PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2023

TABLA DE CONTENIDO

1. PRESENTACIÓN

El presente plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno digital en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca guardar los datos de los ciudadanos, garantizando la seguridad de la información.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la Empresa de Desarrollo Urbano y Vivienda de Interés Social de Barrancabermeja **-**EDUBA con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

2.2 OBJETIVOS ESPECÍFICOS

Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en la Empresa de Desarrollo Urbano y Vivienda de Interés Social de Barrancabermeja **–** EDUBA para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

Aplicar las metodologías del MIN. TIC respectivamente en seguridad y riesgo de la información, en la Empresa de Desarrollo Urbano y Vivienda de Interés Social de Barrancabermeja - EDUBA.

3. DEFINICIONES

ACCESO A LA INFORMACIÓN PÚBLICA

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

ACTIVO

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, personas…) que tenga valor para la organización.

ACTIVO DE INFORMACIÓN

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

ARCHIVO

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.
(Ley 594 de 2000, art 3).

AMENAZAS

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGO

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

AUDITORÍA

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

AUTORIZACIÓN

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

BASES DE DATOS PERSONALES

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

CIBERSEGURIDAD

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

CIBERESPACIO

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre
usuarios. (Resolución CRC 2258 de 2009).

CONTROL

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información 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.

DATOS ABIERTOS

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

DATOS PERSONALES

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

DATOS PERSONALES PÚBLICOS

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

DATOS PERSONALES MIXTOS

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

DATOS PERSONALES SENSIBLES

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

DECLARACIÓN DE APLICABILIDAD

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

DERECHO A LA INTIMIDAD

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

ENCARGADO DEL TRATAMIENTO DE DATOS

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. (Ley 1581 de 2012, art 3)

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

INFORMACIÓN PÚBLICA CLASIFICADA

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

INFORMACIÓN PÚBLICA RESERVADA

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

PLAN DE CONTINUIDAD DEL NEGOCIO

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

PLAN DE TRATAMIENTO DE RIESGOS

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptable e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

PRIVACIDAD

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

RESPONSABILIDAD DEMOSTRADA

Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

RESPONSABLE DEL TRATAMIENTO DE DATOS

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art3).

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.

SEGURIDAD DE LA INFORMACIÓN

Preservación de la confidencialidad, integridad, y disponibilidad de la información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

TITULARES DE LA INFORMACIÓN

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

TRAZABILIDAD

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

4. RECURSOS

HUMANO:

- Gerente General, Oficina de Control Interno y Unidad de Sistemas

FÍSICO:

- Equipos tecnológicos activos y Equipos de Comunicación.

5. RESPONSABLES

- Gerente General
- Oficina de Control Interno
- Unidad de Sistemas

6. POLITICA DE ADMINSITRACIÓN DE RIESGOS

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Ministerio TIC. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
- Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos
- Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos
- Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros

7. PLANIFICACIÓN DE ACTIVIDADES

No.	Actividad	Resultados Esperados	Fecha Finalización	Responsable
1	Realizar Diagnóstico	Estado del arte de los riesgos de seguridad y privacidad de la información	Marzo 2023	Unidad de Sistemas, Ingeniero de Sistemas
2	Elaborar el alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.	Definición de las unidades y áreas a abarcar con el plan	Abril 2023	Unidad de Sistemas, Ingeniero de Sistemas,, Gerencia
3	Realizar la Identificación de los Riesgos con los líderes del Proceso.	**Documento con los riesgos de seguridad identificados en cada unidad**	Mayo 2023	Unidad de Sistemas, Ingeniero de Sistemas
4	Valoraciones del riesgo y del riesgo residual	**Especificación de los riesgos tratados y su riesgo residual**	Junio 2023	Unidad de Sistemas, Ingeniero de Sistemas
5	Plantear al plan de tratamiento de riego aprobado por los lideres	**Socialización del plan de tratamiento de riesgos**	Julio 2023	Unidad de Sistemas, Ingeniero de Sistemas
6	Seguimiento y Control	**Se realiza un seguimiento a los incidentes de seguridad que puedan surgir**	Seguimiento Constante	Unidad de Sistemas, Ingeniero de Sistemas

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo con lo establecido por la Empresa de Desarrollo Urbano y Vivienda de Interés Social de Barrancabermeja **-**EDUBA.

- Revisión y/o Modificación de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información.
- Seguridad Ligada a los recursos humanos.
- Revisión del Control de acceso.
- Seguridad en la operatividad.
- Seguridad en las telecomunicaciones.
- Gestión de Incidentes de Seguridad de la Información.

9. SEGUIMIENTO Y EVALUACIÓN

Al finalizar cada etapa se realizará una reunión con la Unidad de Sistemas, Control Interno, así como con el Gerente de la Empresa para presentar el informe del avance del proyecto y de esta manera evaluar todos los pasos que se han ido realizado.

10. ENTREGABLES

- Informe de avance o resumen ejecutivo
- Acta de Reunión.
- Plan de tratamiento de riego aprobado
- Política de Seguridad.

Control del Documento

	Cargo	***Firma***	***Fecha***
Elaboró	*Martin Alonso Castillo Gómez – CPS -003 de 2023*		*Enero de 2023*
Aprobó:	*Emel Darío Harnache Bustamante – Gerente*		*Enero de 2023*