RESOLUCIÓN No. 0083 DE 2020 31 ENE 2020

"Por medio de la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información la Secretaría Distrital de Desarrollo Económico"

LA SECRETARIA DISTRITAL DE DESARROLLO ECONÓMICO

En uso de sus atribuciones legales y administrativas, en especial las previstas en la Constitución Política de Colombia de 1991, la Ley 1753 de 2015, el Acuerdo 257 de 2006, el Decreto 437 de 2016, el Decreto 717 de 2018, el Decreto 1083 de 2015, en concordancia con lo dispuesto en el artículo 9 del Decreto Distrital 591 de 2018, y,

CONSIDERANDO:

Que el **Decreto 1078 de 2015** "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" en el numeral 5 del artículo artículo 2.2.5.5.2. sobre prestación del servicio en casos de emergencia, desastres y calamidad pública, exige "Realizar análisis de vulnerabilidad y riesgos en los equipos, estaciones y redes de telecomunicaciones, para soportar debidamente las telecomunicaciones en casos de emergencias y restablecerlas prontamente".

Que mediante el Decreto 2434 de 2015 se adicionó el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, 1078 de 2015, para crear el **Sistema Nacional de Telecomunicaciones de Emergencias (SNTE)** como parte del Sistema Nacional de Gestión del Riesgo de Desastres.

Que la Ley 1273 de 2009 adicionó el Código Penal con el título VII Bis denominado "De la Protección de la información y de los datos", e incluyó los siguientes artículos: Artículo 269A: Acceso abusivo a un sistema informático. Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Artículo 269C: Interceptación de datos informáticos. Artículo 269D: Daño Informático. Artículo 269E: Uso de software malicioso. Artículo 269F: Violación de datos personales. Artículo 269G: Suplantación de sitios web para capturar datos personales.

Que la "Política Nacional de Seguridad Digital" "documento CONPES 3854 de 2017" ratifica que el incremento en la participación digital de los ciudadanos, trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida en el sentido de brindar protección en el ciberespacio para atender estas amenazas, así como a través de la reducción de la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo.

RESOLUCIÓN No. 0083 **DE 2020** 31 ENE 2020

"Por medio de la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información la Secretaría Distrital de Desarrollo Económico"

Que el objetivo del Documento CONPES 3701 de 2011 fue fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa)10, creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y (iii) fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.

Que la norma internacional NTC / ISO 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información para una empresa. Esta norma incluye los requisitos para realizar la valoración y el tratamiento de riesgos de seguridad de la información, conforme las necesidades de una empresa.

Que a su vez la norma NTC/ISO 31000:2009 brinda las directrices genéricas sobre la gestión del riesgo y contribuye al logro de los objetivos y mejorar el desempeño de la organización, a través de la revisión de su sistema de gestión y sus procesos.

Que de conformidad con el anterior marco jurídico, se hace necesario adoptar el **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**, el cual constituye el instrumento de gestión y tratamiento de los riesgos de la Información de la Secretaría Distrital de Desarrollo Económico.

Que mediante acta número 002 del 31 de enero de 2020 el Comité Institucional de Gestión y Desempeño, aprobó el **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**.

En mérito de lo expuesto, este Despacho

RESUELVE:

ARTÍCULO PRIMERO. ADOPTAR el **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** de la Secretaría Distrital de Desarrollo Económico para la vigencia 2020, el cual hace parte integral del presente acto administrativo.

31 ENE 2020

RESOLUCIÓN No. 0083 DE 2020

"Por medio de la cual se adopta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información la Secretaría Distrital de Desarrollo Económico"

ARTÍCULO SEGUNDO. Este acto administrativo rige a partir de la fecha de su expedición y deroga cualquier disposición anterior que le sea contraria.

PUBLIQUESE Y CÚMPLASE

Dada en Bogotá, a los 31 ENE 2020

MARIA CAROLINA DURAN PEÑA
Secretaria Distrital de Desarrollo Económico

Acciones	Preparadores	Firmas
Proyectó:	Profesional Especializado Hilda Jiménez Guerrero	
Revisó	Subdirector de Informática y Sistemas Armando Calderón Loaiza	
Revisó	Directora de Gestión Corporativa Beatriz Helena Zamora González	
Revisó	Jefe Oficina Asesora Jurídica Jaime Andrés Riascos I.	

BOGOTÁ | SECRETARÍA DE DESARROLLO ECONÓMICO

0083

31 ENE 2020

SECRETARIA DESARROLLO ECONOMICO

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE DESARROLLO ECONÓMICO

PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá, D.C. 2020

0083

31 ENE 2020

TABLA DE CONTENIDO

1. PLAN TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requerido para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

En este sentido, acorde con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI, en la Guía No. 7 – Guía de Gestión de Riesgos y Guía No. 8 – Controles de Seguridad y Privacidad de la Información, en el presente Plan se estipulan directrices, fechas de ejecución y responsables para lograr un adecuado proceso de administración y evaluación de los riesgos de seguridad y privacidad de la información.

Objetivo

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía No. 7 – Guía de Gestión de Riesgos y la Guía No. 8 – Controles de Seguridad y Privacidad de la Información, con el propósito de adoptar medidas y acciones encaminadas a modificar, reducir o eliminar riesgos relacionada con la infraestructura de tecnologías de la Información de la Entidad.

Alcance

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas, recursos de infraestructura tecnológica para el tratamiento de la información y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas del Instituto.

2. PROCESO PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

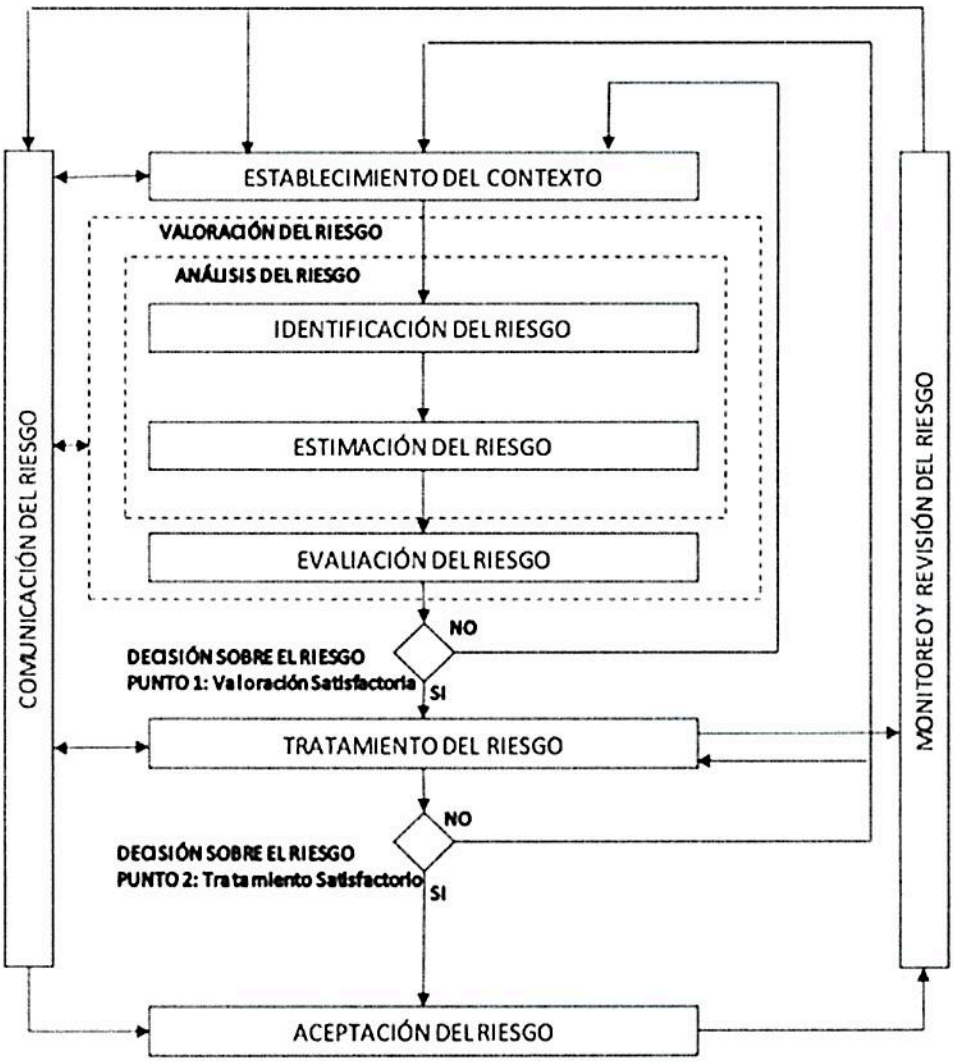

Ilustración 1. Proceso para la administración de riesgos de seguridad y privacidad de la información

Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Para la evaluación de riesgos de seguridad y privacidad de la información se tomará como insumo la matriz de Activos de Información, sobre la cual se implementará el presente Plan sobre los Activos de Información que tengan un nivel alto de clasificación al evaluar los criterios de confidencialidad, integridad y disponibilidad, según los siguientes criterios.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 1. Criterios de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 2. Niveles de Clasificación
Fuente: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

3. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, cronograma propuesto para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Entidad y descripción general de las tareas principales.

ID	ACTIVIDAD	Fecha Inicio	Fecha Final
1	Sensibilización institucional sobre política de seguridad de la información	01/02/2020	30/12/2020
2	Revisar y/o actualizar el manual de Políticas de Seguridad y Privacidad de la Información	01/02/2020	30/03/2020
3	Definir roles y responsabilidades de seguridad y privacidad de la información	01/02/2020	30/03/2020
4	Desarrollar y/o actualizar el inventario de activos de información	01/02/2020	30/04/2020
5	Elaborar procedimientos gestión de Riesgos de seguridad de la información	01/02/2020	30/04/2020
6	Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información	01/05/2020	30/08/2020
7	Ejecutar Plan de riesgos de seguridad y privacidad de la información	01/08/2020	30/12/2020

3.1. Sensibilización institucional sobre política de seguridad de la información

Realizar la divulgación de manera apropiada de las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la
Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema.

Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

3.2. Revisar y/o actualizar el manual de Políticas de Seguridad y Privacidad de la Información

La Secretaria de Desarrollo Económico establece las Políticas de Seguridad y Privacidad de la Información, con el fin de garantizar el adecuado uso de los activos de información, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

La Política de Seguridad y Privacidad de la Entidad contendrá la voluntad de la Alta Dirección para apoyar la Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

Esta política contendrá de manera específica la declaración general por parte de la Alta Dirección, en cuanto a los objetivos, alcance y nivel de cumplimiento.

Esta política deberá ser aprobada y divulgada al interior de la Entidad.

3.3. Definir roles y responsabilidades de seguridad y privacidad de la información

Se deberá garantizar la asignación de roles y responsabilidades en todos los niveles (directivo, de procesos, operativo), para lo cual acorde con lo establecido en el Modelo Integrado de Planeación y Gestión – MIPG se deberán designar al Comité Institucional de Gestión y Desempeño como el organismo encargado de la gestión y toma de decisiones.

También se debe conformar el equipo de trabajo que apoyará durante la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información – MSPI, para lo cual se debe establecer y dar a conocer el perfil y responsabilidades de los integrantes del equipo de trabajo.

El equipo de trabajo designado se encargará de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades incluidas en el presente Plan para la adopción del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad, así mismo, estará encargado de planear las actividades necesarias para una adecuada administración y sostenibilidad del Modelo.

3.4. Desarrollar y/o actualizar el inventario de activos de información

La Secretaria de Desarrollo Económico desarrollará una metodología para la identificación, clasificación, mantenimiento y actualización del inventario de activos de información, entendiendo que hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información.

En concordancia, el inventario de activos de la información se registra en la matriz definida por la Entidad incluyendo la información pertinente respecto a los propietarios, custodios y usuarios de los activos de información identificados en cada vigencia.

3.5. Elaborar procedimientos de seguridad de la información

Se realizará la revisión de los actuales procedimientos, con el objeto de identificar las necesidades de documentación y/o actualización de procedimientos en el marco de la implementación del Modelo de Seguridad y Privacidad de la información.

El propósito de esta actividad se fundamenta en desarrollar y formalizar procedimientos que permitan gestionar la seguridad y privacidad de la información en todos los procesos de la Entidad.

3.6. Definir metodología para la gestión de los riesgos de seguridad y privacidad de la información

La Secretaria de Desarrollo Económico debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así, como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

0083

31 ENE 2020

3.7. Ejecutar Plan de riesgos de seguridad y privacidad de la información

ID	TAREAS PRINCIPALES	F. INICIO	F. FINAL
7.1	Definir el contexto estratégico	01/08/2020	30/08/2020
7.2	Establecer equipo de trabajo con asignación responsabilidades	01/08/2020	30/08/2020
7.3	Identificación de Riesgos	01/09/2020	31/09/2020
7.4	Análisis de Riesgos	01/10/2020	30/10/2020
7.5	Valoración de Riesgos	01/11/2020	30/11/2020
7.6	Evaluación de Controles	01/12/2020	30/12/2020
7.7	Socialización y Comunicación Políticas de Riesgos	01/12/2020	30/12/2020
7.8	Monitoreo y Revisión al Tratamiento de los Riegos	Continuo	

3.7.1. Establecer contexto estratégico

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

0083

31 ENE 2020

3.7.2. Establecer equipo de trabajo con asignación responsabilidades

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del Sistema Integrado de Gestión, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.
- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad

3.7.3. Identificación de Riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo las causas y consecuencias de la ocurrencia del riesgo.

3.7.4. Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

3.7.5. Valoración de Riesgos

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del

riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

3.7.6. Evaluación de Controles

Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad

3.7.7. Socialización y Comunicación Políticas de Riesgos

Actividad mediante el cual se da conocer a funcionarios. Contratistas y terceros de la Entidad las políticas de tratamiento de riesgos de Seguridad y Privacidad de la Información, mediante charlas y el uso de las herramientas de comunicaciones disponibles en la Entidad.

3.7.8. Monitoreo y Revisión al Tratamiento de los Riegos

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas