por la Unidad de Archivo Administrativo en relación con los documentos físicos y por la División de Planeación y Sistemas en cuanto a la información automatizada.

4.8.3. ELIMINACIÓN (Véase: GD-PR-08 Procedimiento eliminación Documental)

La eliminación de medios físicos y electrónicos se realiza a través de mecanismos que no permiten su reconstrucción.
La eliminación comprende información contenida en poder de terceros como en instalaciones propias.
La destrucción de dichos medios físicos y electrónicos, será responsabilidad de la jefatura de la Unidad de Archivo

Administrativo cuando los documentos se encuentren en el Archivo central –Procedimiento eliminación documental GD-Pr-08 y los Jefes de cada dependencia (Dueños de proceso) son los responsables de la eliminación de los documentos de apoyo dentro de su archivo de gestión.

4.9. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES (OPERATIVO) (véase: rt-pr01/procedimiento soporte técnico y atención a servicios)

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de las bases de datos o información contenida en las mismas.

En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla a la mesa de servicios, y se informará al oficial de protección de datos personales, para que sea atendida de acuerdo con las actividades establecidas en el procedimiento.

El oficial de protección de datos personales, registrará la información de la incidencia en el sistema de mesa de servicios, a partir del conocimiento de la misma indicando:

- Tipo de incidente
- Fecha de incidente
- Fecha de conocimiento
- Causal
- Información comprometida
- Tipo de información (INDICAR)
- Cantidad de Titulares afectados

La tipología de información como: publico, semi privado, privado y sensible; se corresponde con la categorización de datos que cada dependencia realiza a la información que administra, de acuerdo con el formato de matriz de gestión GD-Fr-16.

Cuando el incidente de seguridad esté relacionado con más de un (1) tipo de información se debe seleccionar de la lista el tipo de información comprometida. El mismo procedimiento se debe realizar tantas veces como tipos de información se hayan visto afectados.

Las incidencias pueden afectar tanto a bases de datos automatizadas como no automatizados.

4.9.1. PROCEDIMIENTO PARA LA NOTIFICACIÓN Y GESTIÓN DE INCIDENTES RELATIVAS A BASES DE DATOS CON INFORMACIÓN PERSONAL. (Véase: Véase: RT-Pr01/procedimiento Soporte Técnico y atención a servicios)

a. Notificación de Incidentes

Cuando se presuma que un incidente pueda afectar o haber afectado a bases de datos con información personal datos personales se deberá informar al Oficial de protección de datos personales quién gestionará su reporte en el RNBD.

b. Gestión de Incidentes

Es responsabilidad de cada funcionario, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal del Senado de la República.

c. Identificación

Todos los eventos sospechosos o anormales deben ser evaluados para determinar si son o no, un incidente y deben ser reportados de acuerdo con el procedimiento de soporte técnico, Cualquier decisión que involucre a las autoridades de investigación y judiciales debe ser tomada por la Dirección Administrativa del SENADO DE LA REPÚBLICA DE COLOMBIA, y desde allí se definirá si es necesaria la comunicación con dichas autoridades.

d. Reporte

Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por el SENADO DE LA REPÚBLICA DE COLOMBIA. Los niveles de escalamiento en la comunicación ante un incidente de seguridad son los establecidos en el procedimiento.

Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el Oficial de protección de datos personales, debe ser notificado de forma inmediata, al correo tratamiento.datospersonales@senado.gov.co.

A menos que exista una solicitud de la autoridad competente, ningún funcionario o contratista de la entidad debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema. Para la entrega de información o datos en virtud de orden de autoridad, la división jurídica deberá intervenir con el fin de prestar el asesoramiento adecuado.

e. Contención, Investigación y Diagnóstico

Se debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe garantizar que todo el proceso de gestión del incidente sea debidamente documentado.

En caso que se identifique un delito informático, la Dirección Administrativa del SENADO DE LA REPÚBLICA con el apoyo de la División de Planeación y Sistemas, reportará tal información a las autoridades de investigaciones judiciales respectivas.

Durante los procesos de investigación se deberá garantizar la “Cadena de Custodia” con el fin de preservarla en caso de requerirse establecer una acción legal.

f. Solución

La División de Planeación y Sistemas debe prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades existentes.

g. Cierre de Incidente y Seguimiento

La División de Planeación y Sistemas a través del oficial de protección de datos personales iniciará todas las tareas de revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad y deben documentarlo.

El Oficial de protección de datos personales preparará un informe anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

h. Reporte de incidentes ante la SIC

Se reportarán como novedades los incidentes de seguridad que afecten la base de datos, mediante los mecanismos dispuestos para estos efectos por la Superintendencia de Industria y Comercio a través de la página **http://www.sic.gov.co/registro-**

nacional-de-bases-de-datos,

4.9.1.1. Ejercicio de derechos de los Titulares (Véase: Uc-Pr02/Proceso Gestión de Atención Ciudadana Procedimiento para Atención a PQRSD)

Procedimiento de Consulta y Reclamo

• Derechos Garantizados:

Mediante el procedimiento consulta y reclamo, SENADO DE LA REPÚBLICA DE COLOMBIA, así como los Encargados, garantizan a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de consultar toda la información contenida en su registro individual o toda aquella que esté vinculada con su identificación conforme en la presente Política de Tratamiento de Datos Personales.

• Responsable de atención de consultas:

El responsable de atender estas solicitudes será el Oficial de protección de datos personales, quien recibirá y dará trámite a las solicitudes que se reciban, en los términos, plazos y condiciones establecidos en la ley 1581 de 2012 y en las presentes políticas.

4.10. MEDIOS DE RECEPCIÓN DE SOLICITUDES DE CONSULTA (Véase: GA-Pr01/Recepción y Envío de Correspondencia)

El Titular o sus causahabientes podrán remitir su reclamación mediante solicitud escrita a la dirección de la unidad de correspondencia sede principal ubicada en Bogotá D.C., (Colombia) en el domicilio Carrera. 7 #8-62 – Bogotá D.C., con dirección electrónica: tratamiento.datospersonales@senado.gov.co. Finalmente para consultar el procedimiento a través del sitio WEB **http://www.senado.gov.co/** en del link “Privacidad”.

4.10.1. REQUISITOS CONSULTA: La consulta dirigida a los Responsables de tratamiento deberá contener como mínimo la siguiente información:

- Nombres y apellidos del Titular o su representante o causahabientes;
- Copia del documento de identidad del titular o su representante o causahabientes;
- Lo que se pretende consultar
- Dirección física, electrónica y teléfono de contacto del Titular o sus causahabientes o representantes;
- Firma, número de identificación y huella o procedimiento de validación correspondiente.
- Haber sido presentada por los medios de consulta descritos en la presente Política de tratamiento de datos personales.

4.10.2. PLAZOS DE RESPUESTA A CONSULTAS: Las solicitudes recibidas mediante los anteriores medios, serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo.

4.10.3. PRÓRROGA DEL PLAZO DE RESPUESTA: En caso de imposibilidad de atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

4.11. RECLAMOS

4.11.1. DERECHOS GARANTIZADOS MEDIANTE EL PROCEDIMIENTO DE RECLAMOS: Corrección o Actualización: EL SENADO DE LA REPÚBLICA DE COLOMBIA y sus Encargados, garantizan a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de corregir o actualizar los datos personales que reposen en sus bases de datos, mediante presentación de reclamación, cuando consideren que se cumplen los parámetros establecidos por la ley para que sea procedente la solicitud de Corrección o Actualización.

Revocatoria de la autorización o Supresión de los datos Personales: EL SENADO DE LA REPÚBLICA DE COLOMBIA y sus Encargados, garantizan a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de Solicitar la Revocatoria de la autorización o solicitar la supresión de la información contenida en su registro individual o toda aquella que esté vinculada con su identificación cuando consideren que se cumplen los parámetros establecidos por la ley.

Así mismo se garantiza el derecho de presentar reclamos cuando adviertan el presunto incumplimiento de la ley 1581 de 2012 o de las presentes Políticas de tratamiento de datos personales.

4.11.1.1. Responsable de atención de Reclamos: El responsable de atender los reclamos presentados por los titulares será el Oficial de protección de datos personales, quien recibirá y dará trámite a los reclamos que se reciban, en los términos, plazos y condiciones establecidos en la ley 1581 de 2012 y en las presentes políticas.

4.11.1.2. Medios de Recepción y Requisitos legales de los Reclamos: El Titular o sus causahabientes podrán remitir su reclamación mediante solicitud escrita a la dirección de la unidad de correspondencia sede principal ubicada en Bogotá D.C., (Colombia) con domicilio en la en la Carrera. 7 #8-62 – Bogotá D.C., con dirección electrónica: tratamiento.datospersonales@senado.gov.co. Finalmente, para consultar el procedimiento a través del sitio WEB **http://www.senado.gov.co/** en el link “Privacidad”.

Las reclamaciones presentadas deberán contener como mínimo la siguiente información:

Nombre del Titular o su representante o Causahabientes;

- Copia del Documento de identidad del Titular o su representante o Causahabientes;
- Descripción de los hechos que dan lugar al reclamo;
- Dirección Física, electrónica y teléfono de contacto del Titular o su representante o sus causahabientes;
- Documentos que se quieran hacer valer.
- Firma y número de identificación.
- Haber sido presentada por los medios de reclamo descritos en la presente Política de tratamiento de datos personales.

4.11.1.3. Reclamaciones sin cumplimiento de Requisitos legales: En caso que la reclamación se presente sin el cumplimiento de los anteriores requisitos legales, se solicitara al reclamante dentro de los cinco (5) días siguientes a la recepción del reclamo, para que subsane las fallas y presente la información o documentos faltantes.

4.11.1.4. Desistimiento del Reclamo: Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

4.11.1.5. Recepción de reclamos que no correspondan: En caso que el SENADO DE LA REPÚBLICA DE COLOMBIA reciba un reclamo dirigido a otra organización, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles

e informará de la situación al reclamante.

4.11.1.6. Plazos de Respuesta a los Reclamos: El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

4.11.1.7. Prórroga del plazo de Respuesta: Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

4.12. PROCEDIMIENTO DE SUPRESIÓN DE DATOS PERSONALES.

En caso de resultar procedente la Supresión de los datos personales del titular de la base de datos conforme a la reclamación presentada, el SENADO DE LA REPÚBLICA DE COLOMBIA, deberán realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información, sin embargo, el Titular deberá tener en cuenta que en algunos casos cierta información deberá permanecer en registros históricos por cumplimiento de deberes legales de la organización por lo que su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular.

4.13. PERSONA O DEPENDENCIA RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS.

En el SENADO DE LA REPÚBLICA DE COLOMBIA, el Oficial de protección de datos personales será responsable de velar por el cumplimiento de estas disposiciones. Quien a su vez tendrá una comunicación directa con los responsables de las áreas identificadas a lo largo del presente documentos y cualquier otra área requerida, con el fin de garantizar que todos los aspectos señalados queden debidamente atendidos y que los deberes que estipula la ley se cumplan.

4.14. POLÍTICA DE USO DEL CORREO ELECTRÓNICO (véase: Rt-ma01 manual de políticas de recursos tecnológicos)

EL SENADO DE LA REPÚBLICA DE COLOMBIA, ha definido una política de uso y control del correo electrónico que como usuario deberá conocerla y cumplirla.

Directriz: Las cuentas de correo electrónico son institucionales y de uso exclusivo para el desarrollo de funciones de la Entidad, por lo tanto, la información gestionada a través de este medio es responsabilidad de cada usuario y debe cumplir con las condiciones de confidencialidad, integridad y disponibilidad reglamentadas en la política.

La utilización del correo electrónico corporativo para asuntos diferentes a los relacionados con la Entidad puede afectar la seguridad de la información. Algunos ejemplos de eventos de riesgo relacionados son:

- Fuga de información.
- Proliferación de virus de computador.
- Pérdida de la confidencialidad de la información.
- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico.
- Enviar mensajes mal intencionado que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- No está permitido almacenar información de uso personal en los equipos corporativos.
- Utilizar la dirección de correo electrónico del SENADO DE LA REPÚBLICA DE COLOMBIA como punto de contacto en comunidades interactivas de contacto social, tales como Facebook o Linkedin, o cualquier otro sitio, a no ser que estén relacionadas con actividades netamente laborales.
- El envío de archivos con las siguientes extensiones no permitidas tales como música, videos, ejecutables, etc. (386, acm, ade, adp, ani, asp, avb, bas, bat, cgi, chm, cla, class, cmd, cnv, com, cpl, crt, dll, drv, exe, gms, hlp, ht, hta, htt, inf, ini, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, mht*, mp3, mpd, msc, msi, msp, mst, ocx, opo, ov*, pcd, pif, php, pl, prc, reg, scr, sct, sh, shs, sys, tlb, tsp, url, vb, vbe, vbs, vxd, wbs, wbt, wiz, wsc, wsf, wsh)
- El correo electrónico corporativo no debe usarse para actividades que comprometan la reputación del Senado de la República, los activos de información y los recursos del SENADO DE LA REPÚBLICA DE COLOMBIA.
- El permiso para el envío de correos masivos está restringido, solo se permitirá el uso a las cuentas institucionales que se encuentren respectivamente autorizadas por el jefe de división o director general, y que por sus funciones requiera enviar información masiva.

4.15. PROCEDIMIENTO PARA LOS ENVÍOS TELEMÁTICOS - ENVÍO, INTERCAMBIO Y ENTREGA DE INFORMACIÓN A TERCEROS. (Véase: rt-ma02/manual de políticas de seguridad de información política de transferencia de información)

Todo envío de información confidencial o sensible del SENADO DE LA REPÚBLICA DE COLOMBIA hacia un tercero, deberá ser seguro. Para este fin el SENADO DE LA REPÚBLICA cuenta con los siguientes documentos:

- Procedimiento RT-Pr07 Transferencia Segura de información, donde se establecen las actividades a realizar para lograr una transferencia segura y mantener las evidencias y trazabilidad.
- Política de tratamiento de datos personales, donde se define las condiciones a tener en cuenta para realizar la transferencia segura de información.

4.16. PROCEDIMIENTO DE REGISTRO DE ENTRADA DE SOPORTES Y DOCUMENTOS (VÉASE: Proceso de gestión documental)

Las normas de buenas prácticas en seguridad de la información y protección de datos personales requieren la adopción de determinadas medidas para garantizar la seguridad de los datos que entran o salen de las organizaciones.

En el caso de entradas de soportes que contengan información personal deberá disponerse de un sistema de registro de entrada de los mismos.

Especialmente las salidas de soportes y documentos, constituyen un hecho que puede ser crítico ya que en muchas ocasiones las mismas se realizan sin respetar las obligaciones tanto jurídicas como técnicas dispuestas legalmente y suponen en ocasiones el acceso por parte de terceros a información que no deben conocer. Por lo tanto, ante una entrada o salida de documentos o soportes que contengan bases de datos con datos personales, deberá dirigirse al Oficial de protección de datos personales competente que le informará como proceder.

4.16.1. PROCEDIMIENTO DE ENTRADA DE SOPORTES Y DOCUMENTOS (Véase: Guia DAFP V.4, GD-Pg01)

Las entradas de soportes que contengan datos personales sensibles, cuyo nivel de seguridad sea de nivel ALTO, deberán ser registradas en un registro que contenga siguiente información:

- Tipo de documento o soporte
- Fecha y hora
- Emisor
- Número de documentos o soportes incluidos en el envío
- Tipo de información que contienen
- Forma de envío
- Persona responsable de la recepción que deberá estar debidamente autorizada.

Si la organización lo considera necesario el procedimiento podrá ser de aplicación para tipologías de datos con nivel de riesgo inferior.

4.16.2. Procedimiento de registro de salida de soportes y documentos. (Véase: Guia DAFP V.4, GD-Pg01)

Las normas de buenas prácticas en seguridad de la información y protección de datos personales requieren la adopción de determinadas medidas para garantizar la seguridad de los datos que entran o salen de las organizaciones.

En el caso de salidas de soportes deberá disponerse de un sistema de registro de salida de soportes. Adicionalmente las salidas de soportes que contengan información de carácter sensible deberán estar autorizadas por el responsable de privacidad o responsable de área competente.

Tenga en cuenta que es importante porque, especialmente las salidas de soportes y documentos, constituyen un hecho que puede ser crítico ya que en muchas ocasiones las mismas se realizan sin respetar las obligaciones tanto jurídicas como técnicas dispuestas legalmente y suponen en ocasiones el acceso por parte de terceros a información que no deben conocer. Por lo tanto, ante una entrada o salida de documentos o soportes que contengan bases de datos con datos personales deberá dirigirse al responsable de privacidad competente que le informará de la forma de proceder.

Las salidas de soportes que contengan datos personales especialmente sensibles o de nivel de riesgo alto, deberán ser registradas en un registro que contenga como mínimo la siguiente información:

- Tipo de documento o soporte
- Fecha y hora
- Emisor
- Número de documentos o soportes incluidos en el envío
- Tipo de información que contienen
- Forma de envío
- Persona responsable de la entrega que deberá estar debidamente autorizada.

4.17. LINEAMIENTOS DE DESECHADO Y REUTILIZACIÓN DE SOPORTES AUTOMATIZADOS:

El desechado y reutilización de soportes que contienen datos personales en bases de datos automatizadas pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

Las directrices de SENADO DE LA REPÚBLICA DE COLOMBIA establecen que es responsabilidad del dueño del activo de información (o gestor de base de datos), determinar cuando la información ha dejado de ser útil, de acuerdo con su valoración y acorde a la regulación que aplique.

En el procedimiento RT-Pr10 Borrado seguro de la información, se establecen actividades a seguir para eliminar información en equipos de cómputo y en el procedimiento RT-Pr02 generación de copias de seguridad y restauración de datos para ambientes virtualizados, con los cuales se establecen las actividades relacionadas con el tratamiento de la información durante su vida útil y los mecanismos de destrucción o borrado de acuerdo con el medio que la custodie.

En el caso de soportes automatizados (medida a adoptar para CUALQUIER TIPOLOGIA DE DATOS Y PARA TODOS LOS NIVELES DE RIESGO) siempre que vaya a desecharse cualquier soporte automatizado que contenga datos de carácter personal (cualquiera que sea su nivel) deberá procederse a su destrucción o eliminación, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. También deberá procederse al borrado de la documentación cuando el soporte vaya a reutilizarse.

4.17.1. Reutilización o desechado (Véase: RT-Pr10 Procedimiento Borrado seguro de la información.)

El responsable del área de Planeación y Sistemas debe certificar que toda la información ha sido adecuadamente removida de cualquier componente del sistema informático utilizado por la Entidad, antes de entregar los componentes a terceros.

En caso de requerirse el retiro de un medio de almacenamiento debido a un proceso de garantía, o de otra índole, el responsable del activo debe destruir o eliminar toda información contenida en el medio.

Adicional se deben seguir las siguientes recomendaciones:

La gestión de soportes que contengan datos de carácter personal cubre todo el periodo de vida de los mismos incluida su reutilización. Por tanto, a lo largo del ciclo útil de cualquier soporte deberemos tener en cuenta tres etapas:

a. Creación del soporte

• Éste aloja datos y se anota en el correspondiente registro según se trate de un soporte integrado en el sistema o de un soporte que vaya a salir del mismo con destino a un tercero ya sea con motivo de una comunicación de datos o de un encargado del tratamiento.

b. Reutilización del soporte

• En este caso el soporte causará baja y, sólo si se va a utilizar de nuevo para contener nuevos datos personales, podría causar una nueva alta.

c. Destrucción del soporte

• En este caso causará baja en el inventario.

• Tanto en el caso de reutilización del soporte como en el de desechado existen un conjunto de obligaciones formales y materiales que deben ser tenidas en cuenta y documentadas.

d. Reutilización del soporte

En la reutilización de los soportes se garantizará el borrado físico completo del soporte de manera que resulte imposible la recuperación de los datos. Así por ejemplo:

• Los CD-RW y los DVD-RW se destruyen manualmente.

• Las unidades de disco duro se borrarán mediante procedimientos que garanticen completamente el borrado de los datos. Debe advertirse que la instrucción "borrar" o "enviar a la papelera" no eliminan físicamente los datos de un disco duro. Ni

siquiera formatear un disco duro garantiza plenamente la destrucción de los datos. Por ello se recomienda el uso de algún programa de destrucción segura de datos.

• Los PEN-drive, tarjetas de memoria y otros soportes equivalentes, capaces de almacenar información, deberán ser borrados de modo que los datos resulten inaccesibles de acuerdo con el método más adecuado en cada caso.

4.18. DESECHADO Y REUTILIZACIÓN DE SOPORTES NO AUTOMATIZADOS.

El desechado y reutilización de soportes y documentos que contienen datos personales, en base de datos físicas no automatizadas, pueden suponer el acceso indebido por parte de terceros a los datos personales que se contienen en los mismos si no se realiza de forma correcta.

En el caso de soportes no automatizados (medida que se ciñe a datos sensibles o de nivel de NIVEL ALTO, pero que se puede ampliar si así se indica en el procedimiento a otros niveles) deberá procederse a la eliminación de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

4.18.1. PROCEDIMIENTO DE ELIMINACIÓN DE COPIAS O REPRODUCCIONES DESECHADAS RELACIONADAS CON DOCUMENTOS FÍSICOS.

Siempre que vaya a desecharse cualquier documento o soporte no automatizado que contenga datos de carácter personal deberá procederse a su eliminación, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. Las medidas a aplicar serán:

• En el caso de que se trate de documento en papel, cuando éstos contengan datos de carácter personal, queda prohibida su reutilización (a modo de papel reciclado). En todo caso, se recomienda a su destrucción mediante el uso de una destructora de papel.

• No se aconseja en ningún caso la reutilización del soporte papel impreso a una cara ya que resulta ineficiente y peligroso desde el punto de vista de la seguridad, salvo el caso en el que la segunda impresión afecte a datos contenidos en la Base de Datos y se garantice la seguridad de igual modo. Sin embargo, esta posibilidad debe ser tenida por excepcional ya que la coincidencia debería ser plena alcanzando incluso al hecho de que el propio usuario estuviera autorizado a acceder a los datos contenidos en el soporte reutilizado.

4.19. LINEAMIENTO DE CUSTODIA DE SOPORTES (Véase: rt-ma02 manual de políticas de seguridad. política de pantalla y escritorio

Directriz corporativa: No deben dejarse desprotegidos documentos con información confidencial o sensible. Se debe garantizar su adecuada custodia de tal manera que se asegure las condiciones de confidencialidad, integridad, disponibilidad y privacidad de la información.

4.19.1. LINEAMIENTO DE CUSTODIA:

• Los dispositivos de almacenamiento de los soportes que contienen datos de carácter personal sensible, dispondrán de mecanismos que obstaculizan su apertura.

• En relación con aquellos soportes que no dispongan de dichos mecanismos se encuentran al cargo de una persona que los custodia e impide en todo momento que la información pueda ser accedida por persona no autorizada.

4.20. PROCEDIMIENTO DE ARCHIVO DE BASES DE DATOS NO AUTOMATIZADAS:

4.20.1. PROCEDIMIENTO DE ARCHIVO: Los ambientes donde se guarde información de uso restringido, deberán contar por lo menos con un custodio del activo de información que garantice la seguridad de la información del ambiente.

a. Archivo de gestión

Los archivadores del ambiente de trabajo o del escritorio y las salas de archivos que contengan información restringida deben permanecer cerrados bajo llave durante reuniones, al término de la jornada laboral o en otros tiempos prolongados de ausencia del personal.

Mientras un documento físico no esté siendo utilizado, éste debe de permanecer guardado bajo llave en el archivador o sala de archivo según corresponda.

b. Archivo central

Adicionalmente y debido al volumen de archivos, una vez los soportes han permanecido durante el tiempo estipulado en el archivo de gestión pasan al archivo central de la Entidad.

4.21. RESTRICCIÓN DE ACCESO A BASES DE DATOS NO AUTOMATIZADAS (Véase: GD-Pg01, Guía DAFP V.4)

Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados.

4.21.1. ÁREAS RESTRINGIDAS (Véase: GD-Pg01, Guía DAFP V.4)

La información sensible o de nivel de riesgo alto deberá encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en la base de datos y permitir guardar la trazabilidad de los ingresos y salidas.

Los colaboradores que tienen acceso a estas áreas son responsables de proteger la identificación que le otorga estas facultades y responder por los actos que se cometan con su identificación y en los que se evidencie negligencia o descuido de sus credenciales o claves de ingreso.

4.21.2. COPIA Y REPRODUCCIÓN DE DOCUMENTOS (Véase: GD-Pg01)

Para bases de datos no automatizadas que contengan datos sensibles de nivel de riesgo alto las copias o reproducciones únicamente podrán ser realizadas bajo el control del personal autorizado.

La generación de copias o la reproducción de los documentos que contengan datos sensibles o de nivel de riesgo alto únicamente podrán ser realizadas bajo el control del personal autorizado.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Cada vez que un documento sea impreso, fotocopiado o escaneado no se dejará en las bandejas de las impresoras por largos periodos de tiempo, los colaboradores deberán revisar que han sido recogidos la totalidad de los documentos.

4.21.3. TRASLADO DE DOCUMENTACIÓN (Véase: GD-Pg01)

Es recomendable adoptar ciertas medidas dirigidas a proteger la información contenida en bases de datos no automatizadas que sean objeto de traslado, cuando las mismas contengan información sensible de nivel alto.

El SENADO DE LA REPÚBLICA DE COLOMBIA ha definido dichas medidas para proceder al traslado de documentación

sensible de nivel alto (obligación que podrá ampliarse a cualquier otro nivel de datos si así se considera) las mismas se detallan a continuación. Como colaborador deberá conocerlas y cumplirlas.

4.21.3.1. Traslado de documentación para bases de datos sensibles o nivel de riesgo alto (véase: GD-Pg01, guia dafp v.4)

Siempre que se proceda al traslado de la documentación contenida en bases de datos sensibles o confidenciales deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

4.22. GESTIÓN DE USUARIOS (Véase: Guia DAFP V.4, RT-Pr09 Procedimiento Gestión y administración de cuentas institucionales)

El objetivo del procedimiento es establecer los criterios para la creación, deshabilitación y activación de cuentas de usuarios de los Senadores, funcionarios de planta, UTL, contratistas, practicantes judicantes, terceros y oficinas, que usan los aplicativos y servicios tecnológicos del Senado de la República. Con el cual se tiene un estándar en la creación de las cuentas de usuario de los funcionarios en todos los sistemas informáticos utilizados en SENADO DE LA REPÚBLICA DE COLOMBIA, de forma tal que exista uniformidad y facilidad de identificación de los funcionarios.

4.22.1. PROCEDIMIENTO DE COPIA DE SEGURIDAD (Véase: RT-Pr02 generación de copias de seguridad y restauración de datos para ambientes virtualizados)

El objetivo del procedimiento es establecer los mecanismos para realizar copias de seguridad y restauración de los servicios o servidores del Senado de la República, con el fin de evitar la indisponibilidad de los servicios y aplicaciones que presta la entidad. Con esto el Senado busca garantizar la existencia de procedimientos adecuados para la administración de copias de respaldo sobre la información necesaria para ejecutar los procesos críticos, garantizando la existencia de mecanismos adecuados para restaurar de forma completa y oportuna la información en caso de ser necesario.

El área de Planeación y Sistemas es la encargada de definir y mantener los procedimientos de respaldo acorde con las herramientas tecnológicas implementadas. Las estrategias de respaldo de la información deben estar alineadas a los activos y procesos críticos, así como a la estrategia de continuidad definida. Las copias de respaldo de los activos críticos deberán ser almacenadas en lugares seguros de acuerdo a la Política de Seguridad de la Información

4.22.2. PROCEDIMIENTO DE CONTROL DE ACCESO LÓGICO (Véase: RT-Pr02 Procedimiento Gestión y administración de cuentas institucionales)

La información del SENADO DE LA REPÚBLICA DE COLOMBIA debe ser protegida para prevenir los accesos no autorizados. Los privilegios sobre la información deben ser mantenidos en concordancia con la misionalidad y fines de la Entidad, limitando el acceso solamente a los temas estrictamente requeridos.

El control de acceso físico queda registrado en los formatos RT-Fr08 Formato personal autorizado ingreso áreas seguras RT-Fr09 Formato personal no autorizado ingreso áreas seguras

4.22.3. GESTIÓN DE CREDENCIALES Y CONTRASEÑAS (Véase: RT-Ma02 Manual de políticas de Seguridad. Política de creación, uso y aseguramiento de claves de acceso)

El Senado de la República suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta, comunicándose a la mesa de servicios, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato mediante envió de oficio a la división de planeación y sistemas.

- Las claves o contraseñas cada vez que se cambien deben ser distintas.
- La contraseña debe cumplir como mínimo con tres de los cuatro requisitos:
  - Tener mínimo ocho (8) caracteres alfanuméricos
  - Caracteres en mayúsculas
  - Caracteres en minúsculas
  - Base de 8 dígitos Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)
- El sistema solicitará cambio de contraseña al momento de realizar alguna restauración.

Todos los colaboradores del SENADO DE LA REPÚBLICA DE COLOMBIA deben definir claves de acceso a los sistemas informáticos que cumplan con las condiciones de complejidad que dificulten su conocimiento por personal no autorizado. Adicionalmente, deben protegerlas para garantizar su confidencialidad y uso personal.

4.23. TRATAMIENTO DE BASES DE DATOS TEMPORALES

Los funcionarios del SENADO DE LA REPÚBLICA DE COLOMBIA pueden en la actividad diaria realizar tratamientos en bases de datos temporales cumpliendo los lineamientos, recomendaciones o políticas que en este manual se establecen para tal efecto. Estas se podrán almacenar en las carpetas compartidas que se habiliten para garantizar el resguardo de sus archivos críticos.

Consideraciones:

- Los datos personales estarán ubicados físicamente en bases de datos que deben ser protegidas.
- Por otra parte, en la operación diaria de tratamiento de los registros de la Base de Datos pueden producirse copias de los datos protegidos sobre otras bases de datos o archivos ofimáticos para tratamientos especiales. En estos casos deberá prestarse la adecuada protección a esas bases de datos mientras existan.
- Las bases de datos temporales deberán cumplir el nivel de seguridad correspondiente a la tipología de datos tratados y a su nivel de riesgo y serán borrados o almacenados en los servidores una vez que hayan dejado de ser necesarios.
- Queda expresamente prohibido el tratamiento de datos sensibles extraídos de la base de datos con programas ofimáticos, como procesadores de texto u hojas de cálculo, sin comunicarlo para su aprobación al responsable de área u Oficial de protección de datos personales para que se proceda a implantar las medidas de seguridad adecuadas.
- Se deberá evitar guardar copias de los datos personales de la base de datos en archivos intermedios o temporales. En el caso de que sea imprescindible realizar esas copias temporales por exigencias del tratamiento.
- Tras realizar el tratamiento para los que han sido necesarios esos datos temporales, proceder al borrado o destrucción de estos.
- Las bases de datos temporales creadas exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a la clasificación de los datos y nivel de riesgo de los mismos.
- Si la aplicación o sistema de acceso a la base de datos a utilizarse usualmente bases de datos temporales, o cualquier otro medio en el que pudiesen ser grabadas copias de los datos protegidos, el administrador deberá asegurarse de que

esos datos no son accesibles posteriormente por personal no autorizado.

4.24. TRATAMIENTO DE BASES DE DATOS DESCENTRALIZADAS

Bases de datos descentralizadas son aquellas que responden a un mismo contenido, finalidad y propósito, pero pueden responder a distintos tratamientos o encontrarse en repositorios diferentes, pero forman parte integrante de la base de datos registrada.

En estos casos SENADO DE LA REPÚBLICA DE COLOMBIA prestan la adecuada protección a esas bases de datos durante toda su existencia de acuerdo a los lineamientos establecidos en las políticas, procedimientos e instructivos de seguridad de la información.

En relación con estas bases descentralizadas se adoptan las siguientes medidas:

- Realizar las oportunas copias de seguridad sobre las carpetas compartidas asignadas por tecnología.
- Realizar procedimientos de auditoría periódicos.
- Establecer controles que permitan mantener el inventario de las mismas actualizado.

4.25. TRABAJO FUERA DE LAS INSTALACIONES

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de las instalaciones de la entidad se seguirán las siguientes recomendaciones:

- Los colaboradores, temporales, contratistas, pasantes y, en general, cualquier persona que trabaje para el SENADO DE LA REPÚBLICA DE COLOMBIA utilice equipos móviles con información de la entidad, debe proteger físicamente estos equipos cuando estén fuera de su puesto de trabajo.
- Todo equipo móvil propiedad de SENADO DE LA REPÚBLICA DE COLOMBIA, que se encuentre fuera de las instalaciones de la entidad, no debe dejarse desatendido por su responsable en ningún momento.
- Toda la información contenida, procesada o generada en los equipos de cómputo es propiedad de la Entidad
- Si se debe utilizar el portátil fuera de las instalaciones del Senado de la República, se transportará en condiciones seguras, sin exponerlo ni llevarlo a la vista. No se dejará en sitios públicos o transportes públicos.
- En caso de viajes el portátil hace parte del equipaje de mano, se portará esta manera siguiendo las normas de la aerolínea.
- Cuando se transporte el portátil en un vehículo, se asegurará llevarlo en un lugar seguro de difícil acceso (el baúl preferiblemente, en donde no se vea).
- En caso de pérdida realizar inmediatamente denuncia antes las autoridades correspondientes y notificarlo entregando soporte físico a su jefe inmediato y al oficial de protección de datos personales si el mismo contiene información personal.

4.26. CAPACITACIÓN DE FUNCIONARIOS.

EL SENADO DE LA REPÚBLICA DE COLOMBIA debe desarrollar programas anuales de capacitación y concientización en Protección de datos personales y seguridad de la información.

La entidad debe poner en conocimiento este manual por el medio que considere adecuado.

La entidad capacita a sus funcionarios en la forma que considere pertinente y atendiendo a los procedimientos internos de la misma, en la administración de los datos personales con una periodicidad al menos anual, con el fin de medir sus conocimientos sobre el particular.

Para el desarrollo de los programas de concientización deberán asegurar que los funcionarios, contratistas y terceros entiendan sus responsabilidades con respecto a Protección de datos personales y seguridad de la información.

Los programas de capacitación son actualizados de forma periódica.

El área de Recursos Humanos conjuntamente con el Oficial de Protección de datos, define los planes de capacitación y evaluación de los funcionarios, de acuerdo con los cambios normativos que se vayan presentando.

4.27. CONTINUIDAD DE OPERACIONES

La información debe estar disponible para su uso cuando la entidad lo requiera. Por lo tanto, el SENADO DE LA REPÚBLICA DE COLOMBIA deberá desarrollar, un programa de Gestión de Continuidad del Negocio que permita identificar los procesos vitales de la compañía, definir estrategias y planes de respuesta, así como implementar y probar periódicamente procedimientos para asegurar su recuperación razonable y oportuna, buscando mantener los niveles de seguridad establecidos. La Gestión de Continuidad del Negocio es liderada por la División de Planeación y Sistemas.

Los registros físicos y electrónicos del SENADO DE LA REPÚBLICA DE COLOMBIA deben ser conservados el mínimo de años que establezca la regulación vigente y aquellos que sean objeto de un proceso legal o de investigación interna por el tiempo que sea requerido.

4.28. CONTRATISTAS Y TERCERIZACIÓN

Todos los proveedores o terceros que sean Encargados del tratamiento, es decir, aquellos que realizan tratamiento de datos por cuenta del SENADO DE LA REPÚBLICA DE COLOMBIA, deben cumplir la totalidad de las obligaciones establecidas en la Ley y la política de privacidad de la entidad.

- La entidad suscribe contratos con todos los proveedores, contratistas o terceros que cumplen las características de Encargados en los términos previstos por la legislación vigente.
- La entidad debe verificar, por lo menos una (1) vez al año de forma aleatoria y en consideración de la sensibilidad de los datos tratados, el adecuado manejo de información de los diferentes proveedores en los términos establecidos en el contrato y la Ley como “Encargados del tratamiento de datos personales”.
- Una vez cumplida la prestación contractual, los datos de carácter personal son destruidos o devueltos a la entidad responsable del tratamiento, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.
- En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.
- La entidad tiene establecidos lineamientos para la relación con agentes externos que tengan acceso o puedan tener acceso potencial a la información o recursos informáticos y por tanto a las bases de datos.
- El tercero que accede a la información y a los recursos informáticos de la Organización debe acatar los lineamientos establecidos por la Entidad en sus políticas de privacidad.
- En el acceso a la información y a los recursos informáticos se establecen acuerdos de confidencialidad para que no se otorgue acceso a la información sin la existencia de una autorización y compromiso explícito.
- En el contrato establecido entre la Entidad y los agentes externos, se especifica la necesidad de acceso a la información.

4.29. SEGURIDAD FÍSICA

4.29.1. VISITANTES

Todos los visitantes deben pasar el procedimiento de identificación en la recepción y deben ser recibidos por un colaborador.

4.29.2. CONTROL ACCESO

Las áreas donde se ejecutan procesos relacionados con información confidencial o restringida deben contar con controles de acceso que sólo permitan el ingreso a los colaboradores autorizados.

- **Áreas restringidas:** Deben contar con mecanismos que permitan restringir el acceso sólo a personal autorizado y que permita guardar la trazabilidad de los ingresos y salidas.

4.29.3. VIDEO VIGILANCIA

La entidad ha instalado cámaras de video vigilancia con la única finalidad de dar cumplimiento a las políticas de seguridad física. Las imágenes se conservan por un tiempo máximo de 60 días o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto, RT-Fr01 Formato solicitud de registros y grabaciones de seguridad.

4.30 PROCESOS DE REVISIÓN Y AUDITORÍAS DE CONTROL

La Entidad realizará procesos de revisión o auditorías en materia de protección de datos personales verificando de manera directa o a través de terceros, que las políticas y procedimientos se han implementado adecuadamente en la entidad.

Con base a los resultados obtenidos, se evalúa e implementa los planes de acción (preventivos, correctivos y de mejora) necesarios.

Como norma general el SENADO DE LA REPÚBLICA DE COLOMBIA realiza estos procesos de revisión con una periodicidad mínima de un año o de forma extraordinaria ante incidentes graves que afecten a la integridad de las bases de datos personales.

Los resultados de la revisión junto con los eventuales planes de mejora definidos, son presentados por la Jefatura de la División de Planeación y Sistemas y el Oficial de tratamiento de Datos Personales ante la Dirección Administrativa, para su valoración y aprobación.

4.30.1 REVISIÓN Y CONTROL DE ASPECTOS GENERALES

a. Análisis del ciclo del tratamiento del dato

1. Recolección
2. Necesidad de la recolección.
3. Información recolectada.
4. Finalidades del tratamiento.
5. Aseguramiento de la calidad del dato.
6. Autorización legal para recolección y tratamiento.

b. Mantenimiento y Uso

1. Áreas implicadas en el tratamiento.
2. Procedimiento y actividades internas de proceso de datos.
3. Procesos de depuración de datos.
4. Consolidación de datos.
5. Medidas de seguridad implementadas.
6. Procesos de actualización de datos.
7. Procesos de respaldo de datos.

c. Supresión

1. Tiempo de conservación de los datos.
2. Medios funcionarios para eliminación o supresión.
3. Circunstancias para la eliminación de la información de la base de datos.
4. Almacenamiento de datos eliminados en prevención de solicitudes posteriores.

d. Bases de datos

1. Identificación e inscripción de nuevas bases de datos.
2. Actualización de cambios sustanciales de las bases de datos inscritas.
3. Revisión de bases de datos descentralizadas.
4. Revisión de bases de datos temporales

e. Lineamientos internos para el tratamiento de información personal

1. Metodologías aplicadas para la Administración de Riesgo de Cumplimiento de Protección de Datos
2. Implementación y aplicación de modelos y clausulados de naturaleza legal.
3. Políticas de Tratamiento.
4. Aviso legal y solicitudes de autorización.
5. Cláusulas contractuales con terceros encargados / proveedores.
6. Cláusulas contractuales con trabajadores.
7. Cláusulas contractuales escenarios de transmisión y transferencia de datos.

5. ANEXOS

N.A.

6. FORMATOS

N.A.

7. DOCUMENTOS RELACIONADOS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas-DAFP V.4
- GD-Pg01 Programa de Gestión Documental.
- RT-Pr09 Procedimiento gestión y administración de cuentas institucionales
- RT- Ma02 Manual políticas de seguridad de la información
- DG- Pr08 Procedimiento separación de ambientes
- RT-Pr01 Procedimiento soporte técnico y atención de servicios
- UC- Pr02 Procedimiento para atención de pqrsd
- GD- Pr01 Procedimiento recepción y envío de correspondencia
- RT- Ma01 Manual políticas de gestión de recursos tecnológicos
- GD- Ca 01 Caracterización proceso de gestión documental.
- RT- Pr10 Procedimiento borrado seguro de la información
- RT- Pr02 Procedimiento generación copias de seguridad y restauración de datos para ambientes virtualizados
- DG- Pr08 Procedimiento eliminación documental

8. CONTROL DE CAMBIOS

Control de Cambios

- Ver. 001// Rev. 1// FV. 16 de diciembre de 2020

  Cambios:

  Se crea el documento con el fin de definir y establecer los lineamientos generales, funciones y obligaciones de los responsables y usuarios de la gestión y tratamiento de la información de carácter personal en la Entidad.

  Justificación:

  Responsable: Mary Alexandra Rodriguez Bernal

  Fecha: 2020-12-16

ELABORÓ	REVISÓ	APROBÓ
Nombre: Valentina Alzate	Nombre: Diana Rocio Plata Arango	Nombre: Grupo Evalualdor de Documentos - SGC
Cargo: Contratista DGA	Cargo:Jefe División de Planeación y Sistemas	No. Acta y Fecha:**Acta No. 48 del 16 de diciembre de 2020.**

Mary Alexandra Rodriguez Bernal @ 2020-12-16, 21:21:16